OmniVista 3600 Air Manager 8.2.7.1

Alcatel·Lucent Enterprise

User Guide

Copyright

Open Source Code

Chapter 1
Introduction

Thank you for choosing OmniVista 3600 Air Manager 8.2.7.1. OV3600 makes it easy and efficient to manage your wireless network by combining industry-leading functionality with an intuitive user interface, enabling network administrators and helpdesk staff to support and control even the largest wireless networks.

The User Guide provides instructions for the configuration and operation of OmniVista 3600 Air Manager. This section includes the following topics:

- "A Unified Wireless Network Command Center" on page 15
- "Integrating OV3600 into the Network and Organizational Hierarchy " on page 17

A Unified Wireless Network Command Center

OmniVista 3600 Air Manager 8.2.7.1 is the only network management software that offers you a single intelligent console from which to monitor, analyze, and configure wireless networks in automatic fashion. Whether your wireless network is simple or a large, complex, multi-vendor installation, OV3600 manages it all.

OV3600 supports hardware from leading wireless vendors including: Aruba Networks®, ProCurve™ by HPE®, Avaya™, Cisco® (Aironet and WLC), Dell Networking W-Series, Enterasys®, Juniper Networks®, LANCOM Systems, Meru Networks®, Nortel Networks™, Proxim®, Symbol™, Trapeze™, Tropos™, and many others.

The components of OV3600 are described in the next section.

OV3600 Management Platform

The OV3600 Management Platform, provides the following functions and benefits:

- Core network management functionality, including network discovery, configuration of access points (APs) & controllers, automated compliance audits, firmware distribution, monitoring of all devices and users connected to the network, and reports showing real-time and historical trends.
- Granular administrative access that is role-based and network-based. For more information about roles, see "Administrative Roles" on page 18.
- Flexible device support for thin, thick, or mesh network architecture; multiple vendors; and current or legacy hardware.

Controller Configuration

OV3600 supports global and group-level configuration of Alcatel-Lucent AOS-W (AOS-W), the operating system, software suite, and application engine that operates mobility and centralizes control over the entire mobile environment. For a complete description of Alcatel-Lucent AOS-W, refer to the *Alcatel-Lucent AOS-W User Guide* for your specific version.

OV3600 consolidates and pushes global controller configurations from within OV3600.

The following WebUI pages support controller configuration:

- **Device Setup > Alcatel-Lucent Configuration** for global Alcatel-Lucent Configuration. This page becomes available if you enable the "Use Global Alcatel-Lucent Configuration" option. You can set this option by navigating to **OV3600 Setup > General** and scrolling down to **Device Configuration**.
- **Groups > Basic** has an "Audit Configuration on Devices" option that you can set for all switches in a group.
- **Groups > Controller Config** for setting up Aruba AP groups and Aruba configuration.

For additional information that includes a comprehensive inventory of all pages and settings that support Alcatel-Lucent Configuration, refer to the *OmniVista 3600 Air Manager 8.2.7.1 Controller Configuration Guide*.

Instant Configuration

Alcatel-Lucent Instant (Instant) is a system of access points in a Layer 2 subnet. The Instant APs (OAW-IAPs) are controlled by a single OAW-IAP that serves a dual role as both an OAW-IAP and primary Virtual Controller (VC), eliminating the need for dedicated controller hardware. This system can be deployed through a simplified setup process appropriate for smaller organizations, or for multiple geographically dispersed locations without an on-site administrator.

With AirWave, IT can centrally configure, monitor, and troubleshoot Alcatel-Lucent Instant WLANs, upload new software images, track devices, generate reports, and perform other vital management tasks, all from a remote location.

A Virtual Controller or Instant AP can authenticate to the OV3600 server using a pre-shared key, or using two-way certificate-based authentication using an SSL certificate sent from OV3600 to the Instant device. Virtual Controllers push data to OV3600 via HTTPS. If your enterprise has a security policy that restricts the use of port 443 for inbound communication, you can change the port OV3600 uses to communicate with Instant devices.

For additional information that includes a comprehensive inventory of all pages and settings that support Instant Configuration, refer to the *Alcatel-Lucent Instant* in *OV3600 8.2 Deployment Guide*.

Switch Configuration

OV3600 supports group-level configuration of the Aruba Mobility Access Switch (MAS), the operating system, software suite, and application engine that operates mobility and centralizes control over the entire network environment.

For a complete description of ArubaOS, refer to the ArubaOS User Guide for your specific Aruba Mobility Access Switch version.

OV3600 consolidates and pushes group switch configurations from within OV3600 using the **Groups > Switch Config** page. This page is available if Use Global Alcatel-Lucent Configuration is set to No in **OV3600 Setup > General**.

VisualRF

VisualRF monitors and manages radio frequency (RF) dynamics within your wireless network. Visual RF provides:

- Accurate location information for all wireless users and devices.
- Up-to-date heat maps and channel maps for RF diagnostics; it adjusts for building materials and supports multiple antenna types.
- Floor plan, building, and campus views.
- Visual display of errors and alerts.
- Easy importing of existing floor plans and building maps.
- Planning of new floor plans and AP placement recommendations.

RAPIDS

RAPIDS is a powerful and easy-to-use tool for monitoring and managing security on your wireless network. RAPIDs provides:

- Automatic detection of unauthorized wireless devices.
- Rogue device classification that supports multiple methods of rogue detection.
- Wireless detection, using authorized wireless APs to report other devices within range to calculate and display rogue location on a VisualRF map.

- Wired network detection of rogue APs located beyond the range of authorized APs and sensors, routers, and switches. RAPIDs ranks devices according to the likelihood they are rogues, runs multiple tests to eliminate false positive results, and identifies the switch and port to which a rogue device is connected.

Using the Master Console

You can monitor multiple OV3600 servers using the Master Console. After you add the OV3600 servers to Master Console, they will be polled for basic OV3600 information.

The **Overview** page in the Master Console provides summary statistics for the entire network at a glance.

- Reports can be run from the **Master Console** to display information from multiple OV3600 stations; because such reports can be extremely large, reports can also be run as summary only so that they generate more quickly and finish as a manageable file size.
- The **Master Console** can also be used to populate group-level configuration on managed OV3600 installations using the **Global Groups** feature.
- The **Master Console** offers a display of devices that are in a **Down** or **Error** state anywhere on the network. This information is supported on **Master Console** pages that display device lists such as **Home > Overview** and **APs Devices > List**.
- The **Master Console** and **Failover** servers can be configured with a **Managed OV3600 Down** trigger that generates an alert if communication is lost to a managed or watched OV3600 station. The **Master Console** or **Failover** server can also send email or NMS notifications about the event.

NOTE

XML APIs are not supported on the Master Console.

If you have the Master Console license, you can also monitor your multiple OV3600 servers using Glass. For more information, see the *Glass 1.0.0 User Guide*.

Integrating OV3600 into the Network and Organizational Hierarchy

OV3600 generally resides in the network operations center and communicates with various components of your WLAN infrastructure. In basic deployments, OV3600 communicates solely with indoor wireless access points (and WLAN controllers over the wired network. In more complex deployments, OV3600 seamlessly integrates and communicates with authentication servers, accounting servers, TACACS+ servers, LDAP servers, routers, switches, network management servers, wireless IDS solutions, helpdesk systems, indoor wireless access points, mesh devices. OV3600 has the flexibility to manage devices on local networks, remote networks, and networks using Network Address Translation (NAT). OV3600 communicates over-the-air or over-the-wire using a variety of protocols.

The power, performance, and usability of OV3600 become more apparent when considering the diverse components within a WLAN. Table 1 itemizes some example network components.

Table 1: *Components of a WLAN*

Component	Description
Autonomous AP	Standalone device which performs radio and authentication functions
Thin AP	Radio-only device coupled with WLAN controller to perform authentication
WLAN switch	Used in conjunction with thin APs to coordinate authentication and roaming

Table 1: *Components of a WLAN (Continued)*

Component	Description
NMS	Network Management Systems and Event Correlation (OpenView, Tivoli, and so forth)
RADIUS Authentication	RADIUS authentication servers (ClearPass, Funk, FreeRADIUS, ACS, or IAS)
RADIUS Accounting	OV3600 itself serves as a RADIUS accounting client
Wireless Gateways	Provide HTML redirect and/or wireless VPNs
TACACS+ and LDAP	Used to authenticate OV3600 administrative users
Routers/Switches	Provide OV3600 with data for user information and AP and Rogue discovery
Help Desk Systems	Remedy EPICOR
Rogue APs	Unauthorized APs not registered in the OV3600 database of managed APs

Administrative Roles

The flexibility of OV3600 enables it to integrate seamlessly into your business hierarchy as well as your network topology. OV3600 facilitates various administrative roles to match each individual user's role and responsibility:

- A Help Desk user can be given read-only access to monitoring data without being permitted to make configuration changes.
- A U.S.-based network engineer can be given read-write access to manage device configurations in North America, but not to control devices in the rest of the world.
- A security auditor can be given read-write access to configure security policies across the entire WLAN.
- NOC personnel can be given read-only access to monitoring all devices from the Master Console.

Chapter 2
Configuring OV3600

This section contains procedures to deploy initial OV3600 configuration. Additional configurations are available after you complete the steps described in this section.

Defining General OV3600 Server Settings

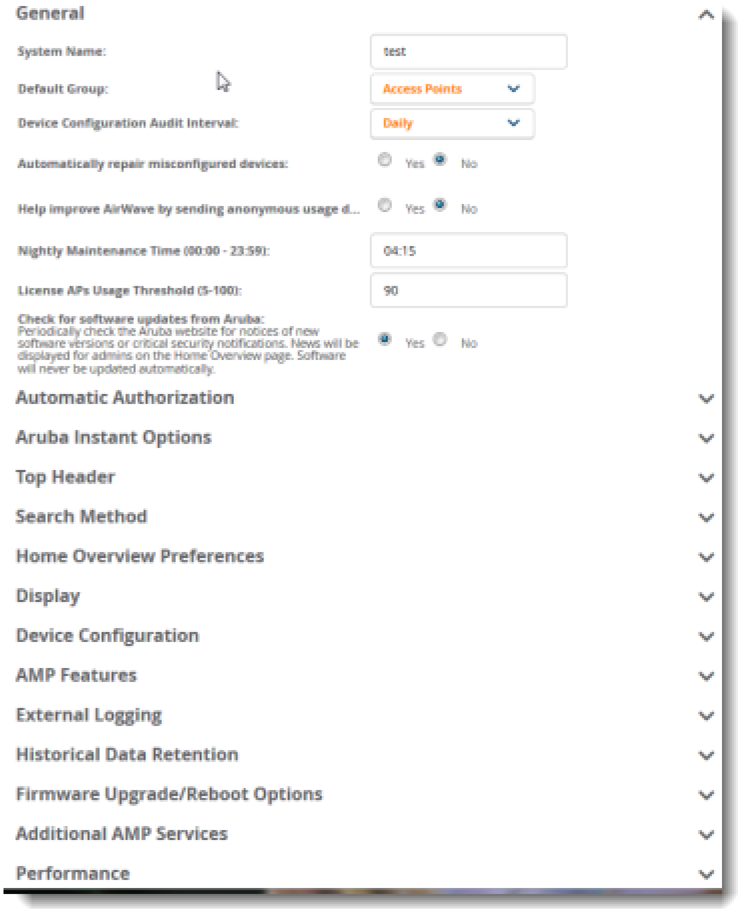
The initial configuration tasks to set up OV3600 include:

- "Configuring the OV3600 Server" on page 19
- "Defining Network Settings" on page 34
- "Configuring OV3600 User Roles" on page 39
- "Creating OV3600 Users" on page 37
- "Configuring the User Login and Authentication" on page 44
- "Enabling OV3600 to Manage Your Devices" on page 53
- "Setting Up Device Types" on page 60

Configuring the OV3600 Server

The following topics describe how to configure the general settings for the OV3600 server. Figure 1 illustrates the **OV3600 Setup > General** page.

Figure 1: *OV3600 Setup > General Settings*



General

System Name: test

Default Group: Access Points

Device Configuration Audit Interval: Daily

Automatically repair misconfigured devices: ○ Yes ● No

Help improve AirWave by sending anonymous usage d... ○ Yes ● No

Nightly Maintenance Time (00:00 - 23:59): 04:15

License APs Usage Threshold (5-100): 90

Check for software updates from Aruba: Periodically check the Aruba website for notices of new software versions or critical security notifications. News will be displayed for admins on the Home Overview page. Software will never be updated automatically. ● Yes ○ No

Whenever you save changes to these settings, OV3600 applies them globally across the product for all users.

General Settings

Browse to the **OV3600 Setup > General** page, locate the **General** section, and enter the information described in Table 2:

Table 2: *OV3600 Setup > General > General Section Fields and Default Values*

Setting	Default	Description
System Name		Defines your name for your OV3600 server using alphanumeric characters.
Default Group	Access Points	Sets the device group that this OV3600 server uses as the default for device-level configuration. Select a device group from the drop-down menu. A group must first be defined on the **Groups > List** page to appear in this drop-down menu. For additional information, refer to "Using Device Groups" on page 72.

Table 2: *OV3600 Setup > General > General Section Fields and Default Values (Continued)*

Setting	Default	Description
Device Configuration Audit Interval	Daily	This setting defines the interval of queries which compares actual device settings to the Group configuration policies stored in the OV3600 database. If the settings do not match, the AP is flagged as mismatched and OV3600 sends an alert via email, log, or SNMP. **NOTE:** Enabling this feature with a frequency of Daily or more frequently is recommended to ensure that your AP configurations comply with your established policies. Specifying **Never** is not recommended.
Automatically repair misconfigured devices	Disabled	If enabled, this setting automatically reconfigures the settings on the device when the device is in **Manage** mode and OV3600 detects a variance between actual device settings and the Group configuration policy in the OV3600 database.
Help improve AirWave by sending anonymous usage data	Disabled	If enabled, OV3600 will send anonymous data to Alcatel-Lucent, which may be used to improve the OV3600 software. To view an example of the data that will be sent, click the preview link.
Nightly Maintenance Time (00:00 - 23:59)	04:15	Specifies the local time of day OV3600 should perform daily maintenance. During maintenance, OV3600 cleans the database, performs backups, and completes a few other housekeeping tasks. Such processes should not be performed during peak hours of demand.
License APs Usage Threshold	90	Sets a threshold to display an alert on the switch monitor page when the license usage has reached this number.

Automatic Authorization Settings

On the **OV3600 Setup > General** page, locate the **Automatic Authorization** section. These settings allow you to control the conditions by which devices are automatically authorized into AP groups and folders. OV3600 validates the Folder and Group to ensure that both settings have been set to valid drop down options. Table 3 describes the settings and default values in this section.

Table 3: *OV3600 Setup > General > Automatic Authorization Fields and Default Values*

Setting	Default	Description
Add New Controllers and Autonomous Devices Location	New Device List	Globally add new controllers and autonomous devices to: ● The New Device List (located in **Devices > New**). ● The same folder and group as the discovering device. ● The same group and folder of their closest IP neighbor on the same subnet. ● Choose a group and folder. If you select this option, enter the folder/group in the **Auto Authorization Group** and **Auto Authorization Folder** fields that display. **NOTE:** This setting can be overridden in **Groups > Basic**.

Table 3: *OV3600 Setup > General > Automatic Authorization Fields and Default Values (Continued)*

Setting	Default	Description
Add New Thin APs Location	New Device List	Globally add new thin APs to: - The **New Devices** list. - The same folder and group as the discovering device. - The same group and folder of their closest IP neighbor on the same subnet. - Choose a group and folder. If you select this option, enter the folder/group in the **Auto Authorization Group** and **Auto Authorization Folder** fields that display. **NOTE:** This setting can be overridden in **Groups > Basic**.
Automatically Authorized Virtual Controller Mode	Manage Read/Write	Specify whether Virtual Controller mode for Instant APs will be in Manage Read/Write mode or Monitor Only mode.

Alcatel-Lucent Instant Settings

A Virtual Controller can communicate with the OV3600 server over a configurable communication port, and authenticate to the server using a pre-shared key, and/or two-way certificate-based authentication using an SSL certificate sent from OV3600 to the Instant device.

The OV3600 Setup > General > Alcatel-Lucent Instant Options page includes the following Configuration settings:

Table 4: *OV3600 Setup > General > Alcatel-Lucent Instant Options Fields and Default Values*

Setting	Default	Description
Communication port (443,1000-65534):	443	By default, an Instant Virtual Controller communicates with AirWave over port 443. If your enterprise has a security policy that restricts the use of port 443 for inbound communication, use this field to change the port the Virtual Controller uses to communicate with OV3600.
Security method for adding new Virtual Controllers:	PSK Only	OV3600 can use the following security methods to authenticate a Virtual Controller to the OV3600 server: - PSK Only - PSK and Certificate - Certificate Only If you enable certificate-based authentication, you are directed to the **OV3600 Setup > General > Upload SSL Certificate** page, where you are prompted to upload an certificate file in PEM format that contains both a private key and certificate.
Allow None-TPM Devices	Yes	If certificate-based authentication is enabled for the Virtual Controller, OV3600 allows low assurance, non-TPM device. This setting is unavailable when PSK authentication is used.
Configuration Only	No	By default, OV3600 will push Instant configuration settings as well as OV3600 settings such as RAPIDS settings and traps from an OV3600 group to a Virtual Controller assigned to that group. Select the **Yes** option to push Instant configuration settings only.

If you select a security method that includes Certificate-based authentication, you must upload the a certificate from a supported certificate authority to the OV3600 server, as the default OV3600 certificate will not be recognized by the Instant AP, and will cause the SSL handshake to fail. Certificate authentication also requires that the **OV3600 IP address** information configured on the Instant AP is a domain name, and not an IP address.

OV3600 supports the following trusted certificate authorities:

- **Chain 1**: Trusted Root CA: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root Intermediate CA: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO High-Assurance Secure Server CA
- **Chain 2**: Trusted Root CA: C=US, O=GeoTrust Inc., CN=GeoTrust Global CA Intermediate CA: Subject: C=US, O=Google Inc, CN=Google Internet Authority G2
- **Chain 3**: Trusted Root CA: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5 Intermediate CA: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Secure Server CA - G3
- **Root C**A: Trusted Root CA: C=US, O=Equifax, OU=Equifax Secure Certificate Authority

If you enable certificate authentication, you are prompted to upload an SSL certificate. you can view the current OV3600 certificate using the **View Certificate** link on that page, or click **Change** to upload a new certificate file to the OV3600 server.

Top Header Settings

The top header of each OV3600 WebUI page displays icons that provide counts on newly discovered devices, device status, mismatches, rogues, clients, and both unacknowledged and severe alerts. These icons also provide direct links for immediate access to key system components.

Figure 2: *Header Statistics Icons*

You can configure what is displayed in the top header for all pages, or for individual AirWave users.

To change the header statistic icons:

1. Navigate to **OV3600 Setup > General**, then scroll down to **Top Header**.
2. Choose the statistics.
3. Choose the devices.
4. Click **Save**.

NOTE

A confirmation message does not appear when you make modifications to the top header statistic icons.

To change statistics that display for an OV3600 user:

1. Navigate to **Home > User Info** page, then scroll down to **Top Header Stats**.
2. Choose the statistics.
3. Choose the devices.
4. Click **Save**. These user settings will override the general settings on the OV3600 Setup page.

Search Method

On the **OV3600 Setup > General** page, locate the **Search Method** section. Select one of the following drop down options as the system-wide default search method. This default search type will be used when a user types an entry in the Search field and then clicks Enter without selecting a specific search type.

- Use System Defaults: The Search Method will be based on the system-wide configuration setting. This method is configured on the **OV3600 Setup > General** page.

- Active clients + historical clients (exact match) + all devices: Commonly referred to as Quick Search, this looks at all active and historical clients and all devices. This search is not case-sensitive. The results of this search display in a pop up window rather than on the **Home > Search** page. This pop up window includes top-level navigation that allows you to filter the results based on Clients, APs, Controllers, and Switches.
- Active clients + all categories: This looks at all active clients (not historical) and all categories. This search is not case-sensitive.
- Active clients + all categories (exact match): This looks at all active clients (not historical) and all categories. This search returns only matches that are exactly as typed (IP, user name, device name, etc). This search is case-sensitive for all searched fields.
- Active + historical clients + all categories: This looks at all active and historical clients and all categories. This search is not case-sensitive.
- Active + historical clients + all categories (exact match): This looks at all active and historical clients and all categories. This search returns only matches that are exactly as typed (IP, user name, device name, etc). This search is case-sensitive for all searched fields.

NOTE

A confirmation message does not appear after you make modifications to Search Preferences.

Per-user search preferences can be set in the **Home > User Info** page.

Home Overview Preferences

On the **OV3600 Setup > General** page, locate the **Home Overview Preferences** section. Table 5 describes the settings and default values in this section.

Table 5: *OV3600 Setup > General > Home Overview Preferences Fields and Default Values*

Setting	Default	Description
Configure Channel Busy Threshold	Yes	Whether you want to configure the threshold at which a channel is considered to be busy at the **Top Folders By Radio Channel Usage** Overview widget.
Channel Busy Threshold (%)	n/a	The threshold percent at which the radio channel is considered busier than normal. This field is only available if the Configure Channel Busy Threshold setting is **Yes**.

Display Settings

On the **OV3600 Setup > General** page, locate the **Display** section and select the options to appear by default in new device groups.

NOTE

Changes to this section apply across all of OV3600. These changes affect all users and all new device groups.

Table 6 describes the settings and default values in this section.

Table 6: *OV3600 Setup > General > Display Fields and Default Values*

Setting	Default	Description
AP Fully Qualified Domain Name Options	No	Sets OV3600 to use fully qualified domain names for APs instead of the AP name. For example, 'testap.yourdomain.com; would be used instead of 'testap.' Select one of the following options: ● **Don't use FQDN** - This default value specifies that the fully qualified domain name will not be used. ● **Use AP Name with FQDN** - The AP name will prepend the FQDN, for example "somehostname (my.hostname.com)." Note that if the AP name is not present, then the FQDN will still appear in parenthesis. ● **Use only FQDN** - Only the fully qualified domain name will be used. **NOTE:** This option is supported only for Cisco IOS, Dell Networking W-Series, Aruba Networks, and Alcatel-Lucent devices.
Show vendor-specific device settings for	All Devices	Displays a drop-down menu that determines which **Group** tabs and options are viewable by default in new groups, and selects the device types that use fully qualified domain names. This field has three options, as follows: ● **All devices**—When selected, OV3600 displays all Group tabs and setting options. ● **Only devices on this** OV3600—When selected, OV3600 hides all options and tabs that do not apply to the APs and devices currently on OV3600. ● **Selected device type**—When selected, a new field appears listing many device types. This option allows you to specify the device types for which OV3600 displays group settings. You can override this setting.
Look up device and wireless user hostnames	Yes	Enables OV3600 to look up the DNS for new user hostnames. This setting can be turned off to troubleshoot performance issues.
DNS Hostname Lifetime	24 hours	Defines the length of time, in hours, for which a DNS server hostname remains valid on OV3600, after which OV3600 refreshes DNS lookup: ● 1 hour ● 2 hours ● 4 hours ● 12 hours ● 24 hours
Device Troubleshooting Hint	N/A	The message included in this field is displayed along with the Down if a device's upstream device is up. This applies to all APs and controllers but not to routers and switches.

Device Configuration Settings

Locate the **Device Configuration** section and adjust the settings. Table 7 describes the settings and default values of this section.

Table 7: *OV3600 Setup > General > Device Configuration Section Fields and Default Values*

Setting	Default	Description
Guest User Configuration	Disabled	Enables or prevents guest users to/from pushing configurations to devices. Options are **Disabled** (default), **Enabled for Devices in Manage(Read/Write)**, **Enabled for all Devices**.
Allow WMS Offload configuration in monitor-only mode	No	When **Yes** is selected, you can enable the AOS-W WMS offload feature on the **Groups > Basic** page for WLAN switches in **Monitor Only** mode. Enabling WMS offload does not cause a controller to reboot. This option is supported only for Aruba and Dell Networking W-Series devices.
Allow disconnecting users while in monitor-only mode	No	Sets whether you can deauthenticate a user for a device in monitor-only mode. If set to **No**, the **Deauthenticate Client** button for in a **Clients > Client Detail** page is enabled only for Managed devices.
Use Global Alcatel-Lucent Configuration	No	Enables Alcatel-Lucent configuration profile settings to be globally configured and then assigned to device groups. If disabled, settings can be defined entirely within **Groups > Controller Config**instead of globally. **NOTE:** Changing this setting may require importing configuration on your devices. When an existing Alcatel-Lucent configuration setup is to be converted from global to group, follow these steps: 1. Set all the devices to Monitor Only mode before setting the flag. 2. Each device Group will need to have an import performed from the **Device Configuration** page of a controller in the OV3600 group. 3. All of the thin APs need to have their settings imported after the device group settings have finished importing. 4. If the devices were set to Monitor Only mode, set them back to Managed mode.

OV3600 Features

Locate the **OV3600 Features** section and adjust settings to enable or disable VisualRF and RAPIDS. Table 8 describes these settings and default values.

Table 8: *OV3600 Setup Setup > General > OV3600 Features Fields and Default Values*

Setting	Default	Description
Display VisualRF	No	Enable or disable the **VisualRF** navigation tab.
Display RAPIDS	No	Enable or disable the **RAPIDS** navigation tab.
Hide setup pages from non-admin users	Yes	Restrict access to following pages to users with the OV3600 Administration role only: ● VisualRF > Setup ● OV3600 Setup > NMS ● RAPIDS > Score Override ● RAPIDS > Rules ● RAPIDS > Setup ● System > Triggers
Allow role based report visibility	Yes	Enable or disable role-based reporting in OV3600. When disabled, reports can only be generated with by-subject visibility.

External Logging Settings

Locate the **External Logging** section and adjust settings to send audit and system events to an external syslog server. Table 9 describes these settings and default values. You can also send a test message using the **Send Test Message** button after enabling any of the logging options.

Table 9: *OV3600 Setup > General > External Logging Section Fields and Default Values*

Setting	Default	Description
Syslog Server	N/A	Enter the IP address of the syslog server. Note that this field is hidden if both "Include event log messages" and "Include audit log messages" are set to **No**.
Syslog Port	514	Enter the port of the syslog server. Note that this field is hidden if both "Include event log messages" and "Include audit log messages" are set to **No**.
Include event log messages	No	Select **Yes** to send event log messages to an external syslog server.
Event log facility	local1	Select the facility for the event log from the drop-down menu. This field is only available if the "Include event log messages" setting is **Yes**.
Include audit log messages	No	Select **Yes** to send audit log messages to an external syslog server.
Audit log facility	local1	Select the facility for the audit log from the drop-down menu. This field is only available if the "Include audit log messages" setting is **Yes**
Send Test Message	N/A	If messaging is enabled and a server and port are configured, click this button to send a test message. Upon completion, a message will appear at the top of this page indicating that the message was sent successfully.

Historical Data Retention Settings

Locate the **Historical Data Retention** section and specify the number of days you want to keep client session records and rogue discovery events. Table 10 describes the settings and default values of this section. Many settings can be set to have no expiration date.

Table 10: *OV3600 Setup > General > Historical Data Retention Fields and Default Values*

Setting	Default	Description
Inactive Client and VPN User Data (0-1500 days, zero disables)	60	Defines the number of days OV3600 stores basic information about inactive clients and VPN users. A shorter setting of 60 days is recommended for customers with high user turnover such as hotels. The longer you store inactive user data, the more hard disk space you require.
Client Association and VPN Session History (0-550 days, zero disables)	14	Defines the number of days OV3600 stores client and VPN session records. The longer you store client session records, the more hard disk space you require.

Table 10: *OV3600 Setup > General > Historical Data Retention Fields and Default Values (Continued)*

Setting	Default	Description
Tag History (0-550 days, zero disables)	14	Sets the number of days OV3600 retains location history for Wi-Fi tags.
Rogue AP Discovery Events (14-550 days, zero disables)	14	Defines the number of days OV3600 stores Rogue Discovery Events. The longer you store discovery event records, the more hard disk space you require.
Reports (0-550 days, zero disables)	60	Defines the number of days OV3600 stores Reports. Large numbers of reports, over 1000, can cause the **Reports > Generated** page to be slow to respond.
Automatically Acknowledge Alerts(0-550 days, zero disables)	14	Defines automatically acknowledged alerts as the number of days OV3600 retains alerts that have been automatically acknowledged. Setting this value to 0 disables this function, and alerts will never expire or be deleted from the database.
Acknowledged Alerts(0-550 days, zero disables)	60	Defines the number of days OV3600 retains information about acknowledged alerts. Large numbers of Alerts, over 2000, can cause the **System > Alerts** page to be slow to respond.
Radius/ARM/IDS Events(0-550 days, zero disables)	14	Defines the number of days OV3600 retains information about RADIUS, ARM, and IDS events. Setting this value to **0** disables this function, and the information will never expire or be deleted from the database.
Archived Device Configurations (0-100, zero disables)	10	Defines the number of configurations that will be retained for archived devices. Whether rogue information is included depends on the setting of the **Archive device configs even if they only have rogue classifications** setting.
Archive device configs even if they only have rogue classifications	No	Sets whether to archive device configurations even if the device only has rogue classifications.
Guest Users (0-550 days, zero disables)	30	Sets the number of days that OV3600 is to support any guest user. A value of **0** disables this function, and guest users will never expire or be deleted from the OV3600 database.
Inactive SSIDs (0-550 days, zero disables)	425	Sets the number of days OV3600 retains historical information after OV3600 last saw a client on a specific SSID. Setting this value to **0** disables this function, and inactive SSIDs will never expire or be deleted from the database.
Inactive Interfaces (0-550 days, zero disables)	425	Sets the number of days OV3600 retains inactive interface information after the interface has been removed or deleted from the device. Setting this value to **0** disables this function, and inactive interface information will never expire or be deleted from the database.

Table 10: *OV3600 Setup > General > Historical Data Retention Fields and Default Values (Continued)*

Setting	Default	Description
Interface Status History (0-550 days, zero disables)	425	Sets the number of days OV3600 retains historical information on interface status. Setting this value to **0** disables this function.
Interfering Devices (0-550 days, zero disables)	14	Sets the number of days OV3600 retains historical information on interfering devices. Setting this value to **0** disables this function.
Device Events (Syslog, Traps)(1-31 days)	2	Sets the number of days OV3600 retains historical information on device events such as syslog entries and SNMP traps. Setting this value to **0** disables this function. Refer to "Viewing Device Events" on page 265. **NOTE:** If your data table has more than 5 million rows, OV3600 will truncate the device event retention data. In this case, the "number of days" setting becomes "number of hours."
Mesh Link History (0-550 days)	30	Sets the number of days OV3600 retains historical information for mesh links.
Device Uptime (0-120 months, zero disables)	60	Sets the number of months OV3600 retains historical information on device uptime. Setting this value to **0** disables this function.
Client Data Retention Interval (1-425 days)	425	Sets the number of days OV3600 retains historical information for clients.
UCC Call History (1-30 days)	30	Sets the number of days that calls remain in OV3600's call history.
UCC Call Details (1-7 days)	2	Sets the number if days that the OV3600 retains details for individual calls.
Config Job Retention Interval (1-31 days)	31	Sets the number of days OmniVista 3600 Air Manager retains information about configuration jobs.

Firmware Upgrade Defaults

Locate the **Firmware Upgrade Defaults** section and adjust settings as required. This section allows you to configure the default firmware upgrade behavior for OV3600Table 11 describes the settings and default values of this section.

Table 11: *OV3600 Setup > General > Firmware Upgrade Defaults Fields and Default Values*

Setting	Default	Description
Allow firmware upgrades in monitor-only mode	No	If **Yes** is selected, OV3600 upgrades the firmware for APs in **Monitor Only** mode. When OV3600 upgrades the firmware in this mode, the desired configuration are not be pushed to OV3600. Only the firmware is applied. The firmware upgrade may result in configuration changes OV3600 does not correct those changes when the AP is in **Monitor Only** mode.

Table 11: *OV3600 Setup > General > Firmware Upgrade Defaults Fields and Default Values (Continued)*

Setting	Default	Description
Maximum Interleaved Jobs (1-20)	20	Defines the number of jobs OV3600 runs at the same time. A job can include multiple APs. When jobs are started by multiple users, OV3600 will interleave upgrades so that one user's job does not completely block another's.
Maximum Interleaved Devices Per Job (1-1000)	20	Defines the number of devices that can be in the process of upgrading at the same time. Within a single job, OV3600 may start the upgrade process for up to this number of devices at the same time. However, only one device will be actively downloading a firmware file at any given time.
Failures before stopping (0-20, zero disables)	1	Sets the default number of upgrade failures before OV3600 pauses the upgrade process. User intervention is required to resume the upgrade process. Setting this value to **0** disables this function.

Additional OV3600 Services

Locate the **Additional OV3600 Services** section, and adjust settings as required. Table 12 describes the settings and default values of this section.

Table 12: *OV3600 Setup > General > Additional OV3600 Services Fields and Default Values*

Setting	Default	Description
Enable FTP Server	No	Enables or disables the FTP server on OV3600. The FTP server is only used to manage Aruba AirMesh and Cisco Aironet 4800 APs. Best practice is to disable the FTP server if you do not have any supported devices in the network.
Enable RTLS Collector	No	Enables or disables the RTLS Collector, which is used to allow AOS-W switches to send signed and encrypted RTLS (real time locating system) packets to VisualRF; in other words, OV3600 becomes the acting RTLS server. The RTLS server IP address must be configured on each switch. This function is used for VisualRF to improve location accuracy and to locate chirping asset tags. This function is supported only for Dell Networking W-Series, Alcatel-Lucent, and Aruba Networks devices. If **Yes** is specified, the following additional fields appear. These configuration settings should match the settings configured on the switch: ● **RTLS Port**—Specify the port for the OV3600 RTLS server. ● **RTLS Username**—Enter the user name used by the switch to decode RTLS messages. ● **RTLS Password**—Enter the RTLS server password that matches the switch's value. ● **Confirm RTLS Password**—Re-enter the RTLS server password.
Use embedded Mail Server	Yes	Enables or disables the embedded mail server that is included with OV3600.
Mail Relay Server	Optional	If you enable the "Use embedded mail server" option, enter information for an optional mail relay server. This field supports a **Send Test Email** button for testing server functionality. Click this button to enter valid email addresses.

Table 12: *OV3600 Setup > General > Additional OV3600 Services Fields and Default Values (Continued)*

Setting	Default	Description
Process user roaming traps from Cisco WLC	Yes	Whether OV3600 should parse client association and authentication traps from Cisco WLC controllers to give real time information on users connected to the wireless network.
Enable AMON data collection	Yes	Allows OV3600 to collect enhanced data from Alcatel-Lucent devices on certain firmware versions. See the *Best Practices Guide* on the **Home > Documentation** page for more details **NOTE:** When enabling AMON, auditing should be set to **daily** and have been successful at least once to allow OV3600 to calculate the proper BSSIDs per radio. If these BSSIDs do not exist, clients are dropped because they do not have any corresponding BSSIDs in the OV3600 database. Auditing should be set to daily because the BSSIDs are kept in cache memory and cleared every 24 hours.
Enable Clarity Data Collection	Yes	Allows OV3600 to collect enhanced Clarity Monitoring data from Alcatel-Lucent devices running AOS-W 6.4.3 and later versions
Enable Traffic Analysis Data Collection	Yes	If AMON is enabled for a controller, you can enable OV3600 to collect Traffic Analysis data from the controller by setting this to Yes. When enabled, the **Home > Traffic Anaylsis** dashboard is available in the WebUI.
Traffic Analysis Storage Allocated (GiB) Greater than or equal to 2 GiB	50	If Traffic Analysis Data Collection is enabled, you can specify the amount of storage to allocate.
Enable UCC Data Collection	Yes	Enables controllers to send UCC data to OmniVista 3600 Air Manager. For this feature to work, OmniVista 3600 Air Manager must be a management server on the switch, the AMON port is set up for UDP port 8211, and the switch profile has UCC monitoring enabled.
Enable UCC Calls Stitching (Heuristics)	Yes	Enables caller-to-callee call stitching for non-SDN deployments. You should turn off this option for NAT and BOC deployments.

Table 12: *OV3600 Setup > General > Additional OV3600 Services Fields and Default Values (Continued)*

Setting	Default	Description
Prefer AMON vs SNMP Polling	Yes	**Prefer AMON** is a configuration setting which causes OV3600 to use an AMON feed to obtain client monitoring information from a switch rather than polling it via SNMP. When you enable this setting, values such as AP lists and rogue AP lists are still polled via SNMP, but the bulk of client monitoring information is delivered via AMON. **NOTE:** ● Auditing needs to have been successful at least once to allow OV3600 to calculate the proper BSSIDs per radio. ● When **Prefer AMON** is enabled, the controller must be configured to send AMON to OV3600. ● The network path from the switch to the OV3600 server must allow traffic on UDP port 8211. ● The switch routinely sends AMON in large UDP packets, (up to 30K bytes). Before enabling this setting, ensure the network path from the switch to OV3600 can pass such large packets intact. ● This setting should only be used in a network environment with low levels of UDP packet loss, as the loss of a single Ethernet frame will potentially result in the loss of up to 30K bytes worth of data.
Prefer SNMP Polling for VPN Clients	Yes	This setting enables OV3600 to communicate with the VIA VPN client using SNMP polling.
Enable Syslog and SNMP Trap Collection	Yes	This option specifies whether traps used to detect roaming events, auth failures, AP up/down status, and IDS events will still be collected if they are sent by managed devices.
Require SSH host key verification	No	This setting reserved for future use.
Validate PAPI key	No	Security improvements in OV3600 8.2.1 and later releases allow you to specify a custom PAPI key and require PAPI key validation. If you select the Yes option, you are prompted to enter a custom PAPI key
Disable TLS 1.0 and 1.1	Yes	This option is set to Yes by default. In order for Aruba switches to automatically check-in to OV3600 by ZTP, you must change this option to No. If you select No, you must restart AMP.

Performance Settings

Locate the **Performance** section. Performance tuning is unlikely to be necessary for many OV3600 deployments, and likely provides the most improvements for customers with extremely large Pro or Enterprise installations. Please contact Alcatel-Lucent support if you think you might need to change any of these settings. Table 13 describes the settings and default values of this section.

Table 13: *OV3600 Setup> General > Performance Fields and Default Values*

Setting	Default	Description
Monitoring Processes	Based on the number of cores for your server	Optional setting configures the throughput of monitoring data. Increasing this setting allows OV3600 to process more data per second, but it can take resources away from other OV3600 processes. Contact Alcatel-Lucent support if you think you might need to increase this setting for your network. Also note that the value range varies based on the number of available process cores.
Maximum number of configuration processes	5	Increases the number of processes that are pushing configurations to your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Contact Alcatel-Lucent support if you think you might need to increase this setting for your network.
Maximum number of audit processes	3	Increases the number of processes that audit configurations for your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Contact Alcatel-Lucent support if you are considering increasing this setting for your network.
SNMP Fetcher Count (2-6)	2	Specify the number of SNMPv2 fetchers.
Verbose Logging of SNMP Configuration	No	Enables or disables logging detailed records of SNMP configuration information.
SNMP Rate Limiting for Monitored Devices	No	When enabled, OV3600 fetches SNMP data more slowly, potentially reducing device CPU load. We recommend enabling this global setting when monitoring Alcatel-Lucent switches only if your network contains a majority of legacy switches . If your network mainly uses newer switches (OAW-4306 Series or the OAW-S3 module in the OAW-6000 Series), we strongly recommends disabling this setting.
Client Association Relevance Factor	0 days (disabled)	Use this setting to hide old client information from clients lists and client search results. For example, a setting of **3** limits the historical client data displayed in client lists and search results to client sessions that have been disconnected within the last three days. When this value is set to **1**, client lists and search results display only the client history for the previous day. This time range can be set from 0-550 days, where a value of zero disables this feature and makes available all historical client data. A shorter time period improves search performance and allows client lists to display more rapidly, though it will also display fewer results.

Table 13: *OV3600 Setup> General > Performance Fields and Default Values (Continued)*

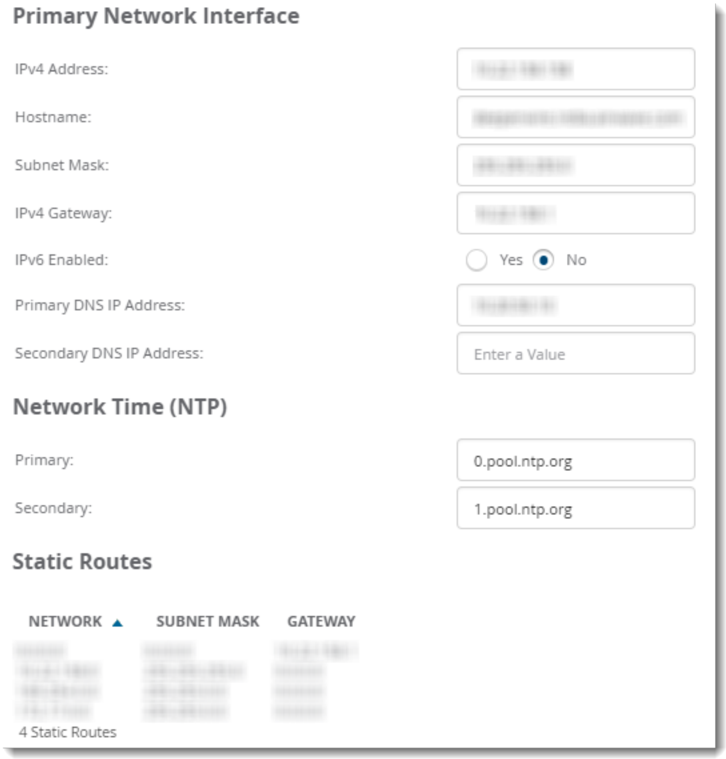
Setting	Default	Description
RAPIDS Processing Priority	Low	Defines the processing and system resource priority for RAPIDS in relation to OV3600 as a whole. When OV3600 is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (such as client connections and bandwidth usage) is not adversely impacted. The default priority is **Low**. You can also tune your system performance by changing group poll periods. If you select **Custom** for the priority, then also specify the RAPIDS custom process limit.
RAPIDS custom process limit (1-16)	1 when **Custom** is specified for the RAPIDS Processing Priority.	Sets the maximum number of monitoring process assigned to RAPIDS work. Note that this option is only available if **Custom** is specified for the RAPIDS Processing Priority.

Defining Network Settings

The next steps in setting up OV3600 are to configure the network interface, DNS settings, NTP servers, and static routes.

Figure 3 illustrates the contents of the **OV3600 Setup > Network** page when setting up an IPv4 interface. Optionally, you can configure an IPv6 interface. For information, see "Primary Network Interface Settings" on page 35.

Figure 3: *Network Page*



Primary Network Interface

IPv4 Address: [redacted]

Hostname: [redacted]

Subnet Mask: [redacted]

IPv4 Gateway: [redacted]

IPv6 Enabled: ○ Yes ● No

Primary DNS IP Address: [redacted]

Secondary DNS IP Address: Enter a Value

Network Time (NTP)

Primary: 0.pool.ntp.org

Secondary: 1.pool.ntp.org

Static Routes

NETWORK ▲	SUBNET MASK	GATEWAY
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

4 Static Routes

Specify the network configuration options described in the sections that follow to define the OV3600 network settings. Select **Save** when you have completed all changes on the **OV3600 Setup > Network** page, or select **Revert** to return to the last settings. **Save** restarts any affected services and may temporarily disrupt your network connection.

Refer to the following topics for configuration information:

- "Primary Network Interface Settings" on page 35
- "Secondary Network Interface Settings" on page 36
- "Network Time Protocol (NTP) Settings" on page 36
- "Static Routes" on page 37

Primary Network Interface Settings

Locate the **Primary Network Interface** section. The information in this sections should match what you defined during initial network configuration and should not require changes. Table 14 describes the settings and default values.

Table 14: ***Primary Network Interface*** *Fields and Default Values*

Setting	Default	Description
IPv4 Address	None	Sets the IPv4 address of the OV3600 network interface. **NOTE:** This address must be a static IP address.
Hostname	None	Sets the DNS name assigned to the OV3600 server.
Subnet Mask	None	Sets the subnet mask for the primary network interface.

Table 14: *Primary Network Interface Fields and Default Values (Continued)*

Setting	Default	Description
IPv4 Gateway	None	Sets the default gateway for the network interface.
IPv6 Enabled	No	By selecting **Yes**, you can enter an optional IPv6 address and gateway address.
IPv6 Address	None	Sets the IPv6 address of the OV3600 network interface.
IPv6 Gateway	None	Sets the default gateway for the network interface.
Primary DNS IP	None	Sets the primary DNS IP address for the network interface.
Secondary DNS IP	None	Sets the secondary DNS IP address for the network interface.

Secondary Network Interface Settings

Locate the **Secondary Network Interface** section. The information in this section should match what you defined during initial network configuration and should not require changes. Table 15 describes the settings and default values.

Table 15: *Secondary Network Interface Fields and Default Values*

Setting	Default	Description
Enabled	No	Select **Yes** to enable a secondary network interface. You will be prompted to define the IP address and subnet mask.
IP Address	None	Specify the IP address of the OV3600 secondary network. **NOTE:** This address must be a static IP address. OV3600 supports IPv4 and IPv6 addresses.
Subnet Mask	None	Specify the subnet mask for the secondary network interface.

Network Time Protocol (NTP) Settings

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

NOTE

Specifying NTP servers is optional. NTP servers synchronize the time on the OV3600 server, not on individual access points.

To disable NTP services, clear both the **Primary** and **Secondary** NTP server fields. Any problem related to communication between OV3600 and the NTP servers creates an entry in the event log. Table 16 describes the settings and default values in more detail. For more information on ensuring that OV3600 servers have the correct time, please see http://support.ntp.org/bin/view/Servers/NTPPoolServers.

Table 16: *OV3600 Setup > Network > Secondary Network Fields and Default Values*

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

Table 16: *OV3600 Setup > Network > Secondary Network Fields and Default Values (Continued)*

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

Static Routes

On the **OV3600 Setup > Network** page, locate the **Static Routes** area. This section displays network, subnet mask, and gateway settings that you have defined elsewhere from a command-line interface.

NOTE

This section does not enable you to configure new routes or remove existing routes.

What Next?

- Go to additional tabs in the OV3600 Setup section to continue additional setup configurations. The next section describes OV3600 roles.
- Complete the required configurations in this chapter before proceeding. Alcatel-Lucent support remains available to you for any phase of OV3600 configuration.

Creating OV3600 Users

OV3600 installs with only one user—the **admin**, who is authorized to perform the following functions:

- Define additional users with varying levels of privilege, be it manage read/write or monitoring.
- Limit the viewable devices as well as the level of access a user has to the devices.

Each general user that you add must have a user name, a password, and a role. Use unique and meaningful user names as they are recorded in the log files when you or other users make changes in OV3600.

NOTE

User name and password are not required if you configure OV3600 to use RADIUS, TACACS, or LDAP authentication. You do not need to add individual users to the OV3600 server if you use RADIUS, TACACS, or LDAP authentication.

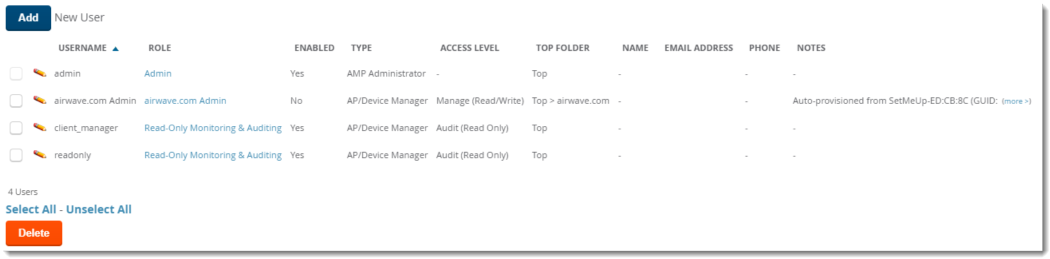
The user role defines the user type, access level, and the top folder for that user. User roles are defined on the **OV3600 Setup > Roles** page. Refer to the previous procedure in this chapter for additional information, "Creating OV3600 User Roles" on page 39.

The **admin** user can provide optional additional information about the user, including the user's real name, email address, phone number, and so forth.

Perform the following steps to display, add, edit, or delete OV3600 users of any privilege level. You must be an **admin** user to complete these steps.

1. Go to the **OV3600 Setup > Users** page. This page displays all users currently configured in OV3600, as shown in Figure 4.

Figure 4: *OV3600 Setup > Users Page*



	USERNAME ▲	ROLE	ENABLED	TYPE	ACCESS LEVEL	TOP FOLDER	NAME	EMAIL ADDRESS	PHONE	NOTES
☐	admin	Admin	Yes	AMP Administrator	-	Top	-		-	-
☐	airwave.com Admin	airwave.com Admin	No	AP/Device Manager	Manage (Read/Write)	Top > airwave.com	-		-	Auto-provisioned from SetMeUp-ED:CB:8C (GUID: (more >)
☐	client_manager	Read-Only Monitoring & Auditing	Yes	AP/Device Manager	Audit (Read Only)	Top	-		-	-
☐	readonly	Read-Only Monitoring & Auditing	Yes	AP/Device Manager	Audit (Read Only)	Top	-		-	-

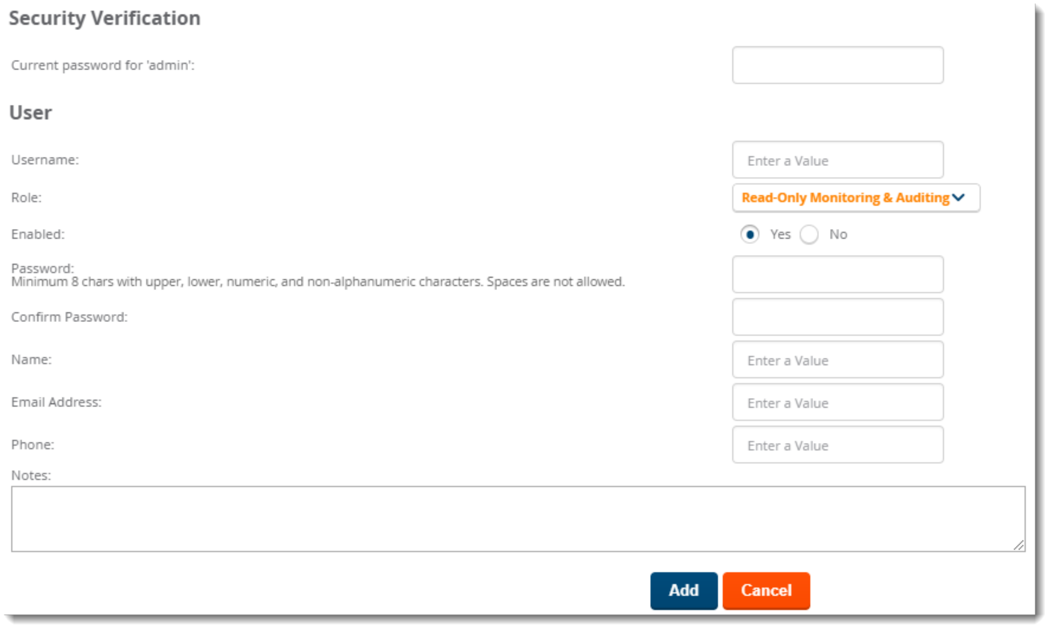
4 Users

2. Select **Add** to create a new user, select the pencil icon to edit an existing user, or select a user and select **Delete** to remove that user from OV3600. When you select **Add** or the edit icon, the **Add User** page appears, illustrated in Figure 5.

NOTE

Current users cannot change their own role. The **Role** drop-down field is disabled to prevent this.

Figure 5: *OV3600 Setup > Users > Add/Edit User Page*



Security Verification

Current password for 'admin':

User

Username: Enter a Value

Role: Read-Only Monitoring & Auditing

Enabled: ● Yes ○ No

Password:
Minimum 8 chars with upper, lower, numeric, and non-alphanumeric characters. Spaces are not allowed.

Confirm Password:

Name: Enter a Value

Email Address: Enter a Value

Phone: Enter a Value

Notes:

3. Enter or edit the settings on this page. Table 17 describes these settings.

Table 17: *OV3600 Setup > Users > Add/Edit User Fields and Default Values*

Setting	Default	Description
Username	None	Sets the user name for the user who logs in to OV3600. This user name is displayed in OV3600 log files.
Role	None	Specifies the user's **Role**, which defines the Top viewable folder as well as the type and access level of the user specified in the previous field. The **admin** user defines user roles on the **OV3600 Setup > Roles** page, and each user in the system is assigned to a role.
Password	None	Sets the password for the user being created or edited. Enter an alphanumeric string without spaces, and enter the password again in the **Confirm Password** field. OV3600 strengthens user passwords with SHA512 encryption. **NOTE:** Because the default user's password is identical to the **Name**, you should change this password. You will be logged out and asked to enter your new password.
Name	None	Allows you to define an optional and alphanumeric text field that takes note of the user's actual name.

Table 17: *OV3600 Setup > Users > Add/Edit User Fields and Default Values (Continued)*

Setting	Default	Description
Email Address	None	Allows you to specify a specific email address that will propagate throughout many additional pages in OV3600 for that user, including reports, triggers, and alerts.
Phone	None	Allows you to enter an optional phone number for the user.
Notes	None	Enables you to cite any additional notes about the user, including the reason they were granted access, the user's department, or job title.

4. Select **Add** to create the new user, **Save** to retain changes to an existing user, or **Cancel** to cancel out of this screen. The user information you have configured appears on the **OV3600 Setup > Users** page, and the user propagates to all other OV3600 pages and relevant functions.

NOTE

OV3600 enables user roles to be created with access to folders within multiple branches of the overall hierarchy. This feature assists non-administrator users who support a subset of accounts or sites within a single OV3600 deployment, such as help desk or IT staff.

Configuring OV3600 User Roles

The **OV3600 Setup > Roles** page defines the viewable devices, the operations that can be performed on devices, and general OV3600 access. User roles can be created that provide users with access to folders within multiple branches of the overall hierarchy. This feature assists non-administrative users, such as help desk or IT staff, who support a subset of accounts or sites within a single OV3600 deployment. You can restrict user roles to multiple folders within the overall hierarchy even if they do not share the same top-level folder. Non-admin users are only able to see data and users for devices within their assigned subset of folders.

Refer to the following additional topics:

- "User Roles and VisualRF" on page 39
- "Creating OV3600 User Roles" on page 39

User Roles and VisualRF

VisualRF uses the same user roles as defined for OV3600. Users can see floor plans that contain an AP to which they have access in OV3600, although only visible APs appear on the floor plan. VisualRF users can also see any building that contains a visible floor plan and any campus that contains a visible building.

NOTE

In **VisualRF > Setup > Server Settings**, the **Restrict visibility of empty floor plans to the user that created them** configuration option allows you to restrict the visibility of empty floor plans to the role of the user who created them. By default, this setting is set to No.

When a new role is added to OV3600, VisualRF must be restarted for the new user to be enabled.

Creating OV3600 User Roles

Roles define the capabilities a user has access to and the privileges and views available for device groups and devices in OV3600. The available configuration options differ for each role type.

NOTE

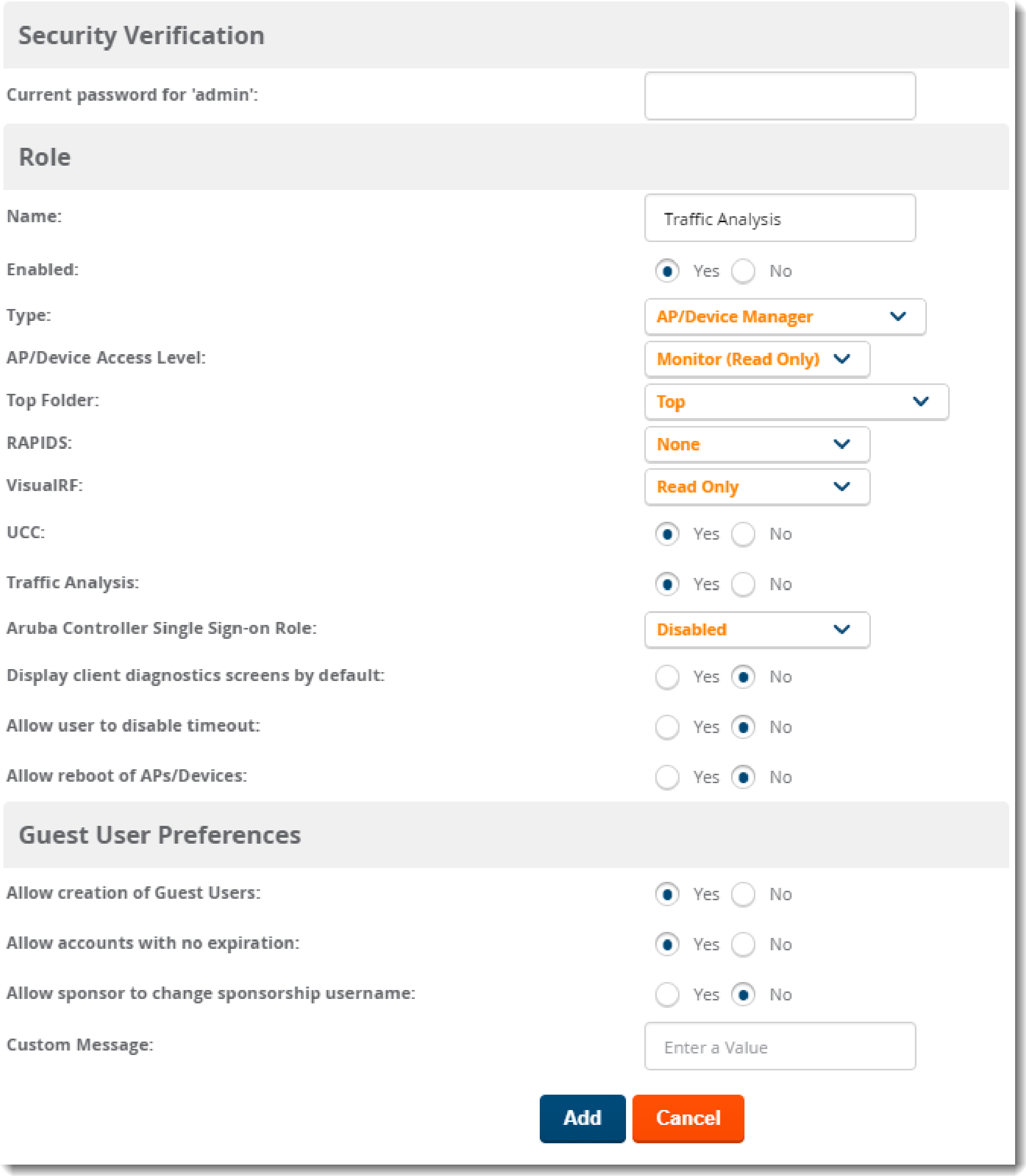
Most users will see two sections on this page: **Role** and **Guest User Preferences**. The **Guest User Preferences** section appears only if **Guest User Configuration** is enabled in **OV3600 Setup > General**.

If you want to create a user role, log in to OV3600 as admin and follow these steps:

1. Go to the **OV3600 Setup** > **Roles** and click **Add**.

2. Enter a name for the user role, select options, and click **Add**. For example, Figure 6 shows a role named Traffic Analysis being created.

Figure 6: *Adding a Non-Admin Role Named Traffic Analysis*



Security Verification

Current password for 'admin':	

Role

Name:	Traffic Analysis
Enabled:	● Yes ○ No
Type:	AP/Device Manager
AP/Device Access Level:	Monitor (Read Only)
Top Folder:	Top
RAPIDS:	None
VisualRF:	Read Only
UCC:	● Yes ○ No
Traffic Analysis:	● Yes ○ No
Aruba Controller Single Sign-on Role:	Disabled
Display client diagnostics screens by default:	○ Yes ● No
Allow user to disable timeout:	○ Yes ● No
Allow reboot of APs/Devices:	○ Yes ● No

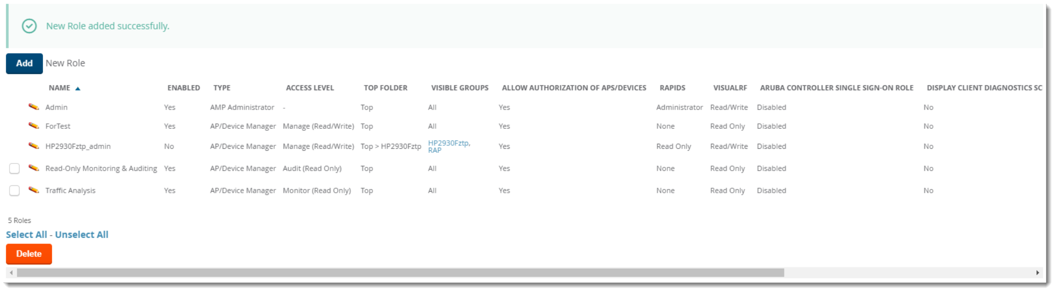
Guest User Preferences

Allow creation of Guest Users:	● Yes ○ No
Allow accounts with no expiration:	● Yes ○ No
Allow sponsor to change sponsorship username:	○ Yes ● No
Custom Message:	Enter a Value

3. Enter additional settings on this page.

shows the newly created Traffic Analysis Admin role in the Role page.

Figure 7: *Newly Created Traffic Analysis Admin Role*



New Role added successfully.

	NAME ▲	ENABLED	TYPE	ACCESS LEVEL	TOP FOLDER	VISIBLE GROUPS	ALLOW AUTHORIZATION OF APS/DEVICES	RAPIDS	VISUALRF	ARUBA CONTROLLER SINGLE SIGN-ON ROLE	DISPLAY CLIENT DIAGNOSTICS SC
	Admin	Yes	AMP Administrator	-	Top	All	Yes	Administrator	Read/Write	Disabled	No
	ForTest	Yes	AP/Device Manager	Manage (Read/Write)	Top	All	Yes	None	Read Only	Disabled	No
	HP2930Fztp_admin	No	AP/Device Manager	Manage (Read/Write)	Top > HP2930Fztp	HP2930Fztp, RAP	Yes	Read Only	Read/Write	Disabled	No
□	Read-Only Monitoring & Auditing	Yes	AP/Device Manager	Audit (Read Only)	Top	All	Yes	None	Read Only	Disabled	No
□	Traffic Analysis	Yes	AP/Device Manager	Monitor (Read Only)	Top	All	Yes	None	Read Only	Disabled	No

5 Roles

AMP Administrator Role

The following table describes the available settings and default values for the AMP Administrator role.

Table 18: *OV3600 Setup > Roles > Add/Edit Roles Fields and Default Values for AMP Administrator Role*

Setting	Default	Description
Name	None	Sets the administrator-definable string that names the role. The role name should indicate the devices and groups that are viewable, as well as the privileges granted to that role.
Enabled	Yes	Disables or enables the role. Disabling a role prevents all users of that role from logging in to OV3600.
Type	AP/Device Manager	Defines the type of role. OV3600 Administrator—The OV3600 Administrator has full access to OV3600 and all of the devices. Only the OV3600 Administrator can create new users or access the OV3600 Setup page, the VisualRF > Setup page, VisualRF > Audit Log page, System > Event Log, and System > Performance.
Alcatel-Lucent Controller Role	Disabled	Enables or disables **Single Sign-On** for the role. If enabled, allows the user read-only access or direct access to the Alcatel-Lucent controller UIs from quick links in the WebUI without having to enter credentials for the controller.
Allow user to disable timeout	No	Whether a user can disable OV3600's timeout feature.
Custom Message	none	A custom message can also be included.

Table 19: *OV3600 Setup > Roles > Add/Edit Roles Fields and Default Values for AP/Device Manager Role*

Setting	Default	Description
Name	None	Sets the administrator-definable string that names the role. The role name should indicate the devices and groups that are viewable, as well as the privileges granted to that role.
Enabled	Yes	Disables or enables the role. Disabling a role prevents all users of that role from logging in to OV3600.

Table 19: *OV3600 Setup > Roles > Add/Edit Roles Fields and Default Values for AP/Device Manager Role (Continued)*

Setting	Default	Description
Type	AP/Device Manager	Defines the type of role. **AP/Device Manager**—AP/Device Managers have access to a limited number of devices and groups based on the Top folder and varying levels of control based on the Access Level.
Access Level	Monitor (Read Only)	Defines the privileges the role has over the viewable device. OV3600 supports three privilege levels, as follows: ● **Manage (Read/Write)**—Manage users can view and modify devices and Groups. Selecting this option causes a new field, **Allow authorization of Devices**, to appear on the page, and is enabled by default. ● **Audit (Read Only)**—Audit users have read only access to the viewable devices and Groups. Audit users have access to the **Device Configuration** page, which may contain sensitive information including AP passwords. ● **Monitor (Read Only)**—Monitor users have read-only access to devices and groups and VisualRF. Monitor users cannot view the **Device Configuration** page which may contain sensitive information, including passwords.
Top Folder	Top	Defines the highest viewable folder for the role. The role is able to view all devices and groups contained by the specified top folder. The top folder and its subfolders must contain all of the devices in any of the groups it can view. **NOTE:** OV3600 enables user roles to be created with access to folders within multiple branches of the overall hierarchy. This feature assists non-administrator users who support *a subset of accounts or sites* within a single OV3600 deployment, such as help desk or IT staff. User roles can be restricted to multiple folders within the overall hierarchy, even if they do not share the same top-level folder. Non-administrator users are only able to see data and users for devices within their assigned subset of folders.
Allow Authorization of Devices	Yes	**NOTE:** This option is only available when the **AP/Device Access Level** is specified as **Manage (Read/Write)**.
RAPIDS	None	Sets the RAPIDS privileges. This field specifies the RAPIDS privileges for the user role and includes these options: ● **None**— Cannot view the RAPIDS tab or any Rogue APs. ● **Read Only**—The user can view the RAPIDS pages but cannot make any changes to rogue APs or perform OS scans. ● **Read/Write**—The user may edit individual rogues, classification, threat levels and notes, and perform OS scans. ● **Administrator**—Has the same privileges as the Read/Write user, but can also set up RAPIDS rules, override scores and is the only user who can access the **RAPIDS > Setup** page.

Table 19: *OV3600 Setup > Roles > Add/Edit Roles Fields and Default Values for AP/Device Manager Role (Continued)*

Setting	Default	Description
VisualRF	Read Only	Sets the VisualRF privileges, which are set separately from the APs/Devices. Options are as follows: ● **Read Only**—The user can view the VisualRF pages but cannot make any changes to floor plans. ● **Read/Write**—The user may edit individual floor plans, buildings, and campuses.
UCC	Yes	Permits access to UCC views and tables. Monitoring and managing privileges are set at the AP/Device level.
Traffic Analysis	Yes	Permits access to Traffic Analysis views and tables. Monitoring and managing privileges are set at the AP/Device level.
Alcatel-Lucent Controller Single Sign-On Role	Disabled	If enabled, the user has read-only or root access to Alcatel-Lucent controller UIs from quick links without having to enter credentials for the controller.
Display Client Diagnostics Screens By Default	No	Sets the role to support helpdesk users with parameters that are specific to the needs of helpdesk personnel supporting users on a wireless network.
Allow User to Disable Timeout	No	Whether a user can disable OV3600's timeout feature.
Allow Reboot of Devices	No	Allows user to reboot devices in OV3600.
Allow Creation of Guest Users	Yes	If this option is enabled, users with an assigned role of Monitoring or Audit can be given access to guest user account creation along with the option to allow a sponsor to change its user name. **NOTE:** This option is not available if the **AP/Device Access Level** is specified as **Manage (Read/Write)**.
Allow Accounts With No Expiration	Yes	Specifies whether to allow accounts that have no expiration set. If this is set to **No**, then enter the amount of time that can elapse before the access expires.
Allow Sponsor to Change Sponsorship User Name	No	Specifies whether a sponsor can change the sponsorship user name.
Custom Message	none	A custom message can also be included.

Guest Access Sponsor Role

The following table describes the available settings and default values for the Guest Access Sponsor role.

Table 20: *OV3600 Setup > Roles > Add/Edit Roles Fields and Default Values for Guest Access Sponsor Role*

Setting	Default	Description
Name	None	Sets the administrator-definable string that names the role. The role name should indicate the devices and groups that are viewable, as well as the privileges granted to that role.
Enabled	Yes	Disables or enables the role. Disabling a role prevents all users of that role from logging in to OV3600.
Type	AP/Device Manager	Defines the type of role. **Guest Access Sponsor**—Limited-functionality role to allow helpdesk or reception desk staff to grant wireless access to temporary personnel. This role only has access to the defined top folder of APs.
Top Folder	Top	Defines the Top viewable folder for the role. The role is able to view all devices and groups contained by the Top folder. The top folder and its subfolders must contain all of the devices in any of the groups it can view. **NOTE:** OV3600 enables user roles to be created with access to folders within multiple branches of the overall hierarchy. This feature assists non-administrator users who support *a subset of accounts or sites* within a single OV3600 deployment, such as help desk or IT staff. User roles can be restricted to multiple folders within the overall hierarchy, even if they do not share the same top-level folder. Non-administrator users are only able to see data and users for devices within their assigned subset of folders.
Allow user to disable timeout	No	Whether a user can disable OV3600's timeout feature.
Allow accounts with no expiration	Yes	Specifies whether to allow accounts that have no expiration set. If this is set to **No**, then enter the amount of time that can elapse before the access expires.
Allow sponsor to change sponsorship user name	No	Specifies whether a sponsor can change the sponsorship user name.
Custom Message	none	A custom message can also be included.

Configuring the User Login and Authentication

OV3600 uses session-based authentication with a configurable login message and idle timeout. As an option, you can set OV3600 to use an external user database to simplify password management for OV3600 administrators and users.

This section contains the following procedures to be followed in **OV3600 Setup > Authentication**:

- "Configuring the User Login" on page 45

- "Configuring Whitelists" on page 46
- "Setting Up Certificate Authentication" on page 45
- "Setting Up Single Sign-On" on page 46
- "Specifying the Authentication Priority" on page 46
- "Configuring RADIUS Authentication and Authorization" on page 46
- "Integrating a RADIUS Accounting Server" on page 48
- "Configuring TACACS+ Authentication" on page 49
- "Configuring LDAP Authentication and Authorization" on page 51

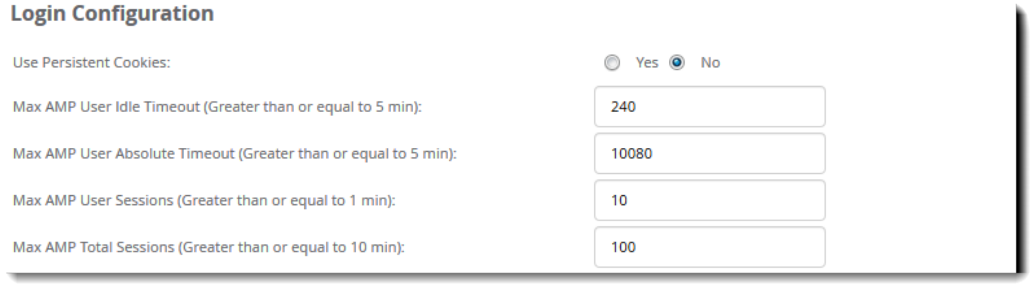
Configuring the User Login

Follow these steps to configure the login banner message, idle timeout, and persistent cookies which are session-based:

To configure user login:

1. Navigate to **OV3600 Setup > Authentication > Login Configuration**.
2. To clear information such as user logins, select **No** for the "Use Persistent Cookies" option.
3. Enter the length of time that passes before AirWave ends an idle user session. 5 minutes is the lowest idle setting.

Figure 8: *Example Settings for the Login Configuration Page*



Login Configuration

Use Persistent Cookies:	○ Yes ● No
Max AMP User Idle Timeout (Greater than or equal to 5 min):	240
Max AMP User Absolute Timeout (Greater than or equal to 5 min):	10080
Max AMP User Sessions (Greater than or equal to 1 min):	10
Max AMP Total Sessions (Greater than or equal to 10 min):	100

4. In the Click Through Agreement field, type the login banner message that will display before the user logs in to OV3600, requiring the user to accept the terms of usage before granting full access to the WebUI.
5. Click **Save** at the bottom of the page.

Setting Up Certificate Authentication

On the **OV3600 Setup > Authentication** page, administrators can specify whether to require a certificate during authentication and whether to use two-factor authentication. A PEM-encoded certificate bundle is required for this feature.

This feature must be enabled per role in **OV3600 Setup > Roles**.

Perform the following steps to enable this feature for this OV3600.

1. Locate the **Certificate Authentication** section in **OV3600 Setup > Authentication**.
2. In the **Enable Certificate Authentication** field, select **Yes**.
3. Specify whether to require a certificate in order to authenticate. If **Yes**, then you can also specify whether to use two-factor authentication.
4. Enter the PEM-encoded CA certificate bundle.
5. Select **Save** if you are finished or follow the next procedure to specify the authentication priority.

Configuring Whitelists

By adding subnets to a whitelist, you can limit OV3600 access to users on a list of trusted subnets.

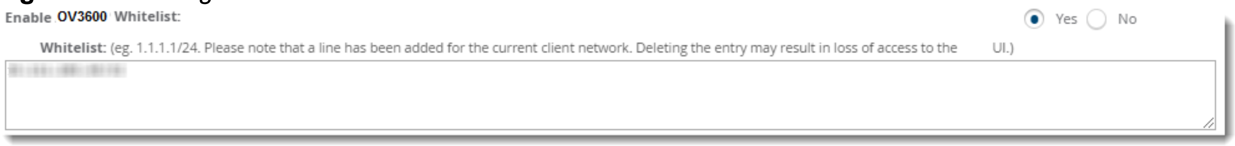
CAUTION

Do not delete the current client network from the OV3600 whitelist, or you might lose access to the OV3600 WebUI.

To configure the whitelist:

1. Navigate to OV3600 Setup > Authentication.
2. In the Login Configuration section, select **Yes** for the "Enable OV3600 Whitelist" option. When you enable this functionality, OV3600 displays the whitelist with the current client network as the first entry.

Figure 9: *Enabling Whitelists*



Enable OV3600 Whitelist: ● Yes ○ No

Whitelist: (eg. 1.1.1.1/24. Please note that a line has been added for the current client network. Deleting the entry may result in loss of access to the UI.)

[redacted]

3. Enter additional subnets, one subnet per line.
4. Scroll down the page, then click **Save**.

Setting Up Single Sign-On

On the **OV3600 Setup > Authentication** page, administrators can set up single sign-on (SSO) for users that have access to OV3600 controllers. This allows users to log in to OV3600 and use the IP Address or Quick Links hypertext links across OV3600 to access the controller’s WebUI without having to enter credentials again. The links the user can select to access a controller can be found on the **Devices > Monitor** page in the **Device Info** section, and on device list pages.

Perform the following steps to enable this feature for this OV3600.

1. Locate the **Single Sign-On** section in **OV3600 Setup > Authentication**.
2. In the **Enable Single Sign-On** field, select **Yes**.
3. Select **Save** if you are finished or follow the next procedure to specify the authentication priority.

Specifying the Authentication Priority

To specify the authentication priority for this OV3600 server, locate the **Authentication Priority** section in **OV3600 Setup > Authentication**, and select either **Local** or **Remote** as the priority.

If **Local** is selected, then remote will be attempted if a user is not available. If **Remote** is selected, then the local database is searched if remote authentication fails. The order of remote authentication is RADIUS first, followed by TACACS, and finally LDAP.

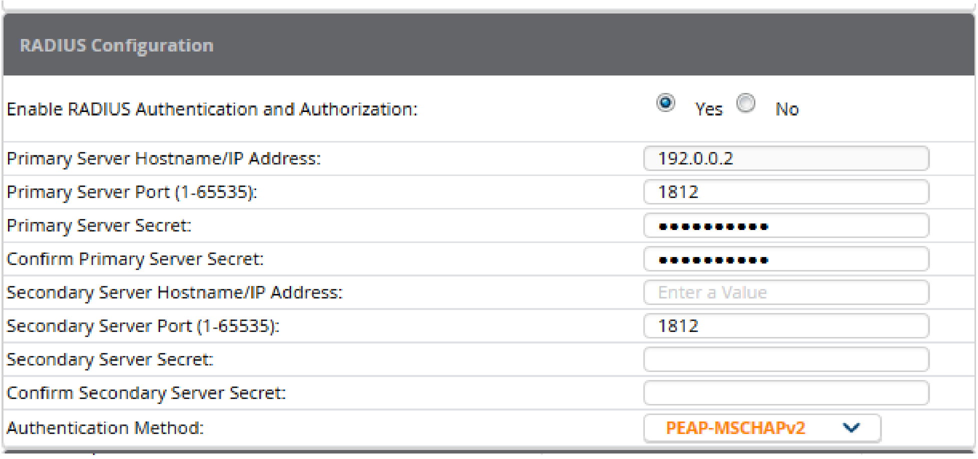
Select **Save** if you are finished or follow the next procedure to configure RADIUS, TACACS+, and LDAP Authentication options.

Configuring RADIUS Authentication and Authorization

For RADIUS capability, you must configure the IP/Hostname of the RADIUS server, the TCP port, and the server shared secret. Perform these steps to configure RADIUS authentication:

1. Go to the **OV3600 Setup > Authentication** page. This page displays current status of RADIUS. Figure 10 illustrates this page.

Figure 10: *OV3600 Setup > Authentication Page Illustration for RADIUS*



RADIUS Configuration

Enable RADIUS Authentication and Authorization:	● Yes ○ No
Primary Server Hostname/IP Address:	192.0.0.2
Primary Server Port (1-65535):	1812
Primary Server Secret:	●●●●●●●●●●●
Confirm Primary Server Secret:	●●●●●●●●●●●
Secondary Server Hostname/IP Address:	Enter a Value
Secondary Server Port (1-65535):	1812
Secondary Server Secret:	
Confirm Secondary Server Secret:	
Authentication Method:	PEAP-MSCHAPv2

2. Select **No** to disable or **Yes** to enable RADIUS authentication. If you select **Yes**, several new fields appear. Complete the fields described in Table 21.

Table 21: *OV3600 Setup > Authentication Fields and Default Values for RADIUS Authentication*

Field	Default	Description
Primary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the primary RADIUS server.
Primary Server Port (1-65535)	1812	Enter the TCP port for the primary RADIUS server.
Primary Server Secret	N/A	Specify and confirm the primary shared secret for the primary RADIUS server.
Confirm Primary Server Secret	N/A	Re-enter the primary server secret.
Secondary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the secondary RADIUS server.
Secondary Server Port (1-65535)	1812	Enter the TCP port for the secondary RADIUS server.
Secondary Server Secret	N/A	Enter the shared secret for the secondary RADIUS server.
Confirm Secondary Server Secret	N/A	Re-enter the secondary server secret.

Table 21: *OV3600 Setup > Authentication Fields and Default Values for RADIUS Authentication (Continued)*

Field	Default	Description
Authentication Method	PAP	Select one of the following authentication methods: - PAP - PEAP-MSCHAPv2 If you use the PEAP-MSCHAPv2 authentication method with the default "Read-Only Monitoring and Auditing" user role, note that the name of this role has been slightly modified in OV3600 8.2.3 to allow support the PEAP-MSCHAPv2 authentication method: the ampersand **(&)** symbol has been changed to the word **and**. - **Role Name in 8.2.2.x and earlier releases**: *Read-Only Monitoring **&** Auditing* - **Role Name in OV3600 8.2.**3: Re*ad-Only Monitoring **and** Auditing* If you used the **Read-Only Monitoring & Auditing** user role prior to upgrading to OV3600 8.2.3 or later releases, you must modify the user role name on the RADIUS server to ensure that the user role name on the RADIUS server exactly matches the user role name in OV3600.

3. Select **Save** to retain these configurations, and continue with additional steps in the next procedure.

Integrating a RADIUS Accounting Server

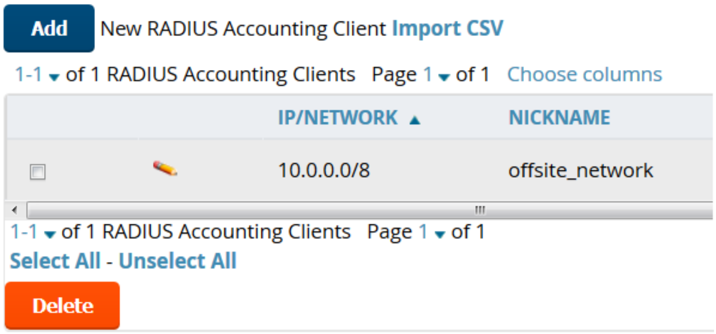
NOTE

OV3600 checks the local user name and password before checking with the RADIUS server. If the user is found locally, the local password and role apply. When using RADIUS, it's not necessary or recommended to define users on the OV3600 server. The only recommended user is the backup admin, in case the RADIUS server goes down.

Optionally, you can configure RADIUS server accounting on **OV3600 Setup > RADIUS Accounting**. This capability is not required for basic OV3600 operation, but can increase the user-friendliness of OV3600 administration in large networks. Figure 11 illustrates the settings of this optional configuration interface.

Perform the following steps and configurations to enable OV3600 to receive accounting records from a separate RADIUS server. Figure 11 illustrates the display of RADIUS accounting clients already configured.

Figure 11: *OV3600 Setup > RADIUS Accounting Page Illustration*



Add
New RADIUS Accounting Client
Import CSV
1-1 of 1 RADIUS Accounting Clients Page 1 of 1
Choose columns

		IP/NETWORK ▲	NICKNAME
□		10.0.0.0/8	offsite_network

1-1 of 1 RADIUS Accounting Clients Page 1 of 1
Select All - Unselect All
Delete

1. To define a the RADIUS authentication server or network, browse to the **OV3600 Setup > RADIUS Accounting** page, select **Add**, and provide the information in Table 22.

Table 22: *OV3600 Setup > Radius Accounting Fields and Default Values for LDAP Authentication*

Setting	Default	Description
IP/Network	None	Specify the IP address for the authentication server if you only want to accept packets from one device. To accept packets from an entire network enter the IP/Netmask of the network (for example, 10.51.0.0/24).
Nickname	None	Sets a user-defined name for the authentication server.
Shared Secret (Confirm)	None	Sets the Shared Secret that is used to establish communication between OV3600 and the RADIUS authentication server.

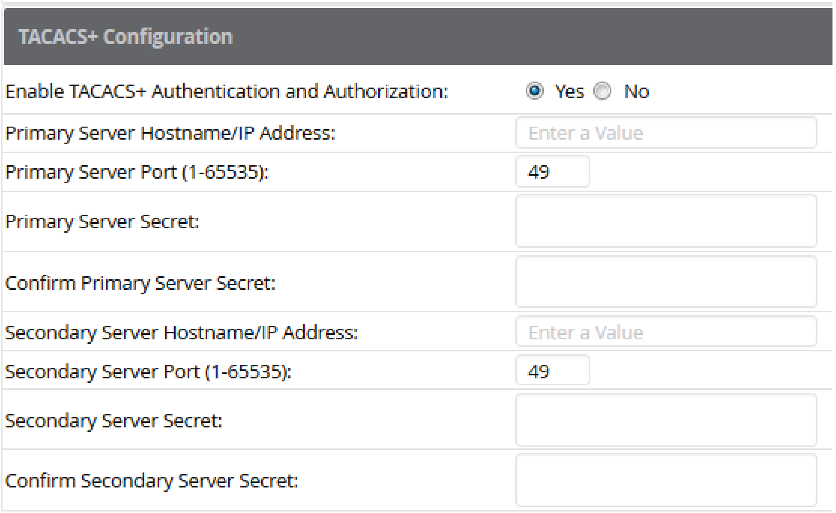
2. Click Add to save your settings.

Configuring TACACS+ Authentication

For TACACS+ capability, you must configure the IP/Hostname of the TACACS+ server, the TCP port, and the server shared secret. This TACACS+ configuration is for OV3600 users and does not affect APs or users logging into APs.

1. Go to the **OV3600 Setup > Authentication** page. This page displays current status of TACACS+. Figure 12 illustrates this page when neither TACACS+, LDAP, nor RADIUS authentication is enabled in OV3600.

Figure 12: *OV3600 Setup > Authentication Page Illustration for TACACS+*



TACACS+ Configuration

Enable TACACS+ Authentication and Authorization:	● Yes ○ No
Primary Server Hostname/IP Address:	Enter a Value
Primary Server Port (1-65535):	49
Primary Server Secret:	
Confirm Primary Server Secret:	
Secondary Server Hostname/IP Address:	Enter a Value
Secondary Server Port (1-65535):	49
Secondary Server Secret:	
Confirm Secondary Server Secret:	

2. Select **No** to disable or **Yes** to enable TACACS+ authentication. If you select **Yes**, several new fields appear. Complete the fields described in Table 23.

Table 23: *OV3600 Setup > Authentication Fields and Default Values for TACACS+ Authentication*

Field	Default	Description
Primary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the primary TACACS+ server.
Primary Server Port (1-65535)	49	Enter the port for the primary TACACS+ server.

Table 23: *OV3600 Setup > Authentication Fields and Default Values for TACACS+ Authentication (Continued)*

Field	Default	Description
Primary Server Secret	N/A	Specify and confirm the primary shared secret for the primary TACACS+ server.
Confirm Primary Server Secret	N/A	Re-enter the primary server secret.
Secondary Server Hostname/IP Address	N/A	Enter the IP address or hostname of the secondary TACACS+ server.
Secondary Server Port (1-65535)	49	Enter the port for the secondary TACACS+ server.
Secondary Server Secret	N/A	Enter the shared secret for the secondary TACACS+ server.
Confirm Secondary Server Secret	N/A	Re-enter the secondary server secret.

3. Select **Save** and continue with additional steps.

Configuring Cisco ACS to Work with OV3600

To configure Cisco ACS to work with OV3600, you must define a new service named **OV3600** that uses HTTPS on the ACS server.

1. The OV3600 HTTPS service is added to the **TACACS+** (Cisco) interface under the **Interface Configuration** tab.
2. Select a checkbox for a new service.
3. Enter **OV3600** in the service column and **https** in the protocol column.
4. Select **Save**.
5. Edit the existing groups or users in TACACS to use the OV3600 service and define a role for the group or user.
   - The role defined on the **Group Setup** page in ACS must match the exact name of the role defined on the **OV3600 Setup > Roles** page.
   - The defined role should use the format: **role=**<*name_of_*OV3600*_role*>. For example role=DormMonitoring.

   As with routers and switches, OV3600 does not need to know user names.
6. OV3600 also needs to be configured as an AAA client.
   - On the **Network Configuration** page, select **Add Entry**.
   - Enter the IP address of OV3600 as the **AAA Client IP Address**.
   - The secret should be the same value that was entered on the **OV3600 Setup > TACACS+** page.
7. Select **TACACS+** (Cisco IOS) in the **Authenticate Using** drop down menu and select **submit + restart**.

NOTE

OV3600 checks the local user name and password store before checking with the TACACS+ server. If the user is found locally, the local password and local role apply. When using TACACS+, it is not necessary or recommended to define users on the OV3600 server. The only recommended user is the backup administrator, in the event that the TACACS+ server goes down.

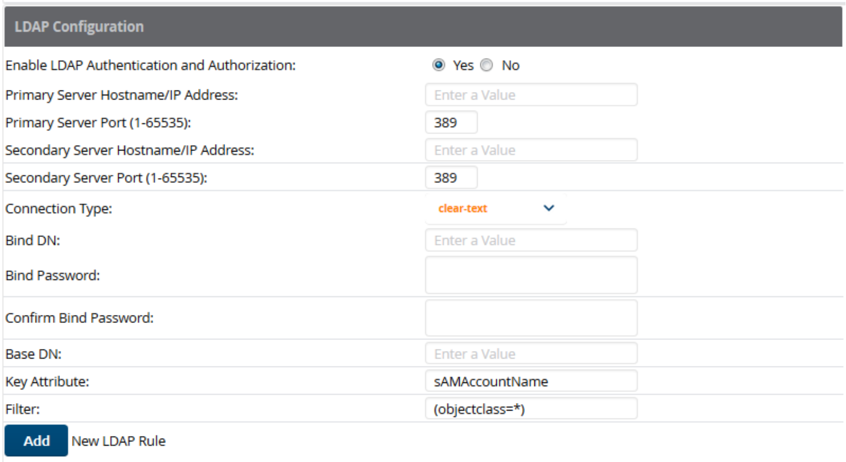
Configuring LDAP Authentication and Authorization

LDAP (Lightweight Directory Access Protocol) provides users with a way of accessing and maintaining distributed directory information services over a network. When LDAP is enabled, a client can begin a session by authenticating against an LDAP server which by default is on TCP port 389.

Perform these steps to configure LDAP authentication:

1. Go to the **OV3600 Setup > Authentication** page.
2. Select the **Yes** radio button to enable LDAP authentication and authorization. Once enabled, the available LDAP configuration options will display. Figure 13 illustrates this page.

Figure 13: *OV3600 Setup > Authentication Page Illustration for LDAP*



LDAP Configuration

Enable LDAP Authentication and Authorization:	● Yes ○ No
Primary Server Hostname/IP Address:	Enter a Value
Primary Server Port (1-65535):	389
Secondary Server Hostname/IP Address:	Enter a Value
Secondary Server Port (1-65535):	389
Connection Type:	clear-text
Bind DN:	Enter a Value
Bind Password:	
Confirm Bind Password:	
Base DN:	Enter a Value
Key Attribute:	sAMAccountName
Filter:	(objectclass=*)

3. Complete the fields described in Table 24.

Table 24: *OV3600 Setup > Authentication Fields and Default Values for LDAP Authentication*

Field	Default	Description
Primary Server Hostname/IP Address	none	Enter the IP address or the hostname of the primary LDAP server.
Primary Server Port (1-65535)	389	Enter the port where the LDAP server is listening. The default port is 389.
Secondary Server Hostname/IP Address	none	Optionally enter the IP address or hostname of the secondary LDAP server. This server will be contacted in the event that the primary LDAP server is not reachable.
Secondary Server Port (1-65535)	389	Enter the port where the LDAP service is listening on the secondary LDAP server. The default port is 389.
Connection Type	clear-text	Specify one of the following connection types OV3600 and the LDAP server: ● **clear-text** results in unencrypted communication. ● **ldap-s** results in communication over SSL. ● **start-tls** uses certificates to initiate encrypted communication.

Table 24: *OV3600 Setup > Authentication Fields and Default Values for LDAP Authentication (Continued)*

Field	Default	Description
View Server Certificate	none	If **Connection Type** is configured as **start-tls**, then also specify whether the **start-tls** connection type uses a certificate. ● **none** - The server may provide a certificate, but it will not be verified. This may mean that you are connected to the wrong server. ● **optional** - Verifies only when the servers offers a valid certificate. ● **require** - The server must provide a valid certificate. A valid **LDAP Server CA Certificate** must be provided in case of optional or require. Certificates uploaded on the **Device Setup > Certificates** page with a type of Intermediate CA or Trusted CA are listed in the drop down for **LDAP Server CA Certificate**.
LDAP Server CA Certificate	none	Specify the LDAP server certificate to use to initiate encrypted communication. Only certificates that have been uploaded with a type of Intermediate CA or Trusted CA will appear in this drop down. **NOTE:** This **LDAP Server CA Certificate** drop down menu only appears if **View Server Certificate** is specified as **optional** or **require**.
Bind DN	none	Specify the Distinguished Name (DN) of the administrator account, such as 'cn=admin01,cn=admin,dn=domain,dn=com'. Note that for the Active directory, the bind DN can also be in the administrator@domain format (for example, administrator@acme.com).
Bind Password	none	Specify the bind DN account password.
Confirm Bind Password	none	Re-enter the bind password.
Base DN	none	The DN of the node in your directory tree from which to start searching for records. Generally, this would be the node that contains all the users who may access OV3600, for example cn=users,dc=domain,dc=com.
Key Attribute	sAMAccountName	The LDAP attribute that identifies the user, such as 'sAMAccountName' for Active Directory
Role Attribute	none	The LDAP attribute that contains the OV3600 role. Users who log in to OV3600 using this LDAP authentication will be granted permissions based on this role. Refer to Configuring OV3600 User Roles for more information about OV3600 User Roles.
Filter	(objectclass=*)	This option limits the object classes in which the key,role attributes would be searched.

Table 24: *OV3600 Setup > Authentication Fields and Default Values for LDAP Authentication (Continued)*

Field	Default	Description
Add New LDAP Rule	none	The LDAP rule parameters are **Position**, **Role Attribute**, **Operation**, **Value**, and **OV3600** role. If you create multiple LDAP rules, rules are processed in order based on the rule position value, so the position you assign to the LDAP rule represents the order in which the LDAP rule is applied to determine the OV3600 role. LDAP rules can only be configured and applied after LDAP authentication is enabled. The LDAP rules are similar to the rules used by the switch to derive the OV3600 role.

4. Select **Save** to retain these configurations, and continue with additional steps in the next procedure.

What Next?

- Go to additional subtabs in **OV3600 Setup** to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* Alcatel-Lucent support remains available to you for any phase of OV3600 configuration.

Enabling OV3600 to Manage Your Devices

Once OV3600 is installed and active on the network, the next task is to define the basic settings that allow OV3600 to communicate with and manage your devices. Device-specific firmware files are often required or are highly desirable. Furthermore, the use of Web Auth bundles is advantageous for deployment of Cisco WLC wireless LAN controllers when they are present on the network.

This section contains the following procedures:

- "Configuring Communication Settings for Discovered Devices" on page 53
- "Uploading Firmware and Files" on page 55

Configuring Communication Settings for Discovered Devices

You can configure OV3600 to communicate with your devices by defining default shared secrets and SNMP settings.

To define the default credentials and SNMP settings:

1. On the **Device Setup > Communication** page, enter the default credentials for each device model on your network. OV3600 assigns default credentials to all discovered devices.

   The **Edit** button edits the default credentials for newly discovered devices. To modify the credentials for existing devices, use the **Devices > Manage** page or the **Modify Devices** link on the **Devices > List** page.

NOTE

Community strings and shared secrets must have read-write access for OV3600 to configure the devices. Without read-write access, OV3600 may be able to monitor the devices but cannot apply any configuration changes.

2. Enter the SNMP timeout and retries settings. Table 25 lists the settings and default values.

Table 25: *Device Setup > Communication > SNMP Settings Fields and Default Values*

Setting	Default	Description
SNMP Timeout (3-60 sec)	3	Sets the time, in seconds, that OV3600 waits for a response from a device after sending an SNMP request.

Table 25: *Device Setup > Communication > SNMP Settings Fields and Default Values (Continued)*

Setting	Default	Description
SNMP Retries (1-40)	3	Sets 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). If OV3600 does not receive an SNMP response from the device after the specified number of retries, OV3600 classifies that device as **Down**. **NOTE:** Although the upper limit for this value is 40, some SNMP libraries still have a hard limit of 20 retries. In these cases, any retry value that is set above 20 will still stop at 20.

3. Click **Add** and enter the following information :
   - **Username** - User name of the SNMP v3 user as configured on the controller.
   - **Auth Protocol** - MD5 or SHA. The default setting is SHA.
   - **Auth and Priv Protocol Passphrases** - Authentication and privilege protocol passphrases for the user, as configured on the controller.
   - **Priv Protocol** - DES or AES. The default setting is DES.

NOTE

The SNMP Inform receiver will restart when users are changed or added to the controller.

4. Enter or adjust the default value for the Telnet/SSH timeout. Table 26 shows the setting and default value.

Table 26: *Device Setup > Communication > Telnet/SSH Settings Fields and Default Values*

Setting	Default	Description
Telnet/SSH Timeout (3-120 sec)	10	Sets the timeout period in seconds used when performing Telnet and SSH commands.

5. Locate the **HTTP Discovery Settings** section and adjust the default value. Table 27 shows the setting and default value.

Table 27: *Device Setup > Communication > HTTP Discovery Settings Fields and Default Values*

Setting	Default	Description
HTTP Timeout (3-120 sec)	5	Sets the timeout period in seconds used when running an HTTP discovery scan.

6. Locate the **ICMP Settings** section and adjust the default value as required. Table 28 shows the setting and default value.

Table 28: *Device Setup > Communication > ICMP Settings Fields and Default Values*

Setting	Default	Description
Attempt to ping devices that were unreachable via SNMP	Yes	● When **Yes** is selected, OV3600 attempts to ping the AP device. ● Select **No** if performance is affected in negative fashion by this function. If a large number of APs are unreachable by ICMP, likely to occur where there is in excess of 100 APs, the timeouts start to impede network performance. **NOTE:** If ICMP is disabled on the network, select **No** to avoid the performance penalty caused by numerous ping requests.

7. Locate the **Symbol 4131 and Cisco Aironet IOS SNMP Initialization** area. Select one of the options listed. Table 29 describes the settings and default values

Table 29: *Device Setup > Communication > Symbol 4131 and Cisco Aironet IOS SNMP Initialization Fields and Default Values*

Setting	Default	Description
Do Not Modify SNMP Settings	Yes	When selected, specifies that OV3600 will not modify any SNMP settings. If SNMP is not already initialized on the Symbol, Nomadix, and Cisco IOS APs, OV3600 is not able to manage them.
Enable read-write SNMP	No	When selected, and when on networks where the Symbol, Nomadix, and Cisco IOS APs do not have SNMP initialized, this setting enables SNMP so the devices can be managed by OV3600.

Uploading Firmware and Files

OV3600 automates firmware distribution to the devices on your network. Once you have downloaded the firmware from the vendor, you can upload the firmware to OV3600 for distribution to devices from the **Upload Firmware & Files** page. After you upload the firmware, OV3600 lists them in the Firmware Files table on this page.

NOTE

For more information about specifying firmware versions for devices in a group, see "Specifying the Minimum Firmware Version for Device Groups" on page 110.

Table 30 below itemizes the contents, settings, and default values for the **Upload Firmware & Files** page.

Table 30: *Device Setup > Upload Firmware & Files Fields and Default Values*

Setting	Default	Description
Type	Alcatel-Lucent switch (any model)	Displays a drop-down list of the primary AP makes and models that OV3600 supports with automated firmware distribution.
Owner Role	None	Displays the user role that uploaded the firmware file. This is the role that has access to the file when an upgrade is attempted.
Description	None	Displays a user-configurable text description of the firmware file.
Server Protocol	None	Displays the file transfer protocol by which the firmware file was obtained from the server. This can be FTP, TFTP, HTTP, HTTPS. or SCP.

Table 30: *Device Setup > Upload Firmware & Files Fields and Default Values (Continued)*

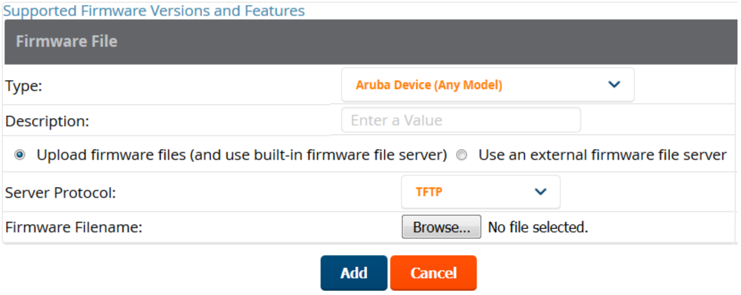
Setting	Default	Description
Use Group File Server	None	If enabled, displays the name of the file server supporting the group.
Firmware Filename	None	Displays the name of the file that was uploaded to OV3600 and to be transferred to an AP when the file is used in an upgrade.
Firmware MD5 Checksum	None	Displays the MD5 checksum of the file after it was uploaded to OV3600. The MD5 checksum is used to verify that the file was uploaded to OV3600 without issue. The checksum should match the checksum of the file before it was uploaded.
Firmware File Size	None	Displays the size of the firmware file in bytes.
Firmware Version	None	Displays the firmware version number. This is a user-configurable field.
HTML Filename	None	Supporting HTML, displays the name of the file that was uploaded to OV3600 and to be transferred to an AP when the file is used in an upgrade.
HTML MD5 Checksum	None	Supporting HTML, displays the MD5 checksum of the file after it was uploaded to OV3600. The MD5 checksum is used to verify that the file was uploaded to OV3600 without issue. The checksum should match the checksum of the file before it was uploaded.
HTML File Size	None	Supporting HTML, displays the size of the file in bytes.
HTML Version	None	Supporting HTML, displays the version of HTML used for file transfer.
Desired Firmware File for Specified Groups	None	The firmware file is set as the desired firmware version on the **Groups > Firmware Files** page of the specified groups. You cannot delete a firmware file that is set as the desired firmware version for a group.

Loading Firmware Files onto OV3600

Perform the following steps to load a device firmware file onto OV3600:

1. Go to the **Device Setup > Upload Firmware & Files** page.
2. Select **Add** by the **New Firmware File** option. The Add Firmware File page appears. Figure 14 illustrates this page.

Figure 14: *Device Setup > Upload Firmware and Files > Add Page*



Supported Firmware Versions and Features

Firmware File

Type:	Aruba Device (Any Model)
Description:	Enter a Value
● Upload firmware files (and use built-in firmware file server)	○ Use an external firmware file server
Server Protocol:	TFTP
Firmware Filename:	Browse... No file selected.

3. Select the **Supported Firmware Versions and Features** link to view supported firmware versions.

Unsupported and untested firmware may cause device mismatches and other problems. Please contact Alcatel-Lucent support before installing non-certified firmware.

4. Enter the appropriate information and select **Add**. The file uploads to OV3600 and once complete, this file appears on the **Device Setup > Upload Firmware & Files** page. This file also appears on additional pages that display firmware files (such as the **Group > Firmware** page and on individual **Devices > Manage** pages).
5. You can also import a CSV list of groups and their external TFTP firmware servers. Table 31 itemizes the settings of this page.

Table 31: *Supported Firmware Versions and Features Fields and Default Values*

Setting	Default	Description
Type	Alcatel-Lucent switch	Indicates the firmware file is used with the specified type. With selection of some types, particularly Cisco controllers, you can specify the boot software version.
Firmware Version	None	Provides a user-configurable field to specify the firmware version number. This open appears if **Use an external firmware file server** is enabled.
Description	None	Provides a user-configurable text description of the firmware file.
Upload firmware files (and use built-in firmware)	Enabled	Allows you to select a firmware from your local machine and upload it via TFTP or FTP.
Use an external firmware file server	N/A	You can also choose to assign the external TFTP server on a per-group basis. If you select this option, you must enter the IP address on the **Groups > Firmware** page. Complete the **Firmware File Server IP Address** field.
Server Protocol	TFTP	Specify whether to use a built-in TFTP server or FTP, HTTP, or HTTPS to upload a firmware file. TFTP is recommended. If you select FTP, OV3600 uses an anonymous user for file upload.

Table 31: *Supported Firmware Versions and Features Fields and Default Values (Continued)*

Setting	Default	Description
Use Group File Server	Disabled	If you opt to use an external firmware file server, this additional option appears. This setting instructs OV3600 to use the server that is associated with the group instead of defining a server.
Firmware File Server IP Address	None	Provides the IP address of the External TFTP Server (like SolarWinds) used for the firmware upgrade. This option displays when the user selects the **Use an external firmware file** option.
Firmware Filename	None	Enter the name of the firmware file that needs to be uploaded. Ensure that the firmware file is in the TFTP root directory. If you are using a non-external server, you select **Choose File** to find your local copy of the file.
HTML Filename	None	Browse to the HTML file that will accompany the firmware upload. Note that this field is only available for certain Firmware File Types (for example, Symbol 4121).
Patch Filename	None	If you selected Symbol WS5100 as the Firmware File Type, and you are upgrading from version 3.0 to 3.1, then browse to the path where the patch file is located.
Boot Software Version	None	If you specified a Cisco WLC device as the Firmware File Type, then also enter the boot software version.

NOTE

Additional fields may appear for multiple device types. OV3600 prompts you for additional firmware information as required. For example, Intel and Symbol distribute their firmware in two separate files: an image file and an HTML file. Both files must be uploaded to OV3600 for the firmware to be distributed successfully via OV3600.

6. Select **Add** to import the firmware file.

Deleting FirmWare Files

To delete a firmware file that has already been uploaded to OV3600, return to the **Device Setup > Upload Firmware & Files** page, select the checkbox for the firmware file and select **Delete**.

NOTE

A firmware file may not be deleted if it is the desired version for a group. Use the **Group > Firmware** page to investigate this potential setting and status.

Adding Web Auth Bundles

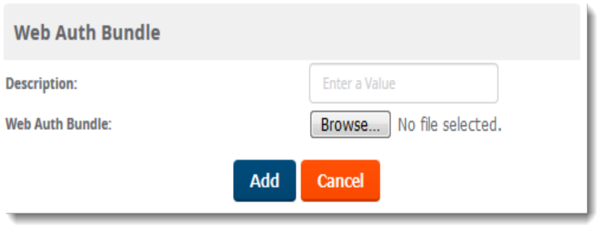
Web authentication bundles are configuration files that support Cisco WLC wireless LAN controllers. This procedure requires that you have local or network access to a Web Auth configuration file for Cisco WLC devices.

To add or edit a Web Authentication Bundle:

1. Go to the **Device Setup > Upload Firmware & Files** page.
2. Click **Add** by the **New Web Auth Bundle** option. This page displays any existing web authentication bundles that are currently configured in OV3600.

3. Select **Add** to create a new bundle (see Figure 15), or select the pencil icon next to an existing bundle to edit. You may also delete a bundle by selecting that bundle with the checkbox, and selecting **Delete**.

Figure 15: *Adding a Web Auth Bundle*



Web Auth Bundle

Description: Enter a Value

Web Auth Bundle: Browse... No file selected.

4. Enter a descriptive label in the description field. This is the label used to identify and track web authentication bundles on the page.
5. Enter the path and file name of the web authentication bundle, or select **Choose File** to locate the file.
6. Select **Add** to complete the web authentication bundle creation, or **Save** if replacing a previous Web Auth configuration file, or **Cancel** to abort the Web Auth integration.

For additional information about using web authentication bundles with Cisco WLC controllers, refer to the Wireless LAN controller Web Authentication Configuration Example, Document ID: 69340 on Cisco's Web site.

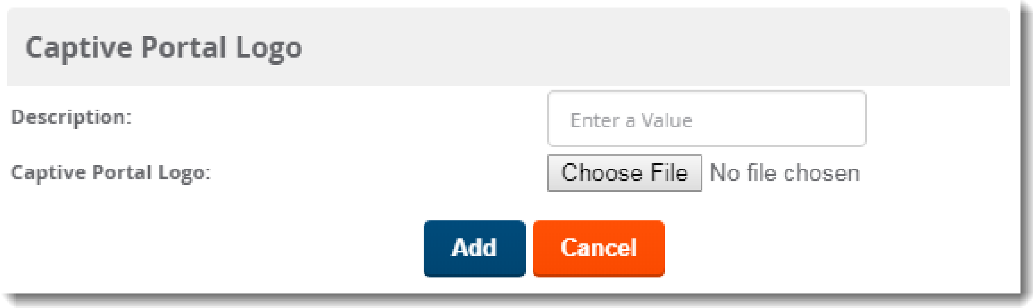
Adding a New Captive Portal Logo

If you want to use a company logo for a guest account that uses a captive portal for network authentication, you upload the logo to OV3600 and then set a group of devices to use the captive portal logo.

To upload a company logo image file:

1. Click **Add** at the bottom of the Upload Firmware & Files page next to New Captive Portal Logo.

Figure 16: *Adding a Captive Portal Logo*



Captive Portal Logo

Description: Enter a Value

Captive Portal Logo: Choose File No file chosen

2. Enter a logo description.
3. Click **Choose File** to select the image file, then click **Open**.
4. Click **Add**. OV3600 displays the newly added image file in the Firmware Files table.

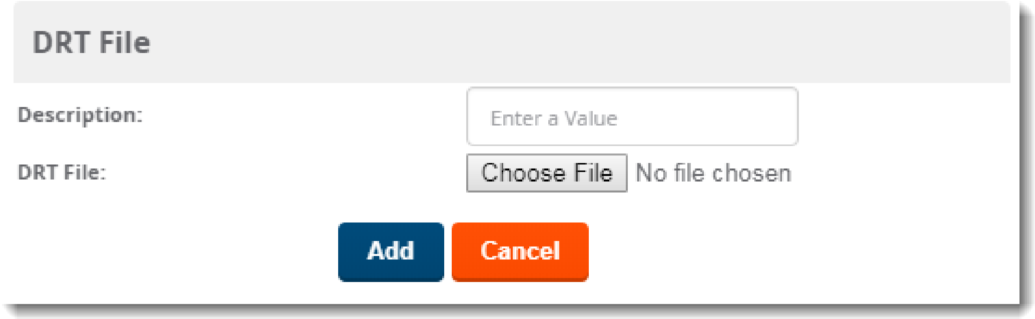
Adding a New DRT File

You can use the downloadable regulatory table (DRT) to update country domain options without upgrading the ArubaOS software version on an AP.

To add a DRT file to OV3600:

1. Click **Add** at the bottom of the Upload Firmware & Files page next to New DRT File.

Figure 17: *Adding a DRT File*



DRT File

Description: Enter a Value

DRT File: Choose File No file chosen

Add Cancel

2. Enter a DRT file description.
3. Click **Choose File** to select the DRT file, then click **Open**.
4. Click **Add**. OV3600 displays the newly added DRT file in the Firmware Files table.

Setting Up Device Types

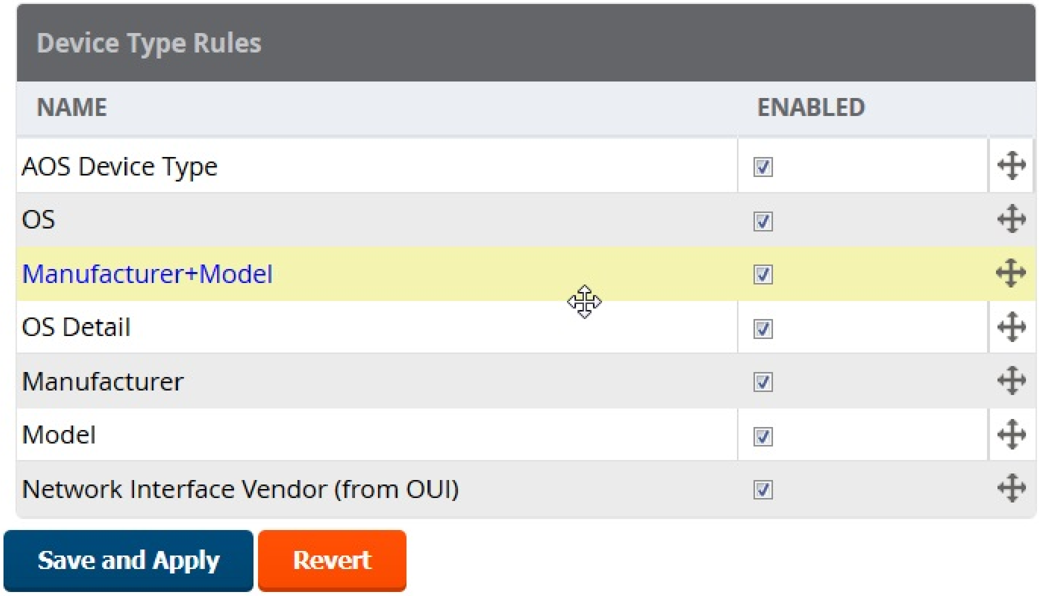
On the **OV3600 Setup > Device Type Setup** page, you can define how the device types displayed for users on your network is calculated from available data. The first matching property is used. These rules cannot be edited or deleted, but only reordered or enabled.

You can change the priority order of rules by clicking on a row and dragging and dropping it into a new location, as shown in Figure 18.

Select the checkbox under the **Enabled** column to turn on device setup rules.

Refer to "Monitoring Wired and Wireless Clients" on page 182 for more information on the **Device Type** column that appears in **Clients** list tables.

Figure 18: *OV3600 Setup > Device Type Setup Page Illustration*



Device Type Rules

NAME	ENABLED	
AOS Device Type	☑	✥
OS	☑	✥
Manufacturer+Model	☑	✥
OS Detail	☑	✥
Manufacturer	☑	✥
Model	☑	✥
Network Interface Vendor (from OUI)	☑	✥

Save and Apply Revert

Configuring Cisco WLSE and WLSE Rogue Scanning

The Cisco Wireless LAN Solution Engine (WLSE) includes rogue scanning functions that OV3600 supports. This section contains the following topics and procedures, and several of these sections have additional sub-procedures:

- "Introduction to Cisco WLSE" on page 61
- "Initial WLSE Configuration" on page 61
- "Configuring IOS APs for WDS Participation" on page 63
- "Configuring ACS for WDS Authentication" on page 64
- "Configuring Cisco WLSE Rogue Scanning" on page 64

You must enter one or more CiscoWorks WLSE hosts to be polled for discovery of Cisco devices and rogue AP information.

Introduction to Cisco WLSE

Cisco WLSE functions as an integral part of the Cisco Structured Wireless-Aware Network (SWAN) architecture, which includes IOS Access Points, a Wireless Domain Service, an Access Control Server, and a WLSE. In order for OV3600 to obtain Rogue AP information from the WLSE, all SWAN components must be properly configured. Table 32 describes these components.

Table 32: *Cisco SWAN Architecture Components*

SWAN Component	Requirements
WDS (Wireless Domain Services)	● WDS Name ● Primary and backup IP address for WDS devices (IOS AP or WLSM) ● WDS Credentials APs within WDS Group **NOTE:** WDS can be either a WLSM or an IOS AP. WLSM (WDS) can control up to 250 access points. AP (WDS) can control up to 30 access points.
WLSE (Wireless LAN Solution Engine)	● IP Address ● Login
ACS (Access Control Server)	● IP Address ● Login
APs	● APs within WDS Group

Initial WLSE Configuration

Use the following general procedures to configure and deploy a WLSE device in OV3600:

- "Adding an ACS Server for WLSE" on page 62
- "Enabling Rogue Alerts for Cisco WLSE" on page 62
- "Configuring WLSE to Communicate with APs" on page 62
- "Discovering Devices" on page 62
- "Managing Devices" on page 62
- "Inventory Reporting" on page 63
- "Defining Access" on page 63
- "Grouping" on page 63

Adding an ACS Server for WLSE

1. Go to the **Devices > Discover > AAA Server** page.
2. Select **New** from the drop-down list.
3. Enter the server name, server port (default 2002), user name, password, and a secret.
4. Select **Save**.

Enabling Rogue Alerts for Cisco WLSE

1. Go to the **Faults > Network Wide Settings > Rogue AP Detection** page.
2. Select the **Enable**.
3. Select **Apply**.

Additional information about rogue device detection is available in "Configuring Cisco WLSE Rogue Scanning" on page 64.

Configuring WLSE to Communicate with APs

1. Go to the **Device Setup > Discover** page.
2. Configure SNMP Information.
3. Configure HTTP Information.
4. Configure Telnet/SSH Credentials
5. Configure HTTP ports for IOS access points.
6. Configure WLCCP credentials.
7. Configure AAA information.

Discovering Devices

The following three methods can be used to discover access points within WLSE:

- Using Cisco Discovery Protocol (CDP)
- Importing from a file
- Importing from CiscoWorks

Perform these steps to discover access points.

1. Go to the **Device > Managed Devices > Discovery Wizard** page.
2. Import devices from a file.
3. Import devices from Cisco Works.
4. Import using CDP.

Managing Devices

Prior to enabling radio resource management on IOS access points, the access points must be under WLSE management.

NOTE

OV3600 becomes the primary management/monitoring vehicle for IOS access points, but for OV3600 to gather Rogue information, the WLSE must be an NMS manager to the APs.

Use these pages to make such configurations:

1. Go to **Device > Discover > Advanced Options**.
2. Select the method to bring APs into management **Auto**, or specify via filter.

Inventory Reporting

When new devices are managed, the WLSE generates an inventory report detailing the new APs. OV3600 accesses the inventory report via the SOAP API to auto-discover access points. This is an optional step to enable another form of AP discovery in addition to OV3600, CDP, SNMP scanning, and HTTP scanning discovery for Cisco IOS access points. Perform these steps for inventory reporting.

1. Go to **Devices > Inventory > Run Inventory**.
2. **Run Inventory** executes immediately between WLSE polling cycles.

Defining Access

OV3600 requires System Admin access to WLSE. Use these pages to make these configurations.

1. Go to **Administration > User Admin**.
2. Configure **Role** and **User**.

Grouping

It's much easier to generate reports or faults if APs are grouped in WLSE. Use these pages to make such configurations.

1. Go to **Devices > Group Management**.
2. Configure **Role** and **User**.

Configuring IOS APs for WDS Participation

IOS APs (1100, 1200) can function in three roles within SWAN:

- Primary WDS
- Backup WDS
- WDS Member

OV3600 monitors AP WDS role and displays this information on **AP Monitoring** page.

NOTE

APs functioning as WDS Master or Primary WDS will no longer show up as Down is the radios are enabled.

WDS Participation

Perform these steps to configure WDS participation.

1. Log in to the AP.
2. Go to the **Wireless Services > AP** page.
3. Select **Enable participation in SWAN Infrastructure.**
4. Select **Specified Discovery**, and enter the IP address of the Primary WDS device (AP or WLSM).
5. Enter the user name and password for the WLSE server.

Primary or Secondary WDS

Perform these steps to configure primary or secondary functions for WDS.

1. Go to the **Wireless Services > WDS > General Setup** page.
2. If the AP is the Primary or Backup WDS, select **Use the AP as Wireless Domain Services**.
   - Select **Priority** (set **200** for Primary, **100** for Secondary).
   - Configure the **Wireless Network Manager** (configure the IP address of WLSE).
3. If the AP is Member Only, leave all options unchecked.

4. Go to the **Security > Server Manager** page.
5. Enter the **IP address** and **Shared Secret** for the ACS server and select **Apply**.
6. Go to the **Wireless Services > WDS > Server Group** page.
7. Enter the **WDS Group** of the AP.
8. Select the **ACS server** in the **Priority 1** drop-down menu and select **Apply**.

Configuring ACS for WDS Authentication

ACS authenticates all components of the WDS and must be configured first. Perform these steps to make this configuration.

1. Login to the ACS.
2. Go to the **System Configuration > ACS Certificate Setup** page.
3. Install a New Certificate by selecting the **Install New Certificate** button, or skip to the next step if the certificate was previously installed.
4. Select **User Setup** in the left frame.
5. Enter the user name that will be used to authenticate into the WDS and select **Add/Edit**.
6. Enter the password that will be used to authenticate into the WDS and select **Submit**.
7. Go to the **Network Configuration > Add AAA Client** page.
8. Add the host name and IP address associated with the AP and the key.
9. Enter the password that will be used to authenticate into the WDS and select **Submit**.

For additional and more general information about ACS, refer to "Configuring ACS Servers" on page 65.

Configuring Cisco WLSE Rogue Scanning

The **OV3600 Setup > WLSE** page allows OV3600 to integrate with the Cisco Wireless LAN Solution Engine (WLSE). OV3600 can discover APs and gather rogue scanning data from the Cisco WLSE.

Perform the following steps for optional configuration of OV3600 for support of Cisco WLSE rogue scanning.

1. To add a Cisco WLSE server to OV3600 , navigate to the **OV3600 Setup > WLSE** page and select **Add**. Complete the fields in this page. Table 33 describes the settings and default values.

Table 33: *OV3600 Setup > WLSE Fields and Default Values*

Setting	Default	Description
Hostname/IP Address	None	Designates the IP address or DNS Hostname for the WLSE server, which must already be configured on the Cisco WLSE server.
Protocol	HTTP	Specify whether to use HTTP or HTTPS when polling the WLSE.
Port	1741	Defines the port OV3600 uses to communicate with the WLSE server.

Table 33: *OV3600 Setup > WLSE Fields and Default Values (Continued)*

Setting	Default	Description
Username	None	Defines the user name OV3600 uses to communicate with the WLSE server. The user name and password must be configured the same way on the WLSE server and on OV3600. The user needs permission to display faults to discover rogues and inventory API (XML API) to discover manageable APs. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow OV3600 to pull the necessary XML APIs.
Password	None	Defines the password OV3600 uses to communicate with the WLSE server. The user name and password must be configured the same way on the WLSE server and on OV3600. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow OV3600 to pull the necessary XML APIs.
Poll for AP Discovery; Poll for Rogue Discovery	Yes	Sets the method by which OV3600 uses WLSE to poll for discovery of new APs and/or new rogue devices on the network.
Polling Period	10 minutes	Determines how frequently OV3600 polls WLSE to gather rogue scanning data.

2. After you have completed all fields, select **Save**. OV3600 is now configured to gather rogue information from WLSE rogue scans. As a result of this configuration, any rogues found by WLSE appear on the **RAPIDS > List** page.

What Next?

- Go to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- Complete the required configurations in this chapter before proceeding. Alcatel-Lucent support remains available to you for any phase of OV3600 installation.

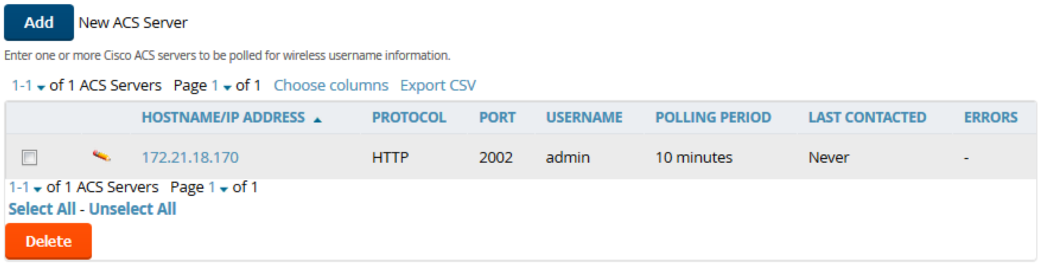
Configuring ACS Servers

This is an optional configuration. The **OV3600 Setup > ACS** page allows OV3600 to poll one or more Cisco ACS servers for wireless user name information. When you specify an ACS server, OV3600 gathers information about your wireless users. Refer to "Setting Up Device Types" on page 60 if you want to use your ACS server to manage your OV3600 users.

Perform these steps to configure ACS servers:

1. Go to the **OV3600 Setup > ACS** page. This page displays current ACS setup, as illustrated in Figure 19.

Figure 19: *OV3600 Setup > ACS Page Illustration*



Add New ACS Server

Enter one or more Cisco ACS servers to be polled for wireless username information.

1-1 of 1 ACS Servers Page 1 of 1 Choose columns Export CSV

		HOSTNAME/IP ADDRESS ▲	PROTOCOL	PORT	USERNAME	POLLING PERIOD	LAST CONTACTED	ERRORS
□	✎	172.21.18.170	HTTP	2002	admin	10 minutes	Never	-

1-1 of 1 ACS Servers Page 1 of 1

Select All - Unselect All

Delete

2. Select **Add** to create a new ACS server, or select a pencil icon to edit an existing server. To delete an ACS server, select that server and select **Delete**. When selecting **Add** or **Edit**, the **Details** page appears.
3. Complete the settings on **OV3600 Setup > ACS > Add/Edit Details**. Table 34 describes these fields:

Table 34: *OV3600 Setup > ACS > Add/Edit Details Fields and Default Values*

Field	Default	Description
IP/Hostname	None	Sets the DNS name or the IP address of the ACS Server.
Protocol	HTTP	Launches a drop-down menu specifying the protocol OV3600 uses when it polls the ACS server.
Port	2002	Sets the port through which OV3600 communicates with the ACS. OV3600 generally communicates over port 2002.
Username	None	Sets the user name of the account OV3600 uses to poll the ACS server.
Password	None	Sets the password of the account OV3600 uses to poll the ACS server.
Polling Period	10 min	Launches a drop-down menu that specifies how frequently OV3600 polls the ACS server for user name information.

4. Select **Add** to finish creating the new ACS server, or **Save** to finish editing an existing ACS server.
5. The ACS server must have logging enabled for passed authentications. Enable the **Log to CSV Passed Authentications report** option, as follows:
   - Log in to the ACS server, select **System Configuration**, then in the **Select** frame, select **Logging**.
   - Under **Enable Logging**, select **CSV Passed Authentications**. The default logging options include the two columns OV3600 requires: **User-Name** and **Caller-ID**.

What Next?

- Go to additional tabs in the OV3600 Setup section to continue additional setup configurations.
- Complete the required configurations in this chapter before proceeding. Alcatel-Lucent support remains available to you for any phase of OV3600 installation.

Integrating NMS Servers

You can integrate OV3600 with Network Management System (NMS) servers. Doing so enables OV3600 to forward SNMP traps to the NMS.

Add an NMS Server

AirWave communicates with the NMS server using the SNMPv1, SNMPv2c, or SNMPv3 protocol over Port 162.

To integrate an NMS server with OV3600:

1. Go to **OV3600 Setup > NMS**, then click **Add**.
2. Enter the NMS server hostname or IP address.
3. Use the default port, or you can enter a new port number.
4. Select the SNMP version:
   - SNMPv1 or SNMPv2c, then enter the community string and confirm the string.
   - SNMPv3, then enter the advanced security options (authentication and privacy protocols and passphrases).
5. Click **Add**.

Download the MIB Files

The necessary OV3600 MIB files are available to download from the **OV3600 Setup > NMS** page.

NOTE

OV3600 provides integration with HP ProCurve Manager (PCM). For help loading the integration files, navigate to **OV3600 Setup > NMS**, then click the HP ProCurve Manager Integration link.

PCI Compliance Monitoring

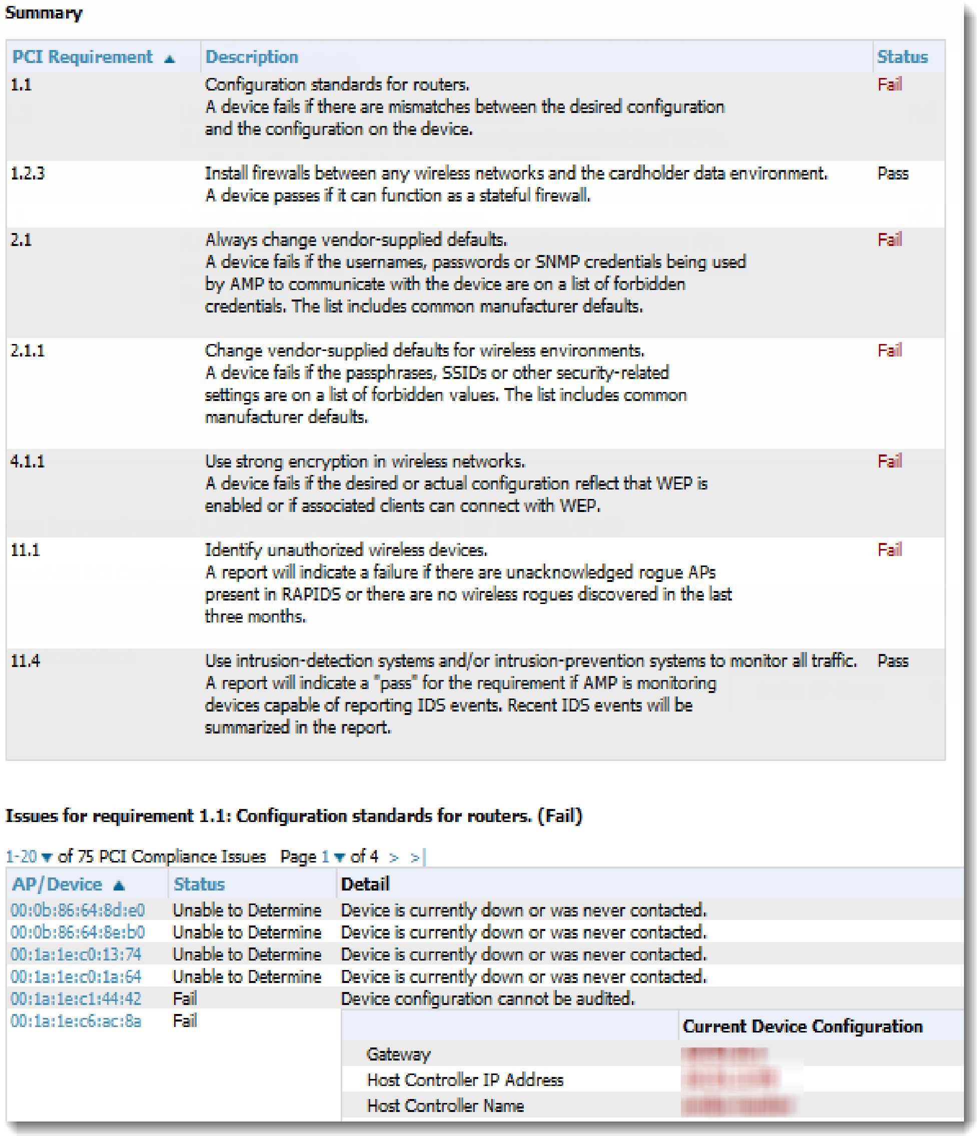
OV3600 provides compliance monitoring tools that can help your organization be prepared for a PCI Data Security Standard (DSS) audit. With use of OV3600, your organization can monitor firewalls, network devices, and other services to show PCI compliance.

Check Compliance

The PCI compliance report displays which requirements OV3600 monitors, provides links to device management pages, and displays any actions required to resolve compliance failures. In addition to displaying pass or fail status, OV3600 provides diagnostic information and recommends actions required to achieve Pass status when sufficient information is available.

You can find the PCI compliance report for a device by navigating to **Devices > List**, hovering the pointer over a device, and clicking **Compliance** from the shortcut menu. If you created a PCI compliance report from the **Reports Definition** page, OV3600 displays the report on the **Generated Reports** page when it is available, as shown in Figure 20. For information, see "Viewing Generated Reports" on page 350.

Figure 20: *PCI Compliance Report Example*



Summary

PCI Requirement ▲	Description	Status
1.1	Configuration standards for routers. A device fails if there are mismatches between the desired configuration and the configuration on the device.	Fail
1.2.3	Install firewalls between any wireless networks and the cardholder data environment. A device passes if it can function as a stateful firewall.	Pass
2.1	Always change vendor-supplied defaults. A device fails if the usernames, passwords or SNMP credentials being used by AMP to communicate with the device are on a list of forbidden credentials. The list includes common manufacturer defaults.	Fail
2.1.1	Change vendor-supplied defaults for wireless environments. A device fails if the passphrases, SSIDs or other security-related settings are on a list of forbidden values. The list includes common manufacturer defaults.	Fail
4.1.1	Use strong encryption in wireless networks. A device fails if the desired or actual configuration reflect that WEP is enabled or if associated clients can connect with WEP.	Fail
11.1	Identify unauthorized wireless devices. A report will indicate a failure if there are unacknowledged rogue APs present in RAPIDS or there are no wireless rogues discovered in the last three months.	Fail
11.4	Use intrusion-detection systems and/or intrusion-prevention systems to monitor all traffic. A report will indicate a "pass" for the requirement if AMP is monitoring devices capable of reporting IDS events. Recent IDS events will be summarized in the report.	Pass

Issues for requirement 1.1: Configuration standards for routers. (Fail)

1-20 ▼ of 75 PCI Compliance Issues Page 1 ▼ of 4 > >|

AP/Device ▲	Status	Detail
00:0b:86:64:8d:e0	Unable to Determine	Device is currently down or was never contacted.
00:0b:86:64:8e:b0	Unable to Determine	Device is currently down or was never contacted.
00:1a:1e:c0:13:74	Unable to Determine	Device is currently down or was never contacted.
00:1a:1e:c0:1a:64	Unable to Determine	Device is currently down or was never contacted.
00:1a:1e:c1:44:42	Fail	Device configuration cannot be audited.
00:1a:1e:c6:ac:8a	Fail	

	Current Device Configuration
Gateway	[redacted]
Host Controller IP Address	[redacted]
Host Controller Name	[redacted]

You can schedule, view, and re-run custom PCI compliance reports. For information about working with reports, see "Creating, Running, and Sending Reports" on page 315.

Enabling PCI Compliance Monitoring

When you enable PCI compliance monitoring, OV3600 displays real-time information and generates PCI compliance reports that can be used to verify whether a merchant is compliant with a PCI requirement.

For information security standards, refer to the *PCI Quick Reference Guide*, accessible online from the PCI Security Council Document Library or see "Supported PCI Requirements" on page 69.

To enable PCI auditing:

1. Navigate to the **OV3600 Setup > PCI Compliance** page.
2. Find the PCI requirement that you want to monitor.
3. Click ✎ to open the Default Credential Compliance page. The compliance settings vary depending on the PCI requirement.
4. Select **Save**.

5. To view and monitor PCI auditing on the network, use generated or daily reports. See "Creating, Running, and Sending Reports" on page 315. In addition, you can view the real-time PCI auditing of any given device online. Perform these steps:
   a. Go to the **Devices > List** page.
   b. Select a specific device. The **Monitor** page for that device displays. The **Devices** page also displays a **Compliance** subtab in the menu bar.
   c. Select **Compliance** to view complete PCI compliance auditing for that specific device.

Supported PCI Requirements

OV3600 currently supports the PCI 3.0. requirements described in Table 35. When the requirements are disabled, OV3600 does not check for PCI compliance or report on status.

NOTE

OV3600 users without RAPIDS visibility will not see the 11.1 PCI requirements in the PCI compliance report.

Table 35: *PCI Requirements*

Requirement	Description
1.1	Establishes firewall and router configuration standards. A device fails if there are mismatches between the desired configuration and the configuration on the device.
1.2.3	Monitors firewall installation between any wireless networks and the cardholder data environment. A device fails if the firewall is not stateful.
2.1	Changes vendor-supplied default passwords before a device connects to the cardholder data environment or transmits data in the network. A device fails if the user name, passwords or SNMP credentials used by OV3600 are on the list of forbidden default credentials. The list includes common vendor default passwords.
2.1.1	Changes vendor-supplied defaults for wireless environments. A device fails if the passwords, SSIDs, or other security-related settings are on a list of forbidden values that OV3600 establishes and tracks. The list includes common vendor default passwords. The user can input new values to achieve compliance.
4.1.1	Uses strong encryption in wireless networks before sending payment cardholder data across open public networks. A device fails if the desired or actual configuration reflect that WEP is enabled on the network, or if associated users can connect with WEP.
11.1	Uses RAPIDS to identify unauthorized devices. A device fails when a rogue device is detected and unacknowledged, or when there are no rogues discovered in the last three months.
11.4	Uses intrusion-detection or intrusion-prevention systems to monitor traffic. Recent IDS events are summarized in the PCI compliance report or the IDS report.

Deploying WMS Offload

The Wireless LAN Management Server (WMS) feature is an enterprise-level hardware device and server architecture with managing software for security and network policy.

WMS components include:

- Air monitor. This operating mode provides wireless IDS, rogue detection and containment.

- WMS server. This server manages devices and network activity, such as rogue detection and network policy enforcement.
- OV3600 WebUI. This graphical user interface (GUI) provides access to the WMS offload feature.

Refer to the *OmniVista 3600 Air Manager 8.2 Best Practices Guide* for additional information, including detailed concepts, configuration procedures, restrictions, AOS-W infrastructure, and OV3600 version differences in support of WMS Offload.

WMS Offload Configuration

WMS offload places the burden of the WMS server data and GUI functions on OV3600. WMS master switches provide this data so that OV3600 can support rigorous network monitoring capabilities.

WMS Offload is supported with ArubaOS Version 2.5.4 or later and AirWave Version 6.0 or later

Follow these steps to configure WMS offload:

1. Configure WLAN switches for optimal OV3600 monitoring:
   a. Disable debugging.
   b. Ensure the OV3600 server is a trap receiver host.
   c. Ensure proper traps are enabled.
2. Configure OV3600 to optimally monitor the OV3600 infrastructure:
   a. Enable WMS offload on the **OV3600 Setup > General** page.
   b. Configure SNMP communication.
   c. Create a proper policy for monitoring the OV3600 infrastructure.
   d. Discover the infrastructure.
3. Configure device classification:
   a. Set up rogue classification.
   b. Set up rogue classification override.
   c. Establish user classification override devices.
4. Deploy AOS-W-specific monitoring features:
   a. Enable remote AP and wired network monitoring.
   b. View switch license information.
5. Convert existing floor plans to VisualRF to include the following elements:
   - Alcatel-Lucent AOS-W
   - RF Plan
6. Use RTLS for increasing location accuracy (optional):
   a. Enable RTLS service on the OV3600 server.
   b. Enable RTLS on AOS-W infrastructure.

Integrating External Servers

OV3600 supports integration with Juniper, Brocade or HPE Intelligent Management Center (IMC) servers. When a device is monitored by OV3600 and an external server, the **Devices > Monitor** page for that device provides a link to that external server.

Add a Juniper Network Director

OV3600 supports integration with Juniper Network Director (ND) 2.0. Once integrated, the **Devices** > **Monitor** page for that device provides access to a link the Juniper Network Director WebUI.

To integrate Juniper Network Director with OV3600:

1. Log in to OV3600, then navigate to **OV3600 Setup > External server**.
2. In the **Juniper Network Director** section, enter the IP address or hostname of the Juniper Network Director.
3. Click **Save**.

Add a Brocade Network Advisor

OV3600 can monitor and secure Brocade wired networks, while Brocade Network Advisor monitors Aruba networks. Once integrated, the Brocade Network Advisor appears in the **Devices** list on the OV3600 **Devices > List** page, and the **Devices > Monitor** page for that device provides access to the Brocade Network Advisor home page.

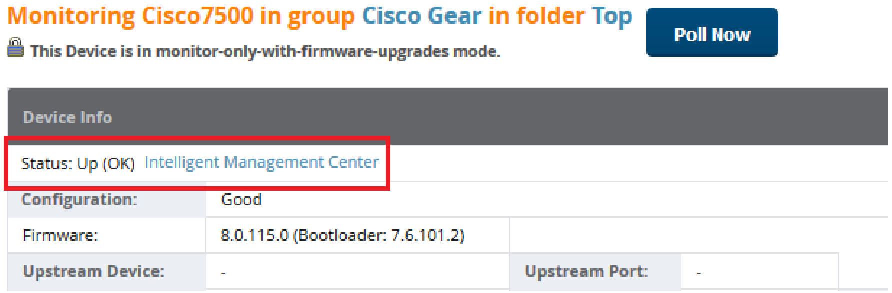
To integrate Brocade Network Advisor with OV3600:

1. Log in to OV3600, then navigate to **OV3600 Setup > External server**.
2. In the **Brocade Network Advisor** section, enter the IP address or hostname of the Brocade Network Advisor.
3. Click **Save**.

Add an HPE Intelligent Management Center

When a managed device is monitored by both OV3600 and the HPE Intelligent Management Center (IMC) Enterprise Software Platform, the **Devices > Monitor** page for that device includes a link to the IMC server.

Figure 21: *IMC Link on the Devices > Monitor page*



Monitoring Cisco7500 in group Cisco Gear in folder Top

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

Status: Up (OK) Intelligent Management Center

Configuration:	Good		
Firmware:	8.0.115.0 (Bootloader: 7.6.101.2)		
Upstream Device:	-	Upstream Port:	-

To integrate an IMC server with OV3600:

1. Log in to OV3600, then navigate to **OV3600 Setup > External server**.
2. In the **Intelligent Management Center** section, enter the IP address or hostname of the IMC server.
3. (Optional) Click the **IMC Protocol** drop down list and select the **HTTPS** or **HTTP** protocol. The default setting is **HTTPS**.
4. (Optional) Enter a port number in the **IMC Port** field. The default port number is **8443**.
5. Enter the user name for accessing the IMC server, then confirm this password.
6. Click **Save**.

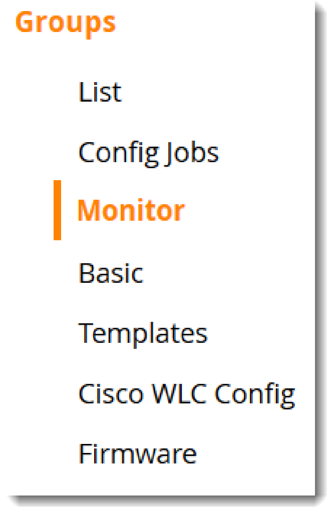
OV3600 automates the processes of device configuration and compliance auditing using device groups. A *Group* can include one device to hundreds of devices that share common configuration settings, and you can define groups based on geography, usage or security policies, function, or another variable. Variables include basic settings, security settings, and radio settings.

Navigation Basics

When you select a device group from the Groups List page, the navigation sidebar varies, depending on the default group and type of devices that you added to OV3600. After you create additional device groups, you can change the default group by navigating to **OV3600 Setup > General** and selecting a group from the Default Group drop-down menu.

Figure 22 shows a navigation sidebar menu that is available when you select a group that contains Cisco WLCs.

Figure 22: *Navigation Sidebar*



The following WebUI pages support group monitoring and configuration:

- List. This page lists all groups configured in OV3600 and provides the foundation for all group-level configurations. For more information, see "Viewing Device Groups" on page 73
- Monitor. This page displays client and bandwidth usage information, lists devices in a given group, provides an **Alert Summary** table for monitoring alerts for the group, and provides a detailed **Audit Log** for group-level activity. The default view of the **Groups > Monitor** page is predefined and cannot be modified. However, you can create a new view, or edit and copy a view, and save the view to access information you frequently use. For more information on filtering data from your view, see "Creating Filtered Views" on page 132.
- Basic. This page becomes available when you create a new group on the **Groups > List** page. For more information, see "Configuring Basic Settings for Device Groups" on page 75.
- Templates. This page manages templates for any device group. You can use templates to manage the configuration of third-party devices in a group using a configuration file. Variables configure device-specific and group-level properties. For more information, see "Creating and Using Templates" on page 223.

- Security. This page defines general security settings for device groups, to include RADIUS, encryption, and additional security settings on devices. For more information, see "Configuring Security for Device Groups" on page 86
- SSID. This page sets SSIDs, VLANs, and related parameters in device groups. Use this submenu is available when you configure RADIUS servers on the **Groups > AAA Servers** page. For more information, see "Configuring SSIDs and VLANs for Device Groups" on page 92.
- AAA Servers. This page configures authentication, authorization, and accounting settings in support of RADIUS servers for device groups. For more information, see "Configuring AAA Servers for Device Groups" on page 85.
- Radio. This page defines general 802.11 radio settings for device groups. "Configuring Radio Settings for Device Groups" on page 96
- Controller Config. This page manages AOS-W Device Groups, AP Overrides, and other profiles specific to Alcatel-Lucent devices on the network. Use this page as an alternative to the **Device Setup > Alcatel-Lucent > Configuration** page. The appearance of this page varies depending on whether OV3600 is configured for global configuration or group configuration. For more information, see the *Alcatel-Lucent Controller Configuration Guide*.
- .
- Instant Config. This page manages Alcatel-Lucent Instant devices on the network. For more information, see the *Alcatel-Lucent Instant User Guide*.
- Cisco WLC Config. This page becomes available when you select a device group that contains Cisco WLC devices and consolidates controller-level settings from several pages (Group Radio, Security, SSIDs, Cisco WLC Radio and AAA Server). For more information, see "Configuring Cisco WLCs for Device Groups" on page 100
- PTMP. This page defines settings specific to Proxim MP devices when present and is only available when a Proxim MP device is added to this group. For more information, see "Configuring PTMP Settings for Device Groups" on page 106.
- Proxim Mesh. This page defines mesh AP settings specific to Proxim devices when present. For more information, see"Configuring Proxim Mesh Radio Settings" on page 107.
- MAC ACL. This page defines MAC-specific settings that apply to Proxim, Symbol, and ProCurve 520 devices when present. For more information, see "Configuring Group MAC ACLs for Device Groups" on page 109.
- Firmware. This page enables you to manage firmware files for many device types in one location. For more information, see "Specifying the Minimum Firmware Version for Device Groups" on page 110.
- Compare. This page allows you to compare line item-settings between two device groups. On the **Groups > List** page, select the **Compare two groups** link, select the two groups from the drop-down menus, and then select **Compare**. For more information, see "Comparing Device Groups" on page 111.

Viewing Device Groups

You can view device groups by navigating to **Groups > List** . When you configure OV3600 for the first time, Access Points is the only group in the list.

From the Groups List page, you can:

- Create a group by clicking Add at the top of the page. Alternatively, you could create a group by selecting group from the list and clicking 📋 to clone the group. The copied group will be added to the group list with "copy of" appended in front of the group name.
- Compare two groups. For more information, see "Comparing Device Groups" on page 111.
- Click 🔧 or hover your mouse over the icon for quick access to other Groups pages. For information about the Groups pages, see "Navigation Basics" on page 72.

For example, you can select Basic from the shortcut menu to change group configurations. Refer to "Configuring Basic Settings for Device Groups" on page 75 .

- Add groups to a global group. For more information, see "Subscribing other Groups to a Global Group" on page 119.
- Delete a group. For more information, see "Deleting a Group" on page 113.

Table 36 describes the device group details available on the **Groups > List** page.

Table 36: *Groups > List Fields and Descriptions*

Field	Description
Name	Uniquely identifies the group by location, vendor, department or any other identifier (such as 'Accounting APs,' 'Floor 1 APs,' 'Cisco devices,' '802.1X APs,' and so forth).
SSID	The SSID assigned to supported device types within the group.
Total Devices	Total number of devices contained in the group including APs, controllers, routers, or switches.
Changes	This field is available when a group has unapplied changes.
Is Global Group	This field is available if a group is designated as global. A global group may not contain APs, but it may be used as a template for other groups. **NOTE:** This column might indicate **Yes** if this group has been pushed to OV3600 from a Master Console.
Global Group	Specifies which group this Subscriber Group is using as its template.
Down	The number of access points within the group that are not reachable via SNMP or are no longer associated to a controller. Note that thin APs are not directly polled with SNMP, but are polled through the controller. That controller may report that the thin AP is down or is no longer on the controller. At this point, OV3600 classifies the device as down.
Mismatched	The number of devices within the group that are in a mismatched state.
Ignored	The number of ignored devices in that group.
Clients	The number of mobile users associated with all access points within the group. To avoid double counting of clients, clients are only listed in the group of the AP with which they are associated. Note that device groups with only controllers in them report no clients.
Usage	A running average of the sum of bytes in and bytes out for the managed radio page.
VPN Sessions	Number of active (connected) VPN sessions under this group.
Up/Down Status Polling Period	The time between Up/Down SNMP polling periods for each device in the group. Detailed SNMP polling period information is available on the **Groups > Basic** configuration page. By default, most polling intervals do not match the up/down period.
Duplicate	Creates a new group with the name **Copy of <Group Name>** with identical configuration settings. (Alcatel-Lucent configuration settings will have to be manually added back.)

Configuring Basic Settings for Device Groups

The first default device group set up in OV3600 is the **Access Points** group, but you can configure additional device groups. After you define the basic group settings, you can save the changes without pushing these settings to the devices in the group. You might want to do this in order to push configuration changes at a later time.

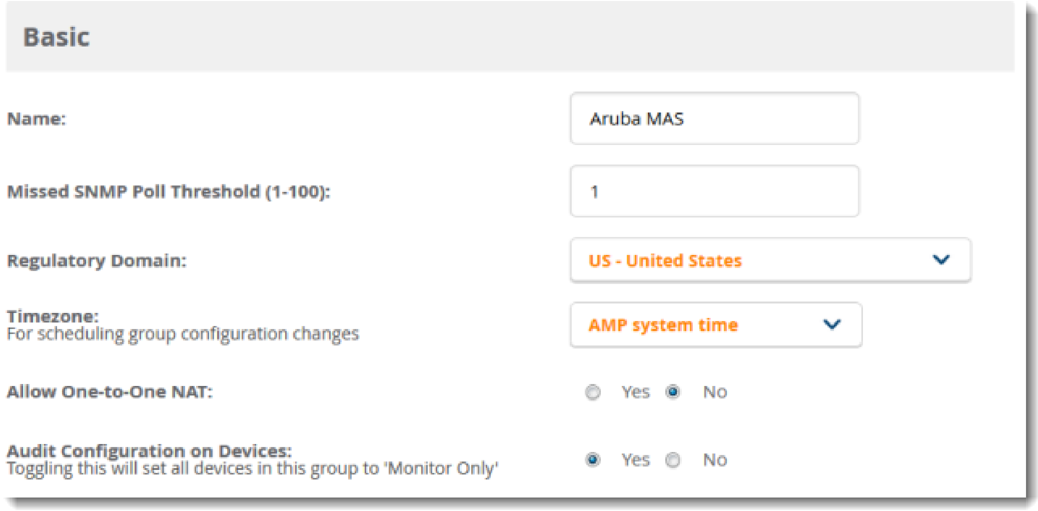
There are three ways to navigate to the Basic Group Settings page.

- Add a device group from the **Groups > List page**. The **Groups > Basic** page displays and becomes available from the navigation sidebar.
- Navigate to **Groups > List** and click the wrench icon next to the group.
- Navigate to **Groups > List**, select a group from the **Groups** table, then select Basic from the shortcut menu see). The shortcut menu varies depending on the group's settings.

Basic Settings

To set up the device group, you need to configure the basic settings described in Table 37.

Figure 23: *Basic Settings*



Basic

Name: Aruba MAS

Missed SNMP Poll Threshold (1-100): 1

Regulatory Domain: US - United States

Timezone:
For scheduling group configuration changes: AMP system time

Allow One-to-One NAT: ○ Yes ● No

Audit Configuration on Devices:
Toggling this will set all devices in this group to 'Monitor Only': ● Yes ○ No

Table 37: *Basic Settings, Default Values, and Descriptions*

Setting	Default	Description
Name	Defined when first adding the group	Displays or changes the group name. Enter a name that helps to identify the group. For example, Accounting APs, Cisco devices, and Alcatel-Lucent switches).
Missed SNMP Poll Threshold (1-100)	1	Sets the number of Up/Down SNMP polls that must be missed before OV3600 considers a device to be down. **NOTE:** Set the number of SNMP retries and the SNMP timeout of a poll on the **Device Setup > Communication** page.
Regulatory Domain	US-United States	Sets the regulatory domain in OV3600, limiting the selectable channels for APs in the group.

Table 37: *Basic Settings, Default Values, and Descriptions (Continued)*

Setting	Default	Description
Timezone	OV3600 system time	Allows group configuration changes to be scheduled relative to the time zone in which the devices are located.
Allow One-to-One NAT	No	Allows OV3600 to talk to the devices on a different IP address than the one configured on the device. **NOTE:** If enabled, the LAN IP Address listed on the **AP/Devices > Manage** configuration page under the **Settings** area is different than the IP Address under the **Device Communication** area.
Audit Configuration on Devices	Yes	Auditing and pushing of configuration to devices can be disabled on all the devices in the group. **NOTE:** Once disabled, all the devices in the groups will not be counted towards mismatched devices.

Global Groups

The global groups option becomes available on the Groups Basic page when you create a new group for the first time and it is a global group.

Table 38 describes the global group options you can define in order to push configurations to group members.

Table 38: *Global Groups Fields and Default Values*

Setting	Default	Description
Is Global Group	No	If set to **Yes**, then this group can be selected in the Use Global Group drop down menu for future group configurations. For more information, refer to"Using Global Groups for Group Configuration" on page 118 .
Use Global Group	No	Click this drop-down list to select a global group to which this (non-global) group should be associated. For more information, refer to "Subscribing other Groups to a Global Group" on page 119 . **NOTE:** This field becomes available when there are more than one groups configured in OV3600.

SNMP Polling Periods

You can override the override default SNMP polling settings with the SNMP polling period options described in Table 39.

Table 39: *SNMP Polling Periods Fields and Default Values*

Setting	Default	Description
Up/Down Status Polling Period	5 minutes	Sets time between Up/Down SNMP polling for each device in the group. The Group SNMP Polling Interval overrides the global parameter configured on the **Device Setup > Communication** page. An initial polling interval of **5** minutes is best for most networks.

Table 39: *SNMP Polling Periods Fields and Default Values (Continued)*

Setting	Default	Description
Override Polling Period for Other Services	No	Enables or disables overriding the base SNMP Polling Period. If you select **Yes**, the other settings in the SNMP Polling Periods section are activated, and you can override default values.
AP Interface Polling Period	10 minutes	Sets the interval at which OV3600 polls for radio monitoring and bandwidth being used by a device.
Client Data Polling Period	10 minutes	Sets time between SNMP polls for client data for devices in the group.
Thin AP Discovery Polling Period	15 minutes	Sets time between SNMP polls for Thin AP Device Discovery. Controllers are the only devices affected by this polling interval.
Device-to-Device link Polling Period	5 minutes	Sets time between SNMP polls for Device-to-Device link polling. Mesh APs are the only devices affected by this polling interval.
802.11 Counters Polling Period	15 minutes	Sets time between SNMP polls for 802.11 Counter information.
Rogue AP and Device Location Data Polling Period	30 minutes	Sets time between SNMP polls for Rogue AP and Device Location Data polling.
CDP Neighbor Data Polling Period	30 minutes	Sets the frequency in which this group polls the network for Cisco Discovery Protocol (CDP) neighbors.
Mesh Discovery Polling Period	15 minutes	Sets time between SNMP polls for Mesh Device Discovery.

Routers and Switches

You can configure how often OV3600 polls devices in the group with the routers and switches options described in Table 40. You can also disable these options.

Table 40: *Routers and Switches Fields and Default Values*

Setting	Default	Description
Read ARP Table	4 hours	Sets the frequency in which devices poll routers and switches for Address Resolution Protocol (ARP) table information. This setting can be disabled, or set to poll for ARP information in a range from every 15 seconds to 12 hours.
Read CDP Table for Device Discovery	4 hours	For Cisco devices, sets the frequency in which devices poll routers and switches for Cisco Discovery Protocol (CDP) information. This setting can be disabled, or set to poll for CDP neighbor information in a range from every 15 seconds to 12 hours.

Table 40: *Routers and Switches Fields and Default Values (Continued)*

Setting	Default	Description
Read Bridge Forwarding Table	4 hours	Sets the frequency in which devices poll the network for bridge forwarding information. This setting can be disabled, or set to poll bridge forwarding tables from switches in a range from every 15 seconds to 12 hours.
Interface Up/Down Polling Period	5 minutes	Sets the frequency in which network interfaces are polled for up/down status. This setting can be disabled, or set to poll from switches in a range from every 15 seconds to 30 minutes.
Interface Bandwidth Polling Period	15 minutes	Sets the frequency in which network interfaces are polled for bandwidth usage. This setting can be disabled, or set to poll from switches in a range from every 5 minutes to 30 minutes.
Interface Error Counter Polling Period	30 minutes	Sets the frequency in which network interfaces are polled for up/down status. This setting can be disabled, or set to poll bridge forwarding tables from switches in a range from every 5 minutes to 30 minutes.
Poll 802.3 error counters	No	Sets whether 802.3 error counters should be polled.
Poll Cisco interface error counters	No	Sets whether the interface error counters for Cisco devices should be polled.

Notes

Use this optional section to record additional information and comments about the group.

Group Display Options

You can configure the group display options as described in Table 41.

Table 41: *Group Display Options Fields and Default Values*

Setting	Default	Description
Show device settings for	Only devices on this OV3600	Drop-down menu determines which Group tabs and options are to be viewable by default in new groups. Settings include the following: ● **All Devices**—OV3600 displays all Group tabs and setting options. ● **Only devices in this group**—OV3600 hides all options and tabs that do not apply to the devices in the group. If you use this setting, then to get the group list to display the correct SSIDs for the group, you must **Save and Apply** on the group. ● **Only devices on this OV3600**— hides all options and tabs that do not apply to the APs and devices currently on OV3600. ● **Use system defaults**—Use the default settings on **OV3600 Setup > General** ● **Selected device types**—Allows you to specify the device types for which OV3600 displays Group settings.
Selected Device Types	N/A	This option appears if you chose to display selected device types, allowing you to select the device types to display group settings. Use **Select devices in this group** to display only devices in the group being configured.

Automatic Static IP Assignment

Use the **Automatic Static IP Assignment** section on the **Groups > Basic** configuration page to automatically assign a range of static IP addresses to new devices as they are added into the group.

These options are relevant for a small number of device types and will appear when they are present.

Table 42 describes the automatic static IP address options.

Table 42: *Automatic Static IP Assignment Fields and Default Values*

Setting	Default	Description
Assign Static IP Addresses to Devices	No	Specify whether to enable OV3600 to statically assign IP addresses from a specified range to all devices in the Group. **NOTE:** If this value is set to **Yes**, then the additional configuration fields described in this table will become available.
Start IP Address	none	Sets the first address OV3600 assigns to the devices in the Group.
Number of Addresses	none	Sets the number of addresses in the pool from which OV3600 can assign IP addresses.
Subnet Mask	none	Sets the subnet mask to be assigned to the devices in the Group.
Subnet Gateway	none	Sets the gateway to be assigned to the devices in the Group.
Next IP Address	none	Defines the next IP address queued for assignment. This field is disabled for the initial Access Points group.

Spanning Tree Protocol

Use the **Spanning Tree Protocol** settings on the **Groups > Basic** page to configure the Spanning Tree Protocol on Wireless LAN Controller (WLC) devices and Proxim APs.

Table 43 describes the settings and default values in this section.

Table 43: *Spanning Tree Protocol Fields and Default Values*

Setting	Default	Description
Spanning Tree Protocol	No	Specify whether to enable STP on Proxim APs. When you set this option to **Yes**, additional configuration fields described in this table become available.
Bridge Priority	32768	Sets the priority for the AP. Values range from 0 to 65535. Lower values have higher priority. The lowest value is the root of the spanning tree. If all devices are at default the device with the lowest MAC address will become the root.
Bridge Maximum Age	20	Sets the maximum time, in seconds, that the device stores protocol information. The supported range is from 6 to 40.
Bridge Hello Time	2	Sets the time, from 1 to 10 seconds, between Hello message broadcasts.
Bridge Forward Delay	15	Sets the time, from 4 to 30 seconds, that the port spends in listening and learning mode if the spanning tree has changed.

NTP

Use the **NTP Settings** section of the **Groups > Basic** page to define an NTP server and configure Network Time Protocol (NTP) settings.

Table 44 describes the NTP settings and default values.

Table 44: *NTP Fields and Default Values*

Setting	Default	Description
NTP Server #1,2,3	None	Sets the IP address of the NTP servers to be configured on the AP.
UTC Time Zone	0	Sets the hour offset from UTC time to local time for the AP. Times displayed in OV3600 graphs and logs use the time set on the OV3600 server.
Daylight Saving Time	No	Enables or disables the advanced daylight saving time settings in the Proxim section of the **Groups > Basic** configuration page.

Aruba Switch Configuration

OV3600 automates provisioning of several models of HPE OfficeConnect access points, which are mainly used for Comware switches. Provisioning uses template-based configuration, zero-touch provisioning (ZTP), and configuration snippets.

There are two methods of switch configuration:

- Full configuration. OmniVista 3600 Air Manager pushes a complete set of changes using a template to the group of devices. By default, the full configuration mode is enabled whenever you create a device group.
- Config job. OV3600 pushes a golden configuration to a group that contains factory-default ZTP devices.

You can also push any command supported by the switch CLI to the device group regardless of their device state (factory or non-factory).

For help with switch configuration, refer to *OV3600 8.2.7 Switch Configuration Guide*.

Aruba/Alcatel-Lucent

To configure settings specific to Alcatel-Lucent locate the **Aruba/Alcatel-Lucent** section and adjust these settings as required.

Table 45 describes the settings and default values of this section of the **Groups > Basic** page.

Table 45: *Aruba Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	The version of SNMP used by OV3600 to communicate to the AP.

Table 45: *Aruba Fields and Default Values (Continued)*

Setting	Default	Description
Offload WMS Database	No	Configures commands previously documented in the OmniVista 3600 Air Manager 8.2.7.1 *Best Practices Guide*. When enabled, this feature allows OV3600 to display historical information for WLAN switches. Changing the setting to **Yes** pushes commands via SSH to all WLAN switches in Monitor Only mode without rebooting the switch. The command can be pushed to switches in manage mode (also without rebooting the switch) if the **Allow WMS Offload** setting on **OV3600 Setup > General** is changed to **Yes**.
Alcatel-Lucent GUI Config	Yes	This setting selects whether you'd like to configure your devices using the **Groups > Controller** method (either global or group) or using Templates.
Manage local configuration on controllers	No	Enables or disables the management of local configuration including audit, push, and import operations.
Ignore Rogues Discovered by Remote APs	No	Configures whether to turn off RAPIDS rogue classification and rogue reporting for RAPs in this group.
Delete Certificates On Controller	No	Specifies whether to delete the current certificates on an AOS-Wswitch.

Alcatel-Lucent Instant

To specify the Alcatel-Lucent Instant settings to be applied to this group, locate the Alcatel-Lucent Instant settings section of the **Groups > Basic** page and adjust these settings as desired.

Table 46 describes the settings and default values.

Table 46: *Virtual Controller Certificate Fields and Default Values*

Setting	Default	Description
Enable Instant GUI Config	No	Select this option to configure your Instant APs via the IGC feature on the **Groups > Instant Config** pages of the OV3600 WebUI, rather than via Instant template configuration.
Configure AirWave communication settings:	No	If the Enable Instant GUI Config setting is set to No, you can use this option to configure t6he primary (and optionally, secondary) OV3600 server settings on an Instant AP via template configuration.
Disable auto join mode	No	If you enable the Disable auto join mode setting, then Instant APs will not automatically join a group of Instant APs in OV3600 when that device becomes active on the network.

Table 46: *Virtual Controller Certificate Fields and Default Values (Continued)*

Setting	Default	Description
HTTPS timeout	5 minutes	the HTTPS timeout for Instant devices is the period for which OV3600 waits for an Instant heartbeat message. The **Missed SNMP Poll Threshold** in the **Basic Settings** section at the top of the **Groups > Basic** page sets the number of Up/Down SNMP polls that must be missed before OV3600 considers a device to be down. If, for example, a group of Instant APs your group settings has a **Missed SNMP Poll Threshold** of 1, then an instant AP is considered to be down if there is 1 missed heartbeat during this HTTPS timeout period, which could be anywhere between 1-30 min.
CA Cert	None	Specify a CA certificate for the Instant virtual controller. The fields in this drop down will populate when a certificate of type **Intermediate CA** or **Trusted CA** is added in the **Device Setup > Certificates** page.
Server Cert	None	Specify a server certificate for the virtual controller. The fields in this drop down will populate when a certificate of type **Server Cert** is added in the **Device Setup > Certificates** page.
Captive Portal Cert	None	Specify a Captive portal certificate for the virtual controller. The fields in this drop down will populate when a certificate of type **Captive Portal Cert** is added in the **Device Setup > Certificates** page.
Captive Portal Logo	None	You can use OV3600 to download a captive portal logo to your Instant APs. Upload the image (which must be 16k bytes or less) on the **Device Setup > Upload** page, then click the Captive Portal Logo drop down list on the Groups > Basic page to select the image to send to the OAW-IAPs.
RadSec Server Cert	None	Specify a RadSec server certificate for the virtual controller. The fields in this drop down will populate when a certificate of type **Server Cert** is added in the **Device Setup > Certificates** page.
RadSec CA Cert	None	Specify a RadSec CA certificate for the virtual controller. The fields in this drop down will populate when a certificate of type **Intermediate CA** or **Trusted CA** is added in the **Device Setup > Certificates** page.

Cisco IOS/Catalyst

Configure group settings specific to Cisco IOS/Catalyst devices, as described in Table 47.

Table 47: *Cisco IOS/Catalyst Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	The version of SNMP used by OV3600 to communicate to the AP.
Cisco IOS CLI Communication	Telnet	The protocol OV3600 uses to communicate with Cisco IOS devices. Selecting **SSH** uses the secure shell for command line page (CLI) communication and displays an **SSH Version** option. Selecting **Telnet** sends the data in clear text via Telnet.

Table 47: *Cisco IOS/Catalyst Fields and Default Values (Continued)*

Setting	Default	Description
Cisco IOS Config File Communication	TFTP	The protocol OV3600 uses to communicate with Cisco IOS devices. Selecting **SCP** uses the secure copy protocol for file transfers and displays an **SCP Version** option. Selecting **TFTP** will use the insecure trivial file transfer protocol. The SCP login and password should be entered in the Telnet user name and password fields.

Cisco WLC

Use the Cisco WLC section of the **Groups > Basic** page to configure settings specific to a Cisco Wireless LAN Controllers (WLC).

Table 48 describes the settings and default values in this section.

Table 48: *Cisco WLC Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	Sets the version of SNMP used by OV3600 to communicate to WLC controllers.
CLI Communication	SSH	Sets the protocol OV3600 uses to communicate with Cisco IOS devices. Selecting **SSH** uses the secure shell for command line page (CLI) communication. Selecting **Telnet** sends the data in clear text via Telnet.

NOTE

When configuring Cisco WLC controllers, refer to "Configuring Wireless Parameters for Cisco Controllers" on page 105.

Proxim/ Avaya

To configure Proxim/Avaya specific settings locate the **Proxim/Avaya** section of the **Groups > Basic** page and adjust these settings as required.

Table 49 describes the settings and default values.

Table 49: *Proxim/Avaya Settings*

Setting	Default	Description
SNMP Version	1	Sets the version of SNMP used by AMP to communicate to the AP.
Enable DNS Client	No	Enables the DNS client on the AP. Enabling the DNS client allows you to set some values on the AP by hostname instead of IP address. If you select Yes for this setting, additional DNS fields display.
Primary DNS server	Blank	Sets the IP address of the Primary DNS server.
Secondary DNS server	Blank	Sets the IP address of the Secondary DNS server.

Table 49: *Proxim/Avaya Settings (Continued)*

Setting	Default	Description
Default DNS domains	Blank	Sets the default DNS domain used by the AP.
HTTP Server Port	80	Sets this port as the HTTP server port on all Proxim APs in the group.
Country Code	United States	Configures AMP to derive its time settings based on the country of location, as specified in this field.

HP ProCurve

To configure HP ProCurve specific settings, locate the **HP ProCurve** section of the **Groups > Basic** page and adjust these settings as required.

The Table 50 describes the settings and default values.

Table 50: *HP ProCurve Settings*

Setting	Default	Description
SNMP Version	2c	Sets the version of SNMP used by OV3600to communicate to the AP.
ProCurve XL/ZWeSM CLI Communication	Telnet	Sets the protocol OV3600 uses to communicate with ProCurve XLWeSM devices. Selecting SSH will use the secure shell for command line (CLI) communication. Selecting Telnet will send the data in clear text via telnet.
switchSNMP Version	2c	Specifies the version of SNMP used by OV3600to communicate to the switch.

Symbol

To configure settings for Symbol switches, locate the **Symbol** section of the **Groups > Basic** page and adjust these settings as required.

Table 51 describes the settings and default values.

Table 51: *Symbol Settings*

Setting	Default	Description
SNMP Version	2c	Specifies the version of SNMP used by AWMS to communicate to the device.
Symbol Client Inactivity Timeout (3-600 min)	3	Sets the minutes of inactivity after which a client associated to a Symbol AP will be considered "inactive." A lower value typically provides a more accurate representation of current WLAN usage. **NOTE:** For other APs, AWMS has more precise methods to determine when inactive clients are no longer associated to an AP.
Symbol Controller CLI Communication	Telnet	The connection type to support the command-line interface (CLI) connection. The options are Telnet and secure shell (SSH). This is supported for WS5100, RFS4000, RFS6000 and RFS7000 devices only.
Web Config Interface	Yes	Enables or disables the http/https configuration page for the Symbol 4131 devices.

Juniper/3Com/Enterasys/Nortel/Trapeze

To configure SNMP settings for 3Com, Enterasys, Nortel, or Trapeze devices, locate the **Juniper/3Com/Enterasys/Nortel/Trapeze** section of the **Groups > Basic** page and click the **SNMP Version** drop-down list to define the version of SNMP to be supported. The default setting is SNMPv2c.

Universal Devices, Routers and Switches

To configure settings for universal devices on the network, including routers and switches that support both wired and wireless networks,, locate the **Juniper/3Com/Enterasys/Nortel/Trapeze** section of the **Groups > Basic** page and click the **SNMP Version** drop-down list to define the version of SNMP to be supported. The default setting is SNMPv2c.

Automatic Authorization

To control the conditions by which devices are automatically authorized into this group, locate the **Automatic Authorization** settings section of the **Groups > Basic** page and adjust these settings as required.

Table 52 describes the automatic authorization options for the device group.

Table 52: *Automatic Authorization Fields and Default Values*

Setting	Default	Description
Add New Controllers and Autonomous Devices Location	Use Global Setting	Whether to auto authorize new controllers to the New Devices List, the same Group/Folder as the discovering devices, the same Group/Folder as the closest IP neighbor, and/or a specified auto-authorization group and folder. The Current Global Setting set in **OV3600 Setup > General** is shown below this field. Selecting a different option overrides the global setting.
Add New Thin APs Location	Use Global Setting	Whether to auto authorize new thin APs to the New Devices List, the same Group/Folder as the discovering devices, the same Group/Folder as the closest IP neighbor, and/or a specified auto-authorization group and folder. The Current Global Setting set in **OV3600 Setup > General** is shown below. Selecting a different option overrides the global setting for this group.

Maintenance Windows

You can use maintenance windows to put multiple devices into Management mode, apply configuration changes to the devices in the group, and then reset them to Monitor-Only mode after the maintenance period is over. For more information, see "Adding a Maintenance Window for a Device" on page 217.

Configuring AAA Servers for Device Groups

Configure RADIUS servers on the **Groups > AAA Servers** page. Once defined on this page, the **Groups > Security** and **Groups > SSIDs** menus appear in the navigation bar, allowing you to select and configure your RADIUS servers.

NOTE

If the **Groups > AAA Servers** page does not appear in the navigation bar, select the group from the **Groups > List** page, select the **Groups > Basic** page, then choose the **Show Device Settings for : All Devices** option in the **Group Display Options** section of the **Groups > Basic** page.

1. Go to the **Groups > List** page and select the group for which to define AAA servers by selecting the group name. The **Monitor** page appears.

2. Select the **AAA Servers** page. The **AAA Servers** page appears, enabling you to add a RADIUS server.
3. To add a RADIUS server or edit an existing server, select **Add New RADIUS Server** or the corresponding pencil icon to edit an existing server. Table 53 describes the settings and default values of the **Add/Edit** page.

Table 53: *Adding a RADIUS Server Fields and Default Values*

Setting	Default	Description
Hostname/IP Address	None	Sets the IP Address or DNS name for RADIUS Server. **NOTE:** IP Address is required for Proxim/ORiNOCO and Cisco Aironet IOS APs.
Secret and Confirm Secret	None	Sets the shared secret that is used to establish communication between OV3600 and the RADIUS server. **NOTE:** The shared secret entered in OV3600 must match the shared secret on the server.
Authentication	No	Sets the RADIUS server to perform authentication when this setting is enabled with **Yes**.
Authentication Port (1-65535)	1812	Appears when **Authentication** is enabled. Sets the port used for communication between the AP and the RADIUS server.
Accounting	No	Sets the RADIUS server to perform accounting functions when enabled with **Yes**.
Accounting Port (1-65535)	1813	Appears when **Accounting** is enabled. Sets the port used for communication between the AP and the RADIUS server.
Timeout (0-86400)	None	Sets the time (in seconds) that the access point waits for a response from the RADIUS server.
Max Retries (0-20)	None	Sets the number of times a RADIUS request is resent to a RADIUS server before failing. **NOTE:** If a RADIUS server is not responding or appears to be responding slowly, consider increasing the number of retries.

4. Select **Add** to complete the creation of the RADIUS server, or select **Save** if editing an existing RADIUS server. The **Groups > AAA Servers** page displays this new or edited server. You can now reference this server on the **Groups > Security** page.

   OV3600 supports reports for subsequent RADIUS Authentication. These are viewable by selecting **Reports > Generated**, scrolling to the bottom of the page, and selecting **Latest RADIUS Authentication Issues Report**.
5. To make additional RADIUS configurations for device groups, use the **Groups > Security** page and continue to the next topic.

NOTE

TACACS+ servers are configurable only for Cisco WLC devices. Refer to "Configuring Cisco WLC Security Parameters and Functions" on page 105.

Configuring Security for Device Groups

The **Groups > Security** page allows you to set security policies for APs in a device group.

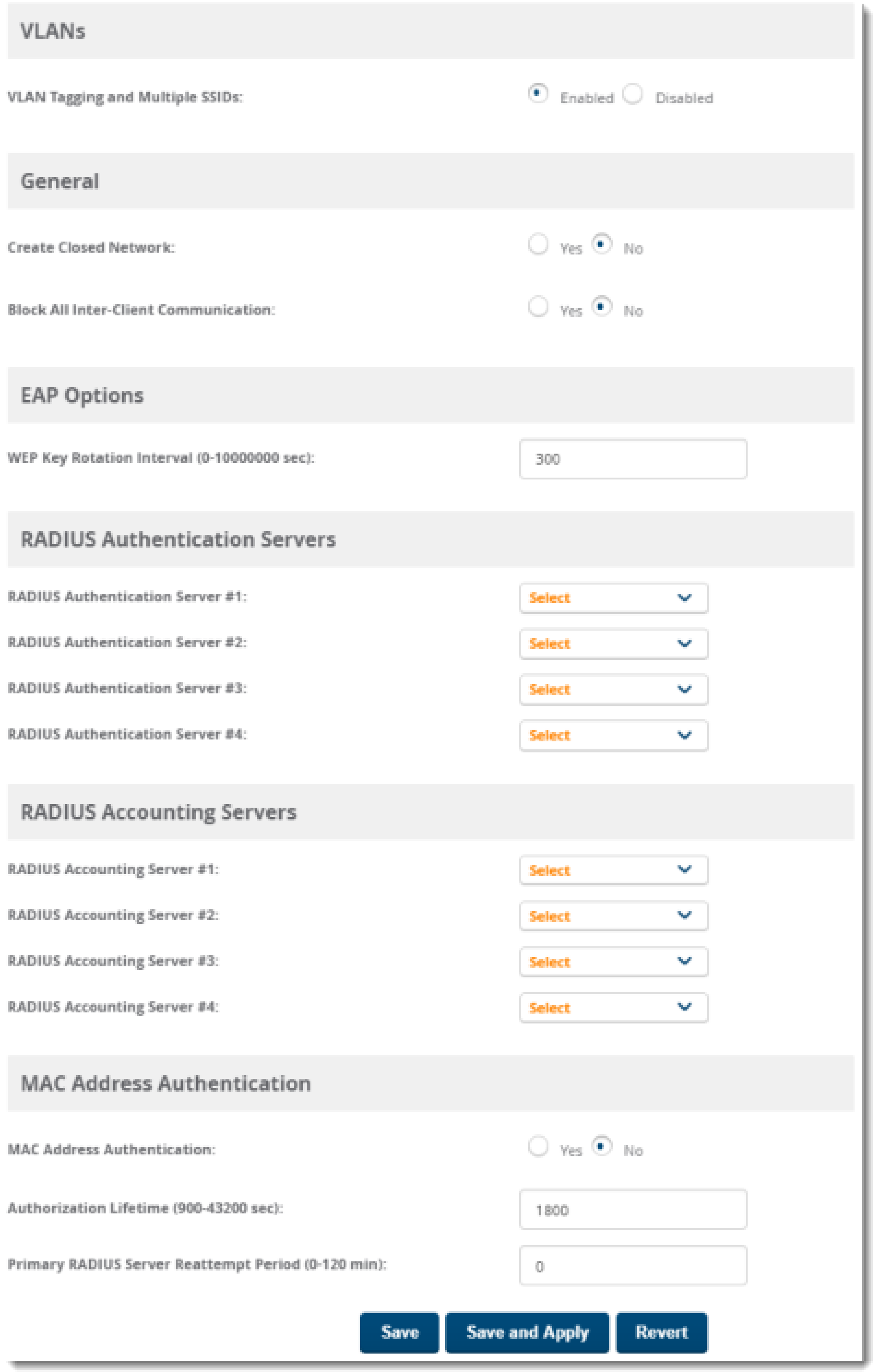
NOTE

This page appears in the WebUI after you configure RADIUS servers on the **Groups > AAA Servers** page. Once RADIUS servers are defined, the **Groups> Security** and **Groups > SSIDs** menus appear in the navigation bar, allowing you to select and configure your RADIUS servers.

1. Select the device group for which to define security settings from the **Groups > List** page.
2. Go to **Groups > Security**. Some controls on this page interact with additional OV3600 pages.

Figure 24 illustrates this page for a group of switches.

Figure 24: *Groups > Security Page*



VLANs

VLAN Tagging and Multiple SSIDs: ● Enabled ○ Disabled

General

Create Closed Network: ○ Yes ● No

Block All Inter-Client Communication: ○ Yes ● No

EAP Options

WEP Key Rotation Interval (0-10000000 sec): 300

RADIUS Authentication Servers

RADIUS Authentication Server #1: Select

RADIUS Authentication Server #2: Select

RADIUS Authentication Server #3: Select

RADIUS Authentication Server #4: Select

RADIUS Accounting Servers

RADIUS Accounting Server #1: Select

RADIUS Accounting Server #2: Select

RADIUS Accounting Server #3: Select

RADIUS Accounting Server #4: Select

MAC Address Authentication

MAC Address Authentication: ○ Yes ● No

Authorization Lifetime (900-43200 sec): 1800

Primary RADIUS Server Reattempt Period (0-120 min): 0

Table 54 explains the fields and default values.

Table 54: *Groups > Security Page Fields and Default Values*

Setting	Default	Description
VLANs Section		

Table 54: *Groups > Security Page Fields and Default Values (Continued)*

Setting	Default	Description
VLAN Tagging and Multiple SSIDs	Enabled	This field enables support for VLANs and multiple SSIDs on the wireless network. If this setting is enabled, define additional VLANs and SSIDs on the **Groups > SSIDs** page. Refer to "Configuring SSIDs and VLANs for Device Groups" on page 92. If this setting is disabled, then you can specify the **Encryption Mode** in the **Encryption** section that displays. Refer to "Groups > Security Encryption Mode settings" on page 90 for information on configuring Encryption.
Management VLAN ID	Untagged	This setting sets the ID for the management VLAN when VLANs are enabled in OV3600 . This setting is supported only for the following devices: ● Proxim AP-600, AP-700, AP-2000, AP-4000 ● Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8 ● ProCurve520WL
General Section		
Create Closed Network	No	If enabled, the APs in the Group do not broadcast their SSIDs. **NOTE:** Creating a closed network will make it more difficult for intruders to detect your wireless network.
Block All Inter-client Communication	No	If enabled, this setting blocks client devices associated with an AP from communicating with other client devices on the wireless network. **NOTE:** This option may also be identified as PSPF (Publicly Secure Packet Forwarding), which can be useful for enhanced security on public wireless networks.
EAP Options Section		
WEP Key Rotation Interval	300	Sets the frequency at which the Wired Equivalent Privacy (WEP) keys are rotated in the device group being configured. The supported range is from 0 to 10,000,000 seconds.
RADIUS Authentication Servers Section		
RADIUS Authentication Server #1 - #4	Not selected	Defines one or more RADIUS Authentication servers to be supported in this device group. Select up to four RADIUS authentication servers from the four drop-down menus.
Authentication Profile Name	OV3600-Defined Server #1	For Proxim devices only, this field sets the name of the authentication profile to be supported in this device group.
Authentication Profile Index	1	For Proxim devices only, this field sets the name of the authentication profile index to be supported in this device group.
RADIUS Accounting Servers Section		
RADIUS Accounting Server #1 - #4	Not selected	Defines one or more RADIUS Accounting servers to be supported in this device group. Select up to four RADIUS accounting servers from the four drop-down menus.

Table 54: *Groups > Security Page Fields and Default Values (Continued)*

Setting	Default	Description
Authentication Profile Name		For Proxim devices only, this field sets the name of the accounting profile to be supported in this device group.
Authentication Profile Index	3	For Proxim devices only, this field sets the name of the accounting profile index to be supported in this device group.
MAC Address Authentication Section		
MAC Address Authentication	No	If enabled, only MAC addresses known to the RADIUS server are permitted to associate to APs in the Group.
MAC Address Format	Single Dash	Allows selection of the format for MAC addresses used in RADIUS authentication and accounting requests: ● Dash Delimited: xx-xx-xx-xx-xx-xx (default) ● Colon Delimited: xx:xx:xx:xx:xx:xx ● Single-Dash: xxxxxx-xxxxxx ● No Delimiter: xxxxxxxxxxxx This option is supported only for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8, HPE ProCurve 520WL
Authorization Lifetime	1800	Sets the amount of time a user can be connected before reauthorization is required. The supported range is from 900 to 43,200 seconds.
Primary RADIUS Server Reattempt Period	0	Specifies the time (in minutes) that the AP awaits responses from the primary RADIUS server before communicating with the secondary RADIUS server, and so forth

The **Encryption** options display on the **Groups > Security** page when the **VLAN Tagging and Multiple SSIDs** option is set to **Disabled**. This setting defaults to **No Encryption**.

Refer to Table 55 for information regarding configuring encryption.

Table 55: *Groups > Security Encryption Mode settings*

Setting	Default	Description
Encryption Mode	Require 802.1X	Encryption Mode options: Require 802.1X, Optional WEP, Require WEP, Require 802.1X, Require LEAP, 802.1X + WEP, 802.1X + WEP, LEAP + WEP, Static CKIP, WPA, WPA/PSK, WPA2, WPA2/PSK, or xSec.
Transmit Key	1	Select the Transmit Key value. This can be a value from 1 through 4. Note that 802.1X + WEP mode sets this key value to 1.
Key #1	None	Enter 40/64-bit Keys in 5 alphanumeric or 10 hexadecimal digits, or enter 104/128-bit Keys in 13 alphanumeric or 26 hexadecimal digits.
Key #2	None	
Key #3	None	
Key #4	None	

Table 55: *Groups > Security Encryption Mode settings (Continued)*

Setting	Default	Description
Encryption Mode Static CKIP		
CKIP Static Key (hex) and Confirm	None	Enter and confirm the Cisco Key Integrity Protocol (CKIP) static key, specified in hexadecimal digits.
CKIP Key Index	1	Select the CKIP Key Index value. This can be a value from 1 through 4.
CKIP Key Permutation	No	Specify whether to use Key Permutation.
CKIP MMH Mode	No	Specify whether to use Multi-Module Has (MMH) mode.
Encryption Mode WPA		
Unicast Cipher (Cisco only)	AES	Specify the Unicast Cipher. Values include AES, TKIP, and AES/TKIP.
Encryption Mode WPA/PSK		
Unicast Cipher (Cisco only)	AES/TKIP	Specify the Unicast Cipher. Values include AES, TKIP, and AES/TKIP.
WPA Preshared Key (Alphanumeric)	None	Enter an alphanumeric value for the preshared key.
Encryption Mode WPA2		
WPA2 WPA Compatibility Mode	Yes	Specify whether to enable WPA2 WPA Compatibility Mode.
WPA1 Cipher (Cisco WLC Only)	TKIP	Specify the WPA1 Cipher. Values include AES, TKIP, and AES/TKIP. **NOTE:** This drop down is only available if WPA2 WPA Compatibility Mode is **Yes**.
Unicast Cipher (Cisco Only)	AES/TKIP	Specify the Unicast Cipher. Values include AES, TKIP, and AES/TKIP.
Encryption Mode WPA2/PSK		
WPA2 WPA Compatibility Mode	Yes	Specify whether to enable WPA2 WPA Compatibility Mode.
WPA1 Cipher (Cisco WLC Only)	TKIP	Specify the WPA1 Cipher. Values include AES, TKIP, and AES/TKIP. **NOTE:** This drop down is only available if WPA2 WPA Compatibility Mode is **Yes**.
Unicast Cipher (Cisco Only)	AES/TKIP	Specify the Unicast Cipher. Values include AES, TKIP, and AES/TKIP.

Table 55: *Groups > Security Encryption Mode settings (Continued)*

Setting	Default	Description
WPA Preshared Key (Alphanumeric)	None	Enter an alphanumeric value for the preshared key.
Encryption Mode xSec		
This indicates to use xSec encryption. No other configuration options are available.		

3. Select **Save** to retain these security configurations for the group, select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.
4. Continue with additional security-related procedures in this document for additional RADIUS and SSID settings for device groups, as required.

Configuring SSIDs and VLANs for Device Groups

Use the **Groups > SSIDs** configuration page to create and edit SSIDs and VLANs that apply to a device group. This configuration page does not appear in the OV3600 WebUI until *after* you configure a RADIUS server using the **Groups > AAA Servers** page, as described on "Configuring AAA Servers for Device Groups" on page 85.

OV3600 reports users by radio and by SSID. Graphs on the AP and controller monitoring pages display bandwidth in and out based on SSID. OV3600 reports can also be run and filtered by SSID. An option on the **OV3600 Setup > General** page can age out inactive SSIDs and their associated graphical data.

NOTE

WLANs that are supported from one or more Cisco WLC controllers can be configured on the **Groups > Cisco WLC Config** page.

To create or edit VLANs and to set SSIDs:

1. Go to **Groups > List** and select the group name for which to define SSIDs/VLANs.
2. Select the **Groups > SSIDs** configuration page. Table 56 describes the information that appears for SSIDs and VLANs that are currently configured for the device group.

Table 56: *Groups > SSIDs Fields and Descriptions*

Field	Description
SSID	Displays the SSID associated with the VLAN.
VLAN ID	Identifies the number of the primary VLAN SSID on which encrypted or unencrypted packets can pass between the AP and the switch.
Name	Displays the name of the VLAN.
Encryption Mode	Displays the encryption on the VLAN.
First or Second Radio Enabled	Enables the VLAN, SSID and Encryption Mode on the radio control.

Table 56: *Groups > SSIDs Fields and Descriptions (Continued)*

Field	Description
First or Second Radio Primary	Specifies which VLAN to be used as the primary VLAN. A primary VLAN is required. **NOTE:** If you create an open network (see the **Create Closed Network** setting below) in which the APs broadcast an SSID, the primary SSID is broadcast.
Native VLAN	Sets this VLAN to be the native VLAN. Native VLANs are untagged and typically used for management traffic only. OV3600 requires a Native VLAN to be set. For AP types do not require a native VLAN, create a dummy VLAN, disable it on both radio controls, and ensure that it has the highest VLAN ID.

3. Select **Add** to create a new SSID or VLAN, or select the pencil icon next to an existing SSID/VLAN to edit that existing SSID or VLAN. The **Add SSID/VLAN** configuration page appears, as explained in Table 57.
4. Locate the **SSID/VLAN** section on the **Groups > SSIDs** configuration page and adjust these settings as required. This section encompasses the basic VLAN configuration. Table 57 describes the settings and default values. Note that the displayed settings can vary.

Table 57: *SSID/VLAN Section Fields and Default Values*

Setting	Default	Description
Specify Interface Name	Yes	Enables or disables an interface name for the VLAN interface. Selecting **No** for this option displays the **Enable VLAN Tagging** and **VLAN ID** options.
Enable VLAN Tagging (Cisco WLC, Proxim, Symbol only)		Enables or disables VLAN tagging. Displays if **Specify Interface Name** is set to **No**.
VLAN ID (1-4094)	None	Indicates the number of the VLAN designated as the **Native VLAN**, typically for management purposes. Displays if **Specify Interface Name** is set to **No** and **Enable VLAN Tagging** is set to **Yes**.
Interface	management	Sets the interface to support the SSID/VLAN combination.
SSID	None	Sets the Service Set Identifier (SSID), which is a 32-character user-defined identifier attached to the header of packets sent over a WLAN. It acts as a password when a mobile device tries to connect to the network through the AP, and a device is not permitted to join the network unless it can provide the unique SSID.
Name	None	Sets a user-definable name associated with SSID/VLAN combination.
Maximum Allowed Associations (0-2007)	255	Indicates the maximum number of mobile users which can associate with the specified VLAN/SSID. **NOTE:** 0 means unlimited for Cisco.

Table 57: *SSID/VLAN Section Fields and Default Values (Continued)*

Setting	Default	Description
Broadcast SSID (Cisco WLC, Proxim and Symbol 4131 only)	No	For specific devices as cited, this setting enables the AP to broadcast the SSID for the specified VLAN/SSID. This setting works in conjunction with the **Create Closed Network** setting on the **Groups > Security** configuration page. Proxim devices support a maximum of four SSIDs. **NOTE:** This option should be enabled to ensure support of legacy users.
Partial Closed System (Proxim only)	No	For Proxim only, this setting enables to AP to send its SSID in every beacon, but it does not respond to any probe requests.
Unique Beacon (Proxim only)	No	For Proxim only, if more than one SSID is enabled, this option enables them to be sent in separate beacons.
Block All Inter-Client Communication	Yes	This setting blocks communication between client devices based on SSID.

5. Locate the **Encryption** area on the **Groups > SSIDs** page and adjust these settings as required. Table 58 describes the available encryption modes. Table 55 in "Configuring Security for Device Groups" on page 86 describes configuration settings for each mode.

Table 58: *Encryption Section Field and Default Values*

Setting	Default	Description
Encryption Mode	No Encryption	Drop-down menu determines the level of encryption required for devices to associate to the APs. The drop-down menu options are as follows. Each option displays additional encryption settings that must be defined. Complete the associated settings for any encryption type chosen: ● No Encryption ● **Optional WEP**—Wired Equivalent Privacy, not PCI compliant as of 2010 ● **Require WEP**—Wired Equivalent Privacy, not PCI compliant as of 2010 ● **Require 802.1X**—Based on the WEP algorithm ● **Require LEAP**—Lightweight Extensible Authentication Protocol ● **802.1X+WEP**—Combines the two encryption types shown ● **802.1X+LEAP**—Combines the two encryption types shown ● **LEAP+WEP**—Combines the two encryption types shown ● **Static CKIP**—Cisco Key Integrity Protocol ● **WPA**—Wi-Fi Protected Access protocol ● **WPA/PSK**—Combines WPA with Pre-Shared Key encryption ● **WPA2**—Wi-Fi Protected Access 2 encryption ● **WPA2/PSK**—Combines the two encryption methods shown ● **xSec**—FIPS-compliant encryption including Layer 2 header info

6. Locate the **EAP Options** area on the **Groups > SSIDs** page, and complete the settings. Table 59 describes the settings and default values.

Table 59: *EAP Options Section Field and Default Value*

Setting	Default	Description
WEP Key Rotation Interval (0-10000000 sec)	120	Time (in seconds) between WEP key rotation on the AP.

7. Locate the **RADIUS Authentication Servers** area on the **Groups > SSIDs** configuration page and define the settings. Table 60 describes the settings and default values.

Table 60: *RADIUS Authentication Servers Fields and Default Values*

Setting	Default	Description
RADIUS Authentication Server 1-3 (Cisco WLC, Proxim only)	None	Drop-down menu to select RADIUS Authentication servers previously entered on the **Groups > RADIUS** configuration page. These RADIUS servers dictate how wireless clients authenticate onto the network.
Authentication Profile Name (Proxim Only)	None	Sets the Authentication Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000.
Authentication Profile Index (Proxim Only)	None	Sets the Authentication Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000.

8. Select **Save** when the security settings and configurations in this procedure are complete.

NOTE

You may need to return to the **Groups > Security** configuration page to configure or reconfigure RADIUS servers.

9. Locate the **RADIUS Accounting Servers** area on the **Groups > SSIDs** configuration page and define the settings. Table 61 describes the settings and default values.

Table 61: *Radius Accounting Servers Fields and Default Values*

Setting	Default	Description
RADIUS Accounting Server 1-3 (Cisco WLC, Proxim Only)	None	Pull-down menu selects RADIUS Accounting servers previously entered on the **Groups > RADIUS** configuration page. These RADIUS servers dictate where the AP sends RADIUS Accounting packets for this SSID/VLAN.
Accounting Profile Name (Proxim Only)	None	Sets the Accounting Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000.
Accounting Profile Index (Proxim Only)	None	Sets the Accounting Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000.

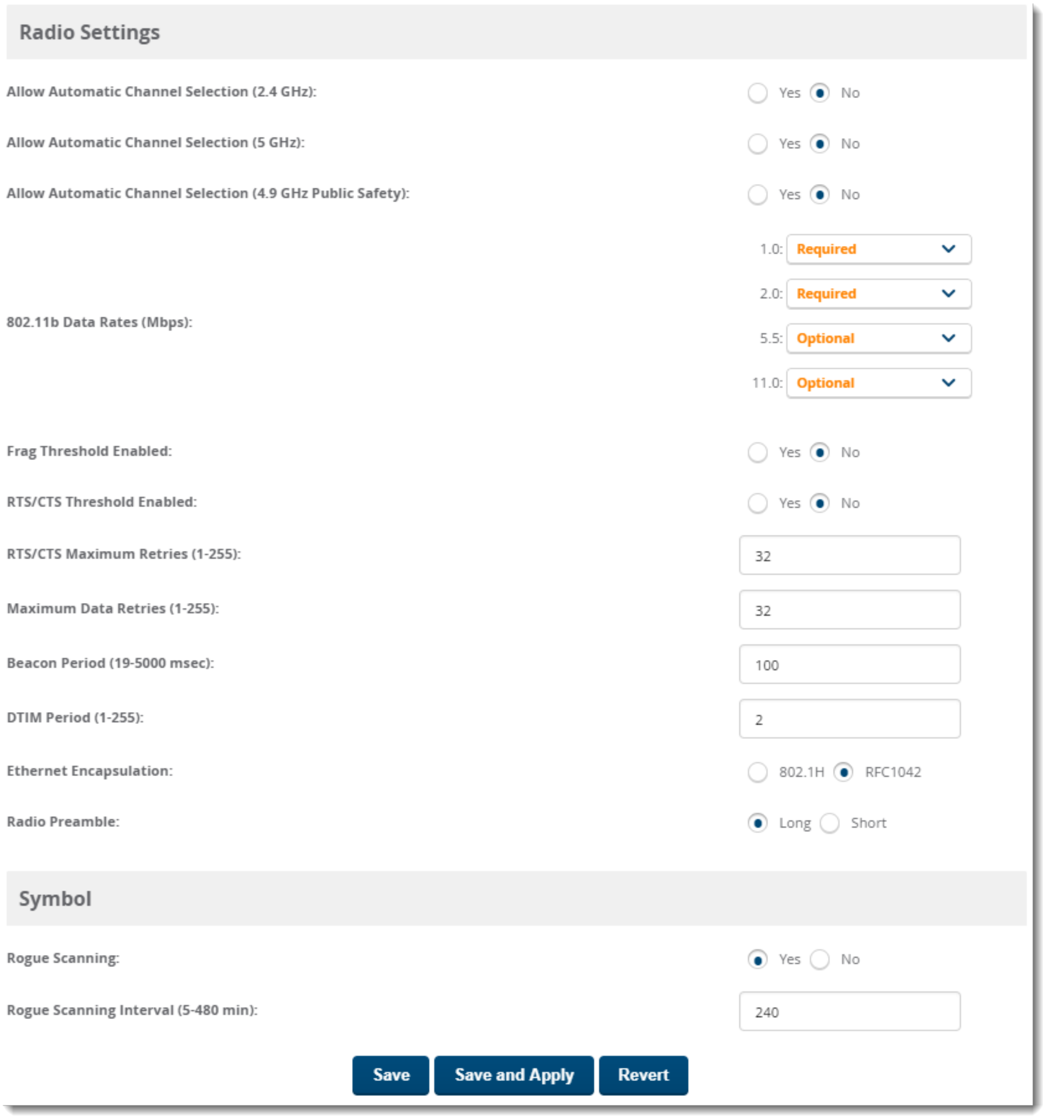
10. Select **Add** when you have completed all sections. This returns you to the **Groups > SSIDs** page.

11. Select **Save** to retain these **SSID** configurations for the group, select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.

Configuring Radio Settings for Device Groups

You can configure detailed RF-related radio settings for devices on the **Groups > Radio** page. If you have existing deployed devices, you might want to use the RF settings on those devices as a guide when configuring the radio settings for your default group.

Figure 25: *Groups > Radio Page*



Radio Settings

Allow Automatic Channel Selection (2.4 GHz):	○ Yes ● No
Allow Automatic Channel Selection (5 GHz):	○ Yes ● No
Allow Automatic Channel Selection (4.9 GHz Public Safety):	○ Yes ● No
802.11b Data Rates (Mbps):	1.0: Required 2.0: Required 5.5: Optional 11.0: Optional
Frag Threshold Enabled:	○ Yes ● No
RTS/CTS Threshold Enabled:	○ Yes ● No
RTS/CTS Maximum Retries (1-255):	32
Maximum Data Retries (1-255):	32
Beacon Period (19-5000 msec):	100
DTIM Period (1-255):	2
Ethernet Encapsulation:	○ 802.1H ● RFC1042
Radio Preamble:	● Long ○ Short

Symbol

Rogue Scanning:	● Yes ○ No
Rogue Scanning Interval (5-480 min):	240

To define RF-related radio settings for a device group:

1. Go to the **Groups > List** page, then select a group for which to define radio settings. The monitor page for the group appears.
2. Navigate to **Groups > Radio** to open the radio page for the group. Figure 25 illustrates this page.
3. Locate the **Radio Settings** area and adjust these settings as required. Table 62 describes the settings and default values.

Table 62: *Groups > Radio > Radio Settings Fields and Default Values*

Setting	Default	Description
Allow Automatic Channel Selection (2.4, 5, and 4.9GHz Public Safety)	No	If enabled, whenever the AP is rebooted it uses its radio to scan the airspace and select its optimal RF channel based on observed signal strength from other radios. **NOTE:** If you enable this feature, OV3600 automatically reboots the APs in the group when the change is implemented.
802.11b Data Rates (Mbps)	Required: • 1.0 • 2.0 Optional: • 5.5 • 11.0	Displays pull-down menus for various data rates for transmitting data. **NOTE:** This setting does not apply to Cisco LWAPP devices. The three values in each of the pull-down menus are as follows: • **Required**—The AP transmits only unicast packets at the specified data rate; multicast packets are sent at a higher data rate set to optional. (Corresponds to a setting of **yes** on Cisco devices.) • **Optional**—The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of **basic** on Cisco devices.) • **Not Used**—The AP does not transmit data at the specified data rate. (Corresponds to a setting of **no** on Cisco devices.)
Frag Threshold Enabled	No	If enabled, this setting enables packets to be sent as several pieces instead of as one block. In most cases, leave this option disabled.
Threshold Value (256-2347 bytes)	2337	If Fragmentation Threshold is enabled, this specifies the size (in bytes) at which packets are fragmented. A lower **Fragmentation Threshold** setting might be required if there is a great deal of radio interference.
RTS/CTS Threshold Enabled	No	If enabled, this setting configures the AP to issue a RTS (Request to Send) before sending a packet. In most cases, leave this option disabled.
RTS/CTS Threshold Value (0-2347 bytes)	2338	If RTS/CTS is enabled, this specifies the size of the packet (in bytes) at which the AP sends the RTS before sending the packet.
RTS/CTS Maximum Retries (1-255)	32	If RTS/CTS is enabled, this specifies the maximum number of times the AP issues an RTS before stopping the attempt to send the packet through the radio. Acceptable values range from **1** to **128**.
Maximum Data Retries (1-255)	32	The maximum number of attempts the AP makes to send a packet before giving up and dropping the packet. Acceptable values range from **1** to **255**.
Beacon Period (19-5000 msec)	100	Time between beacons (in microseconds).
DTIM Period (1-255)	2	DTIM alerts power-save devices that a packet is waiting for them. This setting configures DTIM packet frequency as a multiple of the number of beacon packets. The DTIM Interval indicates how many beacons equal one cycle.
Ethernet Encapsulation	RFC1042	This setting selects either the RFC1042 or 802.1h Ethernet encapsulation standard for use by the group.

Table 62: *Groups > Radio > Radio Settings Fields and Default Values (Continued)*

Setting	Default	Description
Radio Preamble	Long	This setting determines whether the APs uses a **short** or **long** preamble. The preamble is generated by the AP and attached to the packet prior to transmission. The short preamble is 50 percent shorter than the long preamble and thus may improve wireless network performance. **NOTE:** Because older WLAN hardware may not support the short preamble, the long preamble is recommended as a default setting in most environments.

4. Certain wireless access points offer proprietary settings or advanced functionality that differ from prevailing industry standards. If you use these APs in the device group, you may wish to take advantage of this proprietary functionality.

   To configure these settings, locate the proprietary settings areas on the **Groups > Radio** page and continue with the additional steps in this procedure.

NOTE

Proprietary settings are only applied to devices in the group from the specific vendor and are not configured on devices from vendors that do not support the functionality.

5. To configure settings specific to the Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3/4/5/6/7/8, and ProCurve 520WL, locate the appropriate section of **Groups > Radio** page and define the required fields. Table 63 describes the settings and default values.

Table 63: *Groups > Radio > Device-Specific Fields and Default Values*

Setting	Default	Description
Load Balancing	No	If enabled, this setting allows client devices associating to an AP with two radio cards to determine which card to associate with, based on the load (# of clients) on each card. **NOTE:** This feature is only available when two 802.11b wireless cards are used in an AP-2000.
Interference Robustness	No	If enabled, this option will fragment packets greater than 500 bytes in size to reduce the impact of radio frequency interference on wireless data throughput.
Distance Between APs	Large	This setting adjusts the receiver sensitivity. Reducing receiver sensitivity from its maximum may help reduce the amount of crosstalk between wireless stations to better support roaming users. Reducing the receiver sensitivity, user stations will be more likely to connect with the nearest access point.
802.11g Operational Mode	802.11b +802.11g	This setting sets the operational mode of all g radios in the group to either b only, g only or b + g.
802.11abg Operational Mode	802.11b +802.11g	This setting sets the operational mode of all a/b/g radios in the group to either a only, b only, g only or b + g.

Table 63: *Groups > Radio > Device-Specific Fields and Default Values (Continued)*

Setting	Default	Description
802.11b Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
802.11g Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
802.11a Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
Rogue Scanning	Yes	If enabled, any ORiNOCO or Avaya APs in the group (with the appropriate firmware) will passively scan for rogue access points at the specified interval. This rogue scan will not break users' association to the network. **NOTE:** This feature can affect the data performance of the access point.
Rogue Scanning Interval (15-1440 min)	15 minutes	If **Rogue Scanning** is enabled, this setting controls the frequency with which scans are conducted (in minutes). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan.

6. To configure settings specific to Proxim 4900M, locate the **Proxim 4900M** section and define the required fields. Table 64 describes the settings and default values.

Table 64: *Groups > Radio > Proxim 4900M Fields and Default Values*

Setting	Default	Description
4.9GHz Public Safety Channel Bandwidth	20	This setting specifies the channel bandwidth for the 4.9 GHz radio. It is only applicable if you are running the 802.11a/4.9GHz radio in 4.9GHz mode.
802.11a/4.9GHz Public Safety Operational Mode	802.11a	This setting specifies if the AP will run the 802.11a/4.9GHz radio in 802.11a mode or in 4.9 GHz mode. Please note that 4.9 GHz is a licensed frequency used for public safety.

7. To configure Symbol-only settings, locate the **Symbol** section and define the required fields. Table 65 describes the settings and default values.

Table 65: *Groups > Radio > Symbol Fields and Default Values*

Setting	Default	Description
Rogue Scanning	Yes	If enabled, Symbol access points with 3.9.2 or later firmware in the group will passively scan for rogue access points at the specified interval. This rogue scan will not break a user’s association to the network.
Rogue Scanning Interval (5-480 min)	240	If **Rogue Scanning** is enabled, this setting controls the frequency with which scans are conducted (in minutes). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan.

8. Select **Save** when radio configurations as described above are complete, select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.

Configuring Cisco WLCs for Device Groups

The **Groups > Cisco WLC Config** page consolidates the settings for Cisco WLC devices from all group pages. The **Groups > SSIDs** subtab applies to SSIDs for all device types except for Cisco WLC, which have WLANs configured on the **Cisco WLC Config** page.

> NOTE
>
> Do not put Symbol 4131 and Proxim APs in the same group as Cisco devices. Alcatel-Lucent recommends setting device preferences to **Only devices in this group**.

Refer to the following topics for additional information:

- "Accessing Cisco WLC Configuration" on page 100
- "Configuring WLANs for Cisco WLC Devices" on page 100
- "Defining and Configuring LWAPP AP Groups for Cisco Devices" on page 104
- "Viewing and Creating Cisco AP Groups" on page 104
- "Configuring Cisco Controller Settings" on page 104
- "Configuring Wireless Parameters for Cisco Controllers" on page 105
- "Configuring Cisco WLC Security Parameters and Functions" on page 105
- "Configuring Management Settings for Cisco WLC Controllers" on page 106

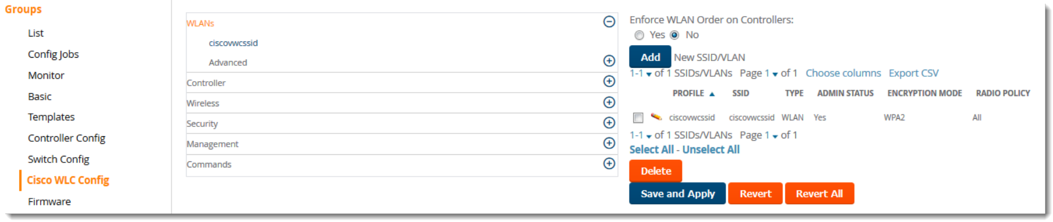
Accessing Cisco WLC Configuration

The Cisco WLC Config navigation submenu becomes available when you create a Cisco WLC device group for the first time.

To access the **Cisco WLC Config** page:

1. Navigate to **Groups > List**, then select a Cisco WLC device group.
2. Select **Groups > Cisco WLC Config** in the navigation sidebar. In the **Groups > Cisco WLC Config** page that displays, click ⊕ to expand the configurable settings.

Figure 26: *Groups > Cisco WLC Config Navigation*



Enforce WLAN Order on Controllers: ○ Yes ● No

New SSID/VLAN

1-1 of 1 SSIDs/VLANs Page 1 of 1

	PROFILE ▲	SSID	TYPE	ADMIN STATUS	ENCRYPTION MODE	RADIO POLICY
□	ciscowcssid	ciscowcssid	WLAN	Yes	WPA2	All

1-1 of 1 SSIDs/VLANs Page 1 of 1

> NOTE
>
> You can pre-populate the group WLC settings from a controller in the same group by performing an import on the controller's **Device Configuration** page.

Configuring WLANs for Cisco WLC Devices

In **Cisco WLC Config**, WLANs are based on SSIDs or VLANs that are dedicated to Cisco WLC controllers. Perform the following steps to define and configure WLANs for Cisco WLC controllers.

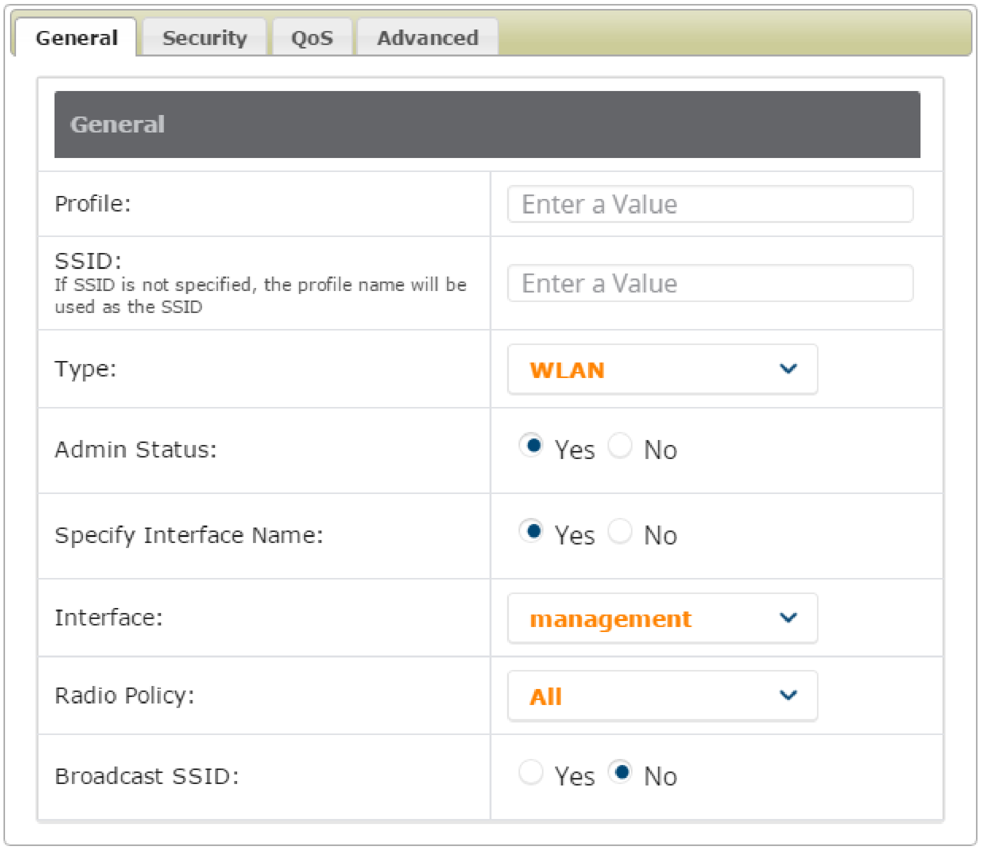
1. Go to the **Groups > Cisco WLC Config** page, and select **WLANs** in the left navigation pane. This page displays the SSIDs or VLANs that are available for use with Cisco WLC devices and enables you to define new SSIDs or VLANs. illustrates this page.

2. To change the ID/position of a WLAN on the controller by dragging and dropping, set the toggle to **Yes**. Note that the by setting this flag to **Yes**, OV3600 will display a mismatch if the WLANs in the desired config and device config differ only on the order.
3. To add or edit SSIDs or VLANs that are dedicated to Cisco WLC devices, either select the **Add** button, or select the pencil icon for an existing SSID/VLAN. A new page appears comprised of four tabs, as follows:
   - **General**—Defines general administrative parameters for the Cisco WLC WLAN.
   - **Security**—Defines encryption and RADIUS servers.
   - **QoS**—Defines quality of service (QoS) parameters for the Cisco WLC WLAN.
   - **Advanced**—Defines advanced settings that are available only with Cisco WLC devices, for example, AAA override, coverage, DHCP and DTIM period.

NOTE

Refer to Cisco documentation for additional information about Cisco WLC devices and related features.

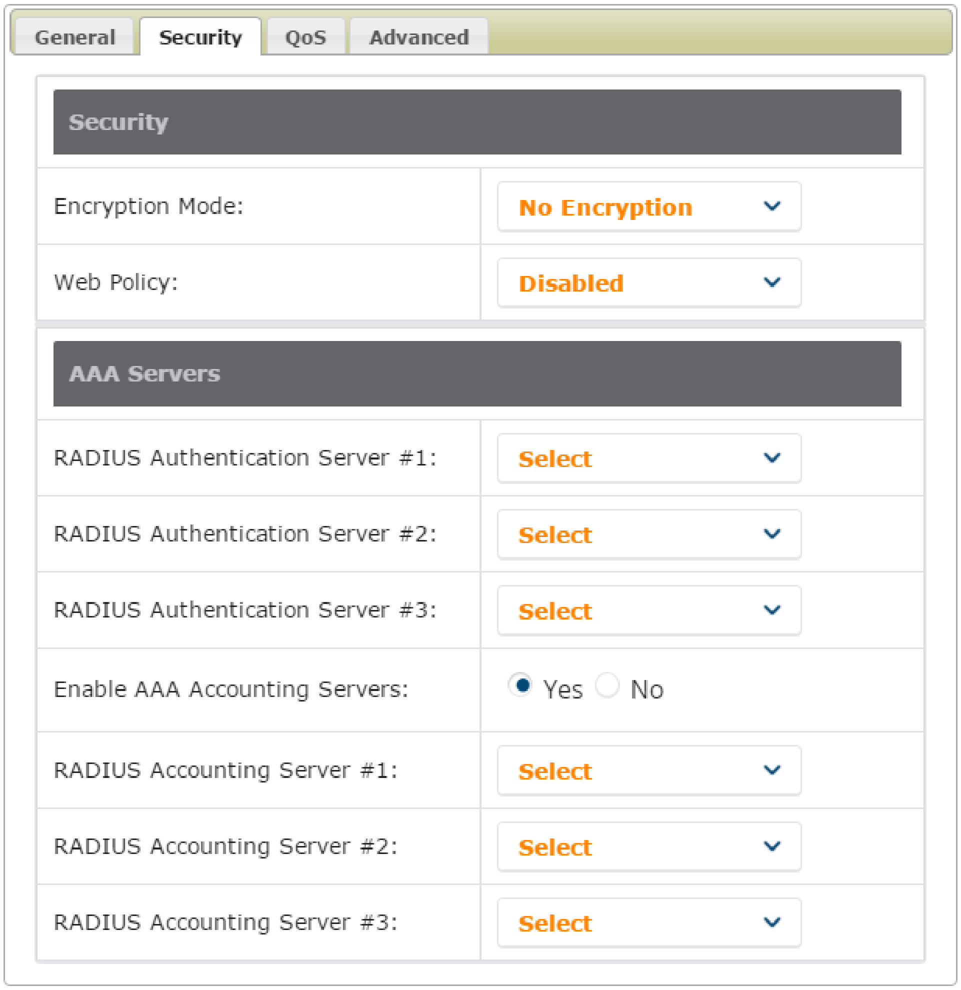
Figure 27: *Add New SSID/VLAN > General Tab Illustration*



General

Profile:	Enter a Value
SSID: If SSID is not specified, the profile name will be used as the SSID	Enter a Value
Type:	WLAN
Admin Status:	● Yes ○ No
Specify Interface Name:	● Yes ○ No
Interface:	management
Radio Policy:	All
Broadcast SSID:	○ Yes ● No

Figure 28: *Add New SSID/VLAN > Security Tab Illustration*



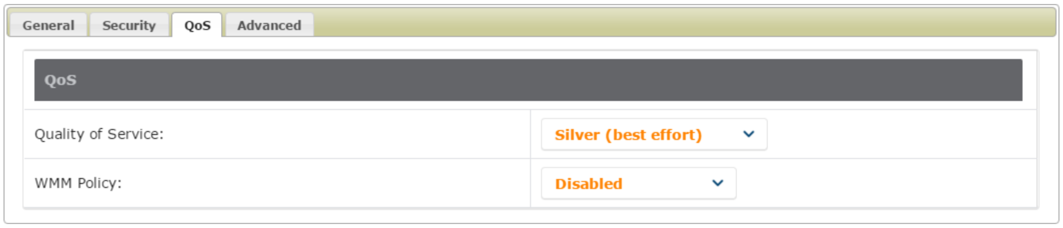
Security

Encryption Mode:	No Encryption
Web Policy:	Disabled

AAA Servers

RADIUS Authentication Server #1:	Select
RADIUS Authentication Server #2:	Select
RADIUS Authentication Server #3:	Select
Enable AAA Accounting Servers:	● Yes ○ No
RADIUS Accounting Server #1:	Select
RADIUS Accounting Server #2:	Select
RADIUS Accounting Server #3:	Select

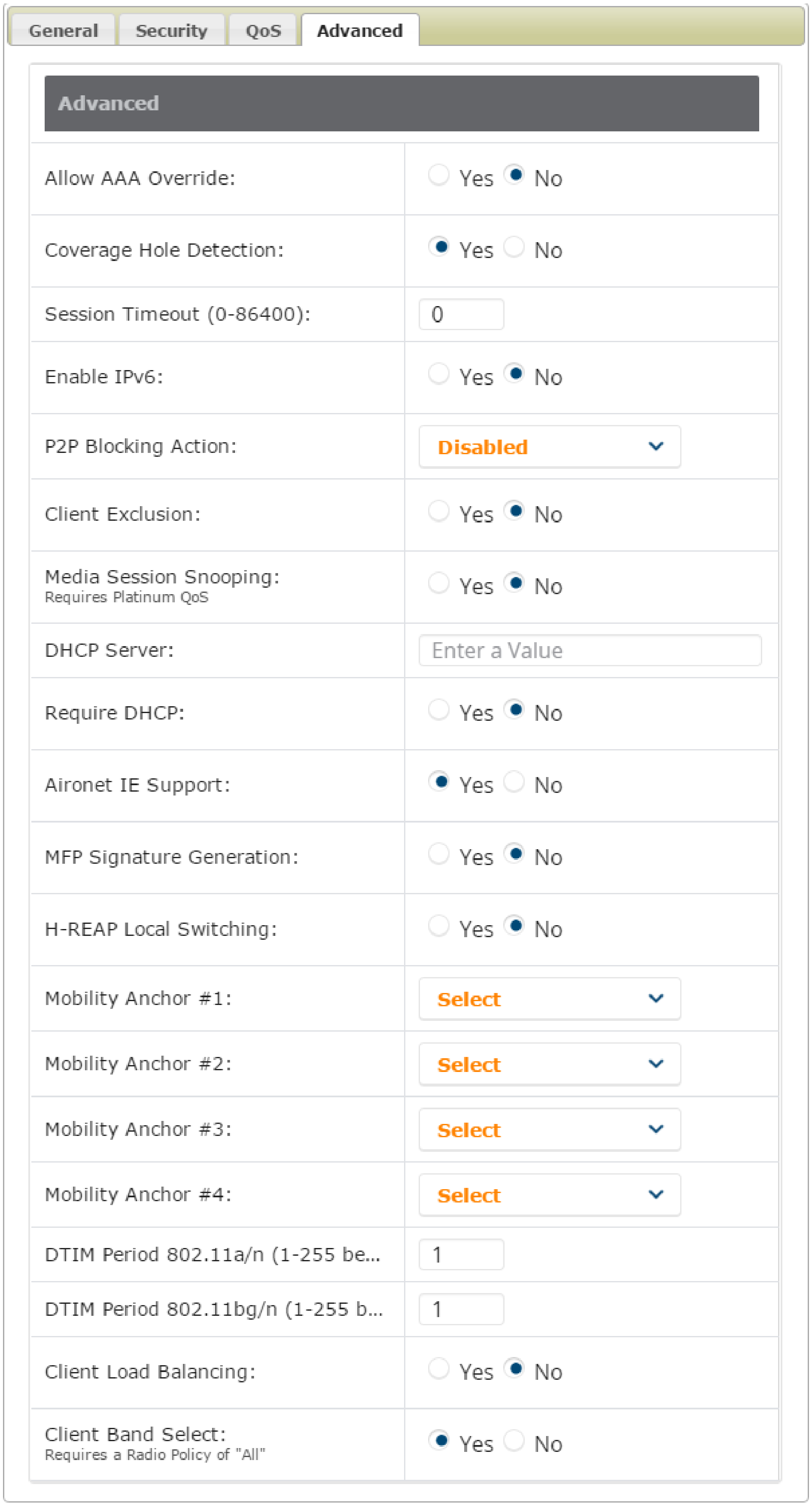
Figure 29: *Add New SSID/VLAN > QoS Tab Illustration*



QoS

Quality of Service:	Silver (best effort)
WMM Policy:	Disabled

Figure 30: *Add New SSID/VLAN > Advanced Tab Illustration*



Advanced

Allow AAA Override:	○ Yes ● No
Coverage Hole Detection:	● Yes ○ No
Session Timeout (0-86400):	0
Enable IPv6:	○ Yes ● No
P2P Blocking Action:	Disabled
Client Exclusion:	○ Yes ● No
Media Session Snooping: Requires Platinum QoS	○ Yes ● No
DHCP Server:	Enter a Value
Require DHCP:	○ Yes ● No
Aironet IE Support:	● Yes ○ No
MFP Signature Generation:	○ Yes ● No
H-REAP Local Switching:	○ Yes ● No
Mobility Anchor #1:	Select
Mobility Anchor #2:	Select
Mobility Anchor #3:	Select
Mobility Anchor #4:	Select
DTIM Period 802.11a/n (1-255 be...	1
DTIM Period 802.11bg/n (1-255 b...	1
Client Load Balancing:	○ Yes ● No
Client Band Select: Requires a Radio Policy of "All"	● Yes ○ No

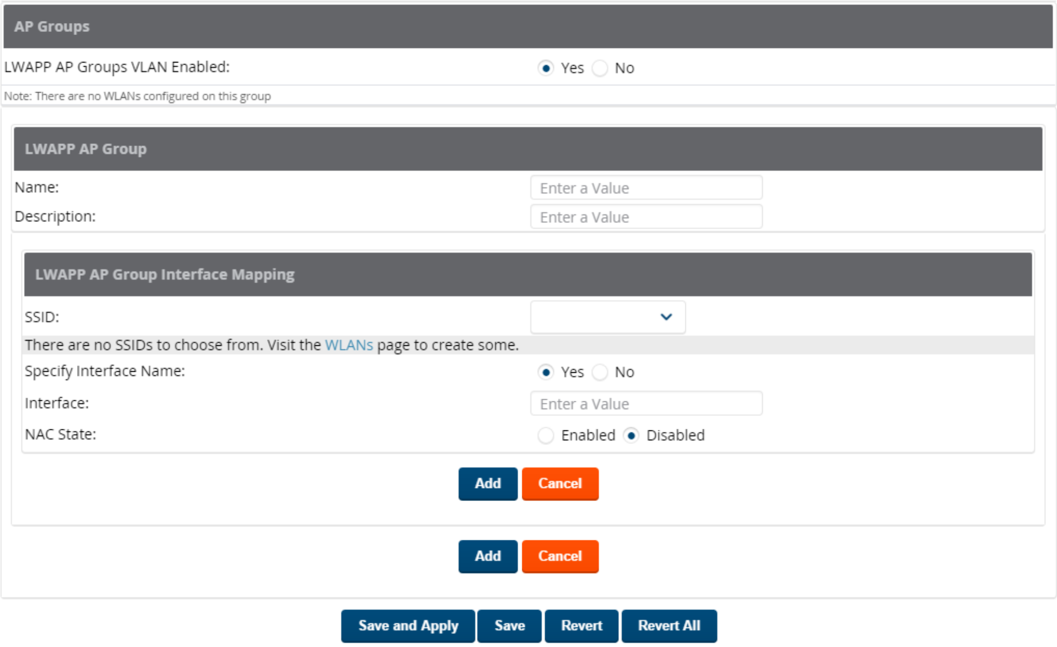
Defining and Configuring LWAPP AP Groups for Cisco Devices

The **Groups > Cisco WLC Config > WLANs > Advanced > AP Groups** page allows you to add/edit/delete AP Groups on the Cisco WLC. LWAPP AP Groups are used to limit the WLANs available on each AP. Cisco thin APs are assigned to LWAPP AP Groups.

Viewing and Creating Cisco AP Groups

1. Go to the **Groups > Cisco WLC Config** page, and select **WLANs > Advanced > AP Groups** in the navigation pane on the left side. This page displays the configured LWAPP APs. Figure 31 illustrates this page.

Figure 31: *Groups > Cisco WLC Config > WLANS > Advanced > AP Groups Page Illustration*



AP Groups

LWAPP AP Groups VLAN Enabled: ● Yes ○ No

Note: There are no WLANs configured on this group

LWAPP AP Group

Name: Enter a Value

Description: Enter a Value

LWAPP AP Group Interface Mapping

SSID:

There are no SSIDs to choose from. Visit the WLANs page to create some.

Specify Interface Name: ● Yes ○ No

Interface: Enter a Value

NAC State: ○ Enabled ● Disabled

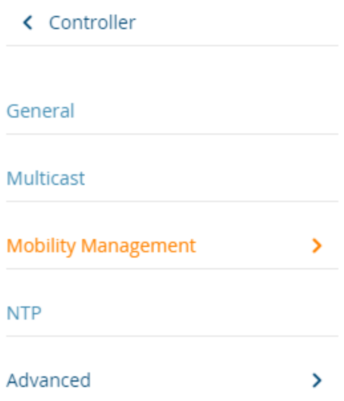
2. To add a new LWAPP AP group, select **Yes** in the **AP Groups** section. Additional controls appear.
3. Select **Add** to create a new LWAPP AP group. To edit an existing LWAPP AP group, select the pencil icon next to that group. Add one or more SSIDs and the interface/VLAN ID mapping on the **Add/Edit** page of the LWAPP AP Group.
4. Select **Save and Apply** to make these changes permanent, or select **Save** to retain these changes to be pushed to controllers at a later time.

Configuring Cisco Controller Settings

The **Groups > Cisco WLC Config > Controller** page defines general Cisco WLC settings, Multicast settings, Cisco mobility groups to be supported on Cisco controllers, Network Time Protocol (NTP), and Spanning Tree Protocol settings.

Go to the **Groups > Cisco WLC Config > Controller** page. This navigation is illustrated in Figure 32.

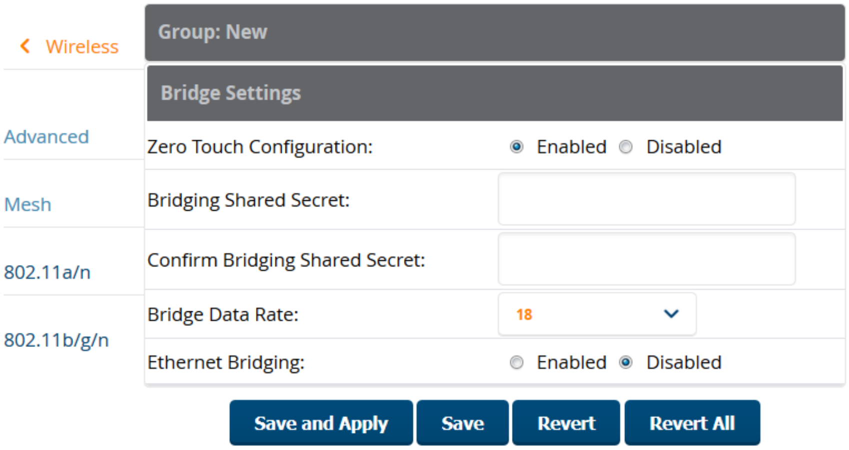
Figure 32: *Groups > Cisco WLC Config > Controller Navigation*



Configuring Wireless Parameters for Cisco Controllers

This section illustrates the configuration of **Wireless** settings in support of Cisco WLC controllers. Select a group with Cisco WLC devices, then navigate to **Groups > Cisco WLC Config**, expand the **Wireless** menu, then expand **Advanced**, **Mesh**, **802.11a/n** and **802.11 b/g/n** menus to display configuration settings for those categories. The navigation for Wireless settings is illustrated in Figure 33.

Figure 33: *Groups > Cisco WLC Config > Wireless Navigation Illustration*



Bridge Settings

Zero Touch Configuration:	● Enabled ○ Disabled
Bridging Shared Secret:	
Confirm Bridging Shared Secret:	
Bridge Data Rate:	18
Ethernet Bridging:	○ Enabled ● Disabled

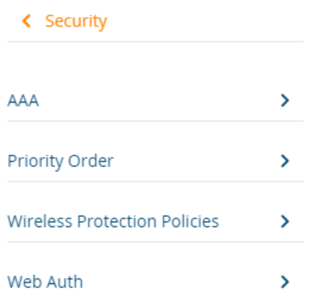
Configuring Cisco WLC Security Parameters and Functions

OV3600 enables you to configure many security settings that are specific to Cisco WLC controllers. This section supports four overriding types of configuration, as follows:

- **AAA**, to cover both RADIUS and TACACS+ server configuration
- **Priority Order**
- **Wireless Protection Policies**
- **Web Auth**

Figure 34 illustrates these components and this navigation:

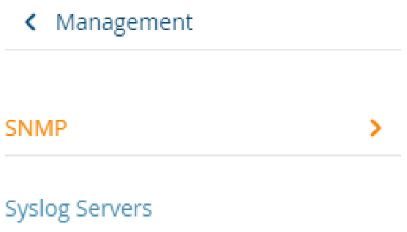
Figure 34: *Groups > Cisco WLC Config > Security Navigation Illustration*



Configuring Management Settings for Cisco WLC Controllers

OV3600 allows you to configure of SNMP and Syslog Server settings for Cisco WLC controllers. You can configure up to four trap receivers on the Cisco WLC including the OV3600 IP that can be used in Global Groups. To define SNMP and server settings, go to the **Groups > Cisco WLC Config > Management** page, illustrated in Figure 35.

Figure 35: *Groups > Cisco WLC Config > Management Navigation Illustration*



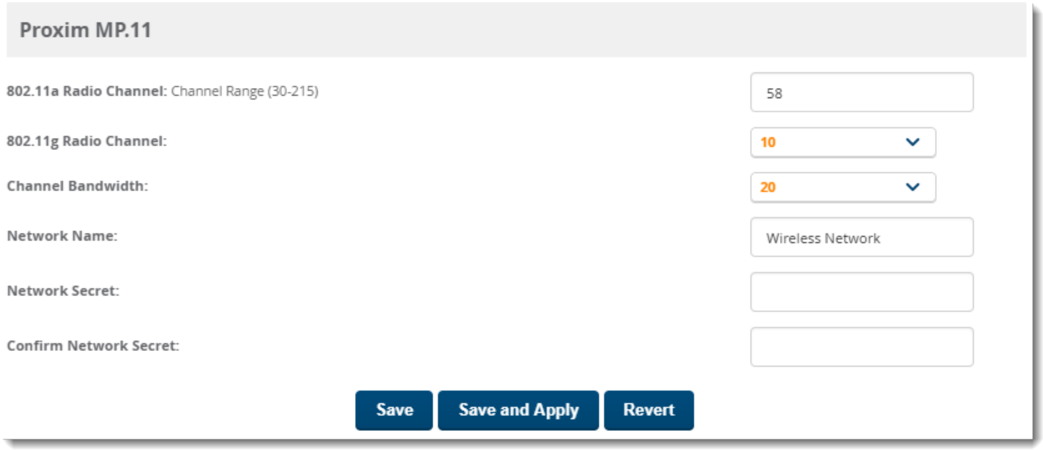
Configuring PTMP Settings for Device Groups

The **Groups > PTMP** configuration page configures Point-to-Multipoint (PTMP) for all subscriber and base stations in the device group. Subscriber stations must be in the same group as all base stations with which they might connect.

To configure these functions:

1. Go to the **Groups > List** page and select the group that supports Proxim MP.11. Alternatively, select **Add** from the **Groups > List** page to create a new group.
2. Select the **Groups > PTMP** from the navigation sidebar. Figure 36 illustrates this page.

Figure 36: *Groups > PTMP Page Illustration*



Proxim MP.11

802.11a Radio Channel: Channel Range (30-215) 58

802.11g Radio Channel: 10

Channel Bandwidth: 20

Network Name: Wireless Network

Network Secret:

Confirm Network Secret:

3. Define the settings on this page. Table 66 describes the settings and default values.

Table 66: *Groups > PTMP Fields and Default Values*

Setting	Default	Description
802.11a Radio Channel	58	Selects the channel used for 802.11a radios by the devices in this group.
802.11g Radio Channel	10	Selects the channel used for 802.11g radios by the devices in this group.
Channel Bandwidth	20	Defines the channel bandwidth used by the devices in this group.
Network Name	Wireless Network	Sets the Network name, with a range of length supported from two to 32 alphanumeric characters.
Network Secret	None	Sets a shared password to authenticate clients to the network.

4. Select **Save and Apply** when configurations are complete to make them permanent, or select **Save** to retain these settings prior to pushing to controllers later.

Configuring Proxim Mesh Radio Settings

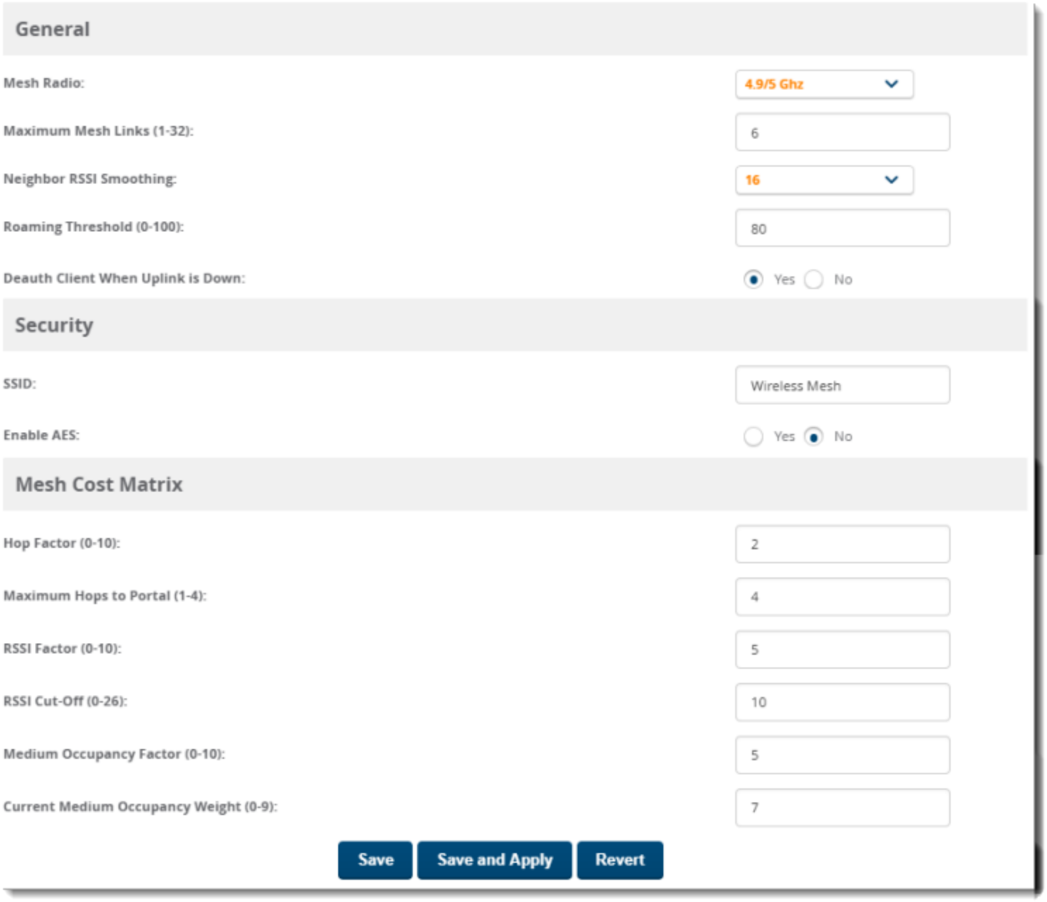
To configure mesh radio settings:

1. Go to the **Groups > Proxim Mesh** configuration page.
2. Define the settings as required for your network.
3. Do one of the following:

- Select **Save** when configurations are complete to retain these settings.
- Select **Save and Apply** to make the changes permanent.
- Select **Revert** to discard all unapplied changes.

Figure 37 illustrates this page. The tables that follow describe the settings and default values.

Figure 37: *Groups > Proxim Mesh Page*



General

Mesh Radio:	4.9/5 Ghz
Maximum Mesh Links (1-32):	6
Neighbor RSSI Smoothing:	16
Roaming Threshold (0-100):	80
Deauth Client When Uplink is Down:	● Yes ○ No

Security

SSID:	Wireless Mesh
Enable AES:	○ Yes ● No

Mesh Cost Matrix

Hop Factor (0-10):	2
Maximum Hops to Portal (1-4):	4
RSSI Factor (0-10):	5
RSSI Cut-Off (0-26):	10
Medium Occupancy Factor (0-10):	5
Current Medium Occupancy Weight (0-9):	7

The **General** section contains settings for mesh radio, number of mesh links, RSSI smoothing, roaming threshold and de-auth client.

Table 67: *General Fields and Default Values*

Setting	Default	Description
Mesh Radio	4.9/5Ghz	Drop-down selects the radio that acts as the backhaul to the network.
Maximum Mesh Links (1-32)	6	Sets the maximum number of mesh links allowed on an AP. This number includes the uplink to the portal as well as downlinks to other mesh APs.
Neighbor RSSI Smoothing	16	Specifies the number of beacons to wait before switching to a new link.
Roaming Threshold (0-100)	80	Specifies the difference in cost between two paths that must be exceeded before the AP roams. To switch to a new path it must have a cost that is less by at least the roaming threshold. A high threshold results in fewer mesh roams.
Deauth Client when Uplink is Down	Yes	With **Yes** selected, clients have authentication removed (are deauthenticated) if the uplink is lost.

The **Security** section contains settings for SSID and enabling AES encryption.

Table 68: *Security Fields and Default Values*

Setting	Default	Description
SSID	None	Sets the SSID used by the Mesh Radio to connect to the mesh network.
Enable AES	No	Enable or disable AES encryption.
Shared Secret	None	Specify a shared secret if **Enable AES** is **Yes**.

The **Mesh Cost Matrix** configuration section contains settings for hop factor and maximum hops to portal, RSSI factor and cut-off, medium occupancy factor and current medium occupancy weight. Adjust these settings as required for your network. Table 69 describes these settings and default values.

Table 69: *Mesh Cost Matrix Fields and Default Values*

Setting	Default	Description
Hop Factor (1-10)	5	Sets the factor associated with each hop when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
Maximum Hops to Portal (1-4)	4	Set the maximum number of hops for the AP to reach the Portal AP.
RSSI Factor (0-10)	5	Sets the factor associated with the RSSI values used when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
RSSI Cutoff (0-26)	10	Specifies the minimum RSSI needed to become a mesh neighbor.
Medium Occupancy Factor (0-10)	5	Sets the factor associated with Medium Occupancy when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
Current Medium Occupancy Weight (0-9)	7	Specifies the importance given to the most recently observed Medium Occupancy against all of the previously viewed medium occupancies. Lower values place more importance on previously observed Medium Occupancies.

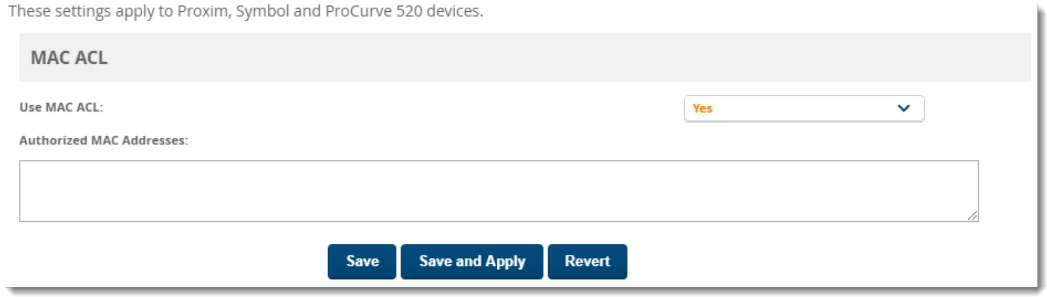
Configuring Group MAC ACLs for Device Groups

If you use Symbol, Proxim, or ProCurve 520WL wireless access points, you can specify the MAC addresses of devices that are permitted to associate with APs in the Group. Other devices are not able to associate to APs in the Group, even if the users of those devices are authorized users on the network.

To enable MAC ACL:

1. Browse to the **Groups > MAC ACL** configuration page. Figure 38 illustrates this page.

Figure 38: *Groups > MAC ACL Page*



These settings apply to Proxim, Symbol and ProCurve 520 devices.

MAC ACL

Use MAC ACL: Yes

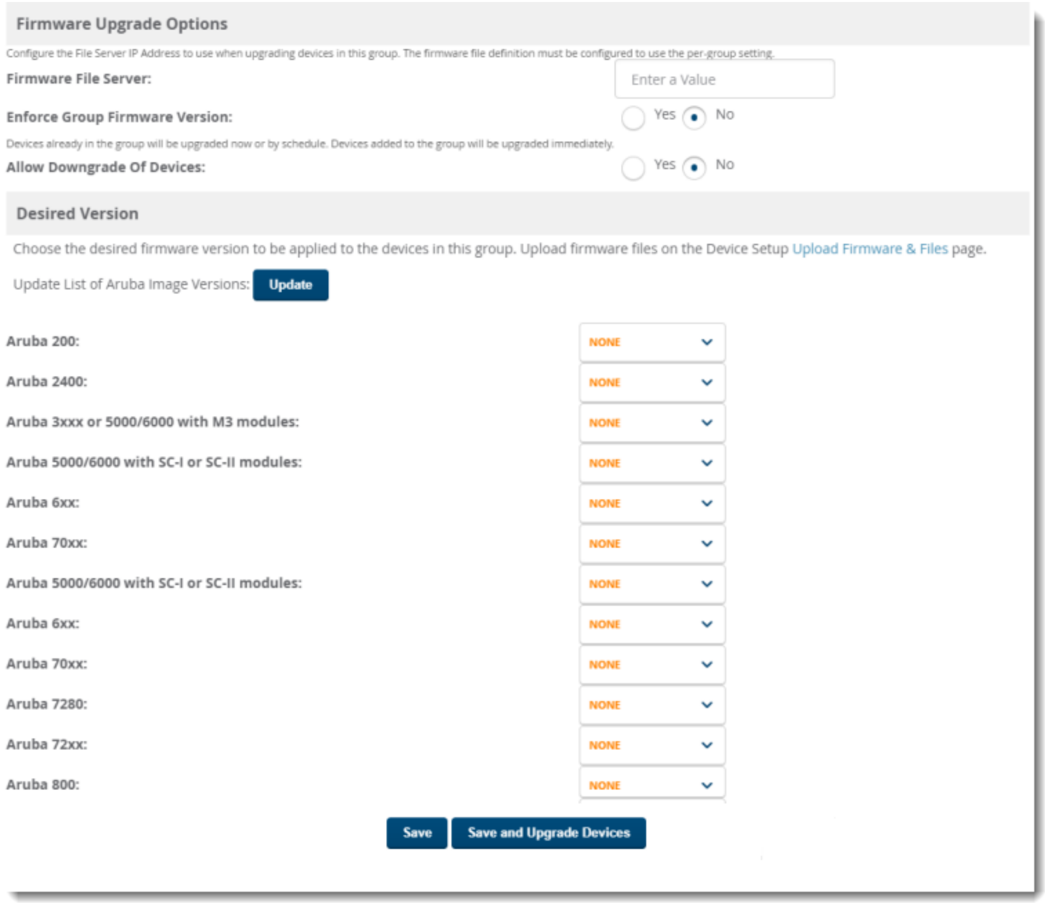
Authorized MAC Addresses:

2. Select **Yes** on the **Use MAC ACL** drop-down menu.
3. Type all authorized MAC addresses, separated by white spaces.
4. Select **Save** when configurations are complete to retain these settings, or select **Save and Apply** to make the changes permanent. Alternatively, select **Revert** to cancel your changes.

Specifying the Minimum Firmware Version for Device Groups

OV3600 automatically upgrades all eligible devices in a device group when you set the minimum firmware version on the **Groups > Firmware** page. When you add devices to the device group later, you must upgrade the firmware on those devices manually.

Figure 39: *Groups > Firmware Page*



Firmware Upgrade Options

Configure the File Server IP Address to use when upgrading devices in this group. The firmware file definition must be configured to use the per-group setting.

Firmware File Server: Enter a Value

Enforce Group Firmware Version: ○ Yes ● No

Devices already in the group will be upgraded now or by schedule. Devices added to the group will be upgraded immediately.

Allow Downgrade Of Devices: ○ Yes ● No

Desired Version

Choose the desired firmware version to be applied to the devices in this group. Upload firmware files on the Device Setup Upload Firmware & Files page.

Update List of Aruba Image Versions:

Aruba 200: NONE

Aruba 2400: NONE

Aruba 3xxx or 5000/6000 with M3 modules: NONE

Aruba 5000/6000 with SC-I or SC-II modules: NONE

Aruba 6xx: NONE

Aruba 70xx: NONE

Aruba 5000/6000 with SC-I or SC-II modules: NONE

Aruba 6xx: NONE

Aruba 70xx: NONE

Aruba 7280: NONE

Aruba 72xx: NONE

Aruba 800: NONE

To set the minimum firmware version for a device group:

1. Navigate to **Groups > Firmware** .

2. For each device type in the group, specify the minimum acceptable firmware version. If no firmware versions are listed, go to **Device Setup > Upload Firmware & Files** to upload the firmware files to OV3600.
3. Select **Upgrade** to apply firmware preferences to devices in the group. The device types that display will vary based on the device types that were selected on the **Groups > Basic** page.
4. Select **Save** to save the firmware file as the desired version for the group.
5. If you have opted to assign an external TFTP server on a per-group basis on the **Device Setup > Upload Firmware & Files** configuration page, you can enter the IP address in the **Firmware Upgrade Options** field on the top of this configuration page.
6. Once you have defined your first group, you can configure that group to be the default group on your network. When OV3600 discovers new devices that need to be assigned to a management group, the default group appears at the top of all drop-down menus and lists. Newly discovered devices are place automatically in the default group if OV3600 is set to automatically monitor/manage new devices.
7. Browse to the **OV3600 Setup > General** page.
8. In the **General** section, select the desired group from the **Default Group** drop down menu to make it the default.

NOTE

For more information about loading firmware on to an OV3600 server, see "Uploading Firmware and Files" on page 55.

Comparing Device Groups

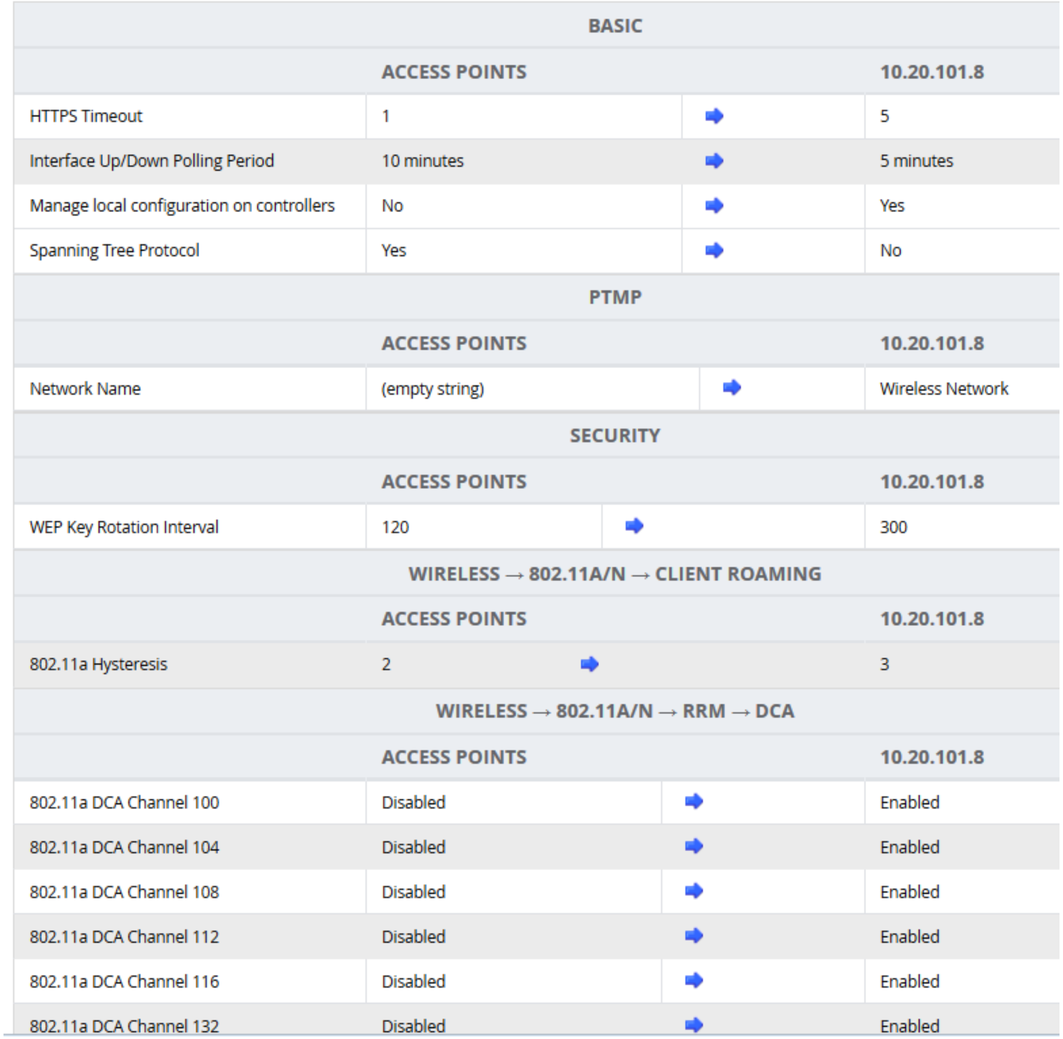
You can compare two existing device groups with a detailed line-item comparison. Group comparison allows several levels of analysis including the following:

- Compare performance, bandwidth consumption, or troubleshooting metrics between two groups.
- Debug one device group against the settings of a similar and better performing device group.
- Use one group as a model by which to fine-tune configurations for additional device groups.

This topic presumes that at least two device groups are at least partly configured in OV3600, each with saved configurations. Perform the following steps to compare two existing device groups:

1. From the **Groups > List** page, select the **Compare two groups** link. Two drop-down menus appear.
2. Select the two groups to compare in the drop-down menus, and select **Compare**. The **Compare** page appears, displaying some or many configuration categories. Figure 40 illustrates this page.

Figure 40: *Comparing Two Devices Groups on the* ***Groups > List > Compare*** *Page (Partial View)*



	BASIC		
	ACCESS POINTS		10.20.101.8
HTTPS Timeout	1	➡	5
Interface Up/Down Polling Period	10 minutes	➡	5 minutes
Manage local configuration on controllers	No	➡	Yes
Spanning Tree Protocol	Yes	➡	No
	PTMP		
	ACCESS POINTS		10.20.101.8
Network Name	(empty string)	➡	Wireless Network
	SECURITY		
	ACCESS POINTS		10.20.101.8
WEP Key Rotation Interval	120	➡	300
	WIRELESS → 802.11A/N → CLIENT ROAMING		
	ACCESS POINTS		10.20.101.8
802.11a Hysteresis	2	➡	3
	WIRELESS → 802.11A/N → RRM → DCA		
	ACCESS POINTS		10.20.101.8
802.11a DCA Channel 100	Disabled	➡	Enabled
802.11a DCA Channel 104	Disabled	➡	Enabled
802.11a DCA Channel 108	Disabled	➡	Enabled
802.11a DCA Channel 112	Disabled	➡	Enabled
802.11a DCA Channel 116	Disabled	➡	Enabled
802.11a DCA Channel 132	Disabled	➡	Enabled

3. Note the following factors when using the **Compare** page:
   - The **Compare** page can be very long or very abbreviated, depending on how many configurations the device groups share or do not share.
   - When a configuration differs between two groups, the setting is flagged in red text for the group on the right.
   - The default setting of the **Compare** page is to highlight settings that differ between two groups.
     - To display settings that are similar or identical between two device groups, select **Show Similar Fields** at the top left of the page. The result may be a high volume of information.
     - Select **Hide Similar Fields** to return to the default display, emphasizing configuration settings that differ between two groups.
   - You can change the configuration for either or both groups by selecting **Edit** in the corresponding column heading. The appropriate configuration page appears.
   - If you make and save changes to either or both groups, go back to the **Groups > List** page and select **Compare two groups**. Select the same two groups again for updated information.
   - Additional topics in this document describe the many fields that can appear on the **Groups > List > Compare** page.

Deleting a Group

Perform the following steps to delete an existing Group from the OV3600 database:

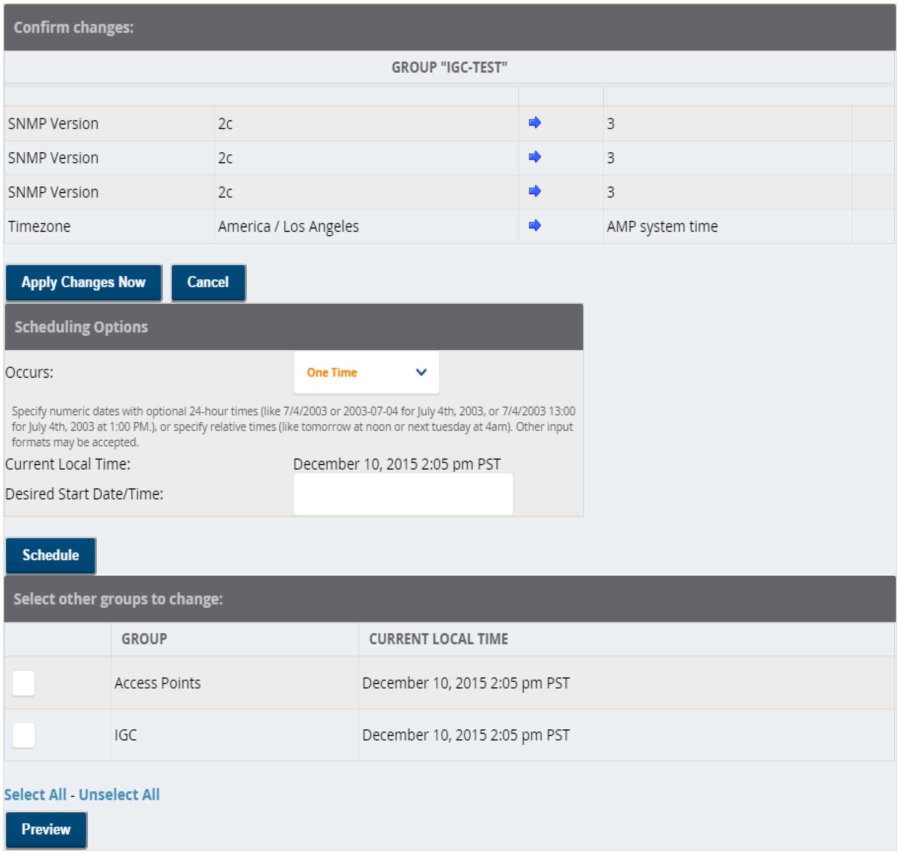
1. Browse to the **Groups > List** configuration page.
2. Ensure that the group you wish to delete is not marked as the **default** group. (See the **OV3600 Setup > General** page.) OV3600 does not permit you to delete the current default group.
3. Ensure that there are no devices in the group that you want to delete. OV3600 does not permit you to delete a group that still contains managed devices. You must move all devices to other groups before deleting a group.
4. Ensure that the group is not a global group that has subscriber groups, and is not a group that was pushed from a Master Console. OV3600 will not delete a group in which either of those cases is true.
5. Select the checkbox, and click the **Delete** button.

Changing Group Configurations

Perform the following steps to make any changes to an existing group's configuration:

1. Browse to the **Groups > List** configuration page.
2. Select the **Modify** button (the wrench icon) for the group you wish to edit. The **Groups > Basic** configuration page appears.
3. Select the fields to be edited on the **Basic** configuration page. Other group configuration pages may be available, depending upon the type of devices included in that group. or go to **Radio**, **Security**, **VLANs**, or **MAC ACL** configuration page and edit the fields. Use the **Save** button to store the changes prior to applying them.
4. When all changes for the group are complete select the **Save and Apply** button to make the changes permanent. Figure 41 illustrates the confirmation message that appears.

Figure 41: *Groups > Basic Configuration Change Confirmation Page Illustration*



Confirm changes:

GROUP "IGC-TEST"			
SNMP Version	2c	➡	3
SNMP Version	2c	➡	3
SNMP Version	2c	➡	3
Timezone	America / Los Angeles	➡	AMP system time

Scheduling Options

Occurs: One Time

Specify numeric dates with optional 24-hour times (like 7/4/2003 or 2003-07-04 for July 4th, 2003, or 7/4/2003 13:00 for July 4th, 2003 at 1:00 PM.), or specify relative times (like tomorrow at noon or next tuesday at 4am). Other input formats may be accepted.

Current Local Time: December 10, 2015 2:05 pm PST

Desired Start Date/Time:

Select other groups to change:

	GROUP	CURRENT LOCAL TIME
□	Access Points	December 10, 2015 2:05 pm PST
□	IGC	December 10, 2015 2:05 pm PST

5. OV3600 displays a **Configuration Change** screen confirming the changes that will be applied to the group's settings.
6. There are several action possibilities from within this confirmation configuration page.
   - **Apply Changes Now** — Applies the changes immediately to access points within the group. If you wish to edit multiple groups, you must use the **Preview** button.

NOTE

You cannot apply Alcatel-Lucent Config changes to other groups. If the only changes on the configuration page are to Alcatel-Lucent devices, the list of groups and the preview button will not appear.

   - **Scheduling Options** — Schedules the changes to be applied to this group in the future. Enter the desired change date in the **Start Date/Time field**. You can also specify if this is a one-time schedule or a recurring schedule. Recurring options are **Daily**, **Weekly**, **Monthly**, and **Annually**. OV3600 takes the time zone into account for the group if a time zone other than OV3600 System Time has been configured on the **Groups > Basic** configuration page.
   - **Cancel** — Cancels the application of changes (immediately or scheduled).

NOTE

To completely nullify the change request, select **Revert** on one of the group configuration pages after you have selected **Cancel**.

7. Apply changes to multiple groups by selecting the appropriate group or groups and selecting **Preview**.

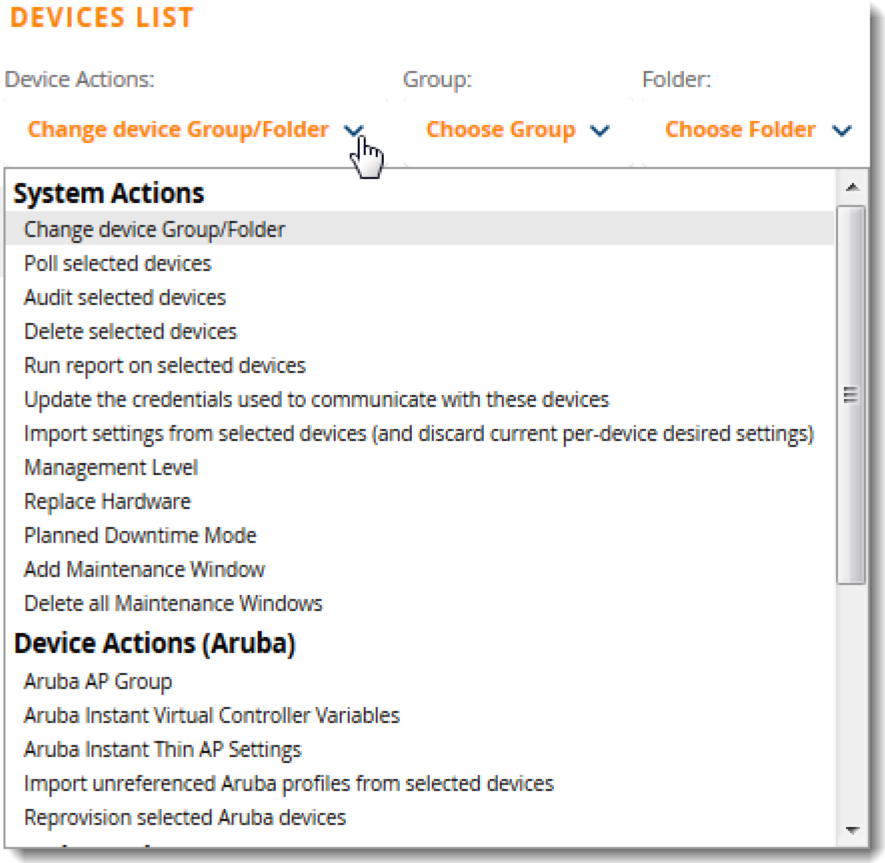
Modifying Multiple Devices

OV3600 provides a Modify Devices tool that enables you to make bulk changes to devices, including switches that have thin APS. Some of the device actions you can make include deleting multiple devices, migrating devices to another group or folder, updating credentials, and optimizing channels.

To modify multiple devices:

1. Navigate to one of the following pages that has a Device List:
   - **Devices > List**. You can also click the Up, Down, Mismatched hyperlinks on the List page to open monitoring pages for the devices with those devices states.
   - **Groups > Monitor**.
2. Click ✎ at the top right corner of the device list, then select the devices you want to modify.
3. Select as many changes as you want from the Device Actions drop-down menu.

Figure 42: *Selecting the Device Actions*


DEVICES LIST
Device Actions:
Group:
Folder:
Change device Group/Folder
Choose Group
Choose Folder
System Actions
Change device Group/Folder
Poll selected devices
Audit selected devices
Delete selected devices
Run report on selected devices
Update the credentials used to communicate with these devices
Import settings from selected devices (and discard current per-device desired settings)
Management Level
Replace Hardware
Planned Downtime Mode
Add Maintenance Window
Delete all Maintenance Windows
Device Actions (Aruba)
Aruba AP Group
Aruba Instant Virtual Controller Variables
Aruba Instant Thin AP Settings
Import unreferenced Aruba profiles from selected devices
Reprovision selected Aruba devices

4. Click **Apply All**.

Table 70 describes the changes you can apply to multiple devices at the same time.

Table 70: *Modify Multiple Devices Section Fields and Default Values*

Action	Description
System Actions	

Table 70: *Modify Multiple Devices Section Fields and Default Values (Continued)*

Action	Description
Change Device Group/Folder	Move the selected devices to a new group or folder. If the device is in managed mode when it is moved to a new group, it will be reconfigured. When you select this option, you must also click the **Group** and/or **Folder** drop down menu and select the destination group or folder for the devices. Click **Move** and then select **Apply All** to save your changes.
Poll selected devices	Click **Poll Now** to poll selected devices for current user count and bandwidth data. This action overrides default poll settings for the group. Polling numerous devices may create a temporary performance load on your OV3600 server.
Audit selected devices	Fetches the current configuration from the device and compares it to the desired OV3600 configuration. The audit action updates the Configuration Status. **NOTE:** If a group has audit disabled for its devices, OV3600 does not show the **Audit** button in the **Modify devices** list.
Delete selected devices	Click **Delete** to remove the selected devices from OV3600. A new window opens and asks you to confirm your changes. Select **Apply Changes Now**. The deletions will be performed in the background and it may take a minute to remove the selected devices from the list.
Run report on selected devices	Takes you to the **Reports > Definitions** page where you can define or run a custom report for selected devices. For more details and a procedure, see "Creating Custom Reports" on page 348.
Update the credentials used to communicate with these devices	**Update** changes the credentials OV3600 uses to communicate with the device. It does *not* change the credentials on the AP.
Import settings from selected devices (and discard current pre-device desired settings)	Audit updates a number of the AP-specific settings that OV3600 initially read off of the AP including channel, power, antenna settings and SSL certifications. OV3600 recommends using this setting if APs have been updated outside of OV3600. Most settings on the **Devices > Manage** configuration page are set to the values currently read off of the devices.
Management Level	When you select this action, you must select either **Monitor Only + Firmware Upgrade** or **Manage Read/Write** to choose new the management level for the devices.
Replace Hardware	Select the down device that will be replaced and view the list of OV3600 devices that match the name or IP address of the selected device. The down devices can be replaced with any device in the **New Devices** list or in the current folder or group.
Planned Downtime Mode	When you select this action, you must select either **Enable** or **Disable** to change the downtime mode for the selected devices. When this option is enabled, the selected devices are put into Planned Maintenance mode. When this mode is enabled, no AP Down triggers will be deployed on these devices. Users will not be able to delete folders that contain devices in Planned Maintenance. The devices in Planned Maintenance will show the Up status, but will not be tracked in historical graphs and logs as Up.

Table 70: *Modify Multiple Devices Section Fields and Default Values (Continued)*

Action	Description
Add Maintenance Window	Automate the manual action of putting the selected devices into Manage mode at once so that changes can be applied, and after the maintenance period is over, the devices automatically revert to Monitor-Only mode. Maintenance windows can be set as a one-time or recurring event.
Delete all Maintenance Windows	Deletes all maintenance windows set for these devices.
Device Actions (Alcatel-Lucent)	
Alcatel-Lucent AP Group	When you select this option then click Update Alcatel-Lucent AP Group, a new window opens that allows you to assign the devices to a new AP group.
Alcatel-Lucent Instant Virtual Controller Variables	Opens the Variable Editor page for selected Alcatel-Lucent Instant APs.
Import unreferenced Alcatel-Lucent profiles from selected devices	Select the devices that include unreferenced profiles, then click this button to import those profiles from the selected devices.
Reprovision selected Alcatel-Lucent devices	Configures the switch to send provisioning parameters such as radio, antenna, and IP address settings to the selected APs. Please note that APs will be rebooted as part of reprovisioning.
Device Actions	
Rename devices	Rename all the selected devices in bulk. Note that you can also rename the devices one at a time using the editable Name fields in each row.
Upgrade firmware for selected devices	Upgrades firmware for the selected devices. Refer to the firmware upgrade help under **Devices > Manage** configuration page for detailed help on Firmware job options.
Cancel firmware upgrade for selected devices	Cancels any firmware upgrades that are scheduled or in progress for the selected APs.
Reboot selected devices	Reboots the selected devices. Use caution when rebooting devices because this can disrupt wireless users.
Factory reset	Resets the selected devices back to factory-default settings.
Desired Radio Status	Enables or disables the radios on the selected device. This parameter does *not* apply to Cisco IOS APs.
Cisco Thin AP Settings	Bulk configuration for per-thin AP settings, previously configured on the **Group LWAPP AP** tab, can be performed from **Modify Devices** on the **Devices > List** page. Make changes to LWAPP AP groups, including the option that was under Modify Devices.

Using Global Groups for Group Configuration

The OV3600 group configuration feature allows you to push configurations defined on a global group to the managed groups subscribed to that global group.

About Global Group Membership

To have Global Group status, a group must contain no devices; accordingly, access points can never be added to a Global Group. Global groups are visible to users of all roles, so they may not contain devices, which can be made visible only to certain roles. illustrates the **Groups > List** page.

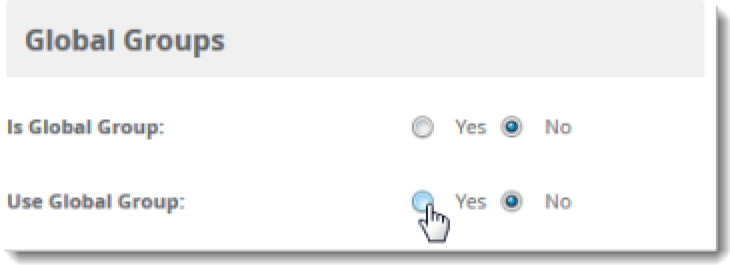
Creating a Global Group

The Use Global Group option becomes available when you have at least two groups configured in OV3600. You can configure OV3600 to push a group configuration to a group when you enable this option.

To configure a global group:

1. Navigate to **Groups > List**.
2. Select a the group from the list.
3. Navigate to **Groups > Basic**. The **Global Groups** section of this page contains the **Use Global Group** option.
4. Select **Yes** for the **Use Global Group** option.

Figure 43: *Selecting the Use Global Group Option*



Global Groups

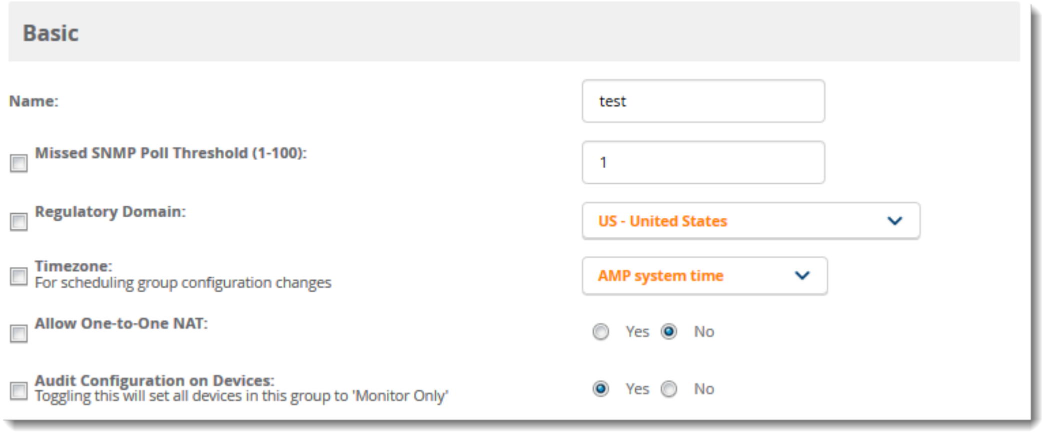
Is Global Group: ○ Yes ● No

Use Global Group: ○ Yes ● No

5. To associate the group with a global group, select the group from the Global Group drop-down menu.
6. Click **Save and Apply**.
7. Click **Apply Changes Now**.

When the Groups list is updated with the global group, you will see **Yes** in the "Is Global Group" column, and when you go to the Basic page for the global group, there will be checkboxes next to the basic settings. Figure 44 shows an example for a global group called "test".

Figure 44: *Basic Settings for the Global Group*



Basic

Name:	test
□ Missed SNMP Poll Threshold (1-100):	1
□ Regulatory Domain:	US - United States
□ Timezone: For scheduling group configuration changes	AMP system time
□ Allow One-to-One NAT:	○ Yes ● No
□ Audit Configuration on Devices: Toggling this will set all devices in this group to 'Monitor Only'	● Yes ○ No

When OV3600 pushes a global group configuration to subscriber groups, all settings are static except for those with the checkbox selected; you can change the value or setting of the checked field on the corresponding tab for each managed group. In the case of the **Groups > SSIDs** configuration page, override options are available only on the **Add** configuration page (go to the **Groups > SSIDs** configuration page and select **Add**).

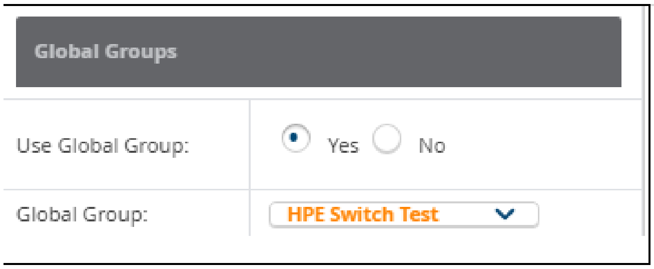
Global templates are also configurable as part of global groups; for more information, see "Creating and Using Templates" on page 223.

Subscribing other Groups to a Global Group

Once one or more global groups have been configured, other groups may subscribe to a particular Global Group. To subscribe a (non-global) group to a Global Group:

1. Navigate to **Groups > List**.
2. Select a the group from the **Groups** table.
3. Navigate to **Groups > Basic**.
4. In the **Global Groups** section of this page, click the **Global Group** drop-down list and select a global group.
5. Select **Save and Apply** to make the changes permanent.

Figure 45: *Subscribe to a Global Group*



Global Groups

Use Global Group:	● Yes ○ No
Global Group:	HPE Switch Test

Once the configuration is pushed, the unchecked fields from the Global Group appears on the Subscriber Group as static values and settings. Only fields that had the override checkbox selected in the Global Group appear as fields that can be set at the level of the Subscriber Group. Any changes to a static field must be made on the Global Group.

NOTE

If you want to change a global group into a regular group and it has subscribers, you need to remove the subscribers first before you can change the "Is Global Group" option to **No** on the **Groups > Basic** page.

Chapter 4
Discovering, Adding, and Auditing Devices

This chapter describes the steps you should perform after you have deployed OV3600 on the network. The following sections describe:

- "How to Set Up Device Discovery" on page 120
- "Adding Devices into " on page 1
- "Verifying the Device Configuration" on page 126
- "Setting the Management Mode" on page 127
- "Ignoring Discovered Devices" on page 128
- "Troubleshooting a Newly Discovered Down Device" on page 129

How to Set Up Device Discovery

In order for OV3600 to discover devices on your network, you must first enable SNMP/HTTP scanning from the **Device Setup > Discover** page and then configure SNMP/HTTP scanning.

NOTE

This page is only visible to users with the OV3600 Administrator role or roles that have **Allow authorization of Devices** enabled in **OV3600 Setup > Roles.**

This process includes:

- "Adding Networks for SNMP/HTTP Scanning" on page 120
- "Adding Credentials for Scanning" on page 121
- "Defining a Scan Set" on page 122
- "Running a Scan Set" on page 122

Adding Networks for SNMP/HTTP Scanning

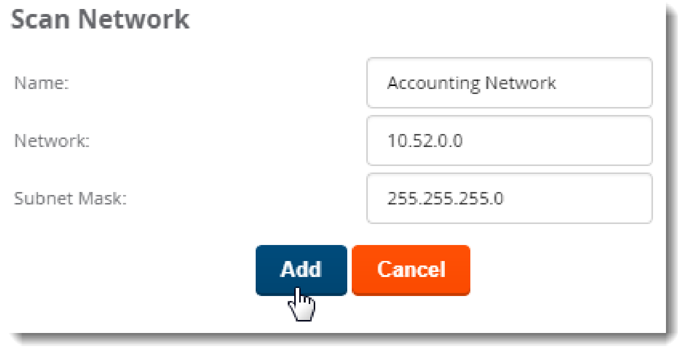
The first step when enabling SNMP/HTTP scanning for devices is to define the network segments to be scanned.

To add networks for SNMP/HTTP scanning:

1. Go to the **Device Setup > Discover** page.
2. Scroll down to the **Networks** section, and click **Add**.
3. Enter a network name.
4. Enter the IP network range to be scanned. Or, enter the first IP address on the network.
5. Enter the network subnet mask. The largest subnet OV3600 supports is 255.255.255.0.
6. Click **Add**.

Figure 46 shows an example of adding a scan network called Accounting Network, where the network IP address is 10.52.0.0, and the subnet mask is 255.255.255.0.

Figure 46: *Adding a Scan Network*



Scan Network

Name: Accounting Network

Network: 10.52.0.0

Subnet Mask: 255.255.255.0

OV3600 displays all network segments in the **Network** section of the **Device Setup > Discover** page.

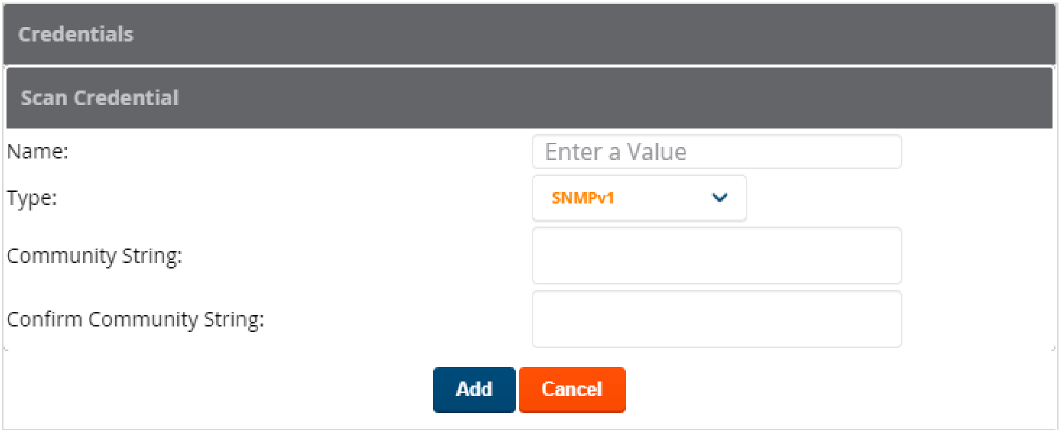
Adding Credentials for Scanning

The next step in SNMP/HTTP device discovery is to define the scan credentials that govern scanning of a given network. New devices inherit scan credentials from the System Credentials that you configure on the **Device Setup > Communications** page.

Perform these steps to define scan credentials for SNMP/HTTP scanning:

1. Locate the **Credentials** section on the **Device Setup > Discover** page. (Scroll down if necessary.) This page displays scan sets, networks, and credentials that have been configured so far, and allows you to define new elements for device scanning.
2. To create a new scan credential, select the **Add button to add a new scan credential**. Figure 47 illustrates this page. (Note that you may have to scroll down the page again to view this section.)

Figure 47: *Device Setup > Discover > Add/Edit New Scan Credential Section Illustration*



Credentials

Scan Credential

Name: Enter a Value

Type: SNMPv1

Community String:

Confirm Community String:

3. Enter a name for the credential in the **Name** field (for example, **Default**). This field supports alphanumeric characters (both upper and lower case), blank spaces, hyphens, and underscore characters.
4. Choose the type of scan to be completed (**SNMPv1, SNMPv2,** or **HTTP**). In most cases, perform scans using SNMP for device discovery, but consider the following factors in your decision:
   - SNMPv1 and SNMP v2 differ between in their supported traps, supported MIBs, and network query elements used in device scanning.
   - HTTP discovers devices using the HyperText Transfer Protocol in communications between servers and additional network components. HTTP is not as robust in processing network events as is SNMP, but HTTP may be sufficient, simpler, or preferable in certain scenarios.

a. If you selected SNMPv1 or SNMPv2, then define and confirm the **Community String** to be used during scanning. In this section, the community string used can be either read-only or read/write because OV3600 only uses it for discovering devices. To bring devices under management, OV3600 uses the credentials supplied in the **Device Setup > Communication SNMP** section. Once the device is authorized, it will use the non-scanning credentials.

b. If you selected HTTP for the type, then enter a user name and password for the scan credentials.

NOTE

OV3600 automatically appends the type of scan (SNMP or HTTP) to the Label.

5. Select **Add** after you have completed the previous steps. The **Device Setup > Discover** page displays the new scan credential or credentials just created or edited.
6. Repeat these steps to add as many credentials as you require.
7. Once scan networks and scan credentials are defined, combine them by creating scan sets using the next procedure: "Defining a Scan Set" on page 122.

Defining a Scan Set

After you have defined at least one network and one scan credential, you can create a scan set that combines the two for device discovery.

To create a scan set.

1. Locate the **Scan Set** area at the top of the **Device Setup > Discover** page.
2. Select **Add New Scan Set** to see all scan components configured so far. If you wish to create a new network, or new scanning credentials, you can select **Add** in either of these fields to create new components prior to creating a scan set.
3. Select the network(s) to be scanned and the Credential(s) to be used. OV3600 defines a unique scan for each Network-Credential combination.
4. In the **Automatic Authorization** section, select whether to override the global setting in **OV3600 Setup > General** and have New Devices be automatically authorized into the New Device List, the same Group/Folder as the discovering devices, the same Group/Folder as the closest IP neighbor, and/or a specified auto-authorization group and folder.
5. Select **Add** to create the selected scans, which then appear in a list at the top of the **Device Setup > Discover** page.
6. To edit an existing scan, select the **pencil** icon next to the scan on the **Device Setup > Discover** page.
7. When ready, proceed to the next task, "Running a Scan Set" on page 122.

NOTE

Scheduling an HTTP scan to run daily on your network can help you to discover rogues. Some consumer APs, like most D-Link, Linksys, and NetGear models, do not support SNMP and are found only on the wired side with an HTTP scan. These devices are discovered only if they have a valid IP address. Proper credentials are not required to discover these APs. Wireless scans discover these rogues without any special changes.

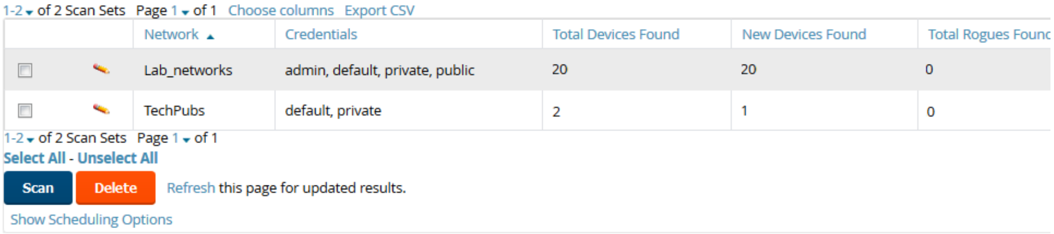
Running a Scan Set

Once a scan has been defined on the **Device Setup > Discover** page, OV3600 can now scan for devices.

To run a scan set:

1. Browse to the **Device Setup > Discover** page and locate the list of all scan sets that have been defined so far. Figure 48 illustrates this page.

Figure 48: *Device Setup > Discover Executing a Scan Illustration*



1-2 ▾ of 2 Scan Sets Page 1 ▾ of 1 Choose columns Export CSV

		Network ▲	Credentials	Total Devices Found	New Devices Found	Total Rogues Founc
□	✎	Lab_networks	admin, default, private, public	20	20	0
□	✎	TechPubs	default, private	2	1	0

1-2 ▾ of 2 Scan Sets Page 1 ▾ of 1

Select All - Unselect All

Scan Delete Refresh this page for updated results.

Show Scheduling Options

2. Check the box next to the scan(s) that you would like to execute.
3. Select **Scan** to execute the selected scans, and the scan immediately begins. The **Stop** column indicates the scan is **In Progress**. Clicking this column heading will stop the scan(s).
4. For future scans, select the **Show Scheduling Options** link and enter the desired date and time to schedule a future scan.
5. After several minutes have passed, refresh the browser page and view the results of the scan. When the **Start** and **Stop** columns display date and time information, the scan is available to display the results.
6. Select the **pencil** icon for the scan to display the results. Table 71 describes the scan results and related information.

Table 71: *Device Setup > Discover > Discovery Execution Fields*

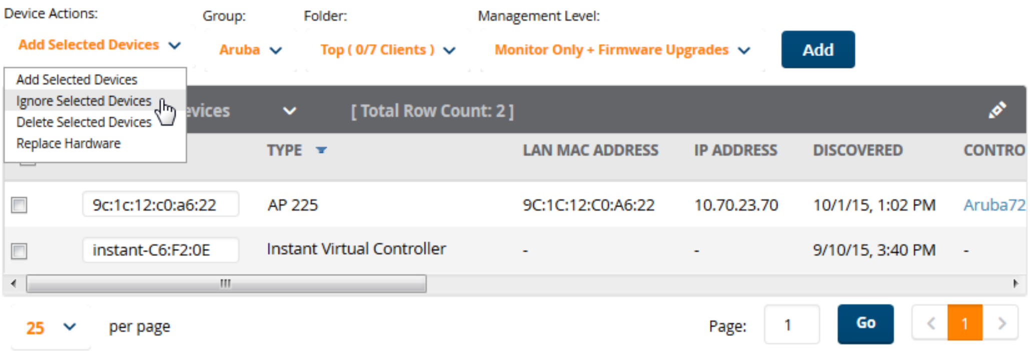
Column	Description
Network	Displays the network to be scanned.
Credentials	Displays the credentials used in the scan.
Total Devices Found	Displays the total number of APs detected during the scan that OV3600 can configure and monitor. **Total** includes both APs that are currently being managed by OV3600 as well as newly discovered APs that are not yet being managed.
New Devices Found	Displays the number of discovered APs that are not yet managed, but are available.
Total Rogues Found	Displays the total number of APs detected during the scan that OV3600 could not configure or monitor. **Total** includes both APs that have been discovered in earlier scans as well as newly discovered APs from the most recent scan.
New Rogues Found	Displays the number of rogue APs discovered on the most recent scan.
Start	Displays the date and time the most recent scan was started.
Stop	Displays the date and time the scan most recently completed.
Scheduled	Displays the scheduled date and time for scans that are scheduled to be run.

7. Go to the **Devices > New** page to see a full list of the newly discovered devices that the scan detected. Figure 49 illustrates this page.

NOTE

This page is only visible to users with the OV3600 Administrator role or roles that have **Allow authorization of Devices** enabled in **OV3600 Setup > Roles**.

Figure 49: *Devices > New Page Illustration*



Device Actions: Add Selected Devices

Group: Aruba

Folder: Top (0/7 Clients)

Management Level: Monitor Only + Firmware Upgrades

evices [Total Row Count: 2]

		TYPE	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED	CONTRO
☐	9c:1c:12:c0:a6:22	AP 225	9C:1C:12:C0:A6:22	10.70.23.70	10/1/15, 1:02 PM	Aruba72
☐	instant-C6:F2:0E	Instant Virtual Controller	-	-	9/10/15, 3:40 PM	-

25 per page

Page: 1

The Cisco Discovery Protocol (CDP)

CDP uses the polling interval configured for each individual Cisco switch or router on the **Groups > List** page. OV3600 requires read-only access to a router or switch for all subnets that contain wired or wireless devices. The polling interval is specified on the **Groups > Basic** page.

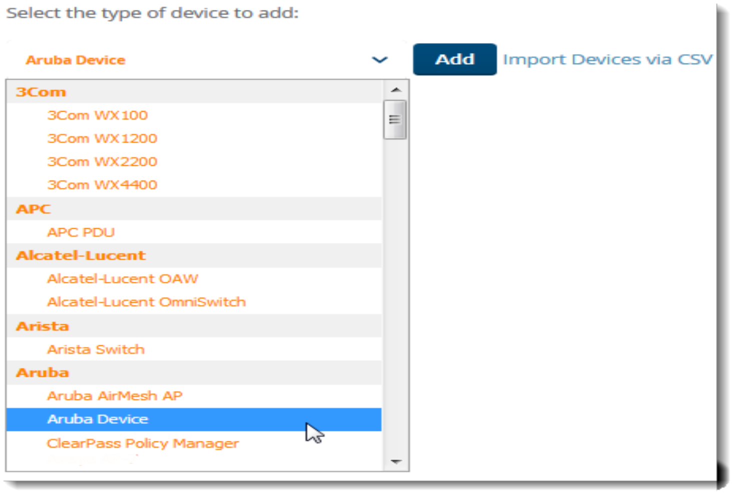
Manually Adding Devices

If OV3600 doesn't discover devices automatically, you can follow these steps to add the devices manually. When you select a Cisco or Alcatel-Lucent device, OV3600 automatically adds the specific make and model information into its database.

To manually add devices to OV3600:

1. Go to the **Device Setup > Add** page, then select the vendor and model from the device drop-down menu (see Figure 50. The configuration options on this page vary depending on the device.

Figure 50: *Selecting the Device*



Select the type of device to add: Aruba Device

2. Select **Add**.
3. From the Add page, enter the device communications settings and location settings. See Table 72 for information about each setting.
4. At the bottom of the page, set the device management mode to **Monitor Only** or **Management read/write**.

NOTE

If you select **Manage read/write**, OV3600 overwrites existing device settings with the **Groups** settings. Place newly discovered devices in **Monitor read/only** mode to enable auditing of actual settings instead of Group Policy settings. For more information, see "Setting the Management Mode" on page 127.

5. Select **Add** to finish adding the devices to the network.

Table 72 describes the settings on the Add Page. Several settings are derived from the **Device Setup > Communication** page.

Table 72: *Device Communication and Location Fields and Default Values*

Setting	Default	Description
Name	None	User-configurable name for the AP (maximum of 20 characters).
IP Address	None	IP address of the device (required). OV3600 supports IPv4 and IPv6 addresses.
SNMP Port	161	The port OV3600 uses to communicate with the AP using SNMP.
SSH Port	22	For devices that support SSH, specify the SSH port number.
Community String (Confirm)	Taken from **Device Setup > Communication**	Community string used to communicate with the AP. **NOTE:** The **Community String** should have RW (Read-Write) capability. New, out-of-the-box Cisco devices typically have SNMP disabled and a blank user name and password combination for HTTP and Telnet. Cisco supports multiple community strings per AP.
SNMPv3 Username	Taken from **Device Setup > Communication**	User name of the SNMP v3 user on the switch. If you are going to manage configuration for the device, this field provides a read-write user account (SNMP, HTTP, and Telnet) within the Cisco Security System for access to existing APs. OV3600 initially uses this user name and password combination to control the Cisco AP. OV3600 creates a user-specified account with which to manage the AP if the **User Creation Options** are set to **Create** and user specified as User.
Auth Password	Taken from **Device Setup > Communication**	SNMPv3 authentication password. **NOTE:** SNMPv3 supports three security levels: (1) no authentication and no encryption, (2) authentication and no encryption, and (3) authentication and encryption. OV3600 currently only supports authentication and encryption.
Privacy Password (Confirm)	Taken from **Device Setup > Communication**	SNMPv3 privacy password. **NOTE:** SNMPv3 supports three security levels: (1) no authentication and no encryption, (2) authentication and no encryption, and (3) authentication and encryption. OV3600 currently only supports authentication and encryption.
SNMPv3 Auth Protocol	Taken from **Device Setup > Communication**	Specifies the SNMPv3 auth protocol, either MD5 or SHA-1.

Table 72: *Device Communication and Location Fields and Default Values (Continued)*

Setting	Default	Description
SNMPv3 Privacy Protocol	Taken from **Device Setup > Communication**	Specifies the SNMPv3 Privacy protocol as either DES or AES. This option is not available for all devices.
Telnet/SSH Username	Taken from **Device Setup > Communication**	Telnet user name for existing Cisco IOS APs. OV3600 uses the Telnet user name/password combination to manage the AP and to enable SNMP if desired. **NOTE:** New, out-of-the-box Cisco IOS-based APs typically have SNMP disabled with a default telnet user name of **Cisco** and default password of **Cisco**. This value is required for management of any existing Cisco IOS-based APs.
Telnet/SSH Password (Confirm)	Taken from **Device Setup > Communication**	Telnet password for existing Cisco IOS APs. OV3600 uses the Telnet user name/password combination to manage the AP and to enable SNMP if desired. **NOTE:** New, out-of-the-box Cisco IOS-based APs typically have SNMP disabled with a default telnet user name of **Cisco** and default password of **Cisco**. This value is required for management of any existing Cisco IOS-based APs.
enable Password (Confirm)	Taken from **Device Setup > Communication**	Password that allows OV3600 to enter **enable** mode on the device.

Adding Universal Devices

OV3600 gets basic monitoring information from any device including switches, routers and APs whether or not they are supported devices. Entering SNMP credentials is optional. If no SNMP credentials are entered, OV3600 will provide ICMP monitoring of universal devices. This allows you to monitor key elements of the wired network infrastructure, including upstream switches, RADIUS servers and other devices. While OV3600 can manage most leading brands and models of wireless infrastructure, universal device support also enables basic monitoring of many of the less commonly used devices.

Perform the same steps to add universal devices to OV3600 that were detailed in "Manually Adding Devices " on page 124.

OV3600 collects basic information about universal devices including name, contact, uptime and location. Once you have added a universal device, you can view a list of its interfaces on **Devices > Manage**.

By selecting the **pencil** icon next to an interface, you can assign it to be non-monitored or monitored as Interface 1 or 2. OV3600 collects this information and displays it on the **Devices > Monitor** page in the **Interface** section. OV3600 supports MIB-II interfaces and polls in/out byte counts for up to two interfaces. OV3600 also monitors sysUptime.

Verifying the Device Configuration

When you have placed a newly discovered device in to a group and set the management mode to Monitor Only, the next step is to check the device configuration status. Determine whether OV3600 will apply changes to the device if you change the management mode to **Manage Read/Write**.

OV3600 uses SNMP or Telnet to read a device's configuration. SNMP is used for Cisco controllers. Alcatel-Lucent devices and wired routers and switches use Telnet/SSH to read device configuration. See "Individual Device Support and Firmware Upgrades" on page 219 for more details.

To verify the device configuration status:

1. Navigate to the **Devices > List**, then locate the device in the Device list.
2. Check the configuration status in the Configuration column:
   - 🔒 indicates that the device is in **Monitor Only** mode. OV3600 won't make any device configuration changes.
   - **Good** indicates that all of the device's current settings match the group policy settings. OV3600 won't make any changes to the device configuration when the management mode changes to **Manage Read/Write**.
   - **Error** indicates that there is a problem with the device configuration. Click the blue **Error** link to access the Device Configuration page and review the error.
   - **Mismatch** indicates that at least one of the device's current configuration settings doesn't match the group policy. OV3600 will push configuration changes to the device when the management mode changes to **Manage Read/Write**.
3. If there is a configuration mismatch, from the Device Configuration page, click the blue **Error** link toview the device configuration settings and it with the group configuration. When the device management mode is set to **Manage Read/Write**, the settings on the right side of the Compare Configurations page will be pushed to the device.
4. Review the list of changes to be applied to the device to determine whether the changes are appropriate. If not, you need to change the group settings or move the device to another group.

Setting the Management Mode

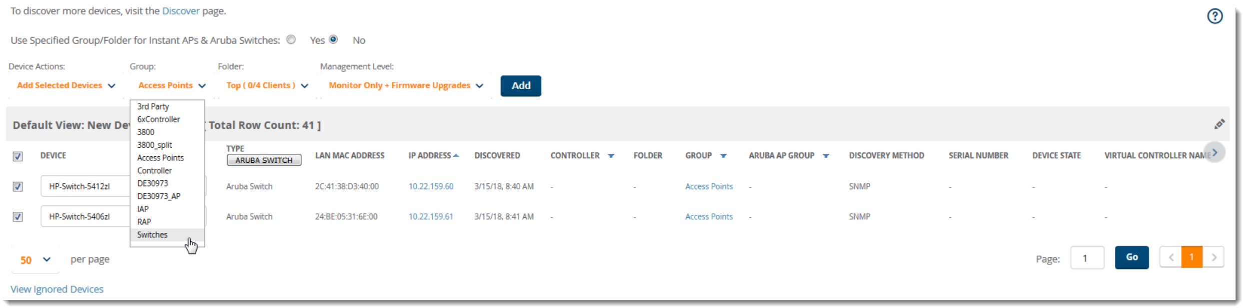
After OV3600 discovers devices on your network, you need to add the devices to a group and set the management mode to **Monitor Only** to avoid overwriting important configuration settings. In this read-only mode, OV3600 monitors the device, updates the firmware, compares the current configuration with the policy, and displays any discrepancies on the **Devices > Device Configuration** page. For information about device groups, refer to "Using Device Groups" on page 72.

NOTE

Placing newly discovered devices in Monitor Only mode is strongly recommended until you can confirm that all group configuration settings are appropriate for the devices. Change the management mode to **Manage Read/Write** when you are ready to push configuration changes to the devices in the group.

To put newly discovered devices into a group and set the management mode:

1. Navigate to **Devices > New**, then click ✎ to the newly discovered devices.



To discover more devices, visit the Discover page.

Use Specified Group/Folder for Instant APs & Aruba Switches: ○ Yes ● No

Device Actions: Add Selected Devices
Group: Access Points
Folder: Top (0/4 Clients)
Management Level: Monitor Only + Firmware Upgrades

Default View: New De[illegible] [Total Row Count: 41]

☑	DEVICE	TYPE ARUBA SWITCH	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED	CONTROLLER	FOLDER	GROUP	ARUBA AP GROUP	DISCOVERY METHOD	SERIAL NUMBER	DEVICE STATE	VIRTUAL CONTROLLER NAME
☑	HP-Switch-5412zl	Aruba Switch	2C:41:38:D3:40:00	10.22.159.60	3/15/18, 8:40 AM	-	-	Access Points	-	SNMP	-	-	-
☑	HP-Switch-5406zl	Aruba Switch	24:BE:05:31:6E:00	10.22.159.61	3/15/18, 8:41 AM	-	-	Access Points	-	SNMP	-	-	-

50 per page

Page: 1 Go < 1 >

View Ignored Devices

2. Select the group and folder to which the device will be added. You can't add devices to a global group.

3. Select **Monitor Only + FirmWare Upgrades** from the Management Level drop-down menu, then select **Add**.
4. From the **Devices > List** page, select the folder that contains one or more devices to verify that your device has been properly assigned.

Ignoring Discovered Devices

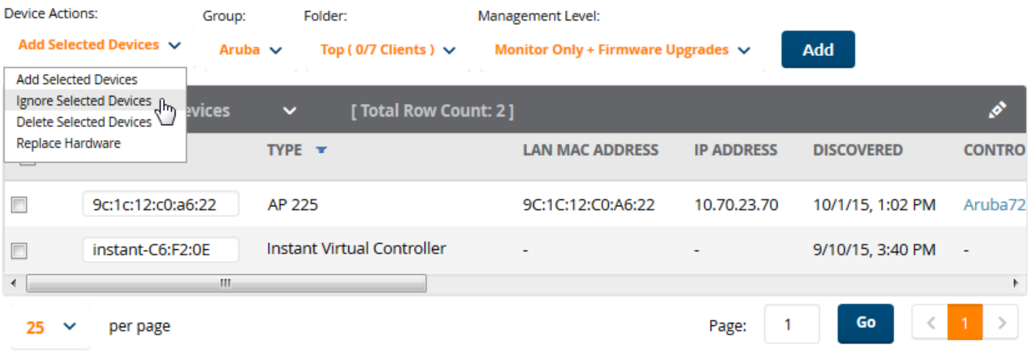
You might want to ignore a discovered device. If you know that the device will be down temporarily, you can add it to the ignore list and then remove it from the ignored list when it is online again.

If OV3600 discovers an ignored device in a subsequent scan, it doesn't display the device in the list of new devices on the **AP/Devices > New** page. However, OV3600 lists a deleted device on this page if it discovers it again.

To ignore a device:

1. Go to the **Devices > New** page.
2. Select the checkbox beside the device, and then select **Ignore Selected Devices** from the drop-down menu (see Figure 51. You can select more than one at a time.

Figure 51: *Devices > New Page Illustration*



Device Actions: Add Selected Devices

Group: Aruba

Folder: Top (0/7 Clients)

Management Level: Monitor Only + Firmware Upgrades

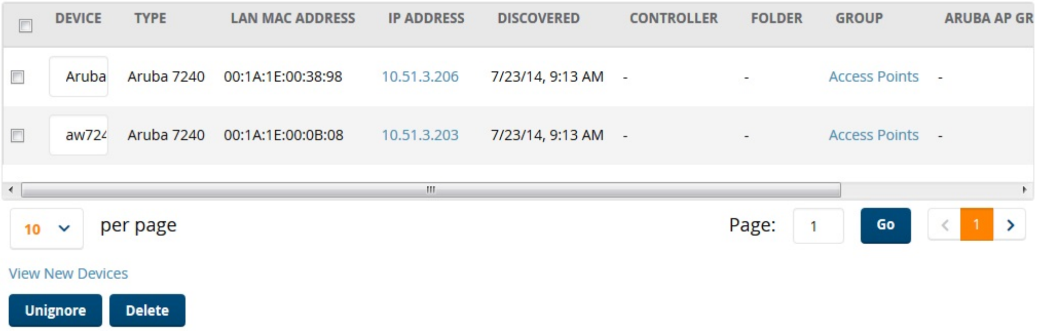
		TYPE	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED	CONTRO
□	9c:1c:12:c0:a6:22	AP 225	9C:1C:12:C0:A6:22	10.70.23.70	10/1/15, 1:02 PM	Aruba72
□	instant-C6:F2:0E	Instant Virtual Controller	-	-	9/10/15, 3:40 PM	-

Unignoring a Device

Perform these steps to return an ignored device to a managed status.

1. To view all devices that are ignored, go to the **Devices > Ignored** page, illustrated in Figure 52.

Figure 52: *Devices > Ignored Page Illustration*



□	DEVICE	TYPE	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED	CONTROLLER	FOLDER	GROUP	ARUBA AP GR
□	Aruba	Aruba 7240	00:1A:1E:00:38:98	10.51.3.206	7/23/14, 9:13 AM	-	-	Access Points	-
□	aw724	Aruba 7240	00:1A:1E:00:0B:08	10.51.3.203	7/23/14, 9:13 AM	-	-	Access Points	-

This page provides the following information for any ignored device:

- Device name or MAC address, when known
- Controller associated with that device

- Device type
- Device IP address
- LAN MAC address for the LAN on which the device is located
- Date and time of device discovery

2. To change the device parameters for a given device, select its checkbox and adjust group, folder, monitor, and manage settings as desired.
3. Select **Add** to add the device to OV3600 so that it appears on the **Devices > New** list.
4. The **Unignore** button will either return the device to its regular folder or group or send it to the **Devices > New**
   page.

Troubleshooting a Newly Discovered Down Device

If the device status on the **Devices > List** page remains **Down** after being discovered and added to a group, there is usually an error in the SNMP community string used to manage the device.

To troubleshoot a down device:

1. Go to the **Devices > List** or the **Devices > Down** page, then click the **Name** of the down device to access the device monitoring page.
2. Locate the **Status** field in the **Device Info** section. When the device is down, the status includes a description of the problem.

A device might be down for any of the discovery issues described in Table 73.

Table 73: *System Messages for Discovered, Down Devices*

Message	Meaning
AP is no longer associated with controller	This means the AP no longer shows up in any controller's AP list (on the OV3600 server). Either the AP was removed from the controller, or it has roamed to another controller that OV3600 does not have visibility to, or it is offline.
Controller is Down	When a controller goes down, OV3600 automatically marks all associated thin APs down. This is because communication to thin APs are via the controller, and OV3600 assumes that if the Controller has gone offline, then all associated APs are down as well until they are re-associated with another Controller.
Downloading	The AP is in the process of downloading firmware or configuration. **NOTE:** Applicable to Cisco WLC thin APs and some Symbol APs.
Error fetching existing configuration	OV3600 could not fetch a configuration for the device. Usually this is because OV3600 has incorrect credentials and was not able to log in.
ICMP Ping Failed (after SNMP Get Failed)	The device is not responding and is likely offline.
SNMP Get Failed	SNMP credentials and/or configuration may be incorrect. Verify that SNMP is enabled and that credentials and access ports are configured correctly on both the target device and in OV3600.
SNMP Trap	OV3600 received an SNMP trap from the controller indicating that the AP is no longer associated to the controller.

Table 73: *System Messages for Discovered, Down Devices (Continued)*

Message	Meaning
Telnet Error: command timed out	Telnet/SSH user name and password specified for that device is incorrect.
Unexpected LAN MAC Address found at this device’s IP address	If OV3600 detects that the LAN MAC address of a device has changed this error message will appear. This usually indicates that a physical hardware change has occurred (while reusing the same IP Address) without using the **Replace Hardware** feature in OV3600. This error may also indicate an IP address conflict between two or more devices. When an unexpected LAN MAC address is seen in a device's IP address, its **Devices > Manage** page displays the message Click **Replace Hardware** (preferred) or **Reset MAC Address** to reset the LAN MAC address if this device has been replaced with new hardware at the top of the page. Use the **Replace Hardware** button at the bottom of that page in order to avoid this message.

NOTE

To view the detailed status of all your down devices at once, navigate to **Devices > Down** (try the **Down** top header stats link) and look at the **Detailed Status** column for the list of down devices. This column can be sorted using the **Filter** icon (▼).

3. If the **SNMP Get Failed** message appears, select the **Devices > Manage** tab to go to the management page for that device.
4. If the credentials are incorrect, return to the **Device Communications** area on the **Devices > Manage** page. Enter the appropriate credentials, and select **Apply**.
5. Return to the **Devices > List** page to see if the device appears with a Status of **Up**.

OV3600 provides an easy-to-use interface that lets you monitor your entire access infrastructure. When you click a device link from the device list, you can view the monitoring page for the device.

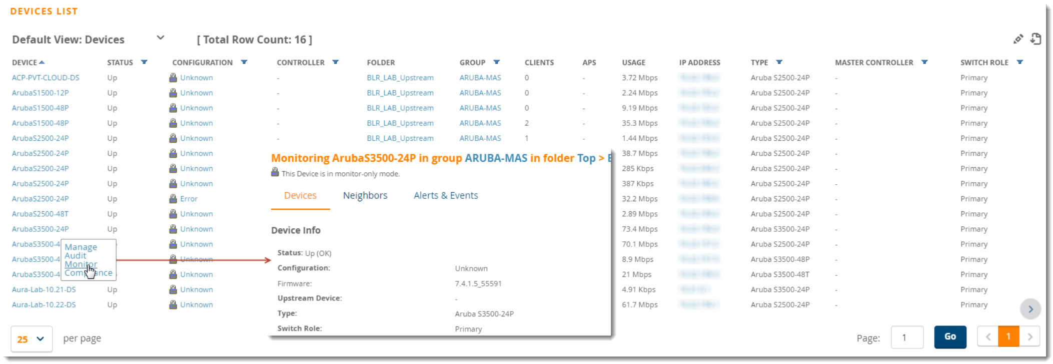
The following sections discuss various monitoring options in OV3600:

- "Monitoring Basics" on page 131
- "Monitoring Access Points, Mesh Devices, and switches" on page 136
- "Monitoring the AOS-W-CX Switches and Mobility Access Switches" on page 153.
- "Monitoring Alcatel-Lucent AOS-W-Switches" on page 159.
- "Monitoring switch Clusters" on page 178
- "Monitoring Clients" on page 181
- "Troubleshooting Client Issues" on page 189
- "Using Topology" on page 194

Monitoring Basics

You can find the monitoring page by navigating to **Devices > List** and selecting a device from the list. Or, you can hover the pointer over a device and click Monitor from the shortcut menu, as shown in Figure 53.

Figure 53: *Opening the Monitoring Page for a Device*



DEVICES LIST

Default View: Devices [Total Row Count: 16]

DEVICE	STATUS	CONFIGURATION	CONTROLLER	FOLDER	GROUP	CLIENTS	APS	USAGE	IP ADDRESS	TYPE	MASTER CONTROLLER	SWITCH ROLE
ACP-PVT-CLOUD-DS	Up	Unknown	-	BLR_LAB_Upstream	ARUBA-MAS	0	-	3.72 Mbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS1500-12P	Up	Unknown	-	BLR_LAB_Upstream	ARUBA-MAS	0	-	2.24 Mbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS1500-48P	Up	Unknown	-	BLR_LAB_Upstream	ARUBA-MAS	0	-	9.19 Mbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS1500-48P	Up	Unknown	-	BLR_LAB_Upstream	ARUBA-MAS	2	-	35.3 Mbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS2500-24P	Up	Unknown	-	BLR_LAB_Upstream	ARUBA-MAS	1	-	1.44 Mbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS2500-24P	Up	Unknown						38.7 Mbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS2500-24P	Up	Unknown						285 Kbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS2500-24P	Up	Unknown						387 Kbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS2500-24P	Up	Error						32.2 Mbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS2500-48T	Up	Unknown						2.89 Mbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS3500-24P	Up	Unknown						73.4 Mbps	[redacted]	Aruba S3500-24P	-	Primary
ArubaS3500-4		Unknown						70.1 Mbps	[redacted]	Aruba S2500-24P	-	Primary
ArubaS3500-4		Unknown						8.9 Mbps	[redacted]	Aruba S3500-48P	-	Primary
ArubaS3500-4		Unknown						21 Mbps	[redacted]	Aruba S3500-48T	-	Primary
Aura-Lab-10.21-DS	Up	Unknown						4.91 Kbps	[redacted]	Aruba S3500-24P	-	Primary
Aura-Lab-10.22-DS	Up	Unknown						61.7 Mbps	[redacted]	Aruba S2500-24P	-	Primary

25 per page Page: 1 Go 1

Monitoring ArubaS3500-24P in group ARUBA-MAS in folder Top > B

This Device is in monitor-only mode.

Device Info

Status: Up (OK)

Configuration: Unknown

Firmware: 7.4.1.5_55591

Upstream Device: -

Type: Aruba S3500-24P

Switch Role: Primary

Here are some of the things you can view on or from the **Devices > Monitor** page:

- Device Information. The information displayed varies depending on the device type. See "Device Information for Access Points, Mesh Devices, and switches" on page 136 or "Device Information" on page 153.
- Graphs. The graphs show historical data and help you identify trends and anomalies. When you hover the pointer over a graph, a detailed pop up view displays. See "Graphs for Access Points, Mesh Devices, and switches" on page 139 and "Graphs" on page 154.
- Detailed summary tables. Click the **Neighbors** tab, located above the device information, to access the summary tables. You can monitor the nearest RF neighbors of an access point and the physical and virtual interfaces on a switch. For information, see "Monitoring Access Points, Mesh Devices, and switches" on page 136 and "Detailed Summary Tables" on page 154, respectively.
- Alerts. Click the **Alerts & Events** tab, located above the device information, to access the alert tables about OV3600, Intrusion Detection System (IDS), RADIUS accounting, and RADIUS authentication issues. For information about alert summaries, see "About Alerts" on page 276.

- Events. Click the **Alerts & Events** tab to access the event tables for device events and recent OV3600 device events. These tables also appear on the **System > Event Log** page. To learn more about these events, see "Using the Event Log" on page 266.

From the **Devices > Monitor** page, you can:

- Use Quick Links. Open the WebUI for a switch in a pop up window, or run a command on a device. For example, use the `show stacking members` command to verify the switches in a stack or the `AP LED Blinking Enable` command to flash the LEDs on an AP.
- Locate a device. Search by typing the IP address, name, version, or other information. Results include hypertext links to additional pages.
- Poll the device. Override the preset polling interval by clicking **Poll Now** in the top right corner of the page. OV3600 refreshes all but rogue data. For information about polling multiple devices, see "Poll selected devices" on page 116.
- Authenticate rogue devices found on wired networks. Look for unauthenticated devices in the **Connected Devices** tables, then acknowledge them by modifying editable fields. Learn how to do this in "Monitoring the AOS-W-CX Switches and Mobility Access Switches" on page 153.
- Diagnose issues. Go to the **Clients > Diagnostics** page, where you can check for network status, location, trends, and alerts. Find more information about "Troubleshooting Client Issues" on page 189.
- Monitor a network interface for a wired device. Find more information about "Interfaces" on page 157.
- Go to Topology by clicking 🖧 in the upper-right corner of the monitoring page to monitor or troubleshoot a device or switch interface from the topology map. For more information, see "Using Topology" on page 194.

Customizing the Monitoring Page

You can adjust how much information displays in your tables, then filter the results. You can also categorize information using groups.

First 25 Results

OV3600 displays only 25 rows of information. To display a different number of entries per page, click ˅ and select 10, 25, 50, 100, 250, or 500. Longer page lengths require more time for the page to load.

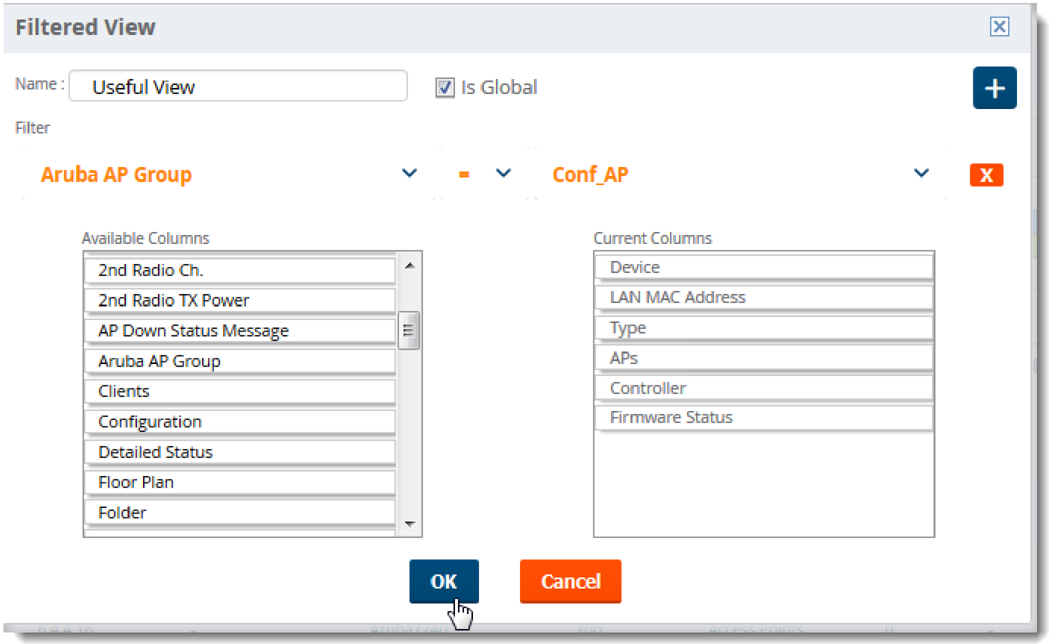
Creating Filtered Views

To create a new filtered view:

1. Navigate to a page that contains a default view list, such as **Devices > List** or **RAPIDS > List**.
2. In the Devices List, select **New View** from the Default View drop-down menu to create a filtered view.
3. In the **Name** field, type the name for the filtered view.
4. If you want to give all users access to the filtered view, select **Is Global**. Only Administrators can edit global filtered views.
5. Click + to add device groups to the filtered view, or X to remove them.
   a. Scroll the list of parameters and select a **Device** or **Radio** parameter.
   b. If required, enter search parameters such as "=" to refine the filter parameters.
   c. To create a filtered view with multiple filter parameters, click **Add Filter** again and define any additional filter parameters. For example, to create a view that displays APs with more than zero clients but less than five clients, you would need to create one filter with the parameters **Clients > 0**, and a second filter with the parameters **Clients < 5**.

6. Drag and drop data columns from the **Available Columns** list to the **Current Columns** list to select which columns display in the view. You can reorder the columns in the **Current Columns** list by dragging and dropping the data column to a different place in the list.

Figure 54: *Customizing the View*



Filtered View

Name : Useful View ☑ Is Global

Filter

Aruba AP Group = Conf_AP

Available Columns

- 2nd Radio Ch.
- 2nd Radio TX Power
- AP Down Status Message
- Aruba AP Group
- Clients
- Configuration
- Detailed Status
- Floor Plan
- Folder

Current Columns

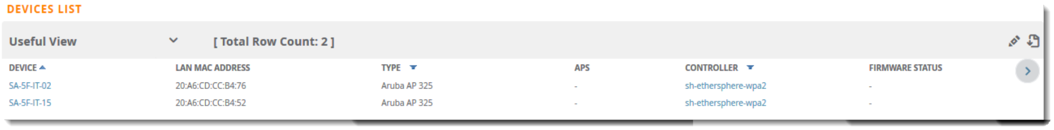
- Device
- LAN MAC Address
- Type
- APs
- Controller
- Firmware Status

7. Click **OK**.

Figure 55: *Creating a Filtered View*

The Devices List displays the new filtered view.

Figure 56: *New Filtered View*



DEVICES LIST

Useful View [Total Row Count: 2]

DEVICE ▲	LAN MAC ADDRESS	TYPE ▼	APS	CONTROLLER ▼	FIRMWARE STATUS
SA-5F-IT-02	20:A6:CD:CC:B4:76	Aruba AP 325	-	sh-ethersphere-wpa2	-
SA-5F-IT-15	20:A6:CD:CC:B4:52	Aruba AP 325	-	sh-ethersphere-wpa2	-

Editing Filtered Views

You can edit a custom filtered view at any time, by selecting the view in the view list, then selecting the ⚙ icon and modifying filter parameters and column displays.

Table 74: *Filter icons*

Icon	Description
+	Click this icon to create a custom filtered view.
⚙	Click this icon to edit an existing custom filtered view.
⧉	Click this icon to clone a filtered view.
🗑	Click this icon to delete a custom filtered view.

Showing Filters, Clearing Filters, Resetting Grouping

To change how OV3600 displays data, do any of the following:

- Click the column heading to sort the data.
- Click ▼ at the top of column headings to filter the data.
- Click **▼ Show Filters** to add parameters to the table view.
- Click **✖ Clear Filters** to remove filters and return to the default table view.
- Click **✖ Reset Grouping** if you no longer want to group capabilities in the table view.

Using Device Folders

Using folders, you can group your devices in order to manage device reporting, view statistics, and identify status. You *must* use folders if you want to limit the APs and devices OV3600 users can see.

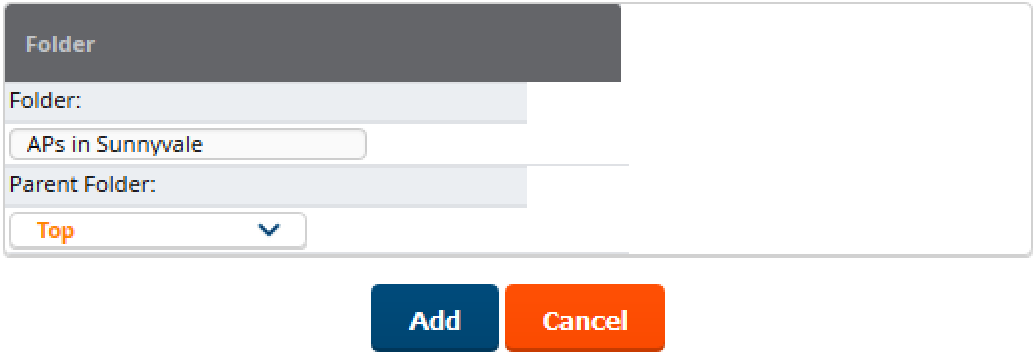
Adding Device Folders

To add a device folder:

1. Go to **Devices > List**, scroll to the end of the Devices List and click **Add New Folder** at the bottom of the page.
2. Enter text that describes the folder, such as *APs in Sunnyvale* if you want to organize the folders by device location.
3. Select the parent folder, then click **Add**.
4. Select the parent folder. If the parent folder contains subfolders, you can create a hierarchical structure that is manageable, for example, by location, building name, or room.

   Figure 57 shows how to create the *APs in Sunnyvale* folder.

Figure 57: *Adding a New Folder*



Folder: APs in Sunnyvale

Parent Folder: Top

Moving Folders

If you want to change the folder hierarchy, OV3600 lets you move and rename folders.

To move folders:

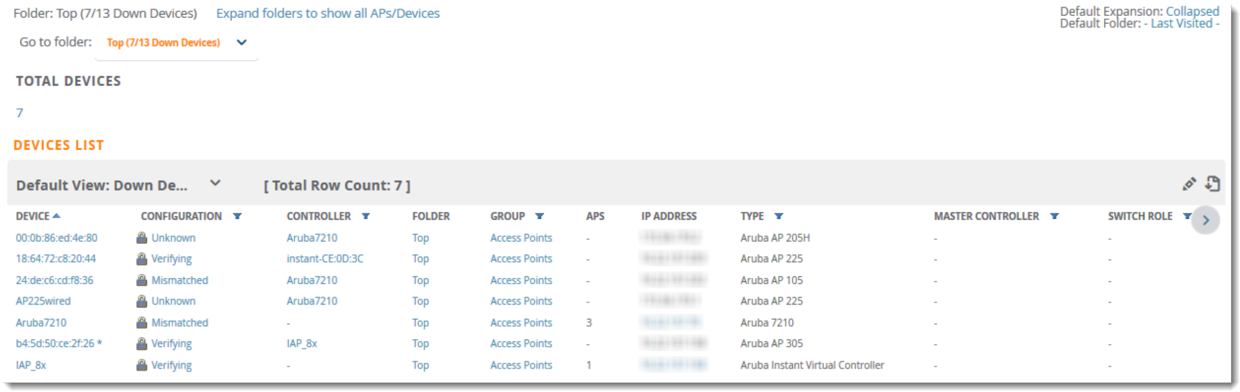
1. Select the folder you want to move from **Go to folder** at the upper left of the **Devices** page.
2. Scroll to bottom of the page and click ✎.
3. Select the new parent folder and click **Save**.

Expanding Folders

You can change the information displayed on the **Devices > List** and **Clients > Connected** pages by selecting a folder at the top left corner of the page.

For example, if you select the **Top** folder and then click **Down** in the navigation bar, OV3600 displays the 7 down devices in the Top folder.

Figure 58: *Collapsed View of the Down Devices in the Top Folder*



Folder: Top (7/13 Down Devices) Expand folders to show all APs/Devices

Default Expansion: Collapsed
Default Folder: - Last Visited -

Go to folder: Top (7/13 Down Devices)

TOTAL DEVICES

7

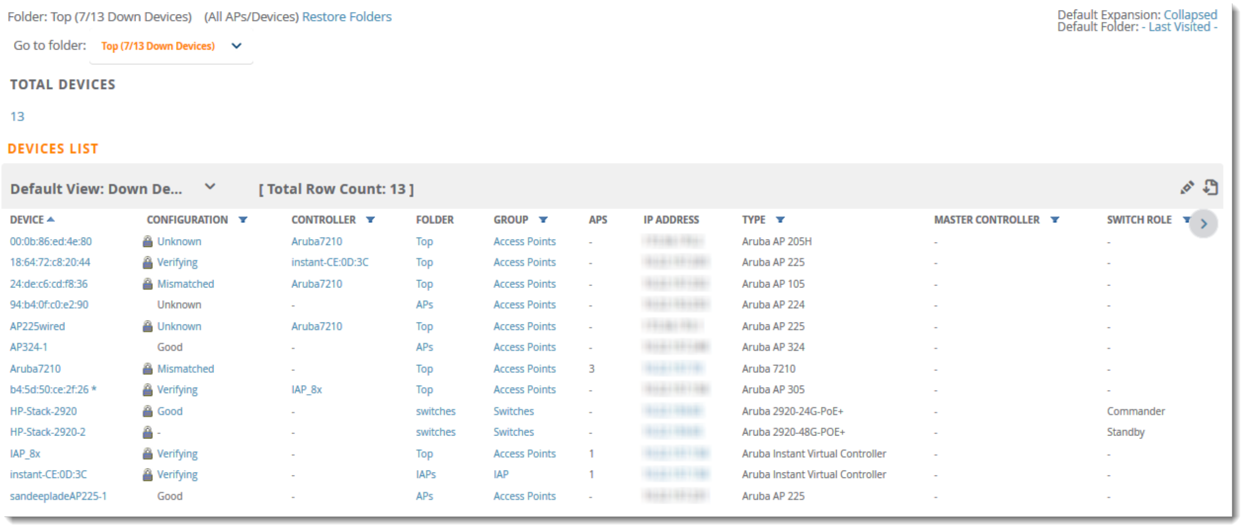
DEVICES LIST

Default View: Down De... [Total Row Count: 7]

DEVICE ▲	CONFIGURATION	CONTROLLER	FOLDER	GROUP	APS	IP ADDRESS	TYPE	MASTER CONTROLLER	SWITCH ROLE
00:0b:86:ed:4e:80	Unknown	Aruba7210	Top	Access Points	-	[redacted]	Aruba AP 205H	-	-
18:64:72:c8:20:44	Verifying	instant-CE:0D:3C	Top	Access Points	-	[redacted]	Aruba AP 225	-	-
24:de:c6:cd:f8:36	Mismatched	Aruba7210	Top	Access Points	-	[redacted]	Aruba AP 105	-	-
AP225wired	Unknown	Aruba7210	Top	Access Points	-	[redacted]	Aruba AP 225	-	-
Aruba7210	Mismatched	-	Top	Access Points	3	[redacted]	Aruba 7210	-	-
b4:5d:50:ce:2f:26 *	Verifying	IAP_8x	Top	Access Points	-	[redacted]	Aruba AP 305	-	-
IAP_8x	Verifying	-	Top	Access Points	1	[redacted]	Aruba Instant Virtual Controller	-	-

When you select **Expand folders to show all devices**, OV3600 displays an expanded view of all 13 down devices in the Top folder and its subfolders.

Figure 59: *Expanded View of Down Devices in the Top Folder and Subfolders*



Folder: Top (7/13 Down Devices) (All APs/Devices) Restore Folders

Default Expansion: Collapsed
Default Folder: - Last Visited -

Go to folder: Top (7/13 Down Devices)

TOTAL DEVICES

13

DEVICES LIST

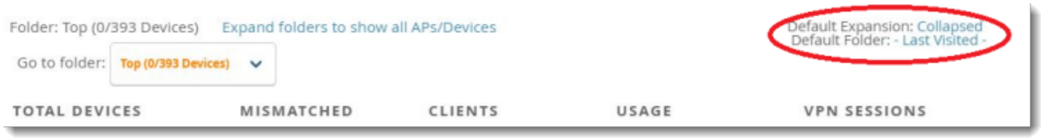
Default View: Down De... [Total Row Count: 13]

DEVICE ▲	CONFIGURATION	CONTROLLER	FOLDER	GROUP	APS	IP ADDRESS	TYPE	MASTER CONTROLLER	SWITCH ROLE
00:0b:86:ed:4e:80	Unknown	Aruba7210	Top	Access Points	-	[redacted]	Aruba AP 205H	-	-
18:64:72:c8:20:44	Verifying	instant-CE:0D:3C	Top	Access Points	-	[redacted]	Aruba AP 225	-	-
24:de:c6:cd:f8:36	Mismatched	Aruba7210	Top	Access Points	-	[redacted]	Aruba AP 105	-	-
94:b4:0f:c0:e2:90	Unknown	-	APs	Access Points	-	[redacted]	Aruba AP 224	-	-
AP225wired	Unknown	Aruba7210	Top	Access Points	-	[redacted]	Aruba AP 225	-	-
AP324-1	Good	-	APs	Access Points	-	[redacted]	Aruba AP 324	-	-
Aruba7210	Mismatched	-	Top	Access Points	3	[redacted]	Aruba 7210	-	-
b4:5d:50:ce:2f:26 *	Verifying	IAP_8x	Top	Access Points	-	[redacted]	Aruba AP 305	-	-
HP-Stack-2920	Good	-	switches	Switches	-	[redacted]	Aruba 2920-24G-PoE+	-	Commander
HP-Stack-2920-2	-	-	switches	Switches	-	[redacted]	Aruba 2920-48G-POE+	-	Standby
IAP_8x	Verifying	-	Top	Access Points	1	[redacted]	Aruba Instant Virtual Controller	-	-
instant-CE:0D:3C	Verifying	-	IAPs	IAP	1	[redacted]	Aruba Instant Virtual Controller	-	-
sandeepladeAP225-1	Good	-	APs	Access Points	-	[redacted]	Aruba AP 225	-	-

Changing Default Views

You can change the way OV3600 displays default views in the **Devices > List** and **Clients > Connected** pages. To change the default view, click the **Default Expansion** or **Default Folder** drop-down menus at the top right corner of the page to change your view, as shown in Figure 60.

Figure 60: *Default Expansion and Default Folder Options*



Folder: Top (0/393 Devices) Expand folders to show all APs/Devices

Go to folder: Top (0/393 Devices)

Default Expansion: Collapsed
Default Folder: - Last Visited -

Table 75: *Ways to View Devices and Clients in Folders*

Default View Options	Description
Default Expansion	- **Collapsed**: OV3600 shows details from the current folder. This view doesn't show details from the subfolders. - **Expanded**: OV3600 shows details of the current folder and its subfolders. - **Remember Last**: OV3600 stores your last view and displays it for you again. **NOTE:** The default expansion view affects the way OV3600 displays the network on the topology map. For more information about topology maps, see "Using Topology" on page 194.
Default Folder	- **Last Visited**: OV3600 displays the last folder you accessed. - **Folder**: When you select a folder, OV3600 limits the information displayed to devices or clients in a specific folder.

Monitoring Access Points, Mesh Devices, and switches

The **Devices > Monitor** page for APs, mesh devices, and controllers includes a graph for users and bandwidth. The controller graph lists the APs connected to it, while the APs include a list of users it has connected. When available, lists of CDP and RF neighbors are also listed.

NOTE

For information about switch monitoring, see "Monitoring the AOS-W-CX Switches and Mobility Access Switches" on page 153 and "Monitoring Alcatel-Lucent AOS-W-Switches" on page 159.

Device Information for Access Points, Mesh Devices, and switches

Table 76 describes the fields and information displayed in the **Device Info** section for different models and types of wireless devices.

Table 76: *Device Information for Wireless Devices*

Field	Description
Status	Displays the connection status between OV3600 and the device: - **Up**. Everything is working as it should. - **Down**. Either OV3600 can reach the device but can't speak with it using SNMP, or OV3600 is unable to reach the device or connect to it using SNMP. **NOTE:** Verify that SNMP is enabled on the device. Many APs ship with SNMP disabled. This usually means OV3600 is blocked from connecting to the device or the device needs to be rebooted or reset.
Configuration	- **Good** means all the settings on the AP agree with the settings OV3600 wants them to have. - **Mismatched** means there is a configuration mismatch between what is on the AP and what OV3600 wants to push to the AP. The **Mismatched** link directs you to this specific **Devices > Device Configuration** page where each mismatch is highlighted. - **Unknown** means the device configuration has not yet been fetched (possible issue with credentials). - **Verifying** means that the device is fetching a configuration that will be compared to the desired settings. - **Error** indicates a problem with the device. This configuration is accompanied with a description of the error.

Field	Description
Firmware	Displays the firmware version running on the AP. Newer AirMesh APs include the new bootloader APBoot. OV3600 helps to identify the new AirMesh APs from the old SKUs by displaying the bootloader information here.
Licenses (Appears for Alcatel-Lucentswitches)	Selecting this link opens a pop-up window that lists the built-in licenses as well as other installed licenses for this switch. This also shows whether any license has expired.
Controller (Appears for APs)	Displays the controller for the associated AP device as a link. Select the link to display the **Devices > Monitor** page for that controller.
Mesh Gateway *	Specifies the mesh AP acting as the wired connection to the network.
Mesh Mode*	Specifies whether the AP is a portal device or a mesh node. The portal device is connected to the network over a wired connection. A node is a device downstream of the portal that uses wireless connections to reach the portal device.
Mesh ID *	The name of the mesh device.
Google Earth*	Selecting the Google Earth icon opens the mesh network view in Google Earth.
Type	Displays the make and model of the device.
Last Contacted	Displays the most recent time OV3600 has polled the AP for information. The polling interval can be set on the **Groups > Basic** page.
Uptime	Displays the amount of time since the AP has been rebooted. This is the amount of time the AP reports and is not based on any connectivity with OV3600.
LAN MAC Address	Displays the MAC address of the Ethernet interface on the device.
Serial	Displays the serial number of the device.
Radio Serial	Displays the serial number of the radios in the device. This field is not available for all APs.
Location	Displays the SNMP location of the device.
Contact	Displays the SNMP contact of the device.
IP Address	Displays the IP address that OV3600 uses to communicate to the device. OV3600 supports IPv4 or IPv6 addresses. This number is also a link to the AP web interface. When the link is moused over a pop-up menu will appear allowing you to access the device using HTTP, HTTPs, telnet or SSH. For Alcatel-Lucentswitches, if Single Sign-On is enabled for your role in this OV3600 and you have access to this controller, you will not have to enter the credentials for this controller again after selecting this link.
Outer IP	Public IP address for a RAP device.
Remote LAN IP	LAN IP address for a RAP. This address is useful for troubleshooting from the local network.

Field	Description
Quick Links	**Open controller UI :** A drop-down menu that allows you to jump to the controller's WebUI in a new window. For Alcatel-Lucentswitches, if Single Sign-On is enabled for your role in OV3600 and you have access to this switch, you will not have to enter the credentials for this controller again after selecting this link. **Run a command:** A drop-down menu with a list of CLI commands you can run directly from the **Devices > Monitor** page.
APs	For controllers, displays the number of APs managed by this device at the time of the last polling.
Clients	Displays the total number of users associated to the device or its APs regardless of which radio they are associated to, at the time of the last polling.
Usage	Combined bandwidth through the device at time of polling.

***These fields are only available for mesh APs. To see an example of mesh monitoring, see "Monitoring Mesh Devices" on page 148.

OV3600 allows you to execute show commands on some models of Aruba or HPE switches by clicking the **Run Command** drop-down list on the **Devices > Monitor** page of the OV3600 WebUI, and selecting a supported show command. For a list of devices that support show commands via the OV3600 **Devices > Monitor** page, refer to the OV3600*Supported Infrastructure Devices* document. For complete information about the output of each command, refer to the documentation for that switch.

Radios

Table 77 describes the information in the **Radio** table for APs.

Table 77: *Devices > Monitor > Radio Fields and Descriptions*

Field	Description
Index	The number of the radio, used to distinguish radios that may be of the same type on a device.
Name	The Radio type (802.11a/b/g/n) as a link to the **Radio Statistics** page for that radio.
MAC address	The MAC address of the corresponding radio in the AP.
Clients	The number of users associated to the corresponding radio at the time of the last polling.
Usage (Kbps)	The amount of bandwidth being pushed through the corresponding radio interface or device at the time of the last polling.
Channel	The channel of the corresponding radio.
Tx Power	Some devices report transmit power reduction rather than transmit power; no value is reported for those devices.
Antenna Type	Indicates **Internal** or **External** radio. For devices where antenna type is defined per AP, the same antenna type will be listed for each radio.

Table 77: *Devices > Monitor > Radio Fields and Descriptions (Continued)*

Field	Description
Channel Width*	The bandwidth of the channel used by 802.11 stations. Legacy devices use **20 MHz** channels, and newer devices that support the 802.11n standard can use **40 MHz** channels to increase throughput.
Mesh Links *	The total number of mesh links to the device including uplinks and downlinks.
Role	Whether the radio acts as a Mesh Node or Access
Active SSIDs	The SSID(s) of the radio.

***These fields are only available for mesh APs. To see an example of mesh monitoring, see "Monitoring Mesh Devices" on page 148.

Wired Interfaces

Devices with wired interfaces (other than Alcatel-Lucent Instant APs) will display the **Wired Interfaces** table, which is described in Table 78:

Table 78: *Devices > Monitor > Wired Interfaces Fields and Descriptions*

Field	Description
Name	Displays the name of the interface.
MAC Address	Displays the MAC address of the corresponding interface in the device.
Clients	Displays the number of users associated to the corresponding interface at the time of the last polling.
Type	Indicates the type of interface - gigabit Ethernet or fast Ethernet for wired interfaces.
Admin Status	The administrator setting that determined whether the port is on or off.
Operational Status	Displays the current status of the interface. If an interface is **Up**, then OV3600 is able to ping it and fetch SNMP information. If the AP is listed as **Down**, then OV3600 is either unable to ping the interface or unable to read the necessary SNMP information from the device.
Duplex	Duplex mode of the link, full or half.
Alcatel-Lucent Port Mode	Either Active Standby (which provides redundancy so that when an active interface fails, the user traffic can failover to the standby interface) or one of the forwarding modes (Split, Bridge).
Input Capacity	The input capacity of the interface.
Output Capacity	The output capacity of the interface.

Graphs for Access Points, Mesh Devices, and switches

Figure 61 illustrates the interactive graphs available on this page. Use the drop down button next to the graph title to select a different graph.

Figure 61: *Interactive graphs for an Alcatel-Lucent switch*

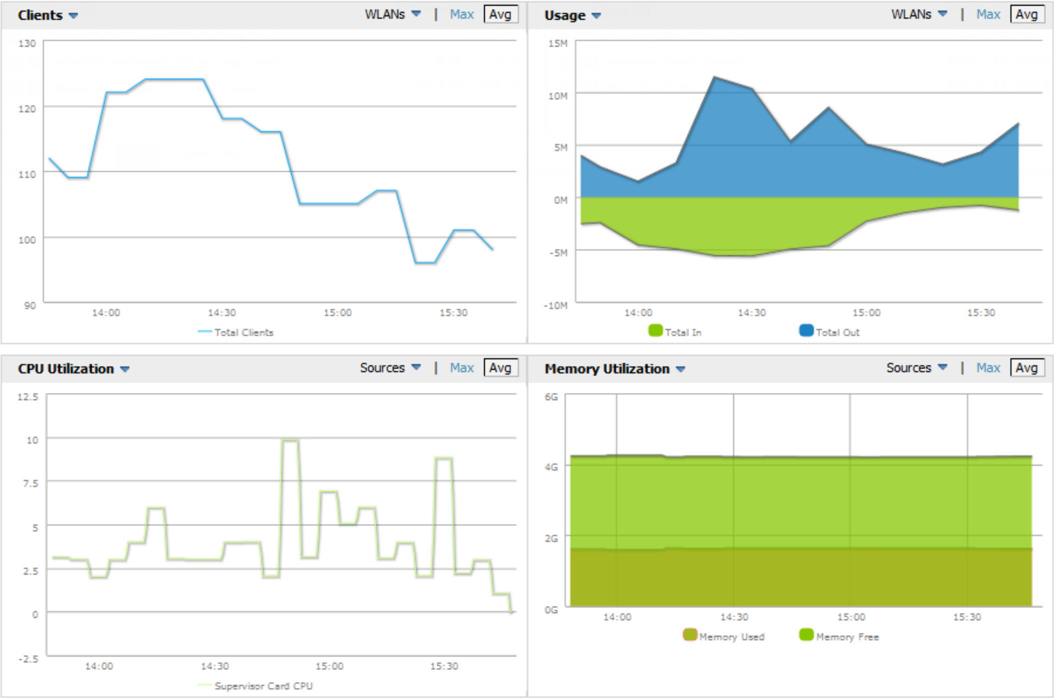


Table 79 describes the graphs on this page.

Table 79: *Devices > Monitor Graphical Data*

Graph	Description
Clients	Formerly Users. Shows the max and average client count reported by the device radios for a configurable period of time. User count for controllers are the sum of the user count on the associated APs. Check boxes below the graph can be used to limit the data displayed.
Usage	Formerly Bandwidth. Shows the bandwidth in and out reported by the device for a configurable period of time. Bandwidth for controllers is the sum of the associated APs. Check boxes below the graph can be used to limit the data displayed.
CPU Utilization (controllers only)	Reports overall CPU utilization (not on a per-CPU basis) of the device.
Memory Utilization (controllers only	Reports average used and free memory and average max memory for the device.

Location

If the device is associated to a VisualRF map, this section of the page displays the device on the map. Click the map to open it in VisualRF.

Connected Clients

Table 80 describes the fields and information displayed for the **Connected Clients** display.

Table 80: *Devices > Monitor > Connected Clients Fields and Default Values*

Field	Description
Username	Provides the name of the User associated to the AP. OV3600 gathers this data in a variety of ways. It can be taken from RADIUS accounting data or traps.
Device Type	The type of device the user is using as determined by the Device Type Rules set up by an administrator in **OV3600 Setup > Device Type Setup**. For more information, refer to "Setting Up Device Types" on page 60.
Role	The role of the connected client such as employee, perforce, or logon (captive portal).
MAC Address	Displays the Radio MAC address of the user associated to the AP. Also provides a link that redirects to the **Users > Detail** page.
Radio	Displays the radio to which the user is associated.
Association Time	Displays the first time OV3600 recorded the MAC address as being associated.
Duration	Displays the length of time the MAC address has been associated.
Auth Type	Displays the type of authentication employed by the user. Supported auth types include: - **EAP**—Extensible Authentication Protocol. - **RADIUS accounting**—RADIUS accounting servers integrated with OV3600 provide the RADIUS Accounting Auth type - **WPA2**—Wi-Fi Protected Access 2 encryption - No Encryption OV3600 considers all other types as not authenticated. The information OV3600 displays in **Auth Type** and **Cipher** columns depends on what information the server receives from the devices it is monitoring. The client devices may all be similar, but if the APs to which they are associated are of different models, or if security is set up differently between them, then different **Auth Type** or **Cipher** values may be reported to OV3600. If all APs are the same model and all are set up the same way, then another reason for differing **Auth Types** might be the use of multiple VLANs or SSIDs. One client device might authenticate on one SSID using one **Auth Type** and another client device might authenticate on a second SSID using a different **Auth Type**.
Cipher	Displays the encryption or decryption cipher supporting the user, when this information is available. The client devices may all be similar, but if the APs to which they are associated are of different models, or if security is set up differently between them, then different **Auth Type** or **Cipher** values may be reported to OV3600.
Auth Time	Shows how long the user has been authenticated, in minutes. A negative number (such as -17 min) indicates that the user has not authenticated for the duration displayed.
Signal Quality	Displays the average signal quality the user experienced.
Usage	Displays the average bandwidth consumed by the MAC address.

Table 80: *Devices > Monitor > Connected Clients Fields and Default Values (Continued)*

Field	Description
Goodput	The ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes. Note that this information is not available for Instant devices running Instant releases prior to Instant 4.1.0.
Speed	The packet and byte counts of data frames successfully transmitted to and received from associated stations. Note that this information is not available for Instant devices running Instant releases prior to Instant 4.1.0.
Location	Displays the VisualRF box that allows users to view features including heatmap for a device and location history for a user.
LAN IP Addresses	Displays the IP assigned to the user MAC. This information is not always available. OV3600 can gather it from the ARP cache of switches discovered by OV3600. This column can accommodate multiple IP addresses for a client if it has both IPv4 and IPv6.
LAN Hostnames	The DNS hostname(s) broadcast by the client. This column can accommodate multiple hostnames for a client if it has both IPv4 and IPv6.

RF Neighbors

This table displays information about other devices in the AP's RF neighborhood, including the name of the AP or device, and the neighboring radio channel(s) and RSSI (in dBm) detected by the AP.

CDP Neighbors

The **Devices > Monitoring** page for devices that support Cisco Discovery Protocol (CDP) may display information for neighbor devices detected using CDP.

NOTE

Wireless controllers also include interface-specific data for wired interfaces on the **Devices > Interfaces** page. For more information, see "Monitoring the AOS-W-CX Switches and Mobility Access Switches" on page 153

Viewing the Radio Statistics Page

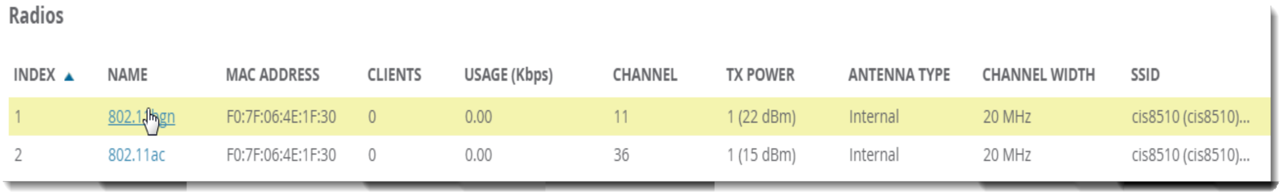
The Radio Statistics page contains statistics for pinpointing network issues for Alcatel-Lucent APs and Cisco WLC thin APs running firmware 4.2 or later.

Depending on the AP, assigned group profiles, and recent activity on a radio, you can evaluate:

- Recent and historical changes in the network
- Real-time statistics from the AP’s controller
- Actively interfering devices (requires that you set Alcatel-Lucent to Spectrum mode)
- Summary of major issues

To open the Radio Statistics page, navigate to the **Devices > Monitoring** page, then select the AP from the Devices List. Or, in the monitoring page for the AP, locate the radio in the Radios table and click the hyperlink to open the Radio Statistics page, as shown in Figure 62.

Figure 62: *Accessing Radio Statistics from an AP Monitoring Page*



Radios

INDEX ▲	NAME	MAC ADDRESS	CLIENTS	USAGE (Kbps)	CHANNEL	TX POWER	ANTENNA TYPE	CHANNEL WIDTH	SSID
1	802.11bgn	F0:7F:06:4E:1F:30	0	0.00	11	1 (22 dBm)	Internal	20 MHz	cis8510 (cis8510)...
2	802.11ac	F0:7F:06:4E:1F:30	0	0.00	36	1 (15 dBm)	Internal	20 MHz	cis8510 (cis8510)...

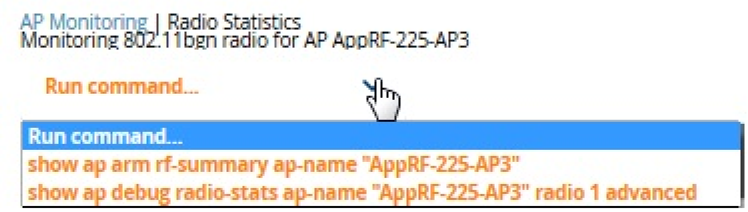
Running Commands from the Radio Statistics Page

Adaptive Radio Management (ARM) provides automated channel optimization, transmit power adjustment and channel width tuning for an individual AP or group of APs.

To run a show command:

1. Navigate to the **Devices > Monitoring** page, then select the switch from the Devices List.
2. In the monitoring page for the switch, locate the radio in the Radios table and click the hyperlink to open the Radio Statistics page.
3. Click **Run a command** and choose a command, as illustrated in Figure 63.

Figure 63: *Running a show command*



AP Monitoring | Radio Statistics
Monitoring 802.11bgn radio for AP AppRF-225-AP3

```
show ap arm rf-summary ap-name "AppRF-225-AP3"
show ap debug radio-stats ap-name "AppRF-225-AP3" radio 1 advanced
```

When this command is selected, a new browser window launches with the statistics in plain text. Other ARM-tracked metrics are visible in the **Radio Statistics** page for Alcatel-Lucent APs.

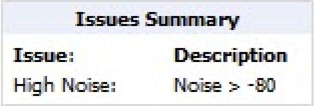
Issues Summary section

The **Issues Summary** section only displays when noise, client count, non-802.11 interfering devices, channel utilization, usage, and MAC and PHY errors reach a certain threshold of concern, as described in Table 81 and illustrated in Figure 64:

Table 81: *Issues Summary labels and thresholds*

Issue	Triggering Threshold
High Noise	> -80
High Number of Clients	> 15
High Channel Utilization	> 75%
High Usage	> 75% of max
Interfering Devices Detected	Detected within the last 5 minutes
High MAC/Phy Errors	> 1000 frames/sec

Figure 64: *Issues Summary Section Illustration*



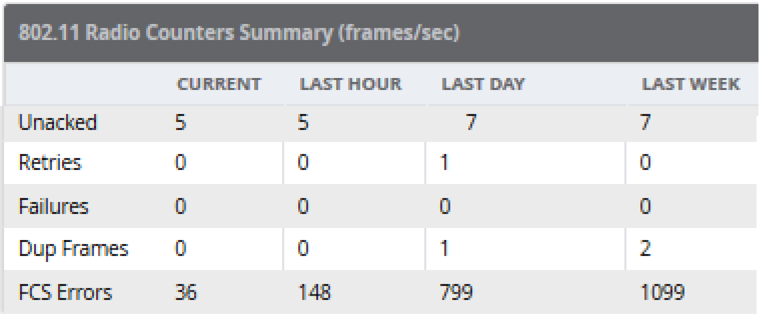
Issues Summary	
Issue:	**Description**
High Noise:	Noise > -80

These issues highlighted in this section can be examined in detail using the corresponding interactive graphs on the same page. See the "Radio Statistics Interactive Graphs" on page 144 section of this chapter for details.

802.11 Radio Counters Summary

This table appears for radios with 802.11 counters and summarizes the number of times an expected acknowledgment frame was not received, the number of duplicate frames, the number of frames containing Frame Check Sequence (FCS) errors, and the number of frame/packet transmission retries and failures. These aggregate error counts are broken down by Current, Last Hour, Last Day, and Last Week time frames, as illustrated in Figure 65.

Figure 65: ***802.11 Radio Counters Summary*** *table*



802.11 Radio Counters Summary (frames/sec)

	CURRENT	LAST HOUR	LAST DAY	LAST WEEK
Unacked	5	5	7	7
Retries	0	0	1	0
Failures	0	0	0	0
Dup Frames	0	0	1	2
FCS Errors	36	148	799	1099

The frame- per-second rate of these and other 802.11 errors over time are tracked and compared in the **802.11 Counters** graph on the same page.

Radio Statistics Interactive Graphs

Time-series graphs for the radio show changes recorded at every polling interval over time when polling with either SNMP or AMON. Clients and Usage data are polled based on the AP's group's **User Data Polling Period**. Channel, Noise, and Power are based on **AP Interface Polling Period**. 802.11 Counters data are based on the APs group’s **802.11 Counters Polling Period**.

Radio Noise and Radio Errors graphs are not supported for Autonomous Cisco Aironet APs.

The two graph panes enable simultaneous display of two different information sets, as detailed in the following table:

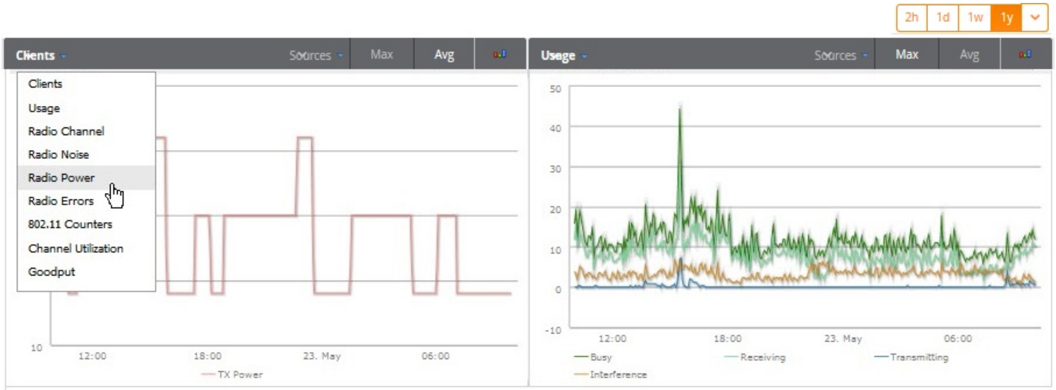
Table 82: *Radio Statistics Interactive Graphs Descriptions*

Graph Title	Description
Clients	A line graph that displays the maximum users associated to the corresponding radio at polling intervals over the time range set in the slider. Select **Show All** for other metrics such as average users and max users for various individual devices.

Table 82: *Radio Statistics Interactive Graphs Descriptions (Continued)*

Graph Title	Description
Usage	An area graph displaying the average bandwidth in each direction for the radio. Select **Show All** for other metrics such as max bandwidth in and out, average and max mesh/overhead or overhead bandwidth, and average/max Enet0.
Radio Channel	An area graph that displays the channel changes (if any) of the radio over time. Frequent, regular channel changes on an Alcatel-Lucent or Cisco WLC AP radio usually indicate that the Adaptive Radio Management feature (ARM) in AOS-W is compensating for high noise levels from interfering devices.
Radio Noise	An area graph that displays signal interference (noise floor) levels in units of dBm. Noise from interfering devices above your AP's noise threshold can result in dropped packets. For ARM-enabled Alcatel-Lucent APs, crossing the noise threshold triggers an automatic channel change.
Radio Power	A line graph that displays the average and maximum radio transmit power, between 0 and 30 dBm, over the time range set in the slider. You can adjust the transmit power manually in the **Devices > Manage** page for this radio's AP, or enable ARM on Alcatel-Lucent APs to dynamically adjust the power toward your acceptable Coverage Index as needed. For more information, see the Adaptive Radio Management chapter of the *Alcatel-Lucent AOS-W User Guide*.
Radio Errors	A line graph displaying the frame reception rate, physical layer error rate (resulting from poor signal reception or broken antennas), and the data link (MAC) layer (corrupt frames, driver decoding issues) for the radio.
802.11 Counters	A line graph that displays statistics such as frame rate, fragment rate, retry rate, duplicate frame rate, and other metrics tracked by 802.11 counters.
Utilization	Displays max and average percentages on this radio for busy, interfering receiving and transmitting signals. Special configuration on the controller is required to enable this data. Consult the *OmniVista 3600 Air Manager Best Practices Guide* for details. **NOTE:** (Alcatel-Lucent and Cisco WLC thin APs on supported firmware versions only)
Goodput	Displays the max and average goodput values. Goodput is the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes. The air time includes the retry effort taken for both successful and dropped frames.

Figure 66: *Radio Statistics Interactive Graphs Illustration – Radio Power and Channel Utilization displayed*

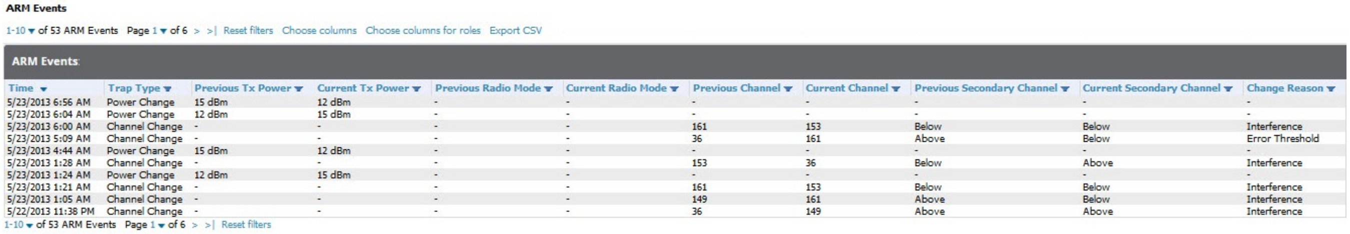


Recent ARM Events Log

If a radio references an active and enabled ARM profile and OV3600 is enabled as a trap host, ARM-initiated events are displayed in the ARM Events table with the original and modified values.

You can filter the results and export the table in CSV format. The columns and values are illustrated in Figure 67.

Figure 67: *ARM Events Table*



ARM Events

1-10 ▾ of 53 ARM Events Page 1 ▾ of 6 > >| Reset filters Choose columns Choose columns for roles Export CSV

ARM Events:

Time ▾	Trap Type ▾	Previous Tx Power ▾	Current Tx Power ▾	Previous Radio Mode ▾	Current Radio Mode ▾	Previous Channel ▾	Current Channel ▾	Previous Secondary Channel ▾	Current Secondary Channel ▾	Change Reason ▾
5/23/2013 6:56 AM	Power Change	15 dBm	12 dBm	-	-	-	-	-	-	-
5/23/2013 6:04 AM	Power Change	12 dBm	15 dBm	-	-	-	-	-	-	-
5/23/2013 6:00 AM	Channel Change	-	-	-	-	161	153	Below	Below	Interference
5/23/2013 5:09 AM	Channel Change	-	-	-	-	36	161	Above	Below	Error Threshold
5/23/2013 4:44 AM	Power Change	15 dBm	12 dBm	-	-	-	-	-	-	-
5/23/2013 1:28 AM	Channel Change	-	-	-	-	153	36	Below	Above	Interference
5/23/2013 1:24 AM	Power Change	12 dBm	15 dBm	-	-	-	-	-	-	-
5/23/2013 1:21 AM	Channel Change	-	-	-	-	161	153	Below	Below	Interference
5/23/2013 1:05 AM	Channel Change	-	-	-	-	149	161	Above	Below	Interference
5/22/2013 11:38 PM	Channel Change	-	-	-	-	36	149	Above	Above	Interference

1-10 ▾ of 53 ARM Events Page 1 ▾ of 6 > >| Reset filters

The columns and values are described in Table 83.

Table 83: *ARM Events table Columns and Values*

Column	Description
Time	The time of the ARM event.
Trap Type	The type of trap that delivered the change information. Current ARM trap types that display in OV3600 are: ● Power Change ● Mode Change ● Channel Change Values that display in the following columns depend on the Trap Type.
Previous Tx Power	Old value for transmit power before the Power Change event took place.
Current Tx Power	New transmit power value after the change.
Previous Radio Mode	Old value for radio mode before the Mode Change event took place.
Current Radio Mode	New radio mode value after the change.

Table 83: *ARM Events table Columns and Values (Continued)*

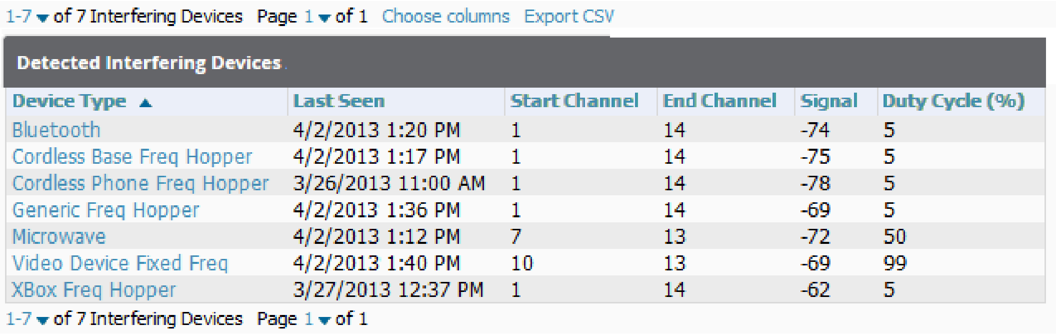
Column	Description
Previous Channel	Old primary channel value before the Channel Change event took place.
Current Channel	New primary channel value after the change.
Previous Secondary Channel	Old secondary channel value (for 40Mhz channels on 802.11n devices) before the Channel Change event took place.
Current Secondary Channel	New secondary channel value after the change.
Change Reason	If the noise and interference cause for the change can be determined, they will be displayed here. Mode change reasons are not yet tracked.

For information about configuring OV3600 as a trap host, see the *OmniVista 3600 Air Manager Best Practices Guide*.

Detected Interfering Devices Table

For Alcatel-Lucent APs running in Spectrum mode, the same non-802.11 interfering devices identified in the **Issues Summary** section are classified in the **Detected Interfering Devices** table along with the timestamp of its last detection, the start and end channels of the interference, the signal to noise ratio, and the percentage of time the interference takes place (duty cycle), as illustrated in Figure 68. This table can be exported to CSV format, and the displayed columns can be moved or hidden as needed.

Figure 68: *Detected Interfering Devices Table Illustration*



1-7 of 7 Interfering Devices Page 1 of 1 Choose columns Export CSV

Detected Interfering Devices

Device Type ▲	Last Seen	Start Channel	End Channel	Signal	Duty Cycle (%)
Bluetooth	4/2/2013 1:20 PM	1	14	-74	5
Cordless Base Freq Hopper	4/2/2013 1:17 PM	1	14	-75	5
Cordless Phone Freq Hopper	3/26/2013 11:00 AM	1	14	-78	5
Generic Freq Hopper	4/2/2013 1:36 PM	1	14	-69	5
Microwave	4/2/2013 1:12 PM	7	13	-72	50
Video Device Fixed Freq	4/2/2013 1:40 PM	10	13	-69	99
XBox Freq Hopper	3/27/2013 12:37 PM	1	14	-62	5

1-7 of 7 Interfering Devices Page 1 of 1

Possible device types for the **Detected Interfering Devices** table include:

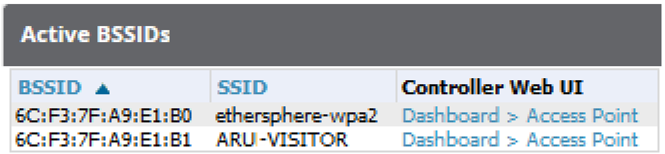
- Audio Device Fixed Freq
- Bluetooth
- Cordless Base Freq Hopper
- Cordless Phone Fixed Freq
- Cordless Phone Freq Hopper
- Generic Fixed Freq
- Generic Freq Hopper
- Microwave
- Microwave Inverter
- Unknown
- Video Device Fixed Freq

- Wi-Fi
- XBox Freq Hopper

Active BSSIDs Table

The Active BSSIDs table maps the BSSIDs on a radio with the SSID it broadcasts to the network, as illustrated in Figure 69. This table appears only for Alcatel-Lucent AP radios.

Figure 69: ***Active BSSIDs** Table Illustration*



Active BSSIDs

BSSID ▲	SSID	Controller Web UI
6C:F3:7F:A9:E1:B0	ethersphere-wpa2	Dashboard > Access Point
6C:F3:7F:A9:E1:B1	ARUI-VISITOR	Dashboard > Access Point

AirMatch Statistics for Mobility Master

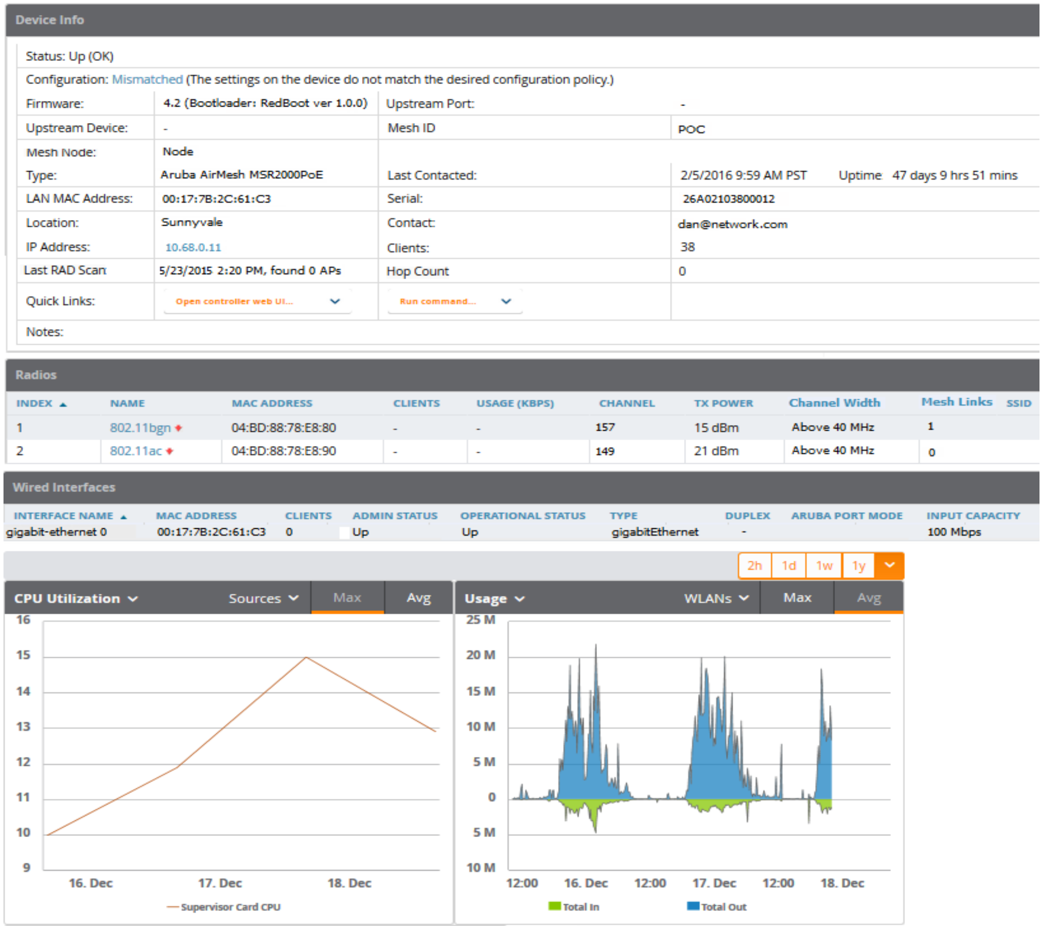
AirMatch enhances ARM by analyzing the past 24 hours of RF network statistics and proactively optimizing the network for the next day.

For more information on AirMatch, refer to the RF Planning and Channel Management chapter in the *Alcatel-Lucent AOS-W User Guide.*

Monitoring Mesh Devices

The monitoring page for mesh devices includes basic device information at the top, two tables for Radios and Wired Interfaces, and Clients, Usage, CPU Utilization, and Memory Utilization graphs. Under these graphs are a list of associated Clients, Mesh Links, RF Neighbors, and other common event logs and information.

Figure 70: *Devices > Monitor page for a Mesh Device*



Device Info

Status: Up (OK)

Configuration: Mismatched (The settings on the device do not match the desired configuration policy.)

Firmware:	4.2 (Bootloader: RedBoot ver 1.0.0)	Upstream Port:	-
Upstream Device:	-	Mesh ID	POC
Mesh Node:	Node		
Type:	Aruba AirMesh MSR2000PoE	Last Contacted:	2/5/2016 9:59 AM PST Uptime 47 days 9 hrs 51 mins
LAN MAC Address:	00:17:7B:2C:61:C3	Serial:	26A02103800012
Location:	Sunnyvale	Contact:	dan@network.com
IP Address:	10.68.0.11	Clients:	38
Last RAD Scan	5/23/2015 2:20 PM, found 0 APs	Hop Count	0
Quick Links:	Open controller web UI...	Run command...	
Notes:			

Radios

INDEX ▲	NAME	MAC ADDRESS	CLIENTS	USAGE (KBPS)	CHANNEL	TX POWER	Channel Width	Mesh Links	SSID
1	802.11bgn ♦	04:BD:88:78:E8:80	-	-	157	15 dBm	Above 40 MHz	1	
2	802.11ac ♦	04:BD:88:78:E8:90	-	-	149	21 dBm	Above 40 MHz	0	

Wired Interfaces

INTERFACE NAME ▲	MAC ADDRESS	CLIENTS	ADMIN STATUS	OPERATIONAL STATUS	TYPE	DUPLEX	ARUBA PORT MODE	INPUT CAPACITY
gigabit-ethernet 0	00:17:7B:2C:61:C3	0	Up	Up	gigabitEthernet	-		100 Mbps

These fields are described in detail in "Device Information for Access Points, Mesh Devices, and switches" on page 136.

Setting up Spectrum Analysis

The spectrum analysis software modules available on many Alcatel-Lucent APs can examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources.

The spectrum analyzer is used in conjunction with Alcatel-Lucent's Adaptive Radio Management (ARM) technology. While the spectrum analyzer identifies and classifies Wi-Fi and non-Wi-Fi sources of interference, ARM automatically ensures that APs serving clients will stay clear of interference.

Individual APs or groups of APs can be converted to dedicated spectrum monitors through the dot11a and dot11g radio profiles of that AP or AP group, or through a special spectrum override profile.

Each 802.11a and 802.11g radio profile references a spectrum profile, which identifies the spectrum band the radio will monitor and analyze, and defines the default ageout times for each monitored device type. By default, an 802.11a radio profile references a spectrum profile named **default-a** (which configures the radio to monitor the upper channels of the 5 GHz radio band), and an 802.11g radio profile references a spectrum profile named **default-g** (which configures the radio to monitor all channels the 2.4 GHz radio band).

Most interference will occur in the 2.4 GHz radio band.

For more information about Spectrum analysis and ARM technology, including a list of APs that support spectrum analysis refer to the *Alcatel-Lucent AOS-W User Guide*.

Spectrum Configurations and Prerequisites

The following prerequisites must be in place to configure an AP to run in Spectrum mode in OV3600:

- The AP must be in **Manage Read/Write** mode.
- The AP's associated switch must have an RFprotect license and must be running AOS-W 6.0 or later.
- Alcatel-Lucent GUI Config must be enabled for that AP's group in the **Groups > Basic** page.

There are three main situations in which you would set one or more devices to Spectrum mode in OV3600:

- Alcatel-Lucent AP Groups running permanently with the default Spectrum profile
- Individual APs running temporarily in Spectrum mode while part of an Alcatel-Lucent AP Group set to ap-mode
- switch-level Spectrum Overrides (an alternative to creating new Alcatel-Lucent AP groups or new radio profiles for temporary changes)

Setting up a Permanent Spectrum Alcatel-Lucent AP Group

If you have multiple supported Alcatel-Lucent APs in multiple switches that you want to run in Spectrum mode over the long run, you create a special Alcatel-Lucent AP group and set up a profile that is set to **spectrum-mode** and references the default **Spectrum** profile. Set up more than one profile if you want to utilize both radio bands in Spectrum mode.

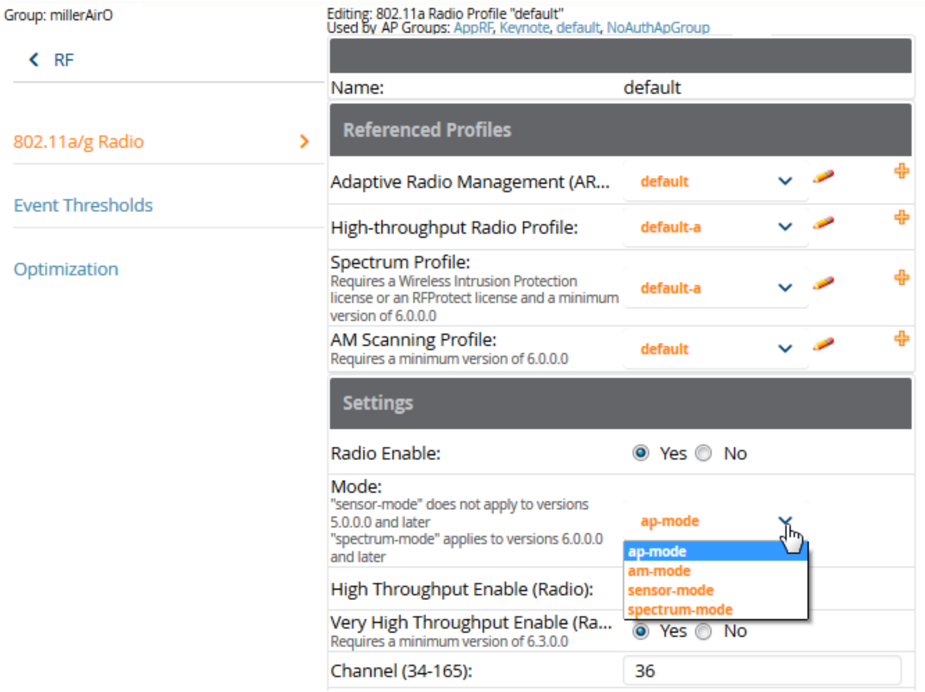
If you use an 802.11a or 802.11g radio profile to create a group of spectrum monitors, all APs in any AP group referencing that radio profile will be set to spectrum mode. Therefore, best practices are to create a new 802.11a or 802.11g radio profile just for spectrum monitors.

If **Use Global Alcatel-Lucent Configuration** is enabled in **OV3600 Setup > General**, create the configuration below, then go to the switch group's **Controller Config** page and select the newly created Alcatel-Lucent AP Group.

Perform these steps to set the AP group to use the default Spectrum profile settings:

1. On the **Groups > Controller Config** page, click the **Add New Alcatel-Lucent Group** button.
2. Give the new Group a name (such as Spectrum APs), and select the plus sign next to the **802.11a Radio Profile** field to create a new radio profile.
3. Enter a name under the General Settings section of **Profiles > RF > 802.11a/g Radio**.
4. In the **Other Settings** section, change the **Mode** field from **ap-mode** to **spectrum-mode**, as illustrated in Figure 71, and then select **Save**.

Figure 71: *Spectrum mode in Controller Config*



Group: millerAirO

‹ RF

802.11a/g Radio ›

Event Thresholds

Optimization

Editing: 802.11a Radio Profile "default"
Used by AP Groups: AppRF, Keynote, default, NoAuthApGroup

Name: default

Referenced Profiles

Adaptive Radio Management (AR...	default
High-throughput Radio Profile:	default-a
Spectrum Profile: Requires a Wireless Intrusion Protection license or an RFProtect license and a minimum version of 6.0.0.0	default-a
AM Scanning Profile: Requires a minimum version of 6.0.0.0	default

Settings

Radio Enable:	● Yes ○ No
Mode: "sensor-mode" does not apply to versions 5.0.0.0 and later "spectrum-mode" applies to versions 6.0.0.0 and later	ap-mode
High Throughput Enable (Radio):	
Very High Throughput Enable (Ra... Requires a minimum version of 6.3.0.0	● Yes ○ No
Channel (34-165):	36

The above steps will use the defaults in the referenced **Spectrum Profile**. In most cases, you should not change the settings in the default profile. If you must change the defaults, however, navigate to **Groups > Controller Config > Profiles > RF > 802.11a/g Radio > Spectrum** page, and create a new Spectrum profile with non-default settings.

If all of the devices in this Alcatel-Lucent AP Group are managed by the same switch and you want to temporarily override one or more profile settings in your spectrum-mode APs, you can set up a switch override.

To disable spectrum mode in this group, change the referenced radio profile back to **default**.

Configuring an Individual AP to run in Spectrum Mode

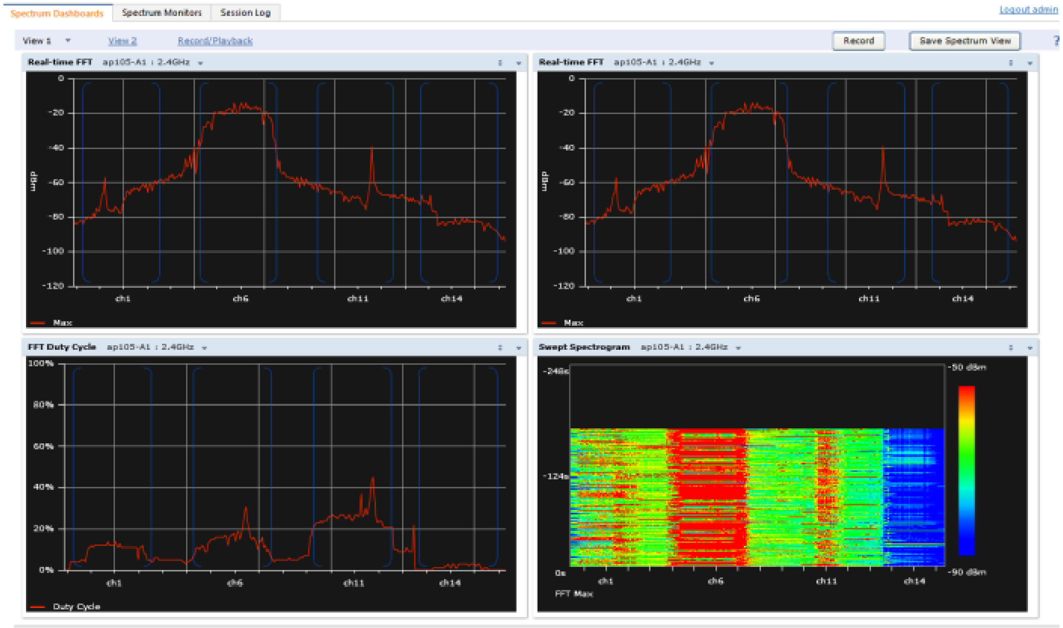
If you want to temporarily set an individual radio in an AP to run in Spectrum mode without creating or changing Alcatel-Lucent AP Groups or radio profiles, perform these steps to set up a Spectrum Override on a supported Alcatel-Lucent AP:

1. Navigate to **Devices > List**, right-click the Spectrum-supported AP in the Devices List, and then select **Audit** from the shortcut menu. Or you can navigate to **Devices > Config** to access the Device Configuration page.
2. After reviewing the device configuration, set the AP to **Manage Read/Write** mode.
3. Select **Yes** on the **Spectrum Override** field for one or both radios, depending on the band and channels you want it to analyze.
4. Select the band that should run in spectrum. If you selected the 5GHz band in the 802.11an Radio section, choose the lower, middle, or upper range of channels that you want to be analyzed by this radio.
5. Select **Save and Apply** and confirm your edit. This overrides the current **Mode** setting for that AP (ap-mode or am-mode).

After making this change, you can view the **Radio Role** field that will appear in the **Radios** section of the **Devices > Monitor** page.

The new role, **Spectrum Sensor**, is a link to the Spectrum Analysis page for the switch that manages this AP, as illustrated in Figure 72.

Figure 72: *Spectrum Analysis on switch Dashboard*

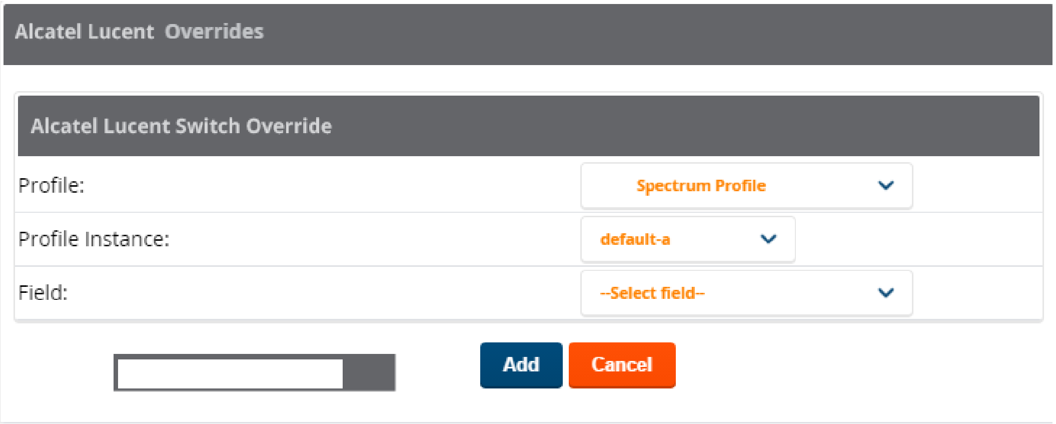


To disable Spectrum mode on this individual AP after it has collected data, return to the **Devices > Manage** page for this AP and set the **Spectrum Override** field back to **No**.

Configuring a switch to use the Spectrum Profile

You can use OV3600 to customize individual fields in the profile instance used by a particular switch without having to create new Alcatel-Lucent AP groups and new radio profiles. To do this, you can set a switch-level override for its referenced Spectrum profile on the **Devices > Manage page**, as illustrated in Figure 73. This will affect all Spectrum-supported APs managed by this switch.

Figure 73: *Override Section of a Supported switch's Manage Page*



Alcatel Lucent Overrides

Alcatel Lucent Switch Override

Profile:	Spectrum Profile
Profile Instance:	default-a
Field:	--Select field--

Perform these steps to override individual profile settings for an Alcatel-Lucent switch that is part of a spectrum-mode Alcatel-Lucent AP group:

1. Select a Spectrum-supported Alcatel-Lucent switch that is referencing a Spectrum profile, and go to its **Devices > Manage** page. Set it to **Manage Read/Write** mode.
2. Under the Alcatel-Lucent Overrides section, click the **Add New Alcatel-Lucent switch Override** button.

3. In the **Profile** drop-down menu, select the **Spectrum Profile** type.
4. In the **Profile Instance** drop-down menu, select the instance of the Spectrum profile used by the switch.
5. In the **Field** drop-down menu, select the setting you would like to change (such as an Age-Out setting or a Spectrum Band), and enter the overriding value below it.
6. Select **Add** to save your changes.
7. Repeat this process to create additional overrides for this switch.
8. When you have finished, select **Save and Apply**.

You can also use the above procedure to turn on Spectrum mode for radio profiles on one particular switch, or use the overrides to point your radio profile to a non-default Spectrum profile for just this switch.

Monitoring the AOS-W-CX Switches and Mobility Access Switches

OV3600 displays the detailed information and tools to help you monitor the AOS-W-CX and Mobility Access Switches.

For information about these features, see the following sections:

- "Device Information" on page 153
- "Graphs" on page 154
- "Detailed Summary Tables" on page 154

> NOTE
>
> For information on the general monitoring data that appears on the **Devices > Monitor** page for all device types, see "Monitoring Basics" on page 131.

Device Information

Table 84 describes the device information that you see in the switch monitoring page for the AOS-W-CX Switches and Mobility Access Switches.

Table 84: *Device Information for the AOS-W-CX Switches and Mobility Access Switches*

Field	Description
Status	Displays the connection status between OV3600 and the wired device: ● **Up**. Everything is working as it should. ● **Down**. Either OV3600 can reach the device but can't speak with it using SNMP, or OV3600 is unable to reach the device or connect to it using SNMP. **NOTE:** When the device is down due to an `SNMP get failed` error, verify that SNMP is enabled on the device and check the SNMP credentials that OV3600 is using on the **Devices > Manage** page. An `ICMP ping failed` error indicates that OV3600 can't connect to the device, or the device needs to be rebooted or reset.
Configuration	● **Good**. All the settings on the device agree with the settings OV3600 wants them to have. ● **Mismatched**. There is a configuration mismatch between what is on the device and what OV3600 wants to push to the device. The **Mismatched** link directs you to this specific **Devices > Device Configuration** page where each mismatch is highlighted. ● **Unknown**. The device configuration has not yet been fetched, and there might be an issue with credentials. ● **Verifying**. The device is fetching a configuration that will be compared to the desired settings. ● **Error**. Indicates a problem with the device. This configuration is accompanied with a description of the error.

Table 84: *Device Information for the AOS-W-CX Switches and Mobility Access Switches (Continued)*

Field	Description
Firmware	The firmware version running on the AP. **NOTE:** Newer AirMesh APs include the new bootloader APBoot. OV3600 helps to identify the new AirMesh APs from the old SKUs by displaying the bootloader information here.
Upstream Device	The upstream device (also called the CDP neighbor) that OV3600 discovers using CDP, or, for non-Cisco devices that OV3600 supports, using bridge forwarding tables.
Upstream Port	The upstream port on the device.
Type	The make of the device.
Model	The model of the device.
Last Contacted	The most recent time OV3600 has polled the device (see "Configuring Basic Settings for Device Groups" on page 75 for information about the poll interval).
Switch Role	The role of the device, which might, for example, be primary or secondary.
LAN MAC Address	The MAC address of the Ethernet interface on the device.
Serial	The serial number of the device.
Location	The SNMP location of the device.
Contact	The person to contact.
IP Address	The IP address that OV3600 uses to communicate with the device. This link provides access to the web management interface. Hover your mouse to access the device using HTTP, HTTPs, telnet or SSH.
Usage	The combined bandwidth through the device at time of polling.

Graphs

The following interactive graphs are available:

- Clients. This graph shows the maximum and average client count reported by the device.
- Usage. This graph shows the bandwidth in and out reported by the device.
- CPU utilization. This graph shows the overall CPU utilization (not on a per-CPU basis) of the device.
- Memory utilization. This graph shows the average used, free memory, and average max memory for the device.

If you click a graph, a full size view opens. Click ⌄ to choose which graph to display on the monitoring page.

Detailed Summary Tables

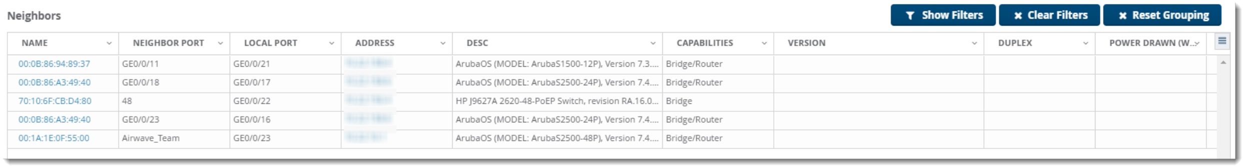
OV3600 can help you monitor the wired infrastructure, providing detailed summary tables about your wired network on the **Devices > Monitor** page. From this page, you can drill down into diagnostics, client details, and interface monitoring pages from links found in these tables.

Neighbors

OV3600 uses the source protocol (SNMP/HTTP or CDP/LLDP) to discover devices on the network and goes a step further and discovers neighbors directly connected to a wired device.

You can view information about all neighbors on the the **Neighbors** table of the monitoring page, as shown in Figure 74.

Figure 74: *Neighbors Table*



NAME	NEIGHBOR PORT	LOCAL PORT	ADDRESS	DESC	CAPABILITIES	VERSION	DUPLEX	POWER DRAWN (W...
00:0B:86:94:89:37	GE0/0/11	GE0/0/21	[redacted]	ArubaOS (MODEL: ArubaS1500-12P), Version 7.3....	Bridge/Router			
00:0B:86:A3:49:40	GE0/0/18	GE0/0/17	[redacted]	ArubaOS (MODEL: ArubaS2500-24P), Version 7.4....	Bridge/Router			
70:10:6F:CB:D4:80	48	GE0/0/22	[redacted]	HP J9627A 2620-48-PoEP Switch, revision RA.16.0...	Bridge			
00:0B:86:A3:49:40	GE0/0/23	GE0/0/16	[redacted]	ArubaOS (MODEL: ArubaS2500-24P), Version 7.4....	Bridge/Router			
00:1A:1E:0F:55:00	Airwave_Team	GE0/0/23	[redacted]	ArubaOS (MODEL: ArubaS2500-48P), Version 7.4....	Bridge/Router			

Table 85 describes the **Neighbors** table fields.

Table 85: *Neighbors Table Fields and Descriptions*

Field	Description
Name	Displays the name of the neighbor device. For example, a MAC address, hostname, or make and model. If an IP address is known for the device, a link provides access to the monitoring page.
Neighbor Port	Displays the port ID of the neighbor device.
Local Port	Displays the port ID of the local device device.
Address Type	Displays the type of address of the neighbor device.
Address	Displays the network address associated with the neighbor. This link provides access to the web management interface. Hover your pointer over the to open a managment window to the device using HTTP, HTTPs, telnet or SSH.
Desc	Specify a description that provides additional information about the neighbor device (recommended).
Capabilities	Displays the device type: router, switch, or none (information is not available)
Version	Displays the software version running on the neighbor device.
CDP Version	Indicates the software version running on the neighbor device.
Duplex	Indicates the mode of operation of the connection: simplex, duplex, or half-duplex.
Power Drawn (Watts)	Displays the amount of power used on the interface of the neighbor device.
VTP Mgmt Domain	Displays the name of the group of VLANs associated with the neighbor device.
Sysname	Displays the system name of the neighbor device.
Primary Mgmt Address Type	Displays the type of address of the primary management interface.

Field	Description
Primary Mgmt Address	Displays the network address of the primary management interface.
Secondary Mgmt Address Type	Displays the type of address of the secondary management interface.
Secondary Mgmt Address	Displays the network address of the secondary management interface.
Physical Location	Displays the location of the neighbor device.
Native VLAN	Displays the ID number of the VLAN on the neighbor device.
Appliance ID	Displays the ID number of the appliance.
VLAN ID	Displays the ID number of the management Vlan on the neighboring device.
Last Change	Indicates when the device was last seen.
MTU	Specifies the largest packet size which can be received on the neighbor device.
Source	Displays the protocol used for device discovery: CDP.

Connected Devices

OV3600 detects authenticated and rogue devices and reports them in the **Connected Devices** table (see Figure 75). OV3600 also uses upstream data to calculate possible neighbors and reports these devices in the **Connected Devices** table.

Most information will not be available for rogue devices. If you click ✎ and add a name, device type, location, contact, or notes to a rogue device, the device will move to the client table and be considered an unauthenticated client. The device category will change from device to client.

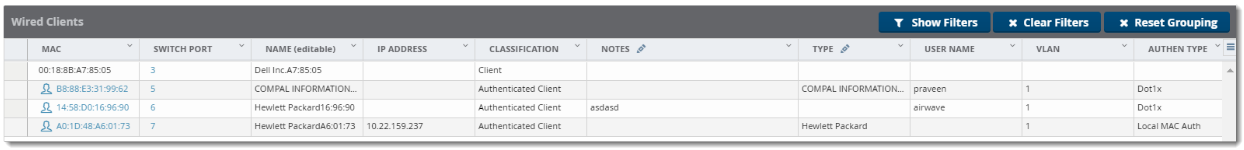
NOTE

When OV3600 discovers more than one MAC address from one port and none of the MAC addresses have LLDP/CDP information, OV3600 will list only one unknown device without a MAC address.

NOTE

When OV3600 discovers a switch that doesn't have a MAC address, it classifies the device as an unknown client. You cannot authenticate the client by modifying the device because it doesn't have a MAC address associated with it.

Figure 75: *Connected Devices Table*



MAC	SWITCH PORT	NAME (editable)	IP ADDRESS	CLASSIFICATION	NOTES	TYPE	USER NAME	VLAN	AUTHEN TYPE
00:18:8B:A7:85:05	3	Dell Inc.A7:85:05		Client					
B8:88:E3:31:99:62	5	COMPAL INFORMATION...		Authenticated Client		COMPAL INFORMATION...	praveen	1	Dot1x
14:58:D0:16:96:90	6	Hewlett Packard16:96:90		Authenticated Client	asdasd		airwave	1	Dot1x
A0:1D:48:A6:01:73	7	Hewlett PackardA6:01:73	10.22.159.237	Authenticated Client		Hewlett Packard		1	Local MAC Auth

Table 86: *Connected Devices Fields and Descriptions*

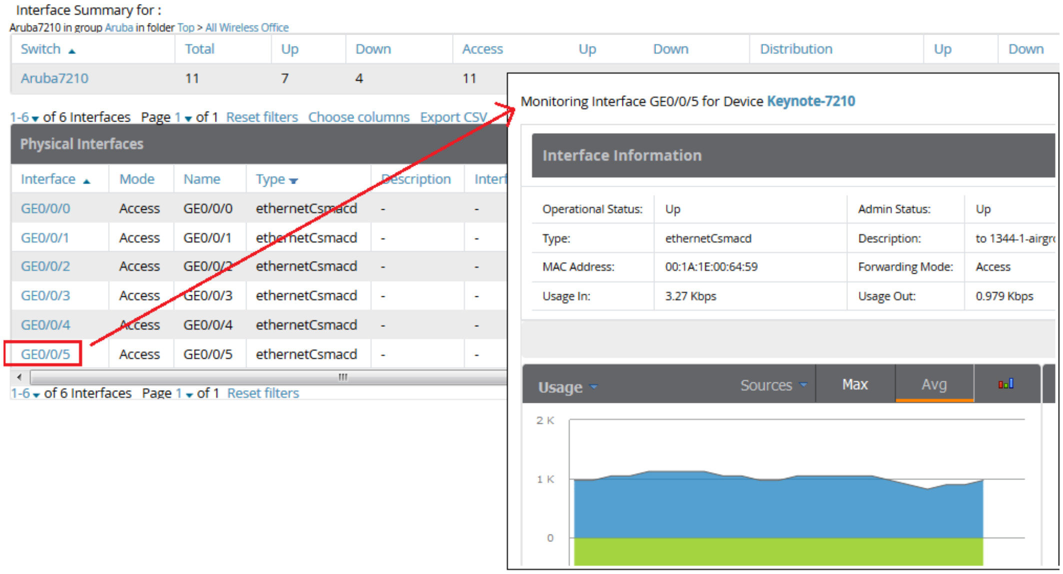
Field	Description
MAC	MAC address for the device. This link provides access to the diagnostics page for the client. Find more information about "Troubleshooting Client Issues" on page 189.
Switch Port	Port number associated with the device. This link provides access to the monitoring page for the interface.
Name	Name of the device. You can enter any name.
IP Address	If the gateway is managed by OV3600, the IP address is shown here.
Classification	Displays the classification of the device after OV3600 detects the device: - Authenticated Client. This link provides access to the Connected Client page. - Client. This link provides access to the Rogue table, where you can identify the device.
Notes	Notes to help you identify the client. You can enter anything.
Type	Type of device. You can enter anything.
User Name	Name that is used on the device for authentication.
User Role	Identifies the role-based operations that can be performed on the device.
VLAN	The number of the VLAN.
Stack Role	In a stack of switches, the role can be: master.
Bandwidth	The bandwidth used by the device. If the device supports bandwidth per MAC address, the bandwidth shown is the total bandwith used by all attached devices.
Host Name	The hostname of the neighbor device, which is retrieved from the DNS lookup.
Authen Type	The authentication server type: - Dot1x - Captive Portal - Local MAC Auth - WPA-PSK

Interfaces

The **Devices > Interfaces** page for managed switches and routers displays interface-specific data, graphs, and detailed summary tables for any connected clients and wired clients. For stacked switches, the master switch displays information for the interfaces of all the members, including its own.

From the **Physical Interfaces** and **Virtual Interfaces** tables, click any interface link to open the **Interface Monitoring** page for that interface, as shown in Figure 76

Figure 76: *Opening the Monitoring Interface Page*



Interface Summary for :
Aruba7210 in group Aruba in folder Top > All Wireless Office

Switch ▲	Total	Up	Down	Access	Up	Down	Distribution	Up	Down
Aruba7210	11	7	4	11					

1-6 ▾ of 6 Interfaces Page 1 ▾ of 1 Reset filters Choose columns Export CSV

Physical Interfaces

Interface ▲	Mode	Name	Type ▾	Description	Interf
GE0/0/0	Access	GE0/0/0	ethernetCsmacd	-	-
GE0/0/1	Access	GE0/0/1	ethernetCsmacd	-	-
GE0/0/2	Access	GE0/0/2	ethernetCsmacd	-	-
GE0/0/3	Access	GE0/0/3	ethernetCsmacd	-	-
GE0/0/4	Access	GE0/0/4	ethernetCsmacd	-	-
GE0/0/5	Access	GE0/0/5	ethernetCsmacd	-	-

1-6 ▾ of 6 Interfaces Page 1 ▾ of 1 Reset filters

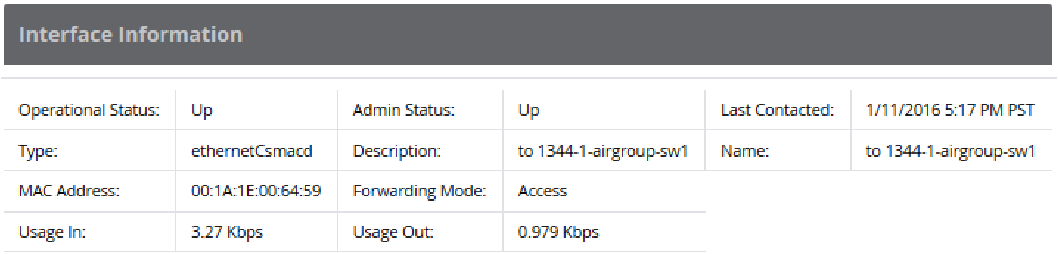
Monitoring Interface GE0/0/5 for Device **Keynote-7210**

Interface Information

Operational Status:	Up	Admin Status:	Up
Type:	ethernetCsmacd	Description:	to 1344-1-airgr
MAC Address:	00:1A:1E:00:64:59	Forwarding Mode:	Access
Usage In:	3.27 Kbps	Usage Out:	0.979 Kbps

Figure 77 shows an example of interface information for an Ethernet CSMA/CD interface.

Figure 77: *Interface Information*



Interface Information

Operational Status:	Up	Admin Status:	Up	Last Contacted:	1/11/2016 5:17 PM PST
Type:	ethernetCsmacd	Description:	to 1344-1-airgroup-sw1	Name:	to 1344-1-airgroup-sw1
MAC Address:	00:1A:1E:00:64:59	Forwarding Mode:	Access		
Usage In:	3.27 Kbps	Usage Out:	0.979 Kbps		

Table 87 describes fields that you see in **Interface Information** for switches and routers.

Table 87: *Interface Information Fields and Descriptions*

Field	Description
Operational Status	Displays the operational state of the interface: Up or Down.
Type	Type of interface.
MAC Address	Displays the MAC address assigned to the interface.
Usage In	Displays the incoming interface load in Kbps.
Admin Status	Displays the configuration on the port: Up or Down.
Description	Information about the interface.
Forwarding Mode	Indicates whether the interface is configured as an access port with one VLAN or a trunk interface with two or more VLANs.

Table 87: *Interface Information Fields and Descriptions (Continued)*

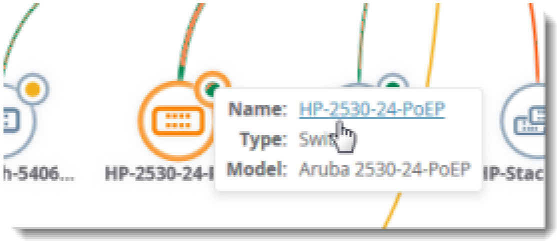
Field	Description
Usage Out	Displays the outgoing interface load in Kbps.
Last Contacted	The most recent time OV3600 has polled the interface.
Name	Name of the interface. You can enter any name.

Monitoring Alcatel-Lucent AOS-W-Switches

Available for AOS-W-Switches, OV3600 puts all your switch monitoring information into a single page. There are horizontal tabs across the top of the page, so you don't have to scroll down to view the data.

You can open the switch monitoring page by navigating to **Devices > List** and selecting a switch from the list. Or, from a topology map, hover over the device to access the quick link in the tooltip (see Figure 78).

Figure 78: *Accessing a Monitoring Page from Topology*



NOTE

Localization isn't available for new switch monitoring pages. Buttons, menus, and tabs display in English.

Getting Started

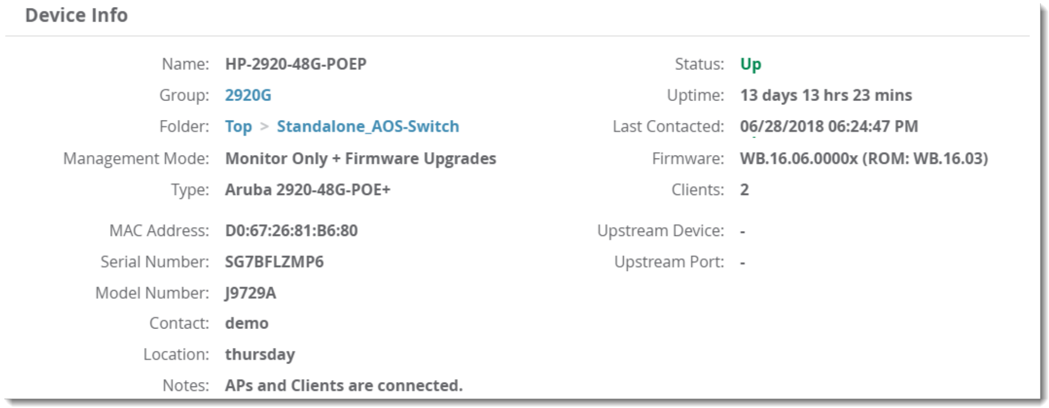
From the monitoring page for a switch or switch stack, you can view color-coded status, navigate using quick links, and get details from tooltips.

Color-Coded Status

Color-coded thresholds and icons help you visualize status and hardware-related alerts. For information on the threshold values that each color represents, see "Hardware Tab" on page 173.

For current device status, green text indicates whether the device is up ().

Figure 79: *Device Information*



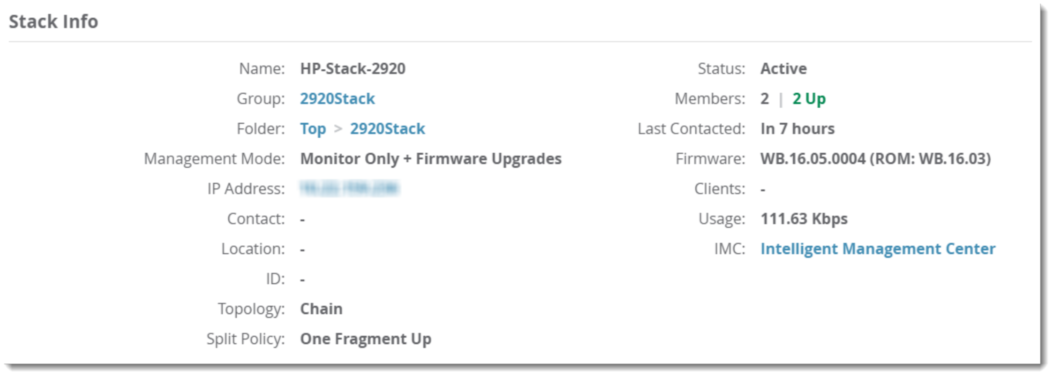
Device Info

Name: HP-2920-48G-POEP
Group: 2920G
Folder: Top > Standalone_AOS-Switch
Management Mode: Monitor Only + Firmware Upgrades
Type: Aruba 2920-48G-POE+
MAC Address: D0:67:26:81:B6:80
Serial Number: SG7BFLZMP6
Model Number: J9729A
Contact: demo
Location: thursday
Notes: APs and Clients are connected.

Status: Up
Uptime: 13 days 13 hrs 23 mins
Last Contacted: 06/28/2018 06:24:47 PM
Firmware: WB.16.06.0000x (ROM: WB.16.03)
Clients: 2
Upstream Device: -
Upstream Port: -

Gray text indicates that the switch is disabled, or the stack is active (Figure 80).

Figure 80: *Stack Information*



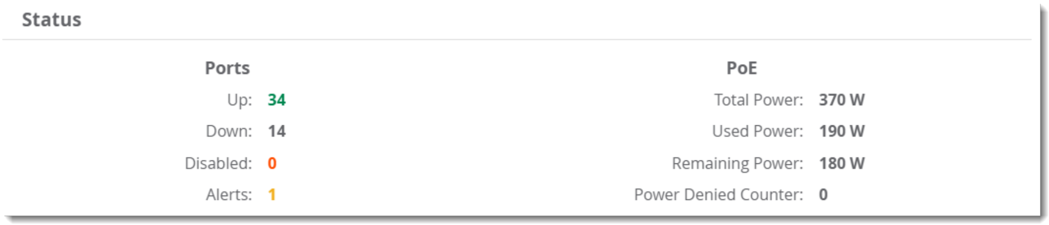
Stack Info

Name: HP-Stack-2920
Group: 2920Stack
Folder: Top > 2920Stack
Management Mode: Monitor Only + Firmware Upgrades
IP Address: [redacted]
Contact: -
Location: -
ID: -
Topology: Chain
Split Policy: One Fragment Up

Status: Active
Members: 2 | 2 Up
Last Contacted: In 7 hours
Firmware: WB.16.05.0004 (ROM: WB.16.03)
Clients: -
Usage: 111.63 Kbps
IMC: Intelligent Management Center

Color-coded port status shows you the health of your ports (Figure 81).

Figure 81: *Ports and Power over Ethernet (PoE) Status*



Status

Ports
Up: 34
Down: 14
Disabled: 0
Alerts: 1

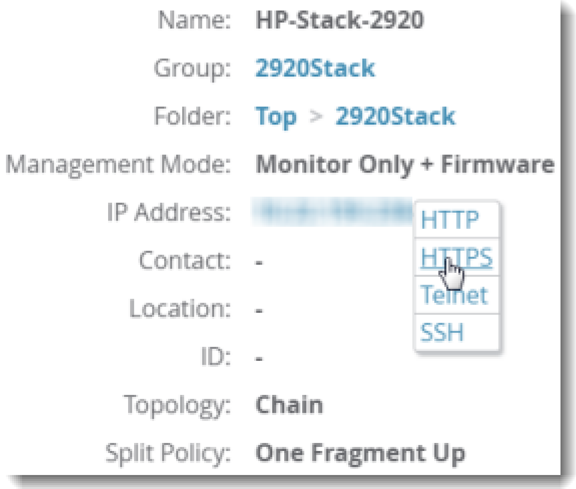
PoE
Total Power: 370 W
Used Power: 190 W
Remaining Power: 180 W
Power Denied Counter: 0

Navigate Using Quick Links

Blue links let you navigate to group and folder monitoring pages; open a WebUI, CLI session, or the Intelligent Management Center (see Figure 80). These quick links also let you switch between stack and stack member monitoring pages .

In Figure 82, clicking the IP address link and selecting HTTPS will open a secure HTTP session with the stack commander.

Figure 82: *Accessing the WebUI from the Stack Information*



Name: HP-Stack-2920

Group: 2920Stack

Folder: Top > 2920Stack

Management Mode: Monitor Only + Firmware

IP Address: [redacted]

Contact: -

Location: -

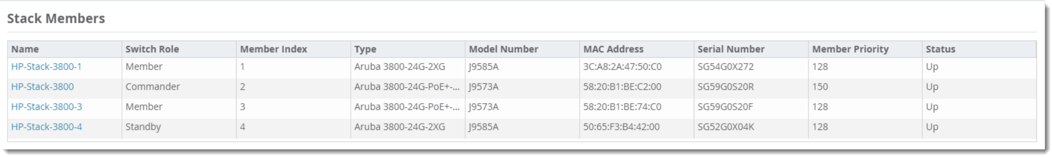
ID: -

Topology: Chain

Split Policy: One Fragment Up

When looking at a stack, OV3600 will display information about each stack member in the Stack Member table at the bottom of the Summary tab. You can easily go from one switch member to another in the stack by clicking the blue stack member link to open the monitoring page for the stack member (see Figure 83).

Figure 83: *Accessing the Monitoring Page for a Stack Member*

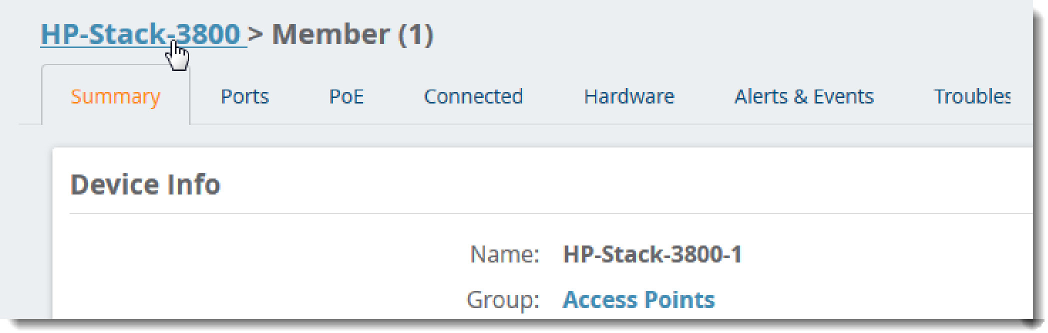


Stack Members

Name	Switch Role	Member Index	Type	Model Number	MAC Address	Serial Number	Member Priority	Status
HP-Stack-3800-1	Member	1	Aruba 3800-24G-2XG	J9585A	3C:A8:2A:47:50:C0	SG54G0X272	128	Up
HP-Stack-3800	Commander	2	Aruba 3800-24G-PoE+-...	J9573A	58:20:B1:BE:C2:00	SG59G0S20R	150	Up
HP-Stack-3800-3	Member	3	Aruba 3800-24G-PoE+-...	J9573A	58:20:B1:BE:74:C0	SG59G0S20F	128	Up
HP-Stack-3800-4	Standby	4	Aruba 3800-24G-2XG	J9585A	50:65:F3:B4:42:00	SG52G0X04K	128	Up

If you navigate away from the monitoring page for the stack, you will see the stack name link in the upper-left corner of the WebUI (see Figure 84). Click this link to return to the monitoring page.

Figure 84: *Navigate Backwards from the Member to the Stack*



Device Info

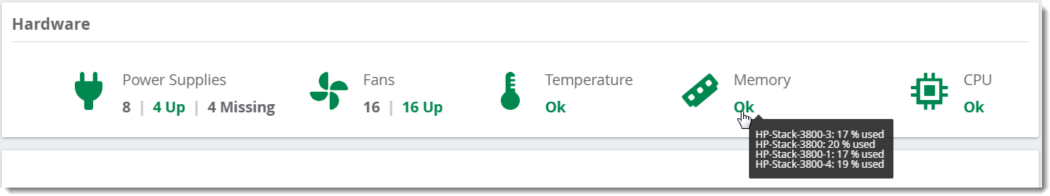
Name: HP-Stack-3800-1

Group: Access Points

Get Details from Tooltips

Find out details about power supplies, environmental information, memory and CPU consumption by pointing your mouse over the statistics. When looking at the hardware status for the stack, icons and color-coded thresholds are the same as for stand-alone switches, but OV3600 displays the details for stack members (see Figure 85). For more information about monitoring your hardware, see "Hardware Tab" on page 173.

Figure 85: *Hardware Tooltips*



Hardware

Power Supplies
8 | 4 Up | 4 Missing

Fans
16 | 16 Up

Temperature
Ok

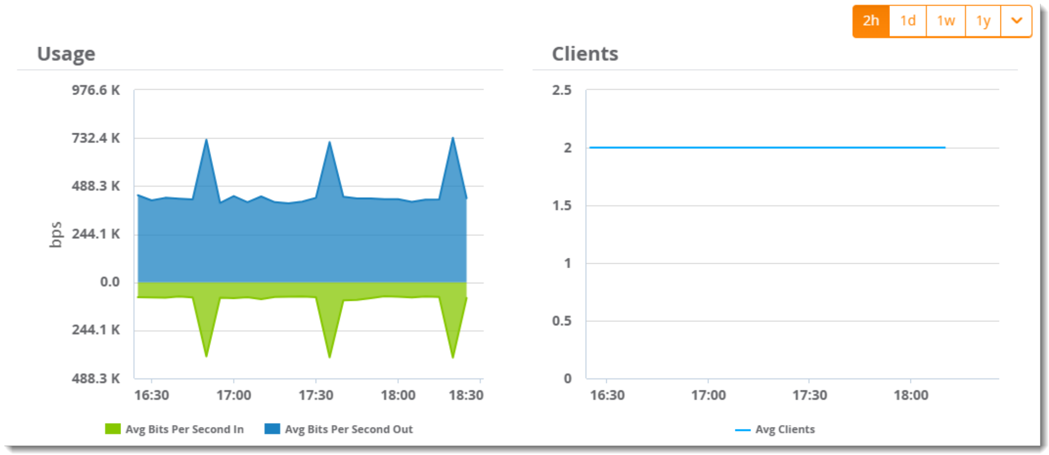
Memory
Ok

HP-Stack-3800-3: 17 % used
HP-Stack-3800: 20 % used
HP-Stack-3800-1: 17 % used
HP-Stack-3800-4: 19 % used

CPU
Ok

Get details about usage and connected clients by pointing your mouse over the graphs. For more information about monitoring connected clients, see "Connected Tab" on page 169.

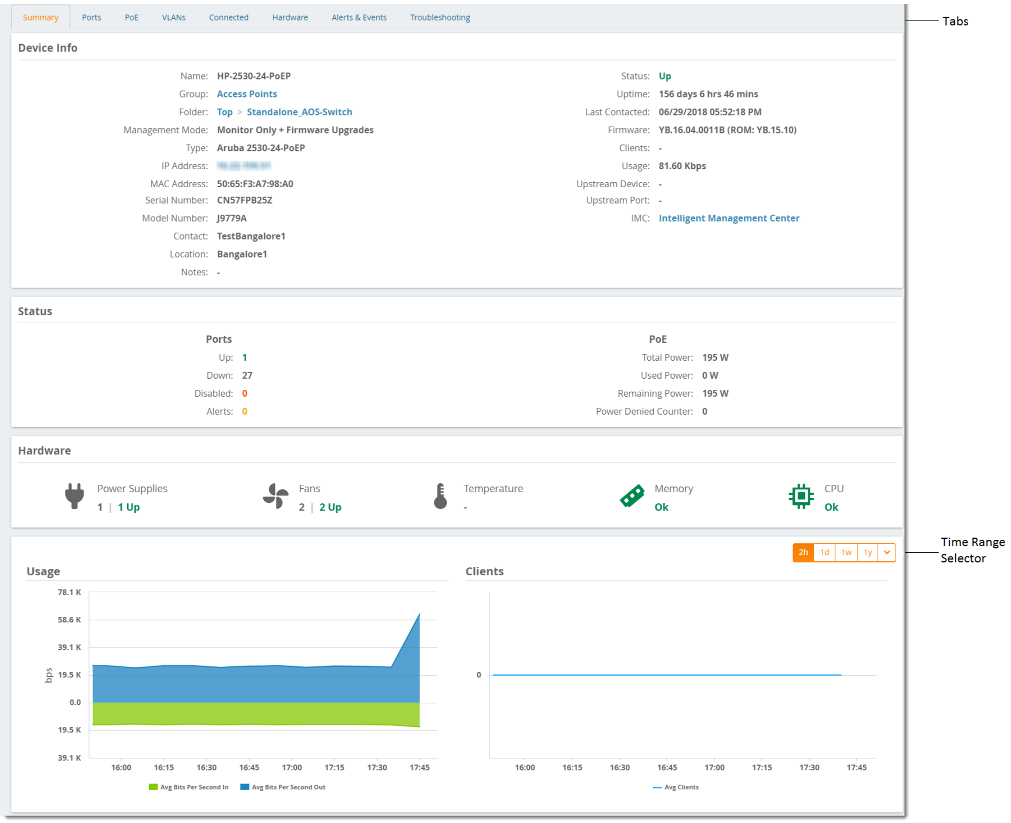
Figure 86: *Viewing Graph Tooltips*



Back to the Top

Summary Tab

The Summary tab is the central point for monitoring your switches and switch stacks. Track status like device uptime, trunk and uplink connectivity, available power, number of fans present, environmental information, CPU and memory usage. For stacks, you can see important information like member status, stack topology, and split stacking policy.



Tabs

Device Info

Name: HP-2530-24-PoEP
Group: Access Points
Folder: Top > Standalone_AOS-Switch
Management Mode: Monitor Only + Firmware Upgrades
Type: Aruba 2530-24-PoEP
IP Address: [redacted]
MAC Address: 50:65:F3:A7:98:A0
Serial Number: CN57FPB25Z
Model Number: J9779A
Contact: TestBangalore1
Location: Bangalore1
Notes: -

Status: Up
Uptime: 156 days 6 hrs 46 mins
Last Contacted: 06/29/2018 05:52:18 PM
Firmware: YB.16.04.0011B (ROM: YB.15.10)
Clients: -
Usage: 81.60 Kbps
Upstream Device: -
Upstream Port: -
IMC: Intelligent Management Center

Status

Ports
Up: 1
Down: 27
Disabled: 0
Alerts: 0

PoE
Total Power: 195 W
Used Power: 0 W
Remaining Power: 195 W
Power Denied Counter: 0

Hardware

Power Supplies 1 | 1 Up
Fans 2 | 2 Up
Temperature -
Memory Ok
CPU Ok

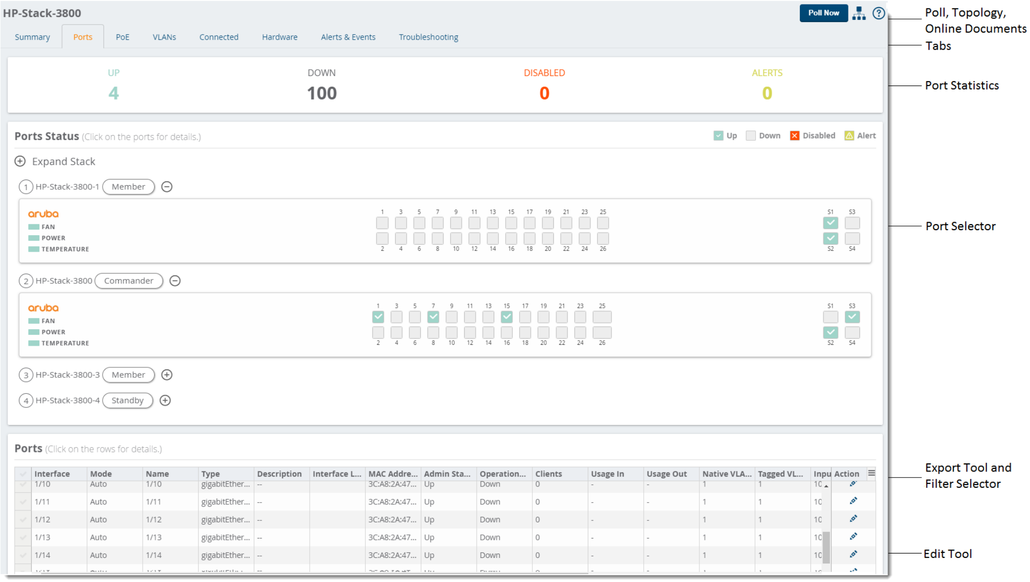
Time Range Selector

[Back to the Top](#)

Ports Tab

With the Ports tab, OV3600 displays the front panel of the switch, letting you visualize port status, hardware status, and other properties. Select **Ports** at the top of the Switch Monitoring page to open the Ports tab.

Figure 87: *Ports Tab for a Switch Stack*



UP 4
DOWN 100
DISABLED 0
ALERTS 0

Ports Status (Click on the ports for details.)

Ports (Click on the rows for details.)

Interface	Mode	Name	Type	Description	Interface L...	MAC Addre...	Admin Sta...	Operation...	Clients	Usage In	Usage Out	Native VLA...	Tagged VL...	Inpu	Action
1/10	Auto	1/10	gigabitEther...	--		3C:A8:2A:47...	Up	Down	0	-	-	1	1	10	
1/11	Auto	1/11	gigabitEther...	--		3C:A8:2A:47...	Up	Down	0	-	-	1	1	10	
1/12	Auto	1/12	gigabitEther...	--		3C:A8:2A:47...	Up	Down	0	-	-	1	1	10	
1/13	Auto	1/13	gigabitEther...	--		3C:A8:2A:47...	Up	Down	0	-	-	1	1	10	
1/14	Auto	1/14	gigabitEther...	--		3C:A8:2A:47...	Up	Down	0	-	-	1	1	10	

Poll, Topology, Online Documents Tabs

Port Statistics

Port Selector

Export Tool and Filter Selector

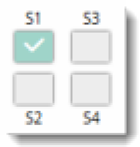
Edit Tool

See Port Counts

You can see from the colored numbers how many ports are up, down, disabled, or how many alerts are red and require action.

You can also identify SFP ports on a Gigabit switch by their rectangular shape, and stack ports by their number. For example, if there are Stack Ports 1, 2, 3, and 4, you'll see them labeled as S1, S2, S3, and S4 on the switch faceplate, as shown in Figure 88.

Figure 88: *Example of Stack Ports*



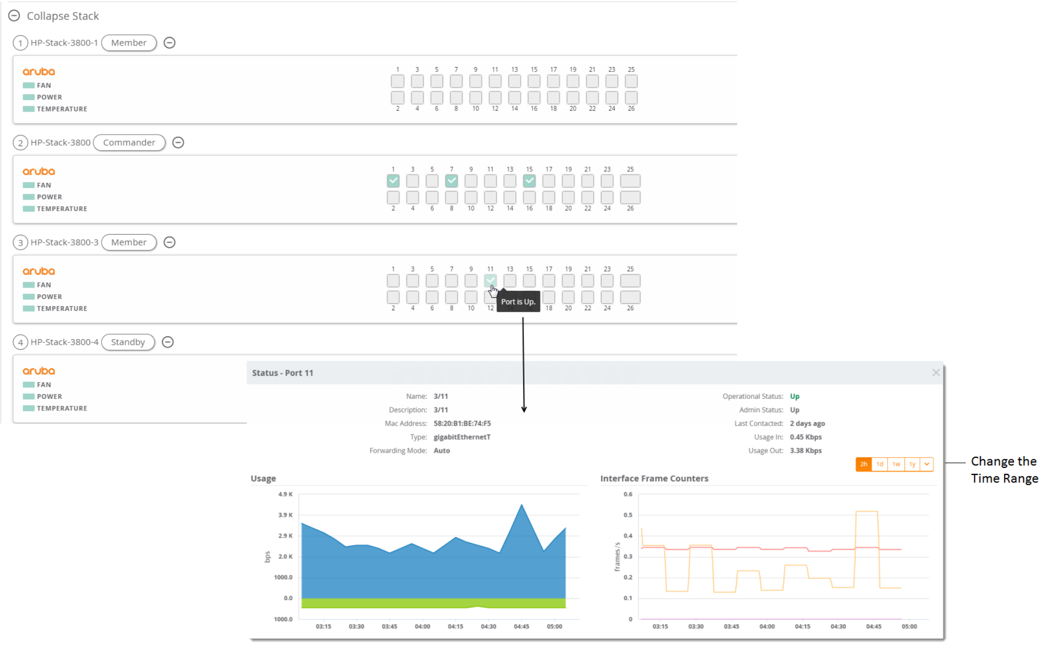
NOTE

Port status isn't available for stack ports.

Open a Port Status Pop-Up

You can point your mouse over the interactive faceplate to view port status, or click the port to view details and graphs in a pop-up window, as shown in Figure 89. If you manage a large number of devices and you want to collapse the view, click ⊖ at the stack or member level.

Figure 89: *Opening the Ports Status Pop-up*



Status - Port 11

Name: 3/11
Description: 3/11
Mac Address: 58:20:B1:BE:74:F5
Type: gigabitEthernetT
Forwarding Mode: Auto

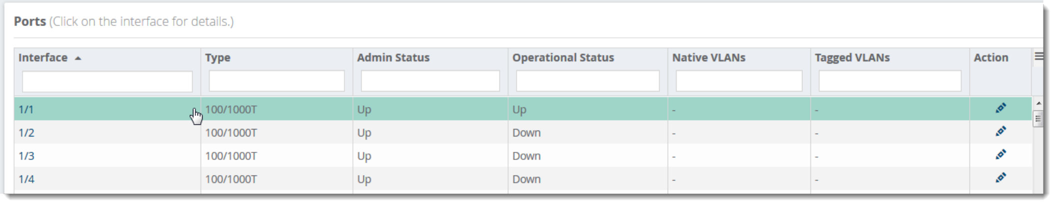
Operational Status: Up
Admin Status: Up
Last Contacted: 2 days ago
Usage In: 0.45 Kbps
Usage Out: 3.38 Kbps

Edit a Physical Interface

You can configure the port interface and add optional details using the Edit tool.

1. From the Ports tab, locate the interface in the Port table.

Figure 90: *Selecting the Interface*



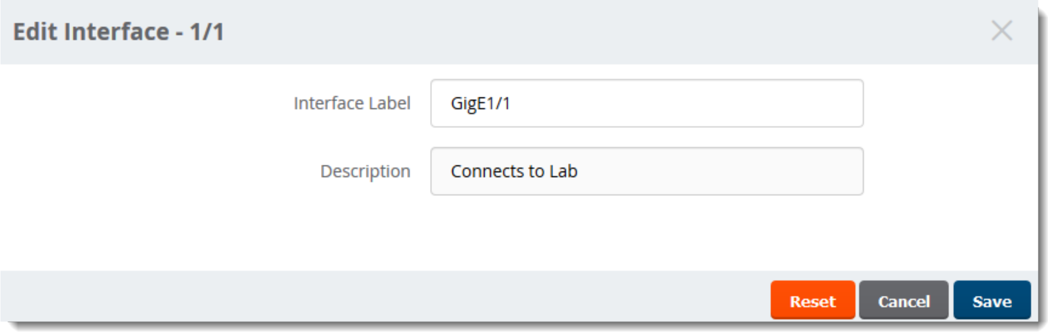
Ports (Click on the interface for details.)

Interface ▲	Type	Admin Status	Operational Status	Native VLANs	Tagged VLANs	Action
1/1	100/1000T	Up	Up	-	-	✎
1/2	100/1000T	Up	Down	-	-	✎
1/3	100/1000T	Up	Down	-	-	✎
1/4	100/1000T	Up	Down	-	-	✎

2. Click ✎ to open the Edit Interface pop-up window.

3. Type a descriptive label to identify the port interface.
4. Type a port description that could be helpful for anyone tracing the port.

Figure 91: *Edit Interface for a Port*



Edit Interface - 1/1

Interface Label: GigE1/1

Description: Connects to Lab

5. Click **Save**.

Get Interface Details

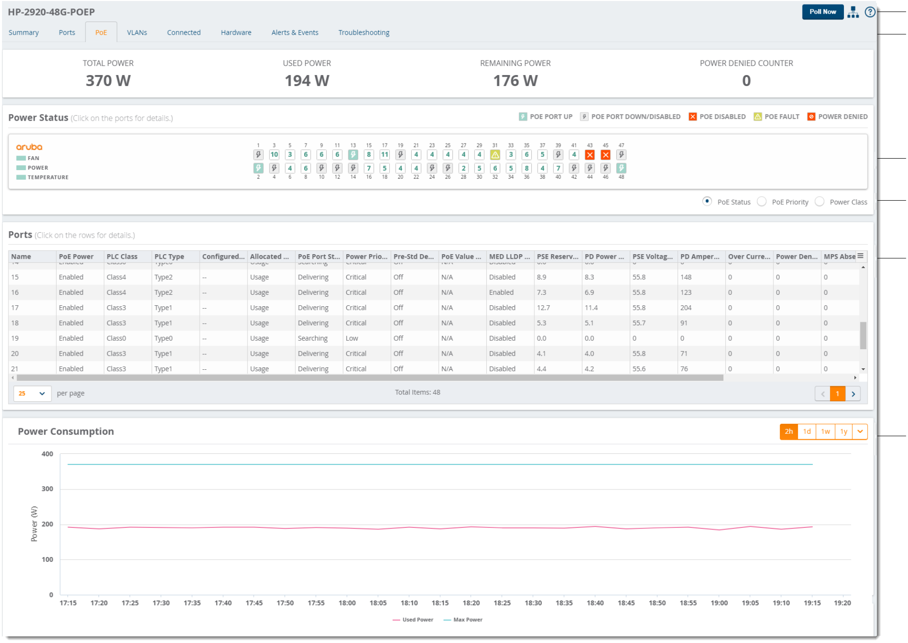
From the Ports table, you can see:

- Interface identfied by the interface number.
- Port speed and duplex (data transfer operation), or mode.
- If available, the name of the interface entered on the Edit Interface pop-up.
- Type of port, such as gigabit Ethernet (gigabitEthernetT) and 10 gigabit Ethernet (tenGbE-T).
- If available, information about the interface entered on the Edit Interface pop-up.
- If available, the interface label.
- MAC Address assigned to the interface.
- Admin Status: up or down.
- Operational status of the interface: up or down.
- How many clients are connected to the device.
- If available, the incoming interface load in Kbps.
- If available, the outgoing interface load in Kbps.
- ID number of the native VLAN on the neighbor device.
- Ports that are part of the specific tagged VLAN.
- Input capacity of the interface in Mbps.
- Output capacity of the interface in Mbps.
- Maximum transaction unit (MTU) which can be received on the neighbor device.
- Port duplex mode, which can be set to auto-negotiate the duplex mode when the device makes a network connection, or manually set to full or half-duplex mode.
- If the port is part of a trunk.
- If the port is part of a group of trunks.

PoE Tab

If the switch supports PoE, OV3600 provides detailed information on the configuration, power usage, and statistics of a selected port. Select **PoE** at the top of the monitoring page for the switch or stack to open the PoE tab.

Figure 92: *PoE Tab*



HP-2920-48G-POEP

TOTAL POWER	USED POWER	REMAINING POWER	POWER DENIED COUNTER
370 W	194 W	176 W	0

Power Status (Click on the ports for details.)

○ PoE Status ○ PoE Priority ○ Power Class

Ports (Click on the rows for details.)

Name	PoE Power	PLC Class	PLC Type	Configured...	Allocated ...	PoE Port St...	Power Prio...	Pre-Std De...	PoE Value ...	MED LLDP ...	PSE Reserv...	PD Power ...	PSE Voltag...	PD Amper...	Over Curre...	Power Den...	MPS Abse
15	Enabled	Class4	Type2	--	Usage	Delivering	Critical	Off	N/A	Disabled	8.9	8.3	55.8	148	0	0	0
16	Enabled	Class4	Type2	--	Usage	Delivering	Critical	Off	N/A	Enabled	7.3	6.9	55.8	123	0	0	0
17	Enabled	Class3	Type1	--	Usage	Delivering	Critical	Off	N/A	Disabled	12.7	11.4	55.8	204	0	0	0
18	Enabled	Class3	Type1	--	Usage	Delivering	Critical	Off	N/A	Disabled	5.3	5.1	55.7	91	0	0	0
19	Enabled	Class0	Type0	--	Usage	Searching	Low	Off	N/A	Disabled	0.0	0.0	0	0	0	0	0
20	Enabled	Class3	Type1	--	Usage	Delivering	Critical	Off	N/A	Disabled	4.1	4.0	55.8	71	0	0	0
21	Enabled	Class3	Type1	--	Usage	Delivering	Critical	Off	N/A	Disabled	4.4	4.2	55.6	76	0	0	0

25 per page Total Items: 48

Power Consumption

Poll, Topology, Online Documents

Tabs

Port Selector

PoE Overlays

Export Tool and Filter Selector

Time Range Selector

See PoE Statistics

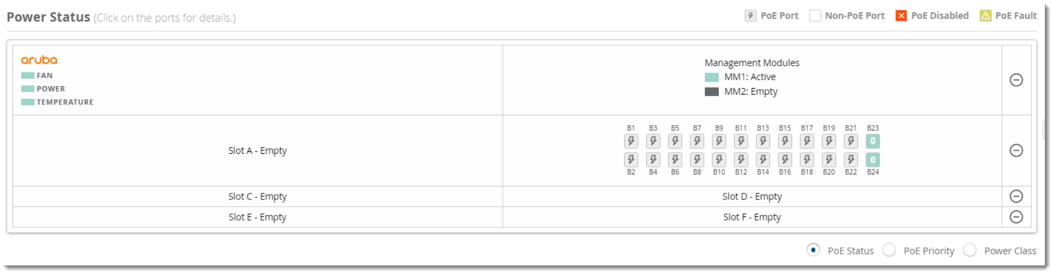
High-level counts tell you the total power available, used, and remaining. When more power is required than allowed for a device or port, OV3600 will display a powered denied count.

Change the Faceplate Using Overlays

You can change the information you see in the faceplate by selecting the PoE status, PoE priority, or Power Class overlays at the lower right corner of the faceplate.

In Figure 93, Ports B23 and B24 are online and not using power.

Figure 93: *Power Status Overlay*

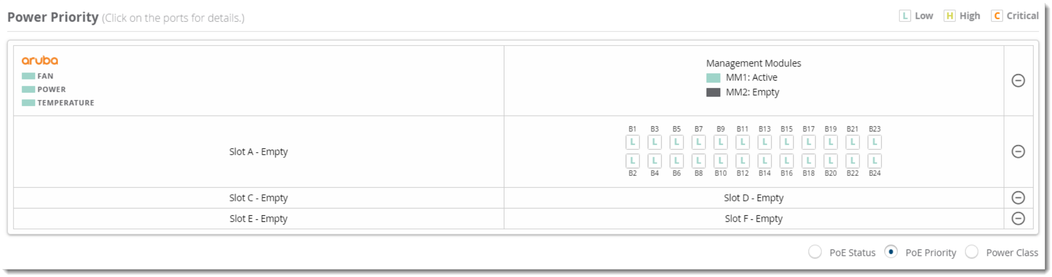


Power Status (Click on the ports for details.)

● PoE Status ○ PoE Priority ○ Power Class

In Figure 94, the power priority for all the PoE ports is low. If there is a power demand higher than the power budget on the switch, Port B1 has priority over Port B24.

Figure 94: *Power Priority Overlay*

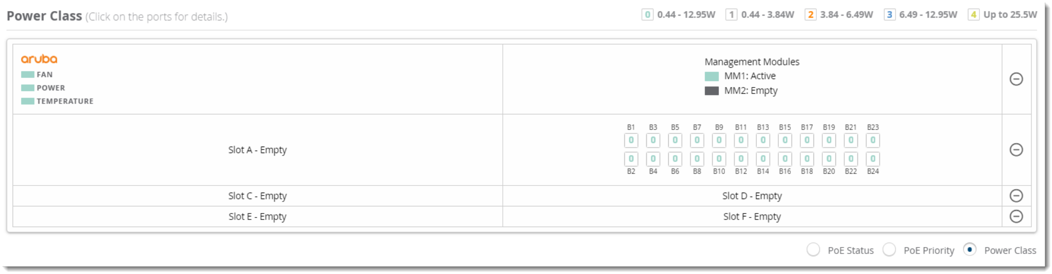


Power Priority (Click on the ports for details.)

○ PoE Status ● PoE Priority ○ Power Class

In Figure 95, all the PoE ports are designated as PoE Power Class 0 and must be allocated up to 12.95 W.

Figure 95: *Power Class Overlay*

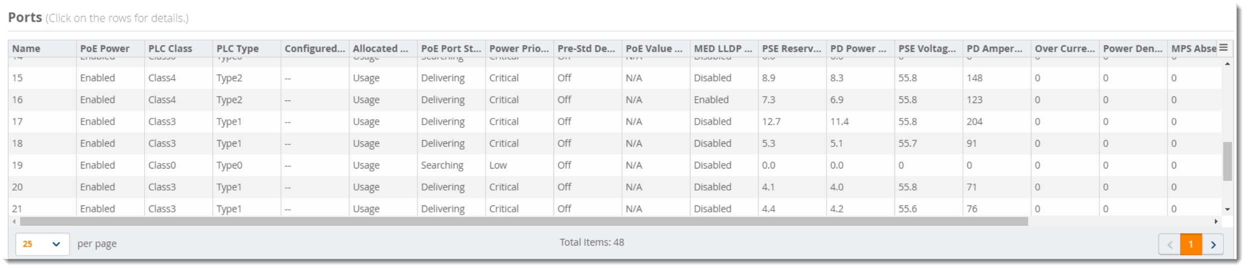


Get Port Details

From the Ports table (Figure 96), you can see :

- PoE configuration, including the PoE power, PLC class/type, power allocation method, current PoE port status, power priority, pre-standard detection, and the maximum power draw allocated to a PD on a port.
- LLDP information, including whether the switch supports PoE negotiation over LLDP.
- Statistics like PSE reserved power, actual power drawn from the PD, over current count, power denied count, PSE voltage, PD power draw, MPS absent count, short count, PSE TLV configured, and PSE TLV configured.

Figure 96: *Ports Table*



Ports (Click on the rows for details.)

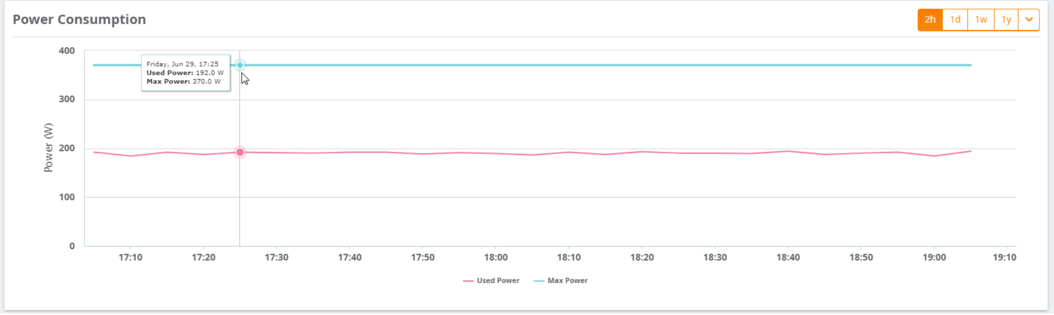
Name	PoE Power	PLC Class	PLC Type	Configured...	Allocated ...	PoE Port St...	Power Prio...	Pre-Std De...	PoE Value ...	MED LLDP ...	PSE Reserv...	PD Power ...	PSE Voltag...	PD Amper...	Over Curre...	Power Den...	MPS Abse
15	Enabled	Class4	Type2	--	Usage	Delivering	Critical	Off	N/A	Disabled	8.9	8.3	55.8	148	0	0	0
16	Enabled	Class4	Type2	--	Usage	Delivering	Critical	Off	N/A	Enabled	7.3	6.9	55.8	123	0	0	0
17	Enabled	Class3	Type1	--	Usage	Delivering	Critical	Off	N/A	Disabled	12.7	11.4	55.8	204	0	0	0
18	Enabled	Class3	Type1	--	Usage	Delivering	Critical	Off	N/A	Disabled	5.3	5.1	55.7	91	0	0	0
19	Enabled	Class0	Type0	--	Usage	Searching	Low	Off	N/A	Disabled	0.0	0.0	0	0	0	0	0
20	Enabled	Class3	Type1	--	Usage	Delivering	Critical	Off	N/A	Disabled	4.1	4.0	55.8	71	0	0	0
21	Enabled	Class3	Type1	--	Usage	Delivering	Critical	Off	N/A	Disabled	4.4	4.2	55.6	76	0	0	0

25 per page   Total Items: 48   1

View Power Consumption

The Power Consumption graph shows you the maximum power and power in use on the PoE slot, as shown in Figure 97.

Figure 97: *Power Consumption Graph*



Back to the Top

VLANs Tab

The VLANs tab shows all the details about the switch, including the configured VLANs and the port mappings for both tagged and untagged VLANs. Selecting **VLANs** at the top of the monitoring page for the switch or stack opens the VLANs tab.

NOTE

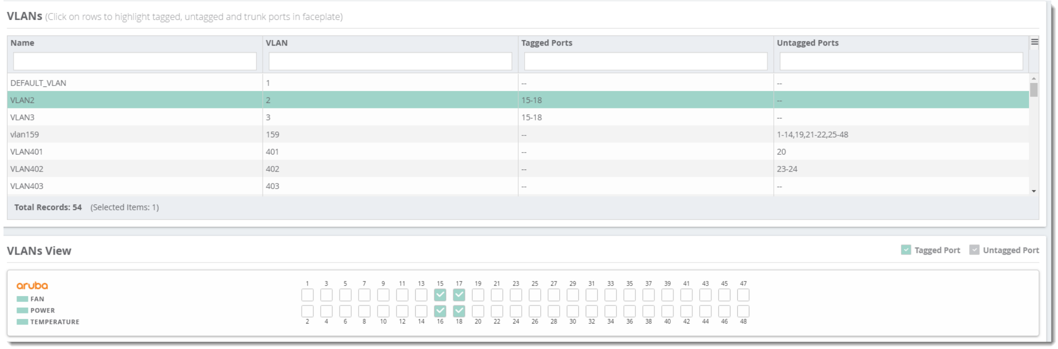
The VLANs tab isn't available for members in the stack, and it is only available from the stack view.

Change the VLANs View in the Faceplate

You can change the VLANs view by select a VLAN from the VLANs table. OV3600 highlights the tagged or untagged ports in the faceplate.

In Figure 98, OV3600 highlights tagged Ports 15 to 18 when you select VLAN 2.

Figure 98: *Highlighting the Tagged Ports in the Faceplate*



VLANs (Click on rows to highlight tagged, untagged and trunk ports in faceplate)

Name	VLAN	Tagged Ports	Untagged Ports
DEFAULT_VLAN	1	--	--
VLAN2	2	15-18	--
VLAN3	3	15-18	--
vlan159	159	--	1-14,19,21-22,25-48
VLAN401	401	--	20
VLAN402	402	--	23-24
VLAN403	403	--	--

Total Records: 54 (Selected Items: 1)

VLANs View

Get Trunk Details

If VLAN trunking information is available, OV3600 displays a list of active trunks on the device or the configured trunk groups. Active trunks are trunk groups that have ports assigned to them.

Get Virtual Interface Details

From the Virtual Interface table, you can see:

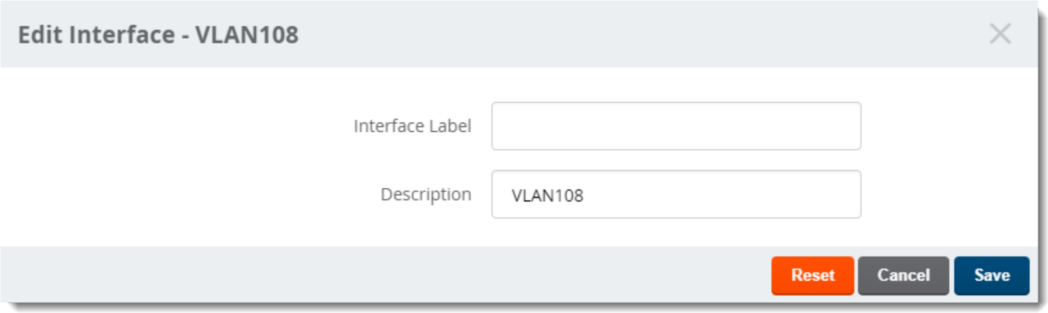
- Interface configuration, including the name, type of interface, MAC address, IP address and an alias, and the IPv6 global unicast address.
- Status on the port and interface.
- If any, interface labels entered on the Edit Interface pop-up. For more information, see "Edit a Virtual Interface" on page 168.

Edit a Virtual Interface

You can configure the virtual interface and add optional details using the Edit tool.

1. Navigate to the monitoring page of a switch that has a configured VLAN.
2. Select the VLANs tab, then scroll down the page to locate the interface in the Virtual Interfaces table.
3. Click ✎ to open the Edit Interface pop-up window.

Figure 99: *Edit Interface*



Edit Interface - VLAN108

Interface Label	
Description	VLAN108

4. Type a descriptive label to identify the port interface.

5. Type details in the Description field that could be helpful for anyone working with the device.
6. Click **Save**.

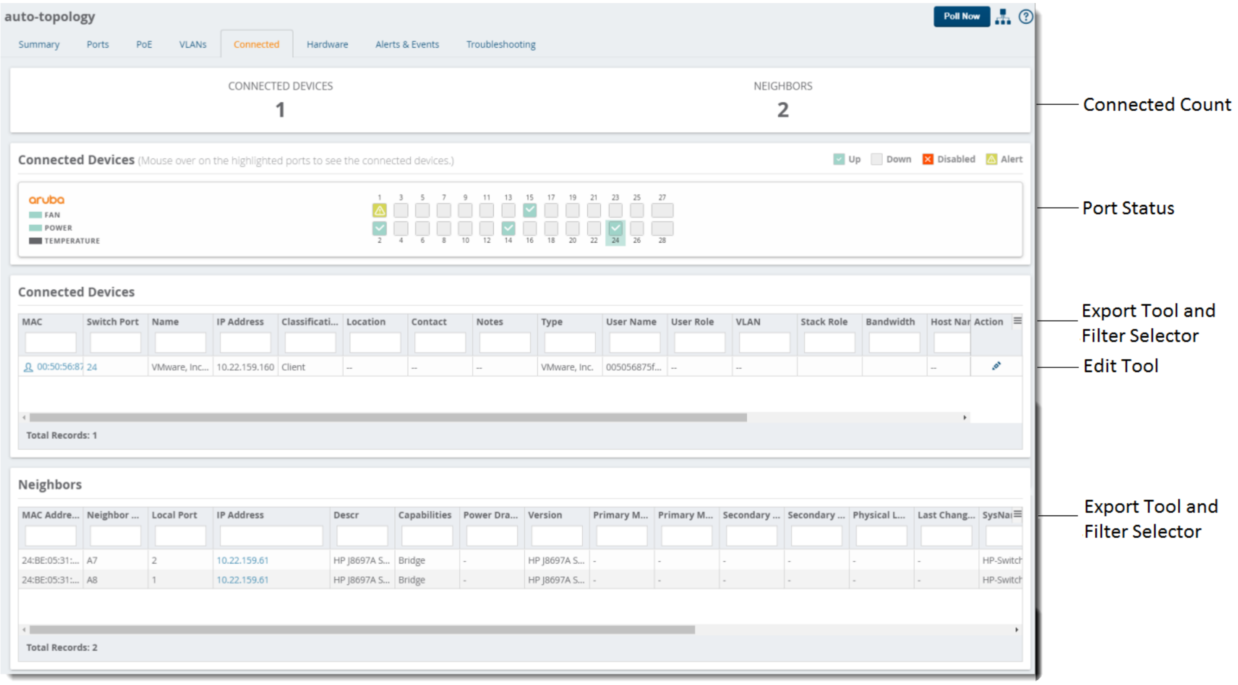
Connected Tab

When OV3600 detects client devices connected to the switch and neighbors that are up or down stream, you can access information about them from the Connected tab.

To view connected devices and neighbors:

1. From the navigation sidebar, go to **Devices > List** and select a switch from the list.
2. Select Connected at the top of the Switch Monitoring page.

Figure 100: *Connected Tab*



CONNECTED DEVICES 1

NEIGHBORS 2

Connected Devices (Mouse over on the highlighted ports to see the connected devices.)

Connected Devices

MAC	Switch Port	Name	IP Address	Classificati...	Location	Contact	Notes	Type	User Name	User Role	VLAN	Stack Role	Bandwidth	Host Nar	Action
00:50:56:87	24	VMware, Inc...	10.22.159.160	Client	--	--	--	VMware, Inc.	005056875f...	--	--			--	

Total Records: 1

Neighbors

MAC Addre...	Neighbor ...	Local Port	IP Address	Descr	Capabilities	Power Dra...	Version	Primary M...	Primary M...	Secondary ...	Secondary ...	Physical L...	Last Chang...	SysNa
24:BE:05:31:...	A7	2	10.22.159.61	HP J8697A S...	Bridge	-	HP J8697A S...	-	-	-	-	-	-	HP-Switch
24:BE:05:31:...	A8	1	10.22.159.61	HP J8697A S...	Bridge	-	HP J8697A S...	-	-	-	-	-	-	HP-Switch

Total Records: 2

Connected Count

Port Status

Export Tool and Filter Selector

Edit Tool

Export Tool and Filter Selector

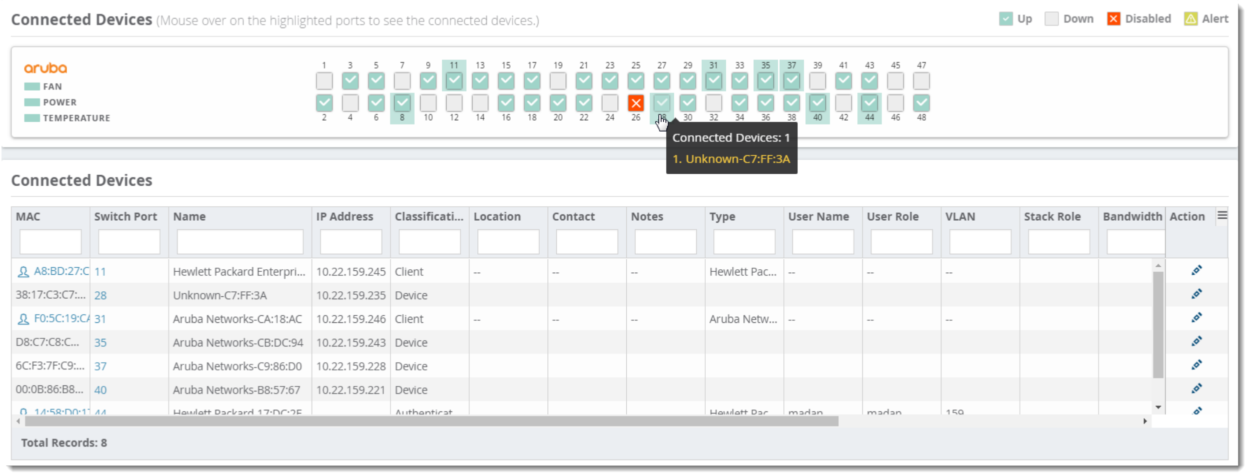
See Connected Device and Neighbor Counts

AirWave detects authenticated and rogue devices and reports them in the Connected Devices table. AirWave also uses upstream data to calculate possible neighbors and reports these devices in the Neighbors table (see Figure 100).

Determine Which Device Is Connected to a Port

Mouse-over the port number to view status and connected devices. In Figure 101, you can see from the tooltip information about the rogue and get the MAC address of the device from the Connected Devices table beneath the faceplate.

Figure 101: *Viewing Connected Device Details from the Tooltip*



Connected Devices (Mouse over on the highlighted ports to see the connected devices.)

Connected Devices: 1
1. Unknown-C7:FF:3A

Connected Devices

MAC	Switch Port	Name	IP Address	Classificati...	Location	Contact	Notes	Type	User Name	User Role	VLAN	Stack Role	Bandwidth	Action
A8:BD:27:C	11	Hewlett Packard Enterpri...	10.22.159.245	Client	--	--	--	Hewlett Pac...	--	--	--			✎
38:17:C3:C7:...	28	Unknown-C7:FF:3A	10.22.159.235	Device										✎
F0:5C:19:CA	31	Aruba Networks-CA:18:AC	10.22.159.246	Client	--	--	--	Aruba Netw...	--	--	--			✎
D8:C7:C8:C...	35	Aruba Networks-CB:DC:94	10.22.159.243	Device										✎
6C:F3:7F:C9:...	37	Aruba Networks-C9:86:D0	10.22.159.228	Device										✎
00:0B:86:B8...	40	Aruba Networks-B8:57:67	10.22.159.221	Device										✎
14:58:D0:1	44	Hewlett Packard 17:DC:2F		Authenticat				Hewlett Pac	madan	madan	159			✎

Total Records: 8

Get Connected Devices Details

Table 88 describes fields that you see in the Connected Devices table.

Table 88: *Connected Devices Fields and Descriptions*

Field	Description
MAC	MAC address for the device. This link provides access to the diagnostics page for the client. Find more information about troubleshooting client issues, see the *OV3600 8.2.7 User Guide*.
Switch Port	Port number associated with the device. This link provides access to the monitoring page for the interface.
Name	Name of the device. You can enter any name.
IP Address	If the gateway is managed by OV3600, the IP address is shown here.
Classification	Displays the classification of the device after OV3600 detects the device: ● Authenticated Client. This link provides access to the Connected Client page. ● Client. This link provides access to the Rogue table, where you can identify the device.
Notes	Notes to help you identify the client. You can enter anything.
Type	Type of device. You can enter anything.
User Name	Name that is used on the device for authentication.
User Role	Identifies the role-based operations that can be performed on the device.
VLAN	The number of the VLAN.
Stack Role	In a stack of switches, the role can be: master.
Bandwidth	The bandwidth used by the device. If the device supports bandwidth per MAC address, the bandwidth shown is the total bandwith used by all attached devices.
Host Name	The hostname of the neighbor device, which is retrieved from the DNS lookup.

Field	Description
Authen Type	The authentication server type: - Dot1x - Captive Portal - Local MAC Auth - WPA-PSK

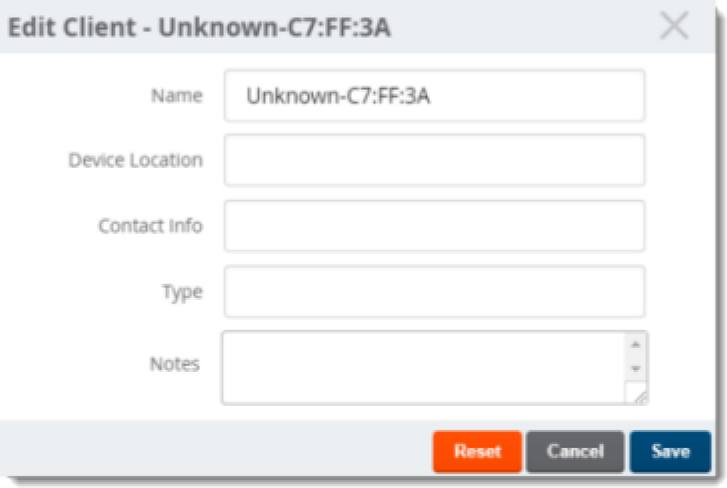
Edit a Connected Device

OV3600 doesn't gather much information about connected devices. If you edit a connected device, OV3600 reclassifies the devices as an unauthenticated client.

To edit a connected device:

1. Navigate to the monitoring page of a switch that has a connected device.
2. From the Connected tab, locate the device in the Connected Devices table.
3. Click ✎ to open the Edit Client pop-up.

Figure 102: *Editing the Connected Device*



Edit Client - Unknown-C7:FF:3A

Name: Unknown-C7:FF:3A

Device Location:

Contact Info:

Type:

Notes:

4. Add a name, device type, location, contact, or notes to the unknown device.
5. Click **Save**.

Get Neighbor Details

OV3600 uses SNMP/HTTP or CDP/LLDP to discover devices on the network and goes a step further, discovering neighbors directly connected to the switch. You can filter the Neighbors table to display neighbors connected to the port.

Table 89 describes the Neighbors Table fields and descriptions.

Table 89: *Neighbors Table Fields and Descriptions*

Field	Description
Name	Displays the name of the neighbor device. For example, a MAC address, hostname, or make and model. If an IP address is known for the device, a link provides access to the monitoring page for the device.

Field	Description
Neighbor Port	Displays the port ID of the neighbor device.
Local Port	Displays the port ID of the local device device.
Address Type	Displays the type of address of the neighbor device.
Address	Displays the network address associated with the neighbor. This link provides access to the web management interface. Hover your pointer over the to open a managment window to the device using HTTP, HTTPs, telnet or SSH.
Desc	Specify a description that provides additional information about the neighbor device (recommended).
Capabilities	Displays the device type: router, switch, or none (information is not available)
Version	Displays the software version running on the neighbor device.
CDP Version	Indicates the software version running on the neighbor device.
Duplex	Indicates the mode of operation of the connection: simplex, duplex, or half-duplex.
Power Drawn (Watts)	Displays the amount of power used on the interface of the neighbor device.
VTP Mgmt Domain	Displays the name of the group of VLANs associated with the neighbor device.
Sysname	Displays the system name of the neighbor device.
Primary Mgmt Address Type	Displays the type of address of the primary management interface.
Primary Mgmt Address	Displays the network address of the primary management interface.
Secondary Mgmt Address Type	Displays the type of address of the secondary management interface.
Secondary Mgmt Address	Displays the network address of the secondary management interface.
Physical Location	Displays the location of the neighbor device.
Native VLAN	Displays the ID number of the VLAN on the neighbor device.
Appliance ID	Displays the ID number of the appliance.
VLAN ID	Displays the ID number of the management Vlan on the neighboring device.
Last Change	Indicates when the device was last seen.

Field	Description
MTU	Specifies the largest packet size which can be received on the neighbor device.
Source	Displays the protocol used for device discovery: CDP.

Hardware Tab

Color-coded thresholds show power status for power supplies, fans, and temperature on the Hardware tab, and graphs show you overall CPU and memory usage (see Figure 103).

NOTE

You can't customize hardware thresholds.

Figure 103: *Hardware Tab*

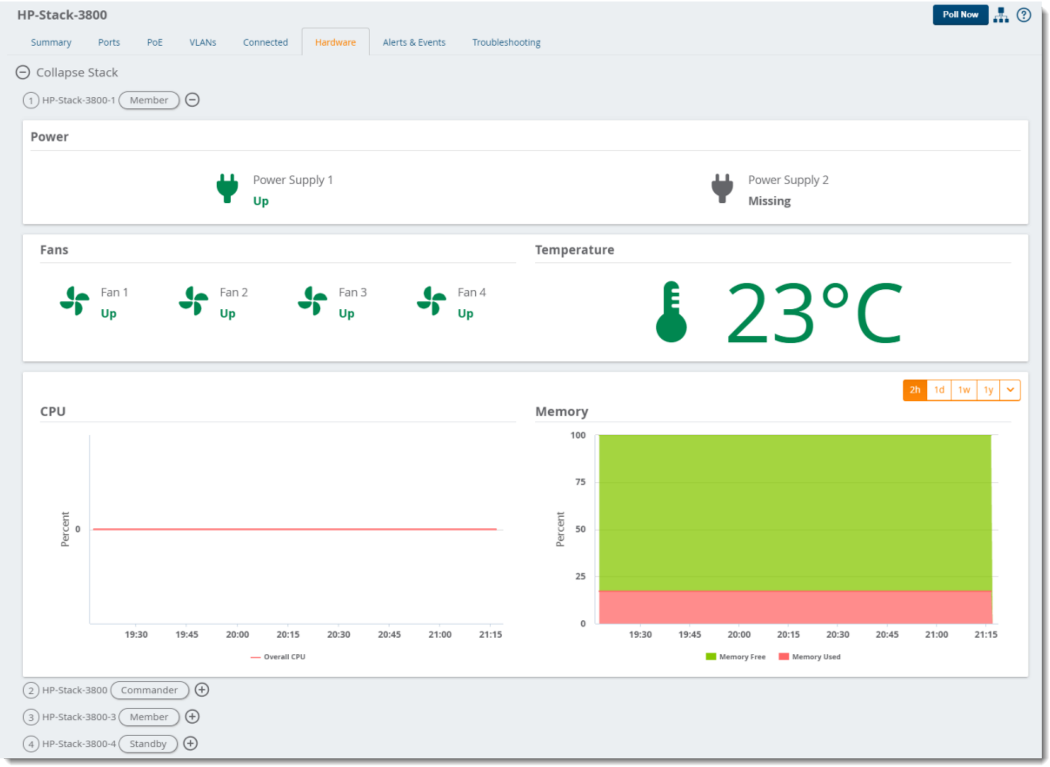


Table 90 describes the color-coded thresholds and icons on the Hardware tab.

Table 90: *Hardware Status and Thresholds*

Status	Power Supply	Fan	Memory	CPU	Temperature
Good	All power supplies are up. **NOTE:** The status is OK even if there are missing power supplies.	All fans are up. **NOTE:** The status is OK even if there are missing fans.	Usage is < 75%.	Usage is < 75%.	The temperature is in the range of 0° C to 55 ° C.

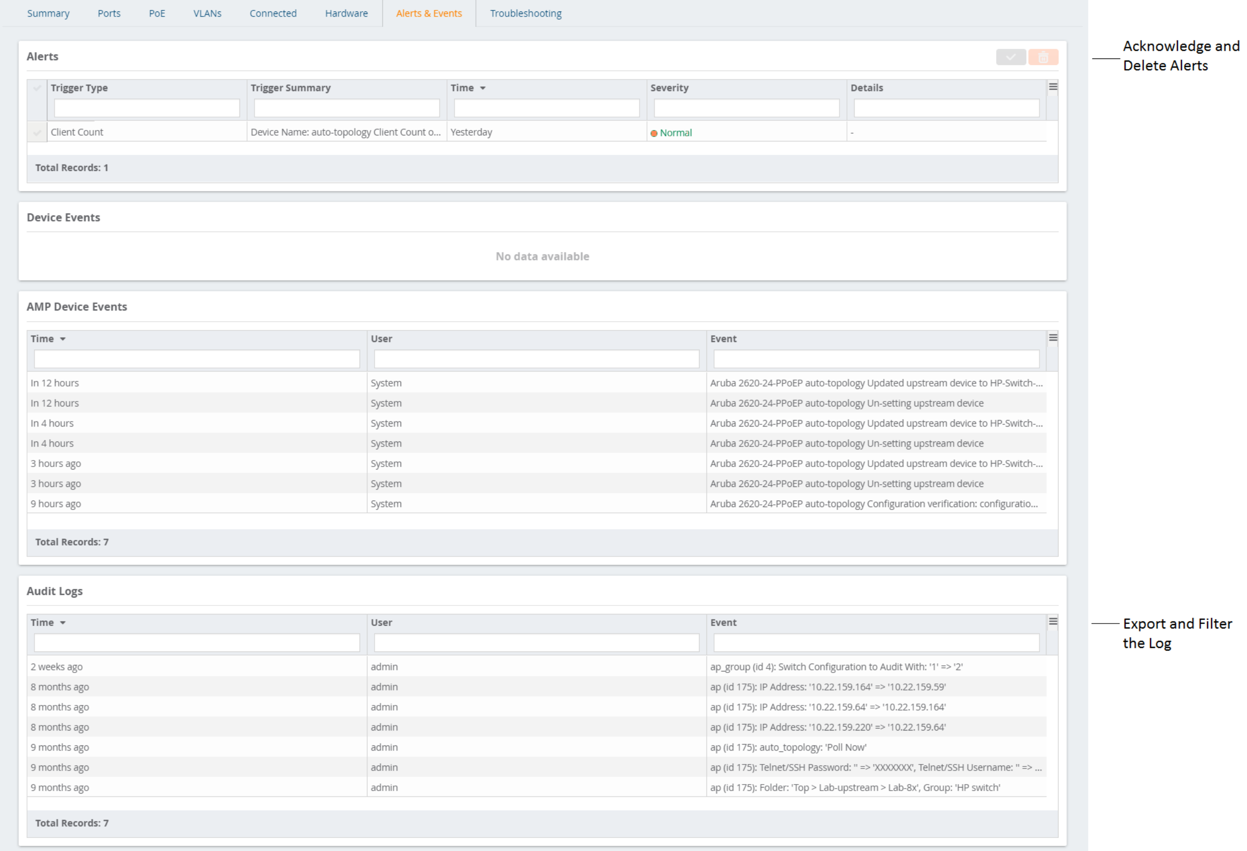
Table 90: *Hardware Status and Thresholds (Continued)*

Status	Power Supply	Fan	Memory	CPU	Temperature
Fair	NA	NA	Usage is between 75% to 90%.	Usage is between 75% to 90%.	NA
Poor	NA	At least 1 fan is down	Usage is > 90%.	Usage is > 90%.	The temperature is <0° C or > 55° C.
Info	Missing power supplies.	Missing or removed fans.	NA	NA	Information is unavailable.

Alerts & Events Tab

The Alerts & Events Tab provides monitoring information for the device (see Figure 104).

Figure 104: *Alerts & Events Tab*



Acknowledge and Delete Alerts

Alerts

Trigger Type	Trigger Summary	Time	Severity	Details
Client Count	Device Name: auto-topology Client Count o...	Yesterday	● Normal	-

Total Records: 1

Device Events

No data available

AMP Device Events

Time	User	Event
In 12 hours	System	Aruba 2620-24-PPoEP auto-topology Updated upstream device to HP-Switch-...
In 12 hours	System	Aruba 2620-24-PPoEP auto-topology Un-setting upstream device
In 4 hours	System	Aruba 2620-24-PPoEP auto-topology Updated upstream device to HP-Switch-...
In 4 hours	System	Aruba 2620-24-PPoEP auto-topology Un-setting upstream device
3 hours ago	System	Aruba 2620-24-PPoEP auto-topology Updated upstream device to HP-Switch-...
3 hours ago	System	Aruba 2620-24-PPoEP auto-topology Un-setting upstream device
9 hours ago	System	Aruba 2620-24-PPoEP auto-topology Configuration verification: configuratio...

Total Records: 7

Audit Logs

Time	User	Event
2 weeks ago	admin	ap_group (id 4): Switch Configuration to Audit With: '1' => '2'
8 months ago	admin	ap (id 175): IP Address: '10.22.159.164' => '10.22.159.59'
8 months ago	admin	ap (id 175): IP Address: '10.22.159.64' => '10.22.159.164'
8 months ago	admin	ap (id 175): IP Address: '10.22.159.220' => '10.22.159.64'
9 months ago	admin	ap (id 175): auto_topology: 'Poll Now'
9 months ago	admin	ap (id 175): Telnet/SSH Password: '' => 'XXXXXXX', Telnet/SSH Username: '' => ...
9 months ago	admin	ap (id 175): Folder: 'Top > Lab-upstream > Lab-8x', Group: 'HP switch'

Total Records: 7

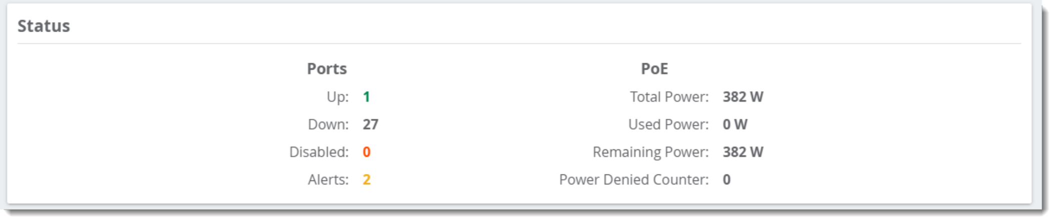
Export and Filter the Log

Acknowledge an Alert

To acknowledge an alert:

1. Go to **Devices > List**, then select a switch from the list. For example, the status in Figure 105 shows 2 alerts on the switch.

Figure 105: *Viewing Alerts on the Summary Tab*

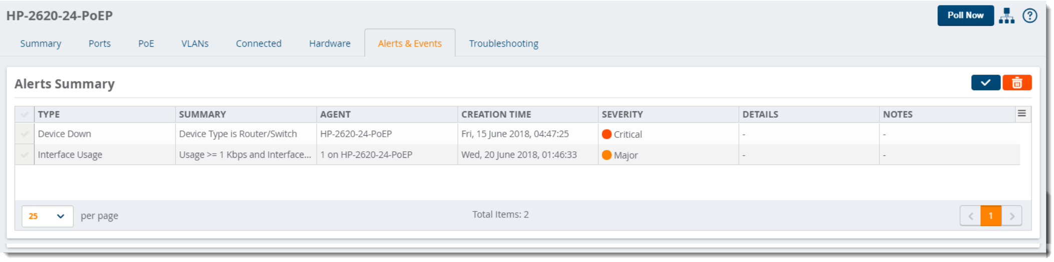


Status

Ports		PoE	
Up:	1	Total Power:	382 W
Down:	27	Used Power:	0 W
Disabled:	0	Remaining Power:	382 W
Alerts:	2	Power Denied Counter:	0

2. Select the **Alerts & Events** tab near the top of the page. Information about the alerts are at the top of the page, as shown in Figure 106.

Figure 106: *Alerts Summary on the Alerts & Events Tab*



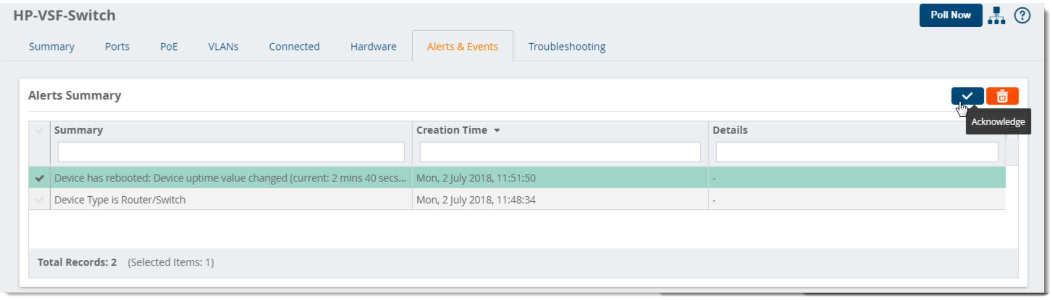
Alerts Summary

TYPE	SUMMARY	AGENT	CREATION TIME	SEVERITY	DETAILS	NOTES
Device Down	Device Type is Router/Switch	HP-2620-24-PoEP	Fri, 15 June 2018, 04:47:25	● Critical	-	-
Interface Usage	Usage >= 1 Kbps and Interface...	1 on HP-2620-24-PoEP	Wed, 20 June 2018, 01:46:33	● Major	-	-

25 per page Total Items: 2

3. Select the alert and click ✓ to acknowledge the alert (Figure 107).

Figure 107: *Acknowledging the Alert*



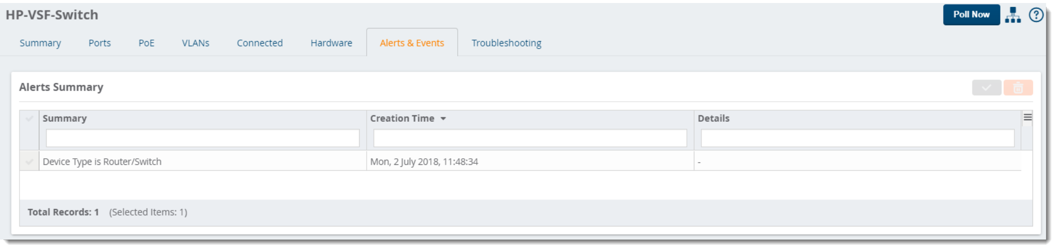
Alerts Summary

	Summary	Creation Time	Details
✓	Device has rebooted: Device uptime value changed (current: 2 mins 40 secs...	Mon, 2 July 2018, 11:51:50	-
	Device Type is Router/Switch	Mon, 2 July 2018, 11:48:34	-

Total Records: 2 (Selected Items: 1)

4. Check the Alerts Summary table to confirm that OV3600 cleared the alert (see Figure 108).

Figure 108: *Confirming That the Alert Cleared*



Alerts Summary

Summary	Creation Time	Details
Device Type is Router/Switch	Mon, 2 July 2018, 11:48:34	-

Total Records: 1 (Selected Items: 1)

Troubleshooting Tab

Schedule commands to run automatically from the CLI, run commands on a device or a stack, and run cable tests in the Troubleshooting tab.

Run a Command

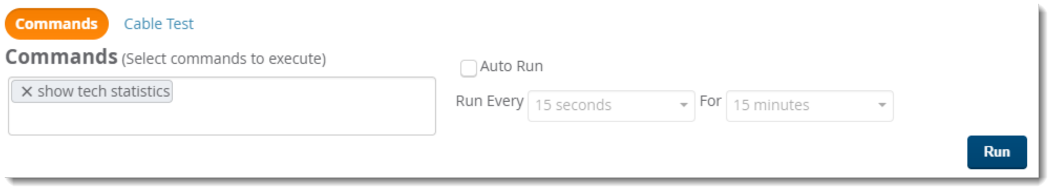
OV3600 put all the useful commands into a drop-down menu on the Troubleshooting tab.

To run a command:

1. Go to **Devices > List**, then select a switch from the list to monitor.

2. In the Troubleshooting tab, click the Command field and select one or more commands from the drop-down.

Figure 109: *Selecting a Command*



Commands (Select commands to execute)

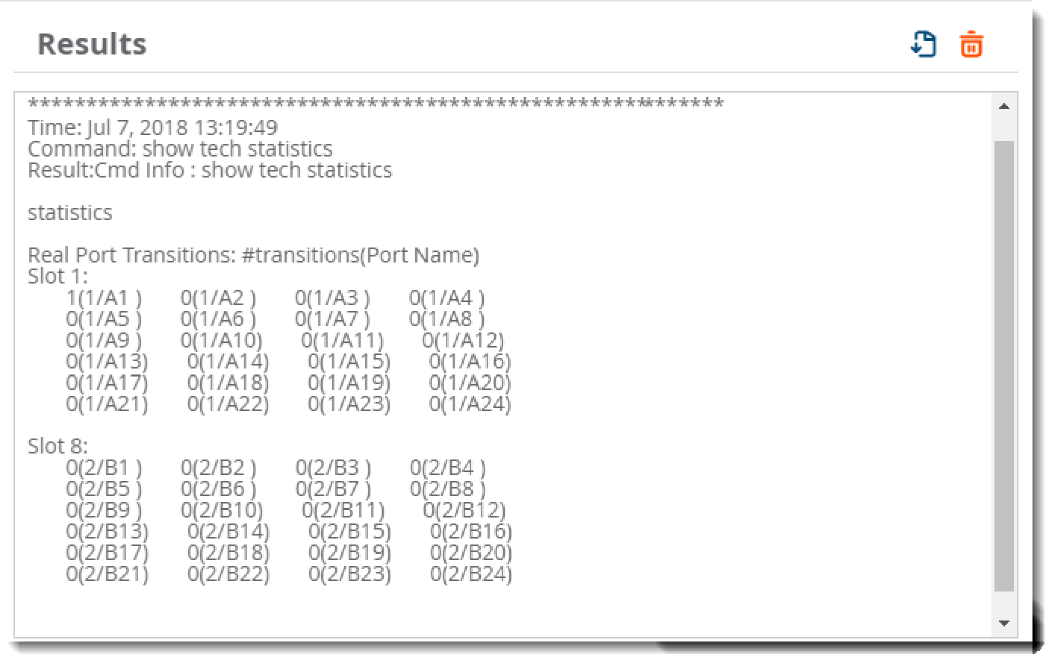
× show tech statistics

□ Auto Run

Run Every 15 seconds For 15 minutes

3. If you want to schedule a set of commands to run automatically at a specific time, select **Auto Run** and enter a time interval.
4. Click **Run**. The output of the show tech statistics command in Figure 110 shows only 1 port transition in Port A1.

Figure 110: *Viewing the CLI Output*



```
************************************************************
Time: Jul 7, 2018 13:19:49
Command: show tech statistics
Result:Cmd Info : show tech statistics

statistics

Real Port Transitions: #transitions(Port Name)
Slot 1:
      1(1/A1 )      0(1/A2 )      0(1/A3 )      0(1/A4 )
      0(1/A5 )      0(1/A6 )      0(1/A7 )      0(1/A8 )
      0(1/A9 )      0(1/A10)      0(1/A11)      0(1/A12)
      0(1/A13)      0(1/A14)      0(1/A15)      0(1/A16)
      0(1/A17)      0(1/A18)      0(1/A19)      0(1/A20)
      0(1/A21)      0(1/A22)      0(1/A23)      0(1/A24)

Slot 8:
      0(2/B1 )      0(2/B2 )      0(2/B3 )      0(2/B4 )
      0(2/B5 )      0(2/B6 )      0(2/B7 )      0(2/B8 )
      0(2/B9 )      0(2/B10)      0(2/B11)      0(2/B12)
      0(2/B13)      0(2/B14)      0(2/B15)      0(2/B16)
      0(2/B17)      0(2/B18)      0(2/B19)      0(2/B20)
      0(2/B21)      0(2/B22)      0(2/B23)      0(2/B24)
```

5. Click 📤 to export the results to a text file, or click 🗑 to clear the results.

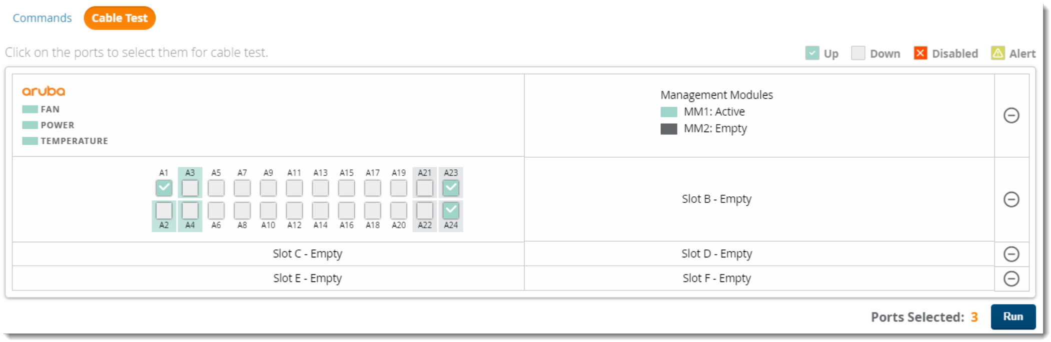
Test a Cable

You can identify a faulty or miswired cable by running a cable test against one or more ports. The cable test might stop or delay the network. OV3600 will notify you if this happens.

To run a cable test:

1. Go to Devices > List, then select a switch from the list to monitor.
2. In the Troubleshooting tab, click **Cable Test**.
3. Select the ports from the faceplate. In Figure 111 shows that Ports A2, A3, and A4 will be tested.

Figure 111: *Selecting Ports*



4. Click **Run**.

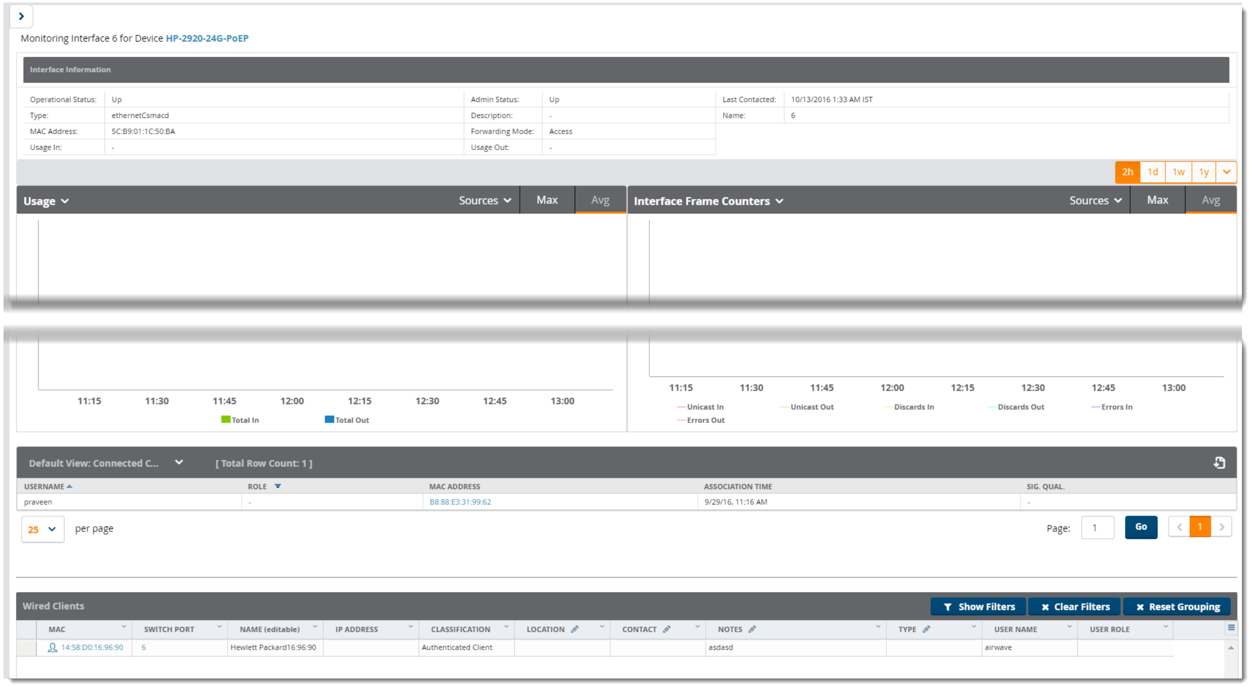
Monitoring Wired Interfaces

The **Interface Monitoring** page for a wired device is comprised of the following sections:

- Interface Information
- Usage and Interface Frame Counters graphs
- Connected Clients
- Wired Clients

To go to the monitoring page for an interface, click the **Interface** link in the Physical or Virtual Interfaces tables on a switch, as shown Figure 112.

Figure 112: *Interface Monitoring Page for a Wired Device*



Monitoring Interface 6 for Device HP-2920-24G-PoEP

Interface Information

Operational Status:	Up	Admin Status:	Up	Last Contacted:	10/13/2016 1:33 AM IST
Type:	ethernetCsmacd	Description:	-	Name:	6
MAC Address:	5C:B9:01:1C:50:BA	Forwarding Mode:	Access		
Usage In:	-	Usage Out:	-		

Default View: Connected C... [Total Row Count: 1]

USERNAME	ROLE	MAC ADDRESS	ASSOCIATION TIME	SIG. QUAL.
praveen	-	B8:88:E3:31:99:62	9/29/16, 11:16 AM	-

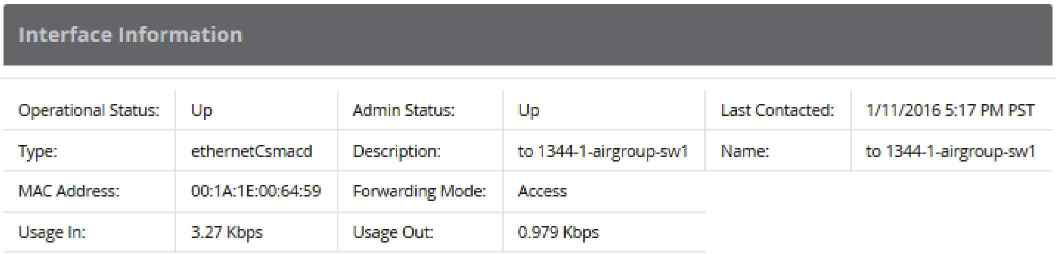
25 per page Page: 1 Go 1

Wired Clients

MAC	SWITCH PORT	NAME (editable)	IP ADDRESS	CLASSIFICATION	LOCATION	CONTACT	NOTES	TYPE	USER NAME	USER ROLE
14:58:D0:16:96:90	6	Hewlett Packard16:96:90		Authenticated Client			asdasd		airwave	

Specifics of the interface are in the Interface Information section, as depicted in Figure 113.

Figure 113: *Interface Information*



Interface Information

Operational Status:	Up	Admin Status:	Up	Last Contacted:	1/11/2016 5:17 PM PST
Type:	ethernetCsmacd	Description:	to 1344-1-airgroup-sw1	Name:	to 1344-1-airgroup-sw1
MAC Address:	00:1A:1E:00:64:59	Forwarding Mode:	Access		
Usage In:	3.27 Kbps	Usage Out:	0.979 Kbps		

Bandwidth, and various standard and enterprise specific error counting information is displayed in the lower section in a tabbed graph, which are shown in "Interface Monitoring Page for a Wired Device" on page 177 above.

Connected Clients, if any, are listed in a table below the interactive graphs.

What Next?

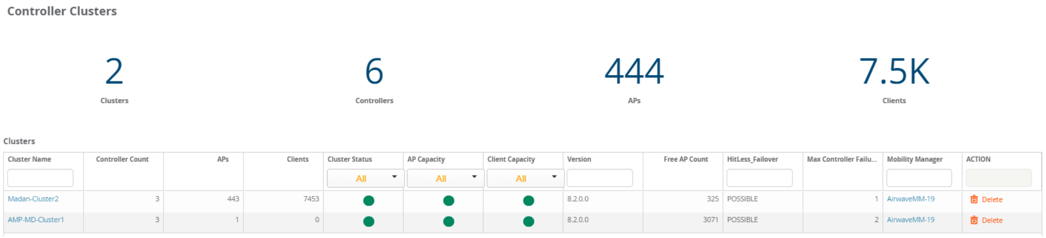
All device lists in OV3600 act as portals to management pages if you have the proper read/write privileges. Selecting the wrench or pencil icon next to a device table entry, or selecting **Modify Devices** where appropriate above a device table, will take you to the appropriate Management page (**Devices > Manage**). For more information, see "Configuring and Managing Devices" on page 208.

Monitoring switch Clusters

After adding switch clusters to OV3600, you can get a quick cluster status on the switch Clusters dashboard. You will find a count of the controllers, APs and clients are associated with these clusters at the top of the page and cluster information, including fault tolerance in the table beneath the counters.

You can access the switch Clusters dashboard by navigating to **Devices> Controller Clusters**.

Figure 114: *switch Cluster Dashboard*



Controller Clusters

2 Clusters | 6 Controllers | 444 APs | 7.5K Clients

Clusters

Cluster Name	Controller Count	APs	Clients	Cluster Status	AP Capacity	Client Capacity	Version	Free AP Count	HitLess_Failover	Max Controller Failu...	Mobility Manager	ACTION
				All	All	All						
Madan-Cluster2	3	443	7453	●	●	●	8.2.0.0	325	POSSIBLE	1	AirwaveMM-19	Delete
AMP-MD-Cluster1	3	1	0	●	●	●	8.2.0.0	3071	POSSIBLE	2	AirwaveMM-19	Delete

Table 91 describes the fields in the Cluster table. You can select any column heading to sort the data, or enter a text into the column search fields to filter the results.

Table 91: *Clusters Table*

Field	Description
Cluster Name	Name of the switch cluster.
switch Count	Number of switches in the cluster.
APs	Number of APs associated to switches in the cluster.
Clients	Number of clients connected to switches in the cluster.

Table 91: *Clusters Table (Continued)*

Field	Description
Cluster Status	🟠 An orange circle indicates that 1 or more cluster controllers is down. 🟢 A green circle indicates that all controllers are active
AP Capacity	🟢 A green circle indicates that the cluster is below 60% AP capacity. 🟡 A yellow circle indicates that the cluster is between 60% and 80% AP capacity. 🟠 An orange circle indicates that the cluster is at greater than 80% AP capacity.
Client Capacity	🟢 A green circle indicates that the cluster is below 60% client capacity. 🟡 A yellow circle indicates that the cluster is between 60% and 80% client capacity. 🟠 An orange circle indicates that the cluster is at greater than 80% client capacity.
Version	Displays the AOS-W version running on all the controllers in the cluster.
Free AP Count	Indicates how many APs you can add to a controller before you must add another controller to the cluster.
Hitless Failover	Indicates whether the cluster can handle a hit less failover. The cluster must be L2-connected.
Max Controller Failover	Indicates how many controllers can survive a failover.
Mobility Manager	Displays the host name of the Mobility Master managing the cluster.
Action	Let's you delete the cluster the cluster from OV3600.

Viewing Details about the switch Cluster

From the Clusters table, you can click on the cluster name to open the **Cluster Detail** page, which displays graphs, switch information, and cluster events.

Capacity Graphs

The graphs show:

- AP Capacity. This graph shows the percentage of a cluster's total AP capacity being used and the percentage of AP capacity being used on each controller in the cluster.
- Client Capacity. This graph shows the percentage of a cluster's total client capacity being used and the percentage of client capacity being used on each controller in the cluster.

Hover your mouse over any section of these graphs to view detailed statistics for that point in the graph. To change the time interval displayed in this graphic, click the schedule toolbar at the top right corner of the page.

switch Statistics

Table 92 describes the fields in the switches table. You can click any table heading to sort the table by that column criteria, or enter a text string into the entry field at the top of any column to filter the table by that value.

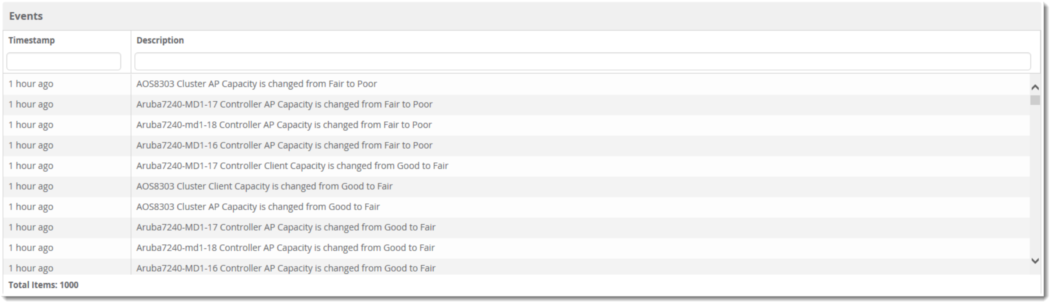
Table 92: *Controllers Table*

Field	Description
Name	Name of the switch in the cluster.
IP	IP address of the switch in the cluster.
Status	🟠 An orange circle indicates that the switch is down. 🟢 A green circle indicates that the switch is active.
AP Capacity	🟢 A green circle indicates that the switch is below 60% AP capacity. 🟡 A yellow circle indicates that the switch is between 60% and 80% AP capacity. 🟠 An orange circle indicates that the switch is at more than 80% AP capacity.
Client Capacity	🟢 A green circle indicates that the switch is below 60% client capacity. 🟡 A yellow circle indicates that the switch is between 60% and 80% client capacity. 🟠 An orange circle indicates that the switch is at greater than 80% client capacity.
Role	Displays the switch's role within the cluster, either **Leader**, **Member**, or **Isolated Leader**.
Type	Displays the switch model type.
Version	Displays the version of AOS-W running on the switch.

Monitoring Cluster Events

The Events table displays a description and timestamp for each cluster event. In Figure 115, you can see events when a cluster member is deleted, crosses a capacity threshold, or changes its role within the cluster. For information about creating a switch cluster trigger, see "Device Triggers " on page 269.

Figure 115: *Cluster Events*



Events

Timestamp	Description
1 hour ago	AOS8303 Cluster AP Capacity is changed from Fair to Poor
1 hour ago	Aruba7240-MD1-17 Controller AP Capacity is changed from Fair to Poor
1 hour ago	Aruba7240-md1-18 Controller AP Capacity is changed from Fair to Poor
1 hour ago	Aruba7240-MD1-16 Controller AP Capacity is changed from Fair to Poor
1 hour ago	Aruba7240-MD1-17 Controller Client Capacity is changed from Good to Fair
1 hour ago	AOS8303 Cluster Client Capacity is changed from Good to Fair
1 hour ago	AOS8303 Cluster AP Capacity is changed from Good to Fair
1 hour ago	Aruba7240-MD1-17 Controller AP Capacity is changed from Good to Fair
1 hour ago	Aruba7240-md1-18 Controller AP Capacity is changed from Good to Fair
1 hour ago	Aruba7240-MD1-16 Controller AP Capacity is changed from Good to Fair

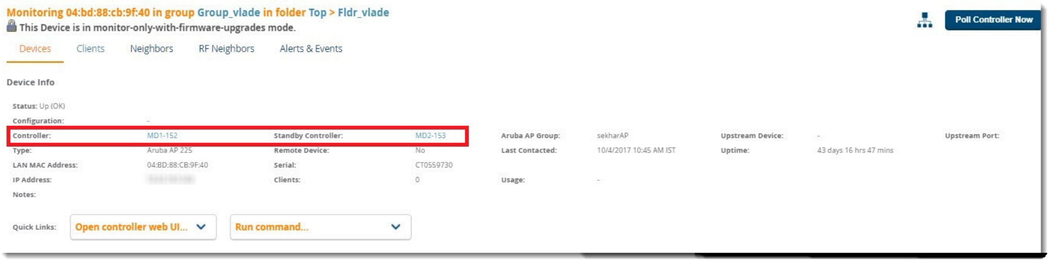
Total Items: 1000

Where to Find Additional Cluster Information

The **Devices > Monitor** page also displays cluster information for switches and APs associated to a cluster.

- The **Device Info** section of the **Devices > Monitor** page for a cluster switch includes the name of the cluster to which that controller belongs.
- The **Device Info** section of the **Devices > Monitor** page for an AP associated to a cluster switch displays information about its active switch and its standby switch. Figure 116 shows the **Devices > Monitor** page for an AP associated to a cluster member.

Figure 116: *Devices > Monitor page for an AP in a Controller Cluster*



Monitoring 04:bd:88:cb:9f:40 in group Group_vlade in folder Top > Fldr_vlade

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

Device Info

Status: Up (OK)

Configuration: -

Controller: MD1-152 Standby Controller: MD2-153

Type: Aruba AP 225 Remote Device: No

LAN MAC Address: 04:BD:88:CB:9F:40 Serial: CT0559730

IP Address: [redacted] Clients: 0

Notes:

Aruba AP Group: sekharAP Upstream Device: - Upstream Port:

Last Contacted: 10/4/2017 10:45 AM IST Uptime: 43 days 16 hrs 47 mins

Usage: -

Quick Links: Open controller web UI... Run command...

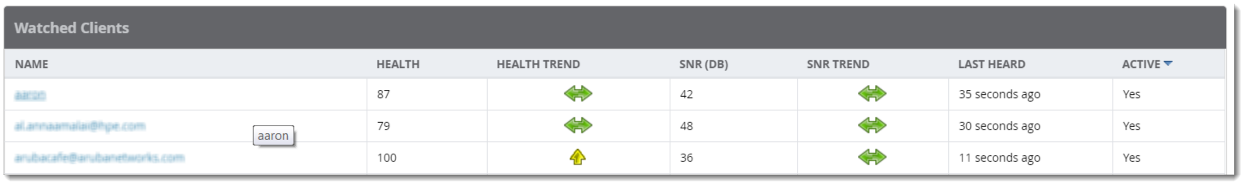
Monitoring Clients

Clients are the end-user devices that access the network through other devices monitored or managed by AirWave. You can view summarized information about all the wired and wireless clients in a dashboard on the **Clients > Overview** page.

Here are some of the things you can view on the dashboard:

- Graphs. The graphs show usage trends for all clients on your network. By default, these graphs show data over the last two hours. You can click in the graph to view details in a popup window, or click 2h | 1d | 1w | 1y ⌄ in the top right corner, to change the reported time interval.
- Watched Clients. If any clients are on the watched list, then a Watched Clients table displays on the Overview page, as shown in Figure 117. You can click the client name link to go to the **Clients > Diagnostics** page. Find more information about "Troubleshooting Client Issues" on page 189.

Figure 117: *Watched Clients Table*

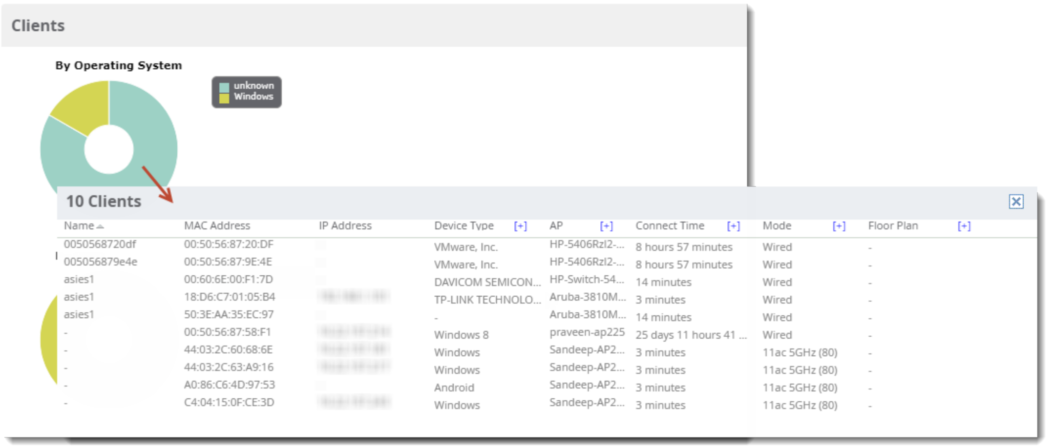


Watched Clients

NAME	HEALTH	HEALTH TREND	SNR (DB)	SNR TREND	LAST HEARD	ACTIVE ▼
[redacted]	87	⇔	42	⇔	35 seconds ago	Yes
[redacted]	79	⇔	48	⇔	30 seconds ago	Yes
[redacted]	100	⇧	36	⇔	11 seconds ago	Yes

- Pie charts. The categories include operating system, device type, SSID, and WLAN vendor. You can click on the chart or the interactive keys to view client details in a popup window, as shown in Figure 118. In the popup window, hyperlinks enable you to drill down further into diagnostic pages, floor plans, and dashboards for UCC, Traffic Analysis, and Clarity. For information about using UCC and Traffic Analysis, see "Using the UCC Dashboard" on page 299 and "Monitoring Application Traffic" on page 298. For information about using Clarity Synthetic, refer to the *OV3600 8.2.3 and Clarity Beta User Guide*.

Figure 118: *Drilling Down to Client Details*



Name	MAC Address	IP Address	Device Type [+]	AP [+]	Connect Time [+]	Mode [+]	Floor Plan [+]
0050568720df	00:50:56:87:20:DF	[redacted]	VMware, Inc.	HP-5406RzI2-...	8 hours 57 minutes	Wired	-
005056879e4e	00:50:56:87:9E:4E	[redacted]	VMware, Inc.	HP-5406RzI2-...	8 hours 57 minutes	Wired	-
asies1	00:60:6E:00:F1:7D	[redacted]	DAVICOM SEMICON...	HP-Switch-54...	14 minutes	Wired	-
asies1	18:D6:C7:01:05:B4	[redacted]	TP-LINK TECHNOLO...	Aruba-3810M...	3 minutes	Wired	-
asies1	50:3E:AA:35:EC:97	[redacted]	-	Aruba-3810M...	14 minutes	Wired	-
-	00:50:56:87:58:F1	[redacted]	Windows 8	praveen-ap225	25 days 11 hours 41 ...	Wired	-
-	44:03:2C:60:68:6E	[redacted]	Windows	Sandeep-AP2...	3 minutes	11ac 5GHz (80)	-
-	44:03:2C:63:A9:16	[redacted]	Windows	Sandeep-AP2...	3 minutes	11ac 5GHz (80)	-
-	A0:86:C6:4D:97:53	[redacted]	Android	Sandeep-AP2...	3 minutes	11ac 5GHz (80)	-
-	C4:04:15:0F:CE:3D	[redacted]	Windows	Sandeep-AP2...	3 minutes	11ac 5GHz (80)	-

OV3600 also provides several pages from the Clients menu which allow you to perform the following tasks:

- "Monitoring Wired and Wireless Clients" on page 182
- "Monitoring Rogue Clients" on page 184
- "Supporting Wireless Guest Users" on page 185
- "Supporting VPN Users" on page 187
- "Monitoring RFID Tags" on page 188

For information about creating OV3600 users and OV3600 user roles, refer to:

- "Creating OV3600 Users" on page 37
- "Creating OV3600 User Roles" on page 39

Monitoring Wired and Wireless Clients

The **Clients > All** page shows all clients that OV3600 monitors, including down clients.

The **Clients > Connected** page contains the following information:

- The Folder field shows the current folder of Connected Clients you are viewing. You can view users under a particular folder from the Go to folder drop down menu.
- Links under the Folder fields showing the **Total Devices**, **Mismatched**, **Clients**, and **Usage** (a static, unlinked statistic) summarize the device information for this folder. Select these links to open detail pages for each:
    - **Total Devices** redirects to the **Devices > List** for that folder,
    - **Mismatched** redirects to the list in **Devices > Mismatched** for that folder.
    - **Clients** refreshes the page but expands to include users in the subfolders.
- Interactive graphs display average and max **Clients** over time, and **Usage** in and out for the selected folder over time.
    - Select a time range option from the upper-right corner of the graphs.
    - Select the WLANs drop down to view up to six clients, or select Total Clients.
    - Click in a graph to view a pop-up of the graph.
- Below the Clients and Usage graphs is the list of connected users.

NOTE

The number of clients in OV3600 can differ from the number of clients that you see on the switch. This is because OV3600 and the switch count clients differently. The switch counts connections to the network as clients, while OV3600 counts devices as clients. For example, in the case where a single device connects to the network multiple times, the switch will count one client for each connection that the device makes to the network. OV3600 will only recognize the device as a single client, though, regardless of the number of connections.

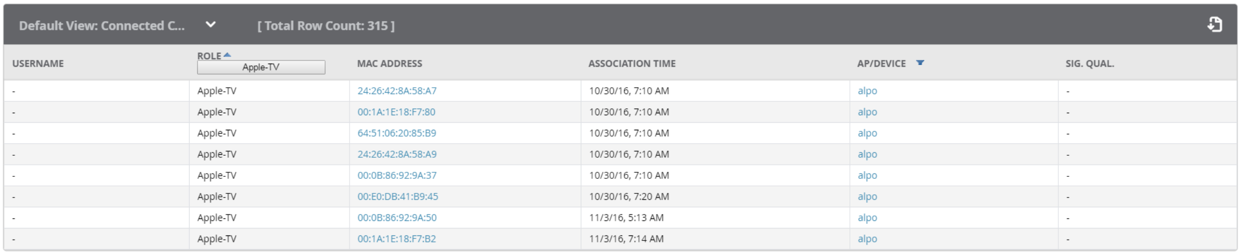
The columns in the default view of the **Clients > Connected** and **Clients > All** pages are defined in OmniVista 3600 Air Manager and cannot be modified. However, you can create a new view in each of these pages that returns custom information based on the filter parameters and data columns you selected when creating that new view. For more information, see "Creating Filtered Views" on page 132.

The information on this page can also be adjusted in the following ways:

- The **Alert Summary** section displays custom configured alerts that were defined in the **System > Alerts** page.
- Use the **Filter** icon (▼) next to certain columns (**AP/Device**, **Role**, **VLAN**, **Connection Mode**, and others) to filter the results by one of the values under that column. You can filter the list by substring match under the **Username** column.

The **Clients > Connected** page includes SSID information for users, and can display wired users using remote Access Point (RAP) devices in tunnel and split-tunnel mode.

Figure 119: *Default View: Connected Clients Table*



USERNAME	ROLE	MAC ADDRESS	ASSOCIATION TIME	AP/DEVICE	SIG. QUAL.
-	Apple-TV	24:26:42:8A:58:A7	10/30/16, 7:10 AM	alpo	-
-	Apple-TV	00:1A:1E:18:F7:80	10/30/16, 7:10 AM	alpo	-
-	Apple-TV	64:51:06:20:85:B9	10/30/16, 7:10 AM	alpo	-
-	Apple-TV	24:26:42:8A:58:A9	10/30/16, 7:10 AM	alpo	-
-	Apple-TV	00:0B:86:92:9A:37	10/30/16, 7:10 AM	alpo	-
-	Apple-TV	00:E0:DB:41:B9:45	10/30/16, 7:20 AM	alpo	-
-	Apple-TV	00:0B:86:92:9A:50	11/3/16, 5:13 AM	alpo	-
-	Apple-TV	00:1A:1E:18:F7:B2	11/3/16, 7:14 AM	alpo	-

Table 93: *Default View: Connected Clients Table Fields and Descriptions*

Field	Description
AP/Device	Displays the name of the AP to which the MAC address is associated as a link to this AP's **Devices > Monitor** page.
Association Time	The first time OV3600 recorded the user for this association.
MAC Address	The radio MAC address of the user associated to APs as a link to the **Users > Detail** page for this user.
Role	Specifies the role that the Alcatel-Lucent switch assigned to the connected user, such as employee.
Username	Displays the name of the user associated to the AP. OV3600 gathers this data from device traps, SNMP polling, or RADIUS accounting. User names appear in italics when a user name for that MAC address has been stored in the database from a previous association, but OV3600 is not getting a user name for the current association. This may indicate that the user has not yet been authenticated for this session or OV3600 may not be getting a user name from an external source.

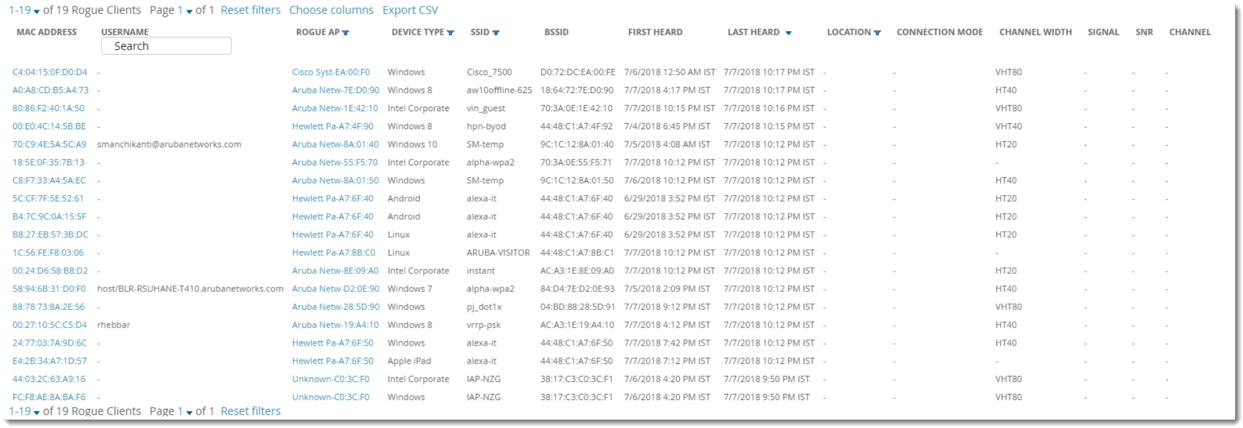
Monitoring Rogue Clients

You can view connected rogue clients in OV3600 by navigating to **Clients > Rogue Clients**, as shown in Figure 120.

From the Rogue Clients page, you can:

- Click the MAC address of a rogue to classify the device on the **Client > Client Details** page.
- Click the Rogue AP link to review the AP Details, rogue associations, and discovery events on the **RAPIDS > Details** page for the AP.

Figure 120: *Clients > Rogue Clients Page*



1-19 of 19 Rogue Clients Page 1 of 1 Reset filters Choose columns Export CSV

MAC ADDRESS	USERNAME Search	ROGUE AP	DEVICE TYPE	SSID	BSSID	FIRST HEARD	LAST HEARD	LOCATION	CONNECTION MODE	CHANNEL WIDTH	SIGNAL	SNR	CHANNEL
C4:04:15:0F:D0:D4	-	Cisco Syst-EA:00:F0	Windows	Cisco_7500	D0:72:DC:EA:00:FE	7/6/2018 12:50 AM IST	7/7/2018 10:17 PM IST	-	-	VHT80	-	-	-
A0:A8:CD:B5:A4:73	-	Aruba Netw-7E:D0:90	Windows 8	aw10offline-625	18:64:72:7E:D0:90	7/7/2018 4:17 PM IST	7/7/2018 10:17 PM IST	-	-	HT40	-	-	-
80:86:F2:40:1A:50	-	Aruba Netw-1E:42:10	Intel Corporate	vin_guest	70:3A:0E:1E:42:10	7/7/2018 10:15 PM IST	7/7/2018 10:16 PM IST	-	-	VHT80	-	-	-
00:E0:4C:14:5B:BE	-	Hewlett Pa-A7:4F:90	Windows 8	hpn-byod	44:48:C1:A7:4F:92	7/4/2018 6:45 PM IST	7/7/2018 10:15 PM IST	-	-	VHT40	-	-	-
70:C9:4E:5A:5C:A9	smanchikanti@arubanetworks.com	Aruba Netw-8A:01:40	Windows 10	SM-temp	9C:1C:12:8A:01:40	7/5/2018 4:08 AM IST	7/7/2018 10:12 PM IST	-	-	HT20	-	-	-
18:5E:0F:35:7B:13	-	Aruba Netw-55:F5:70	Intel Corporate	alpha-wpa2	70:3A:0E:55:F5:71	7/7/2018 10:12 PM IST	7/7/2018 10:12 PM IST	-	-	-	-	-	-
C8:F7:33:A4:5A:EC	-	Aruba Netw-8A:01:50	Windows	SM-temp	9C:1C:12:8A:01:50	7/6/2018 10:12 PM IST	7/7/2018 10:12 PM IST	-	-	HT40	-	-	-
5C:CF:7F:5E:52:61	-	Hewlett Pa-A7:6F:40	Android	alexa-it	44:48:C1:A7:6F:40	6/29/2018 3:52 PM IST	7/7/2018 10:12 PM IST	-	-	HT20	-	-	-
B4:7C:9C:0A:15:5F	-	Hewlett Pa-A7:6F:40	Android	alexa-it	44:48:C1:A7:6F:40	6/29/2018 3:52 PM IST	7/7/2018 10:12 PM IST	-	-	HT20	-	-	-
B8:27:EB:57:3B:DC	-	Hewlett Pa-A7:6F:40	Linux	alexa-it	44:48:C1:A7:6F:40	6/29/2018 3:52 PM IST	7/7/2018 10:12 PM IST	-	-	HT20	-	-	-
1C:56:FE:F8:03:06	-	Hewlett Pa-A7:8B:C0	Linux	ARUBA-VISITOR	44:48:C1:A7:8B:C1	7/7/2018 10:12 PM IST	7/7/2018 10:12 PM IST	-	-	-	-	-	-
00:24:D6:58:B8:D2	-	Aruba Netw-8E:09:A0	Intel Corporate	instant	AC:A3:1E:8E:09:A0	7/7/2018 10:12 PM IST	7/7/2018 10:12 PM IST	-	-	HT20	-	-	-
58:94:6B:31:D0:F0	host/BLR-RSUHANE-T410.arubanetworks.com	Aruba Netw-D2:0E:90	Windows 7	alpha-wpa2	84:D4:7E:D2:0E:93	7/5/2018 2:09 PM IST	7/7/2018 10:12 PM IST	-	-	HT40	-	-	-
88:78:73:8A:2E:56	-	Aruba Netw-28:5D:90	Windows	pj_dot1x	04:BD:88:28:5D:91	7/7/2018 9:12 PM IST	7/7/2018 10:12 PM IST	-	-	VHT80	-	-	-
00:27:10:5C:C5:D4	rhebbar	Aruba Netw-19:A4:10	Windows 8	vrrp-psk	AC:A3:1E:19:A4:10	7/7/2018 4:12 PM IST	7/7/2018 10:12 PM IST	-	-	HT40	-	-	-
24:77:03:7A:9D:6C	-	Hewlett Pa-A7:6F:50	Windows	alexa-it	44:48:C1:A7:6F:50	7/7/2018 7:42 PM IST	7/7/2018 10:12 PM IST	-	-	HT40	-	-	-
E4:2B:34:A7:1D:57	-	Hewlett Pa-A7:6F:50	Apple iPad	alexa-it	44:48:C1:A7:6F:50	7/7/2018 7:12 PM IST	7/7/2018 10:12 PM IST	-	-	-	-	-	-
44:03:2C:63:A9:16	-	Unknown-C0:3C:F0	Intel Corporate	IAP-NZG	38:17:C3:C0:3C:F1	7/6/2018 4:20 PM IST	7/7/2018 9:50 PM IST	-	-	VHT80	-	-	-
FC:F8:AE:8A:BA:F6	-	Unknown-C0:3C:F0	Windows	IAP-NZG	38:17:C3:C0:3C:F1	7/6/2018 4:20 PM IST	7/7/2018 9:50 PM IST	-	-	VHT80	-	-	-

1-19 of 19 Rogue Clients Page 1 of 1 Reset filters

Table 94 describes the fields on this page.

Table 94: *Clients > Rogue Clients Fields*

Field	Description
MAC Address	Displays the MAC address of the rogue client. Click on this to jump to the **Clients > Client Detail** page for this rogue.
Username	The user name associated with this client.
Rogue AP	The name of the Rogue AP. Click on this to jump to the **RAPIDS > Detail** page for this AP.
Device Type	The type of device, such as iPhone, Windows 7, etc.
SSID	The SSID of this client.
BSSID	The BSSID of this client.
First Heard	The date and time when this rogue client was first noticed.
Last Heard	The date and time when this rogue client was last noticed.
Location	If a location is available, you can click on this link to open the VisualRF floor plan and location on which this client resides.
Connection Mode	Shows the type of connection, such as 802.11n, 802.11b, etc.
Ch BW	Shows the channel bandwidth for this rogue client.

Table 94: *Clients > Rogue Clients Fields (Continued)*

Field	Description
Signal	Shows the signal value for this rogue client.
SNR	Shows the signal-to-noise ratio.
Channel	Shows the channel on which this rogue client is broadcasting.

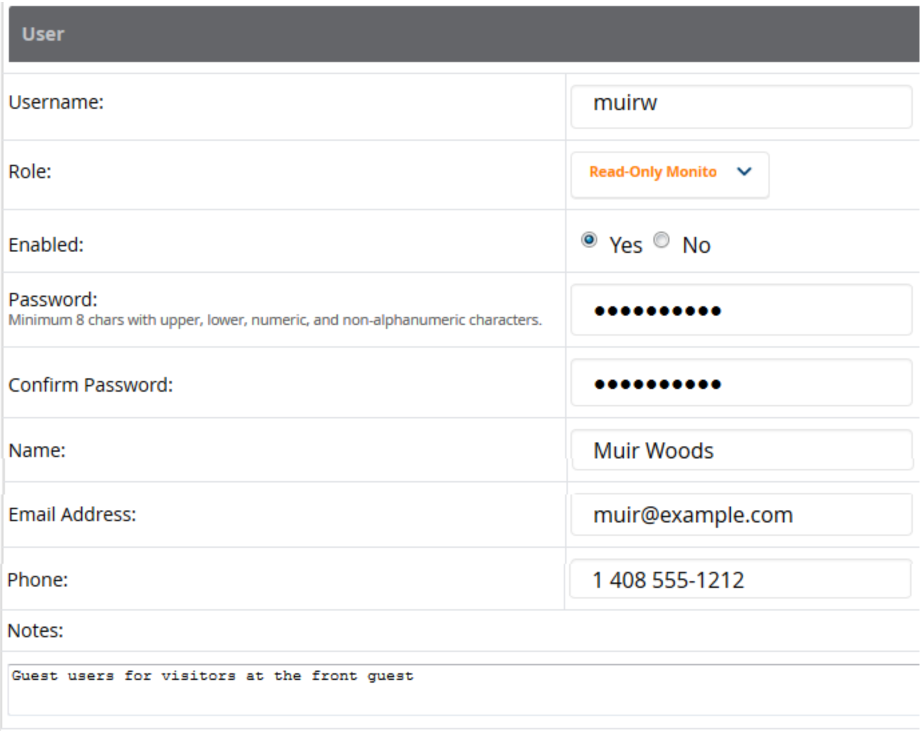
Supporting Wireless Guest Users

OV3600 supports guest user provisioning for Aruba Networks, Dell Networking W-Series, Alcatel-Lucent, and Cisco WLC devices. This allows frontline staff such as receptionists or help desk technicians to grant wireless access to WLAN visitors or other temporary personnel.

Perform the following steps in the pages described to configure these settings.

1. Navigate to the **OV3600 Setup > Roles** page and select the **Read-Only Monitoring & Auditing** role type. Under the Guest User Preferences section, enable **Allow creation of Guest Users**.
2. Next, navigate to the **OV3600 Setup > Users** page and click **Add** to create a new user with the role that was just created. Figure 121 illustrates this page.

Figure 121: *OV3600 Setup > Users Page Illustration*



User

Username:	muirw
Role:	Read-Only Monito
Enabled:	● Yes ○ No
Password: Minimum 8 chars with upper, lower, numeric, and non-alphanumeric characters.	••••••••••
Confirm Password:	••••••••••
Name:	Muir Woods
Email Address:	muir@example.com
Phone:	1 408 555-1212

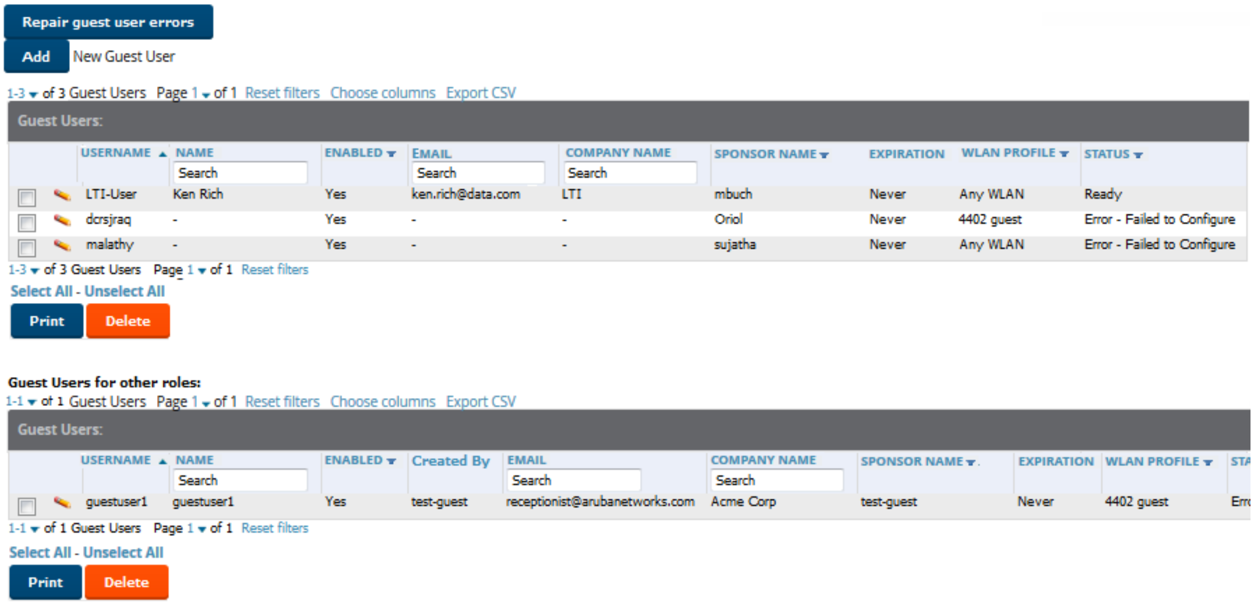
Notes:

```
Guest users for visitors at the front guest
```

3. The newly created login information should be provided to the person or people who will be responsible for creating guest access users.
4. The next step in creating a guest access user is to navigate to the **Users > Guest Clients tab**. From this tab, you can add new guest users, you can edit existing users, and you can repair guest user errors.

   This page displays a list of guest users and data, to include the expiration date, the SSID (for Cisco WLC) and other information. Figure 122 illustrates this page, and Table 95 describes the information.

Figure 122: *Clients > Guest Users Page Illustration*



1-3 of 3 Guest Users Page 1 of 1 Reset filters Choose columns Export CSV

Guest Users:

		USERNAME ▲	NAME	ENABLED ▾	EMAIL	COMPANY NAME	SPONSOR NAME ▾	EXPIRATION	WLAN PROFILE ▾	STATUS ▾
			Search		Search	Search				
□	✎	LTI-User	Ken Rich	Yes	ken.rich@data.com	LTI	mbuch	Never	Any WLAN	Ready
□	✎	dcrsjraq	-	Yes	-	-	Oriol	Never	4402 guest	Error - Failed to Configure
□	✎	malathy	-	Yes	-	-	sujatha	Never	Any WLAN	Error - Failed to Configure

1-3 of 3 Guest Users Page 1 of 1 Reset filters

Guest Users for other roles:

1-1 of 1 Guest Users Page 1 of 1 Reset filters Choose columns Export CSV

Guest Users:

		USERNAME ▲	NAME	ENABLED ▾	Created By	EMAIL	COMPANY NAME	SPONSOR NAME ▾	EXPIRATION	WLAN PROFILE ▾	STA
			Search			Search	Search				
□	✎	guestuser1	guestuser1	Yes	test-guest	receptionist@arubanetworks.com	Acme Corp	test-guest	Never	4402 guest	Err

1-1 of 1 Guest Users Page 1 of 1 Reset filters

Table 95: *Clients > Guest Users Fields*

Field	Description
Repair Guest User Errors	Sets OV3600 to attempt to push the guest user again in an attempt to repair any errors in the **Status** column.
Add New Guest User	Adds a new guest user to a controller via OV3600
Username	Randomly generates a user name for privacy protection. This name appears on the **Guest User** detail page.
Name	Displays the specified guest user name.
Enabled	Enables or disables the user status. Set the status of the guest user as active (enabled) or expired (disabled).
Email	Displays the optional email address of the user.
Company Name	Displays the optional company name for the user.
Sponsor Name	Displays the name of the sponsor for the guest user. This setting is optional.
Expiration	Displays the date the guest user's access is to expire.
WLAN Profile	Select the SSID that the guest user can access. This setting applies to Cisco WLC only.
Status	Reports current status by the controller. If error messages appear in this column, select the user with the checkbox at left, and select the **Repair guest user errors** button.

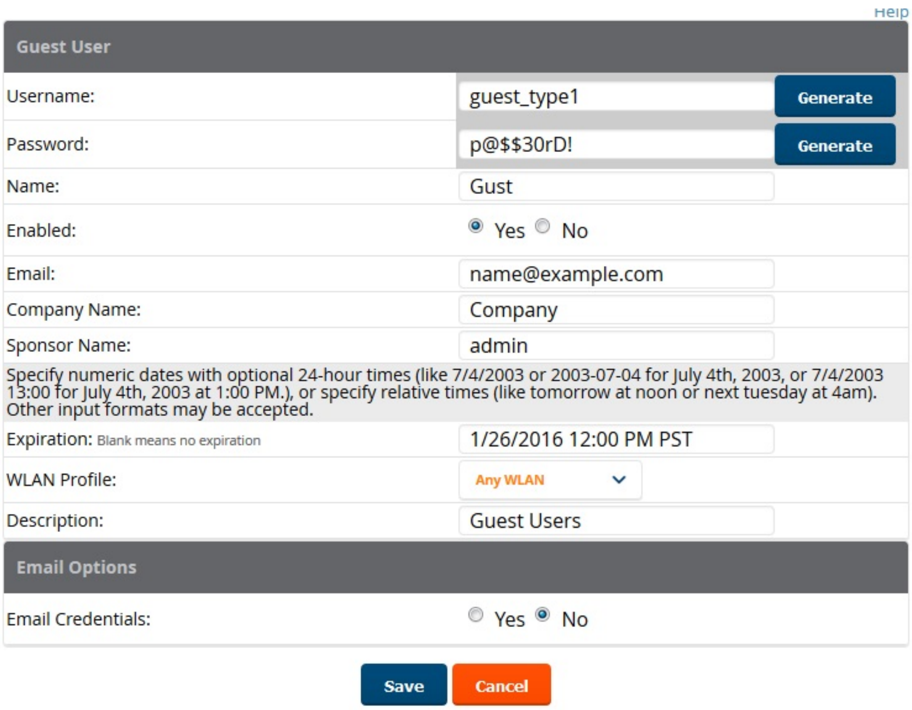
Guest users associated to the wireless network appear on the same list as other wireless users, but are identified as guest users in the **Guest User** column. The **Client Detail** page for a guest user also contains a box with the same guest information that appears for each user on the **Clients > Guest Users** list.

NOTE

The **Enabled, Sponsor Name, WLAN Profile, and Status** columns can be filtered using the funnel icon (▼).

5. To add a new guest user, select **Add**, and complete the fields illustrated in Figure 123. Table 95 above describes most fields. The first three fields are required, and the remaining fields are optional.

Figure 123: *Clients > Guest Users > Add New Guest User Page Illustration*



Guest User

Username:	guest_type1
Password:	p@$$30rD!
Name:	Gust
Enabled:	● Yes ○ No
Email:	name@example.com
Company Name:	Company
Sponsor Name:	admin

Specify numeric dates with optional 24-hour times (like 7/4/2003 or 2003-07-04 for July 4th, 2003, or 7/4/2003 13:00 for July 4th, 2003 at 1:00 PM.), or specify relative times (like tomorrow at noon or next tuesday at 4am). Other input formats may be accepted.

Expiration: Blank means no expiration	1/26/2016 12:00 PM PST
WLAN Profile:	Any WLAN
Description:	Guest Users

Email Options

Email Credentials:	○ Yes ● No

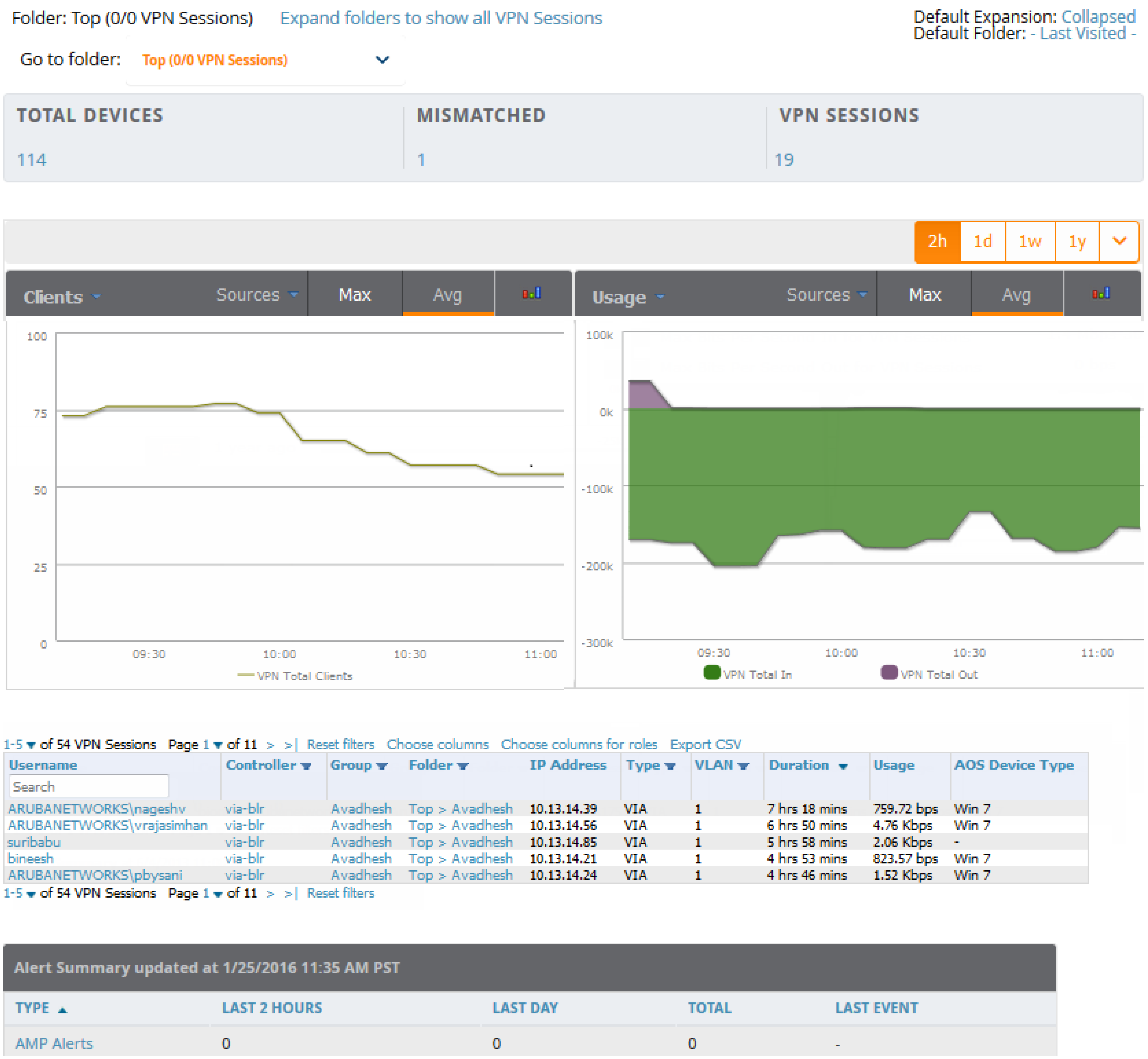
To make the **Username** or **Password** anonymous and to increase security, complete these fields then select **Generate**. The anonymous and secure **Username** and **Password** appear in the respective fields.

6. Select **Add** to complete the new guest user, or select **Cancel** to back out of new user creation. The **Clients > Guest Users** page appears and displays results, as applicable.

Supporting VPN Users

The **Clients > VPN Sessions** page shows active VPN Sessions along with device type and HTTP fingerprinting information.

Figure 124: *Clients > VPN Sessions Page Illustration*



Folder: Top (0/0 VPN Sessions) Expand folders to show all VPN Sessions

Go to folder: Top (0/0 VPN Sessions)

Default Expansion: Collapsed
Default Folder: - Last Visited -

TOTAL DEVICES	MISMATCHED	VPN SESSIONS
114	1	19

1-5 of 54 VPN Sessions Page 1 of 11 > >| Reset filters Choose columns Choose columns for roles Export CSV

Username	Controller	Group	Folder	IP Address	Type	VLAN	Duration	Usage	AOS Device Type
Search									
ARUBANETWORKS\nageshv	via-blr	Avadhesh	Top > Avadhesh	10.13.14.39	VIA	1	7 hrs 18 mins	759.72 bps	Win 7
ARUBANETWORKS\vrajasimhan	via-blr	Avadhesh	Top > Avadhesh	10.13.14.56	VIA	1	6 hrs 50 mins	4.76 Kbps	Win 7
suribabu	via-blr	Avadhesh	Top > Avadhesh	10.13.14.85	VIA	1	5 hrs 58 mins	2.06 Kbps	-
bineesh	via-blr	Avadhesh	Top > Avadhesh	10.13.14.21	VIA	1	4 hrs 53 mins	823.57 bps	Win 7
ARUBANETWORKS\pbysani	via-blr	Avadhesh	Top > Avadhesh	10.13.14.24	VIA	1	4 hrs 46 mins	1.52 Kbps	Win 7

1-5 of 54 VPN Sessions Page 1 of 11 > >| Reset filters

Alert Summary updated at 1/25/2016 11:35 AM PST

TYPE ▲	LAST 2 HOURS	LAST DAY	TOTAL	LAST EVENT
AMP Alerts	0	0	0	-

When a VPN user name is selected, a **Clients > VPN User Detail** page displays with current VPN sessions, a user and bandwidth interactive graph, and a historical VPN sessions list table.

Monitoring RFID Tags

Radio Frequency Identification (RFID) uses radio wave tags to identify and wireless devices with radio waves. Active tags have a battery and transmit signals autonomously while passive tags have no battery. RFID tags often support additional and proprietary improvements to network integration, battery life, and other functions.

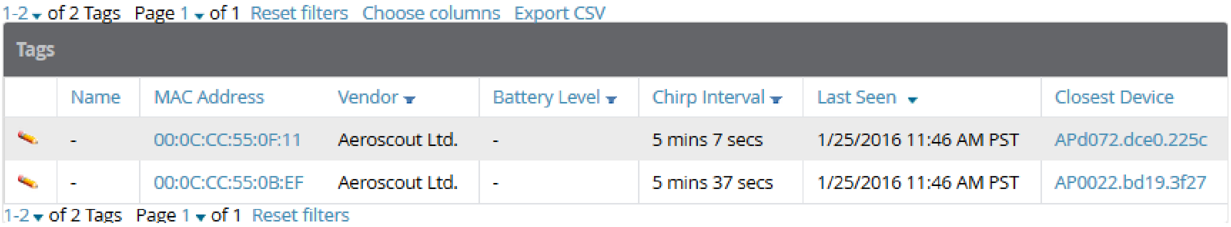
Supported RFID tag vendors include: Aeroscout, Ekahau, Innerwireless-PanGo, Vestac, and Newbury.

The **Clients > Tags** page displays the RFID tags that are heard by thin APs and reported back to a controller that OV3600 monitors. Figure 125 shows an example of the list of tags.

NOTE

To identify lost or stolen inventory, you can use the **Inactive Tag** trigger to generate an alert if a tag is not reported to OV3600 after an interval. For information about enabling this trigger, refer to "Client Triggers" on page 273.

Figure 125: *Tags Table*



1-2 ▾ of 2 Tags Page 1 ▾ of 1 Reset filters Choose columns Export CSV

Tags

	Name	MAC Address	Vendor ▾	Battery Level ▾	Chirp Interval ▾	Last Seen ▾	Closest Device
✎	-	00:0C:CC:55:0F:11	Aeroscout Ltd.	-	5 mins 7 secs	1/25/2016 11:46 AM PST	APd072.dce0.225c
✎	-	00:0C:CC:55:0B:EF	Aeroscout Ltd.	-	5 mins 37 secs	1/25/2016 11:46 AM PST	AP0022.bd19.3f27

1-2 ▾ of 2 Tags Page 1 ▾ of 1 Reset filters

Table 96 describes the **Tags** table fields.

Table 96: *Tags Table Information*

Field	Description
Name	User-editable name associated with the tag. Click the **pencil** icon to edit the name, or add notes to the tag.
MAC Address	MAC address of the AP that reported the tag.
Vendor	Vendor of the tag. You can display all or filter by vendor.
Battery Level	Displays battery information—filterable in drop-down menu at the top of the column; is not displayed for Aeroscout tags.
Chirp Interval	Displays the tag chirp frequency or interval, filterable from the drop-down menu at the top of the column. Note that the chirp interval from the RFID tag influences the battery life of active tags as well as search times. If a tag chirps with very long chirp interval, it may take longer time for the location engine to accurately measure x and y coordinates.
Last Seen	Date and time the tag was last reported to OV3600.
Closest Device	The device that last reported the tag to the controller (linked to the AP monitoring page in OV3600).

Troubleshooting Client Issues

OV3600 enables you to monitor and diagnose end-user issues from the **Clients > Client Detail** and **Clients > Diagnostics** pages. The following sections describe typical tasks you can do.

- "Evaluating User Status" on page 189
- "Diagnosing Status and Connectivity" on page 193

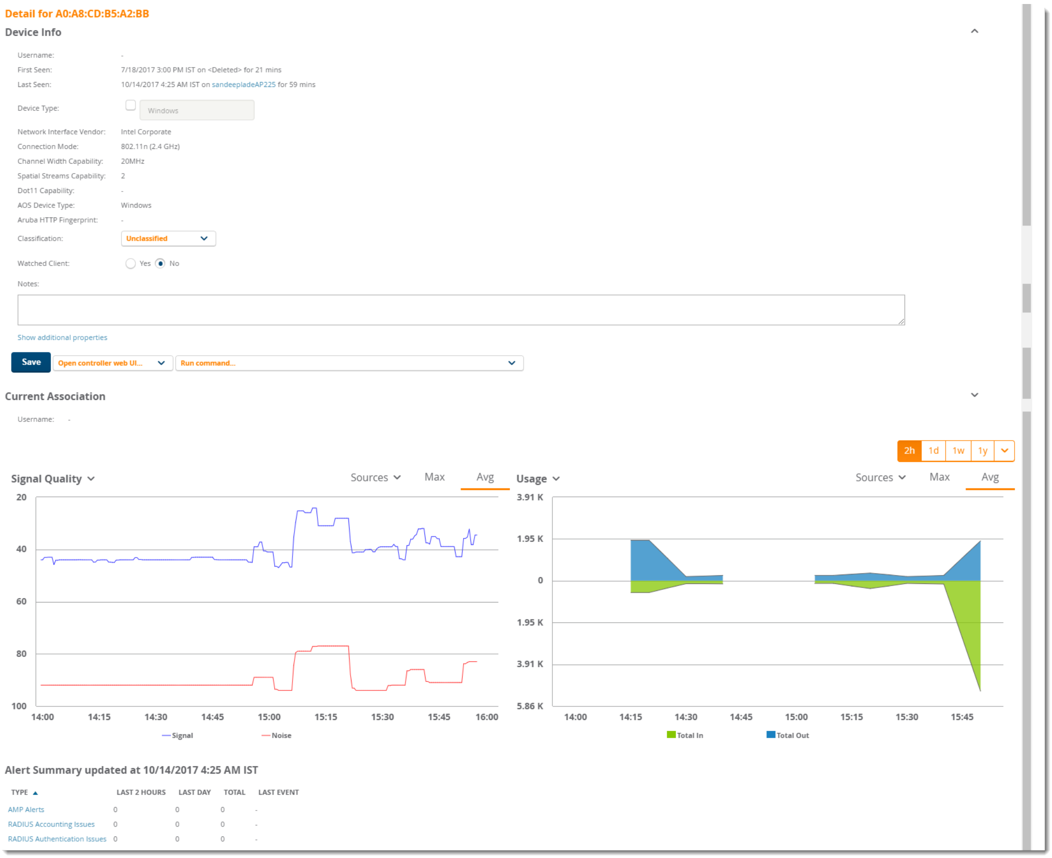
Evaluating User Status

From the **Clients > Client Detail** page, you can review device information for wired and wireless devices, evaluate signal quality and usage graphs, and respond to alerts.

You can access this page by doing one of the following:

- Search for a user. In the resulting window, click the MAC address link.
- Click the MAC address link in the **Devices > Monitor** page, the **Clients > Connected** page, or the **Clients > All** page.

illustrates a partial view of the **Client Detail** page.



Detail for A0:A8:CD:B5:A2:BB

Device Info

Username: -
First Seen: 7/18/2017 3:00 PM IST on <Deleted> for 21 mins
Last Seen: 10/14/2017 4:25 AM IST on sandeepladeAP225 for 59 mins
Device Type: □ Windows
Network Interface Vendor: Intel Corporate
Connection Mode: 802.11n (2.4 GHz)
Channel Width Capability: 20MHz
Spatial Streams Capability: 2
Dot11 Capability: -
AOS Device Type: Windows
Aruba HTTP Fingerprint: -
Classification: Unclassified
Watched Client: ○ Yes ● No
Notes:

Current Association

Username: -

Alert Summary updated at 10/14/2017 4:25 AM IST

TYPE ▲	LAST 2 HOURS	LAST DAY	TOTAL	LAST EVENT
AMP Alerts	0	0	0	-
RADIUS Accounting Issues	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Here are some additional things you can do from the **Clients > Client Detail** page:

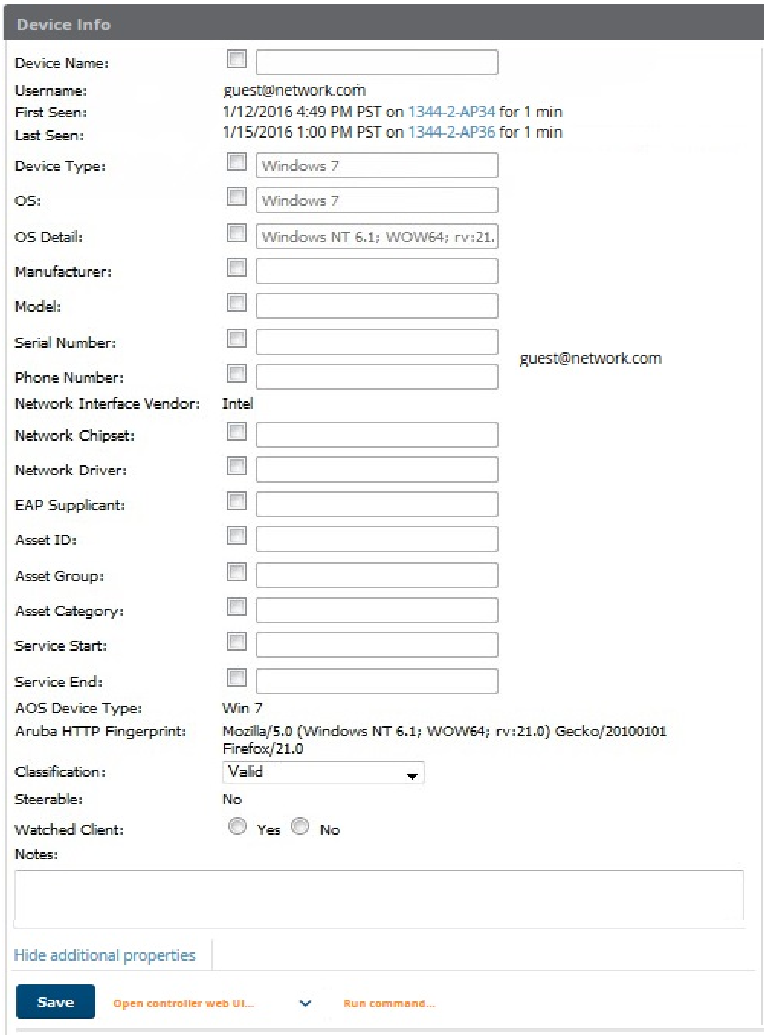
- Location. If VisualRF is enabled, you can view a map of the user location and facility information.
- Watched List. You can add a client as a on a watched list, which enables you to track performance metrics for selected clients. For example, you might have a user who repeatedly reports connectivity issues when moving from one room to another. Adding this client to a watched list allows you to track client issues.
- Client Neighbors. You can monitor neighbors that OV3600 discovers.
- UCC Calls. You can view call details for a client.
- Clarity. You can view a timeline of all phases of the client connecting to a network.
- Association History. For more information, see "Viewing the Client Association History" on page 192.
- Rogue Association History. For more information, see "Viewing the Rogue Association History" on page 193.

Enabling Mobile Device Access Control

Mobile Device Access Control (MDAC) secures, provisions, and manages network access for Apple® iOS and other employee-owned mobile devices by enabling device fingerprinting, device registration, and increased device visibility.

You can enable them by selecting the check box next to the Device Type, OS , OS Detail , and Manufacturer fields on the **Clients > Client Detail** page. To see more options, select the **Show additional properties** link, as shown in Figure 126

Figure 126: *Showing Additional Properties*



Device Info

Device Name:	□	
Username:	guest@network.com	
First Seen:	1/12/2016 4:49 PM PST on 1344-2-AP34 for 1 min	
Last Seen:	1/15/2016 1:00 PM PST on 1344-2-AP36 for 1 min	
Device Type:	□ Windows 7	
OS:	□ Windows 7	
OS Detail:	□ Windows NT 6.1; WOW64; rv:21.	
Manufacturer:	□	
Model:	□	
Serial Number:	□	
Phone Number:	□	guest@network.com
Network Interface Vendor:	Intel	
Network Chipset:	□	
Network Driver:	□	
EAP Supplicant:	□	
Asset ID:	□	
Asset Group:	□	
Asset Category:	□	
Service Start:	□	
Service End:	□	
AOS Device Type:	Win 7	
Aruba HTTP Fingerprint:	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0	
Classification:	Valid	
Steerable:	No	
Watched Client:	○ Yes ○ No	
Notes:		

Classifying Alcatel-Lucent Devices

If you have deployed Alcatel-Lucentswitches and have WMS Offload enabled on the network, the **Clients > Client Detail** page allows you to classify the device in the **Device Information** section, and to push this configuration to the switches that govern the devices. The classifications are as follows:

- **Unclassified**—Devices are unclassified by default.
- **Valid**—If the **Protect Valid Stations** option is enabled, this setting designates the device as a legitimate network device. When this **Valid** setting is pushed, this setting prevents valid stations from connecting to a non-valid AP.
- **Contained**—When this status is pushed to the device, Alcatel-Lucent will attempt to keep it contained from the network.

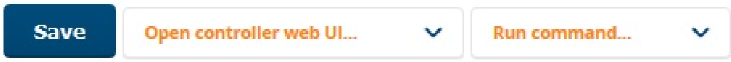
You can classify the user regardless of whether WMS Offload is enabled. If WMS Offload is enabled, the classification will get pushed to the switch.

Quick Links for Clients on Alcatel-Lucent Devices

In **Clients > Client Detail**, the following two drop-down menus appear next to the **Save** button in the **Device Info** section:

- **Open controller web UI:** A drop-down menu that allows you to jump to the controller's WebUI in a new window. Thin APs link to **Controller > Access Points** when not operating in mesh mode, or **Controller > Mesh Nodes** otherwise. Controllers show several more pages in this menu (**Security Dashboard**, for instance) if the controller is running AOS-W version 6.1 or greater.
- **Run a command:** A drop-down menu with a list of CLI commands you can run directly from the **Devices > Monitor** page.

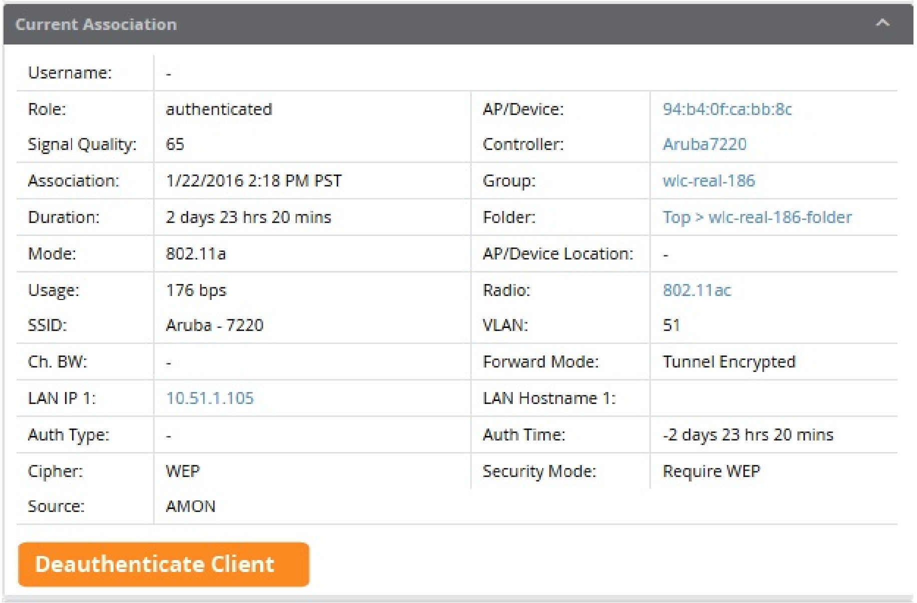
Figure 127: *Open Controller Web UI and Run Command Menus*



Using the Deauthenticate Client Feature

Alcatel-Lucent and Cisco WLC running firmware version v4.0.0.0 or later support a Deauthenticate Client. You can enable this feature in the **Current Association** section of the **Clients > Client Detail** page (see Figure 128).

Figure 128: *Deauthenticating the Client*



Current Association

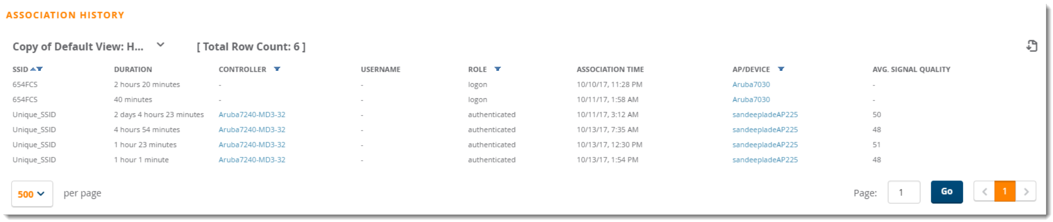
Username:	-		
Role:	authenticated	AP/Device:	94:b4:0f:ca:bb:8c
Signal Quality:	65	Controller:	Aruba7220
Association:	1/22/2016 2:18 PM PST	Group:	wlc-real-186
Duration:	2 days 23 hrs 20 mins	Folder:	Top > wlc-real-186-folder
Mode:	802.11a	AP/Device Location:	-
Usage:	176 bps	Radio:	802.11ac
SSID:	Aruba - 7220	VLAN:	51
Ch. BW:	-	Forward Mode:	Tunnel Encrypted
LAN IP 1:	10.51.1.105	LAN Hostname 1:	
Auth Type:	-	Auth Time:	-2 days 23 hrs 20 mins
Cipher:	WEP	Security Mode:	Require WEP
Source:	AMON		

Viewing the Client Association History

Past association details of a client are tracked in the **Association History** table, which is located under the VisualRF illustration (if available) and the **Alert Summary** in the **Client Detail** page.

The columns in this table, shown in Figure 129, are the same as the fields in the **Current Association** section for this user.

Figure 129: *Client Association History Table*



ASSOCIATION HISTORY

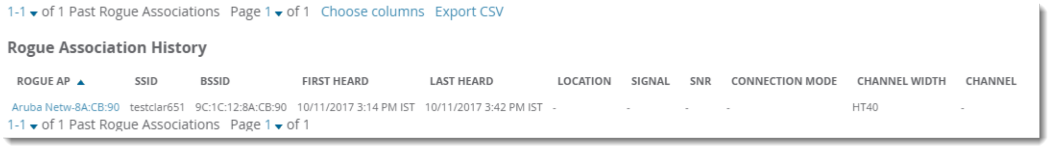
Copy of Default View: H... [Total Row Count: 6]

SSID	DURATION	CONTROLLER	USERNAME	ROLE	ASSOCIATION TIME	AP/DEVICE	AVG. SIGNAL QUALITY
654FCS	2 hours 20 minutes	-	-	logon	10/10/17, 11:28 PM	Aruba7030	-
654FCS	40 minutes	-	-	logon	10/11/17, 1:58 AM	Aruba7030	-
Unique_SSID	2 days 4 hours 23 minutes	Aruba7240-MD3-32	-	authenticated	10/11/17, 3:12 AM	sandeepladeAP225	50
Unique_SSID	4 hours 54 minutes	Aruba7240-MD3-32	-	authenticated	10/13/17, 7:35 AM	sandeepladeAP225	48
Unique_SSID	1 hour 23 minutes	Aruba7240-MD3-32	-	authenticated	10/13/17, 12:30 PM	sandeepladeAP225	51
Unique_SSID	1 hour 1 minute	Aruba7240-MD3-32	-	authenticated	10/13/17, 1:54 PM	sandeepladeAP225	48

Viewing the Rogue Association History

Past association details of a rogue client are tracked in the **Rogue Association History** table, which is located at the bottom of the **Clients > Client Detail** page.

Figure 130: *Rogue Association History Table*



1-1 of 1 Past Rogue Associations Page 1 of 1 Choose columns Export CSV

Rogue Association History

ROGUE AP	SSID	BSSID	FIRST HEARD	LAST HEARD	LOCATION	SIGNAL	SNR	CONNECTION MODE	CHANNEL WIDTH	CHANNEL
Aruba Netw-8A:CB:90	testclar651	9C:1C:12:8A:CB:90	10/11/2017 3:14 PM IST	10/11/2017 3:42 PM IST	-	-	-	-	HT40	-

1-1 of 1 Past Rogue Associations Page 1 of 1

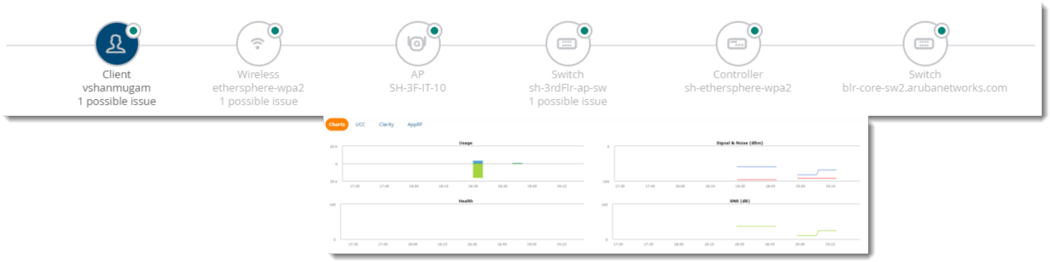
Diagnosing Status and Connectivity

AirWave looks at the client status and network connectivity and then puts them in an interactive dashboard. Devices in the network can include clients, access points, switches, wireless controllers, and routers.

To view client diagnostics:

- Search for a user. In the resulting window, click the MAC address link.
- From the navigation bar, select **Clients** and then click the client's MAC address link from the client list.
- From the navigation bar, select **Clients** and click on the Clients pie chart. In the resulting window, click the client's MAC address link.

Figure 131: *Accessing Client Trend Charts from the Dashboard*



All the information displayed on the **Clients > Diagnostics** page depends on which icon you click at the top of the dashboard. Here are some of the things you can view on the **Clients > Diagnostics** page:

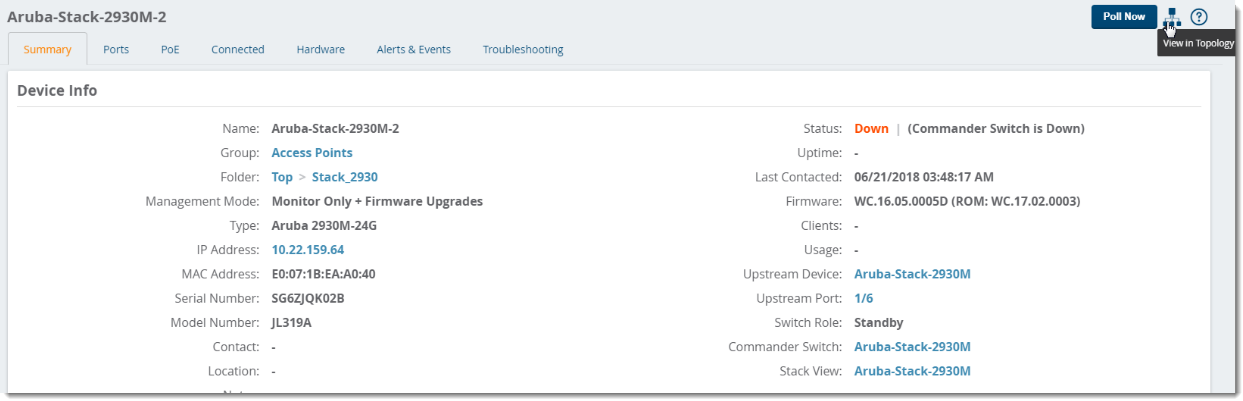
- Trend charts
- Summary details for UCC, Clarity, and Traffic Analysis
- Quality metrics
- Match events
- Device information for a client, AP, or switch
- Current association for a client
- Radio information for a wireless network
- Switch information
- Performance

Using Topology

Topology looks at the devices and links in your network and puts them in an interactive topology map. You can find Topology by navigating to **Home > Topology**.

If you are monitoring or troubleshooting a device or switch interface, you can go to Topology by clicking in the upper-right corner of the monitoring page, as shown in Figure 132.

Figure 132: *Accessing Topology from a Switch Monitoring Page*



Aruba-Stack-2930M-2

Device Info

Name:	Aruba-Stack-2930M-2	Status:	Down | (Commander Switch is Down)
Group:	Access Points	Uptime:	-
Folder:	Top > Stack_2930	Last Contacted:	06/21/2018 03:48:17 AM
Management Mode:	Monitor Only + Firmware Upgrades	Firmware:	WC.16.05.0005D (ROM: WC.17.02.0003)
Type:	Aruba 2930M-24G	Clients:	-
IP Address:	10.22.159.64	Usage:	-
MAC Address:	E0:07:1B:EA:A0:40	Upstream Device:	Aruba-Stack-2930M
Serial Number:	SG6ZJQK02B	Upstream Port:	1/6
Model Number:	JL319A	Switch Role:	Standby
Contact:	-	Commander Switch:	Aruba-Stack-2930M
Location:	-	Stack View:	Aruba-Stack-2930M

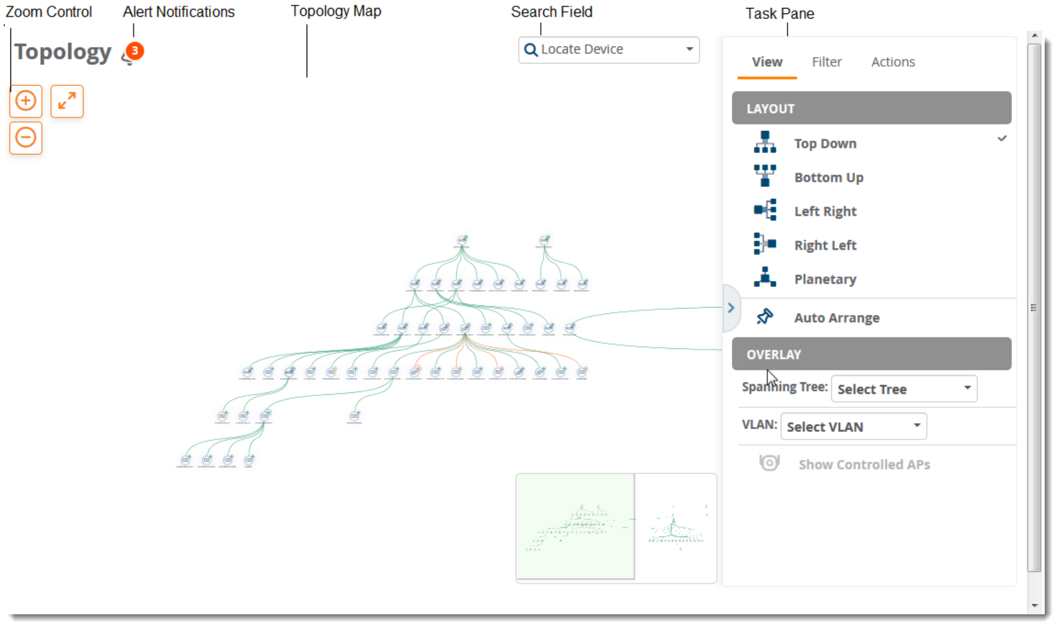
The following sections describe: getting started, setting up your map, checking the status of your network, and taking action from quick links.

Getting Started

From the Topology page, you can see the health of your network at a glance, receive real-time notifications when OV3600 discovers changes in your network, and manually control what you see in your topology map when you use the task pane tools.

Figure 133 shows the main components of the Topology page.

Figure 133: *Topology Page*



The map has several main components:

- Zoom Control. Click ⊕ and ⊖ to change the zoom level of your topology map, or click ⤢ to return to the full screen. For more information about changing the zoom level, see "Navigate the Map" on page 195.
- Alert Notifications. Click the alert notification to view changes in your network topology. For information about alert notifications, see "Respond to Alerts" on page 195.
- Search Field. Find devices by name or IP address. For more information about finding devices in the network topology, see "Locate Your Device" on page 196.
- Task Pane. Click the tabs to access shortcuts to tools and tasks, such as changing the map layout or mapping your network devices, including devices that are part of a spanning tree. For more information about using these tools, see "Setting up Your Map" on page 196.
- Topology Map. Click anywhere in the topology map to rearrange nodes, view tooltips, and access shortcuts to monitoring pages. For more information about accessing monitoring information, see "Checking the Status of Your Network" on page 204.

Navigate the Map

In addition to using the zoom controls at the top left of the topology map, you can use your mouse and keyboard, or touchscreen and trackpad to:

- Pan and zoom to view specific parts of the map
- Recenter your map
- Drag and drop a node (in planetary view). For information about views, see "Select Your Layout" on page 197

Topology puts a bird's eye view in the lower-right corner of the map. As you move around in map view, you can see your location in the topology map in this view from above.

Respond to Alerts

If you see a bell icon at the upper-left corner of the topology map, there are changes to your network for you to review. Alerts make it easy to know when changes to the topology occur (for example, when a node has been added or deleted from the source device).

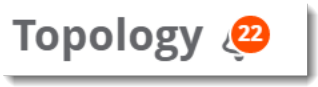
NOTE

When you navigate to Topology from a device monitoring page, the ⚠ Resetting filters. reminder above the zoom controls alerts you that the topology map isn't filtered. If you want to exclude devices from the topology map, see "Apply Filters" on page 200.

To respond to alerts:

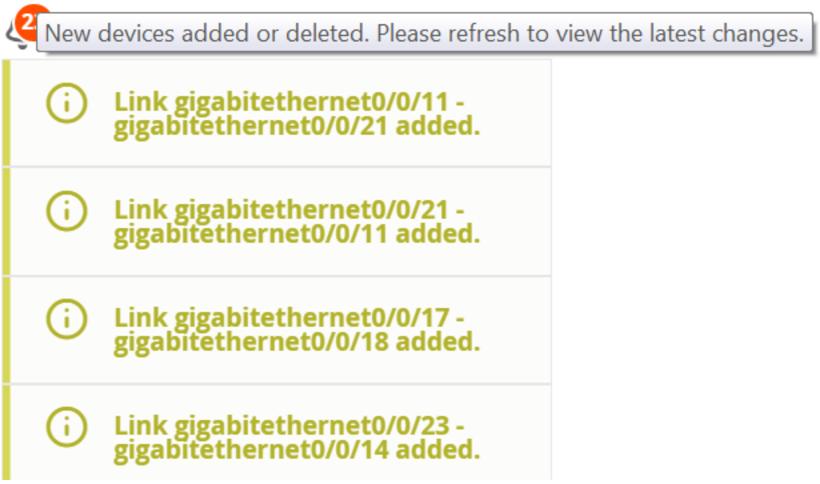
1. Hover your mouse over the bell icon to view the notification.

Figure 134: *Alert Notification*



2. Click the bell icon to review the information.

Figure 135: *Alert Messages*



New devices added or deleted. Please refresh to view the latest changes.

Link gigabitethernet0/0/11 - gigabitethernet0/0/21 added.

Link gigabitethernet0/0/21 - gigabitethernet0/0/11 added.

Link gigabitethernet0/0/17 - gigabitethernet0/0/18 added.

Link gigabitethernet0/0/23 - gigabitethernet0/0/14 added.

Setting up Your Map

Topology provides several ways to make finding your devices and visualizing links fast and easy. When setting up your map, you can locate your device, select your layout, pin a device, show spanning trees and show VLANs, apply filters, set a root node, save your preferences, and collapse your view.

NOTE

If you want to view the network topology in expanded view but the default view is collapsed, you need to adjust these settings on the Devices > List page. For more information, see "Changing the Default Expansion" on page 203.

Locate Your Device

You can search for devices by name or IP address. Topology limits the results to show devices based on your user role permissions.

To search for a device:

1. Go to **Home > Topology**, then click the search field.
2. Select a device from the list. You can narrow down the list by typing at least 2 characters or numbers in the search field, as shown in Figure 136.

Figure 136: *Locating a Device*

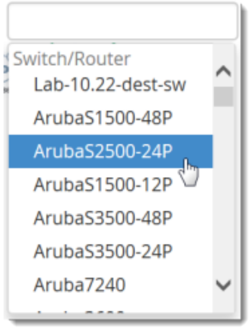
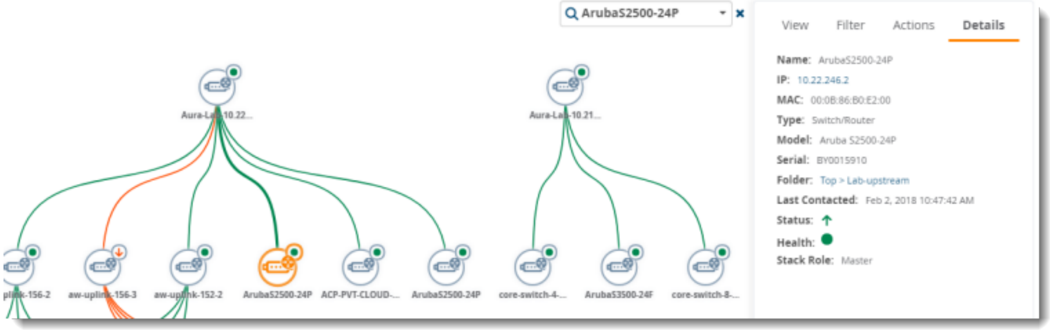


Figure 137 shows the device centered on the map and highlighted in orange with device details displayed in the task pane. For information about device status and health indicators, see "Viewing Device and Stack Membership Details" on page 206 and "Checking the Status of Your Network" on page 204.

Figure 137: *Search Result*



Name: ArubaS2500-24P

IP: 10.22.246.2

MAC: 00:0B:86:B0:E2:00

Type: Switch/Router

Model: Aruba S2500-24P

Serial: BY0015910

Folder: Top > Lab-upstream

Last Contacted: Feb 2, 2018 10:47:42 AM

Status: ↑

Health: ●

Stack Role: Master

Select Your Layout

You can rearrange the way the topology map displays the connections from the root node to other nodes. If you select a device to reposition it on the map, the device and its connections move with it. Some nodes might not have connections and look like islands on the map.

To change the layout, choose from the following **View** options in the task pane:

- Top Down. Creates a topology map that flows from top to bottom.
- Bottom Up. Creates a topology map that flows from bottom to top.
- Left Right and Right Left. Creates a topology map that flows from left to right, or right to left.
- Planetary. Creates topology map that shows devices connected to a hub, spread without overlapping.

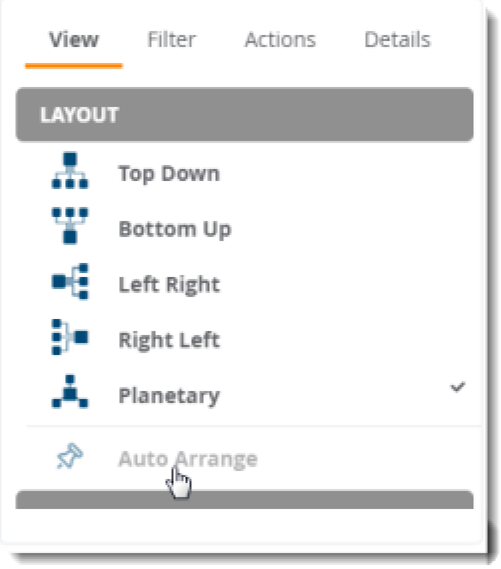
Arrange Devices on the Map

You can arrange the devices anywhere you want on the map, making it easier to see them and work with the map, by turning off Auto Arrange. When moving around the map, Topology keeps your pinned devices in the map.

To arrange a device on the map:

1. Click **Auto Arrange** from the **View** options in the task pane.

Figure 138: *Selecting Auto Arrange*



2. Drag and drop the device to a new location in the map.

To unpin the device, click **Auto Arrange** again. You'll see that Topology removes all pins and redistributes the devices evenly across the map.

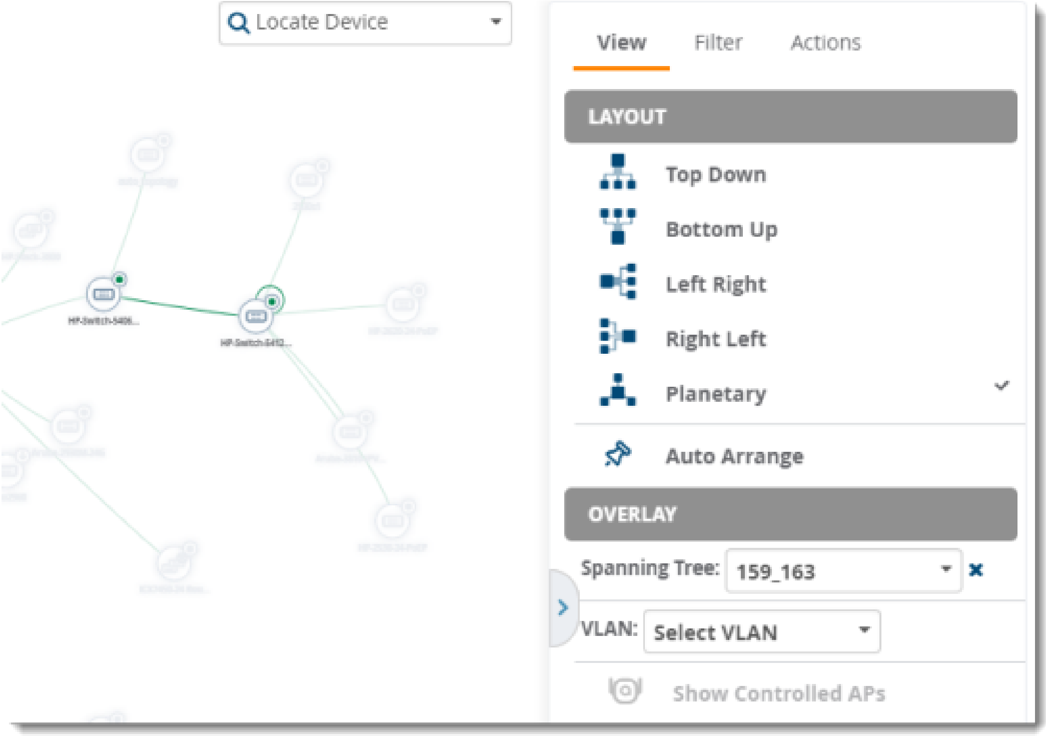
Show Spanning Tree Members

Topology learns which devices are part of a spanning tree from the switch using the STP protocol and highlights the devices that are part of the spanning tree in the topology map, as shown in Figure 139. To view the spanning tree membership, select a spanning tree from the **View > Overlay** menu in the task pane.

NOTE

Topology will show spanning tree data only for switches which support IEEE standard spanning tree MIBS.

Figure 139: *Selecting a Spanning Tree Overlay*



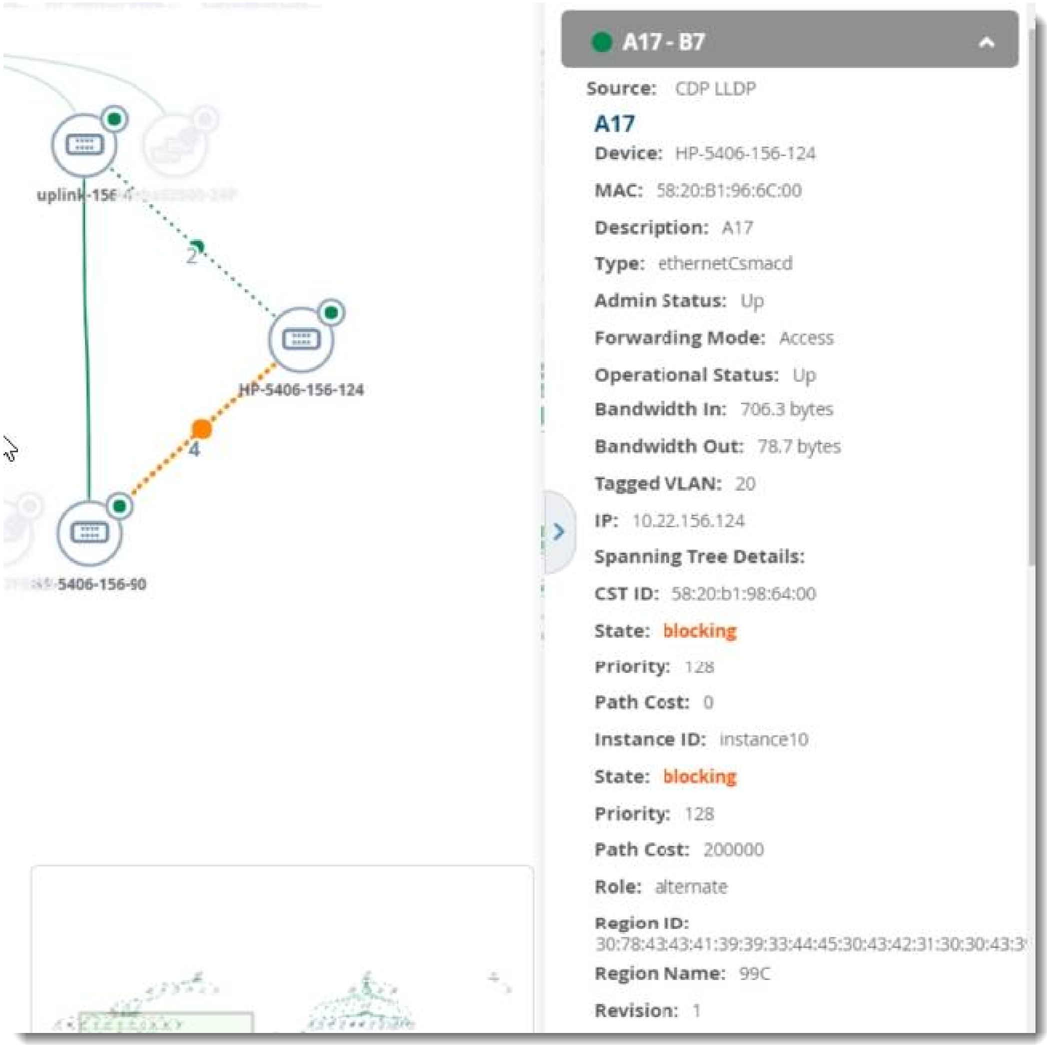
Spanning Tree: 159_163

VLAN: Select VLAN

Topology also displays STP ports that are in blocking state. When you hover over the link circle in the topology map, the tooltip shows the link types and STP port status, as shown in Figure 140.

Clicking on the link shows you link details in the task pane. A link with a circle in middle denotes an aggregated link, and a link with a number label denotes multiple links. A dotted link denotes there is a blocking port--either a single, multiple, or all ports blocked.

Figure 140: *Viewing Blocked STP Ports*



A17 - B7

Source: CDP LLDP

A17

Device: HP-5406-156-124

MAC: 58:20:B1:96:6C:00

Description: A17

Type: ethernetCsmacd

Admin Status: Up

Forwarding Mode: Access

Operational Status: Up

Bandwidth In: 706.3 bytes

Bandwidth Out: 78.7 bytes

Tagged VLAN: 20

IP: 10.22.156.124

Spanning Tree Details:

CST ID: 58:20:b1:98:64:00

State: blocking

Priority: 128

Path Cost: 0

Instance ID: instance10

State: blocking

Priority: 128

Path Cost: 200000

Role: alternate

Region ID: 30:78:43:43:41:39:39:33:44:45:30:43:42:31:30:30:43:3

Region Name: 99C

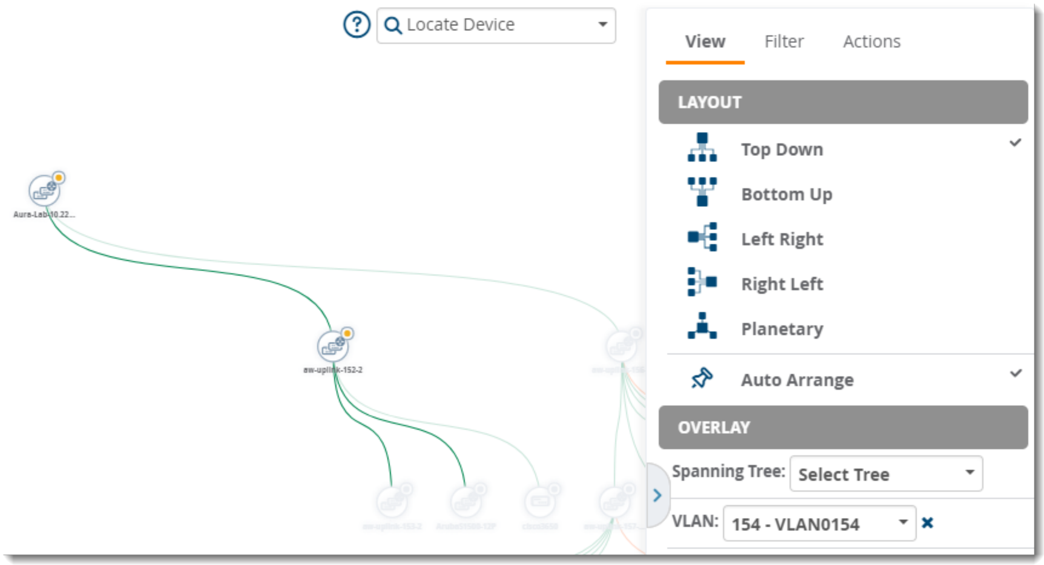
Revision: 1

Show VLANs

When you select a VLAN from the **View > Overlay** menu in the task pane, nodes and their connections are highlighted and shadowed in the VLAN view, as shown in Figure 141.

Topology also displays and highlights down devices, obtaining the VLAN information from the last time OV3600 polled the devices.

Figure 141: *Selecting a VLAN Overlay*



Apply Filters

You can customize the topology map by applying filters to your map. Filters affect which devices show up on your map. For example, you might create a filter to view only switches. When you filter by folders, user roles determine which folders are visible.

Nodes on the map can include access points, switches, switch stacks, wireless controllers, IP access controllers, and routers. By default, access points are hidden from map view to help you visualize your switching infrastructure. Table 97 lists the device icons that you see in the Device menu.

NOTE

By default, OV3600 hides access points from the topology map. To see access points, select AP from the filter list.

To apply a filter:

1. Select **Filter** from the task pane.
2. To show or hide a device in the topology map, click the check mark next to the device type in the **Devices** list.
3. To show only devices from a folder in the topology map, select that folder from the **Folders** dropdown list.

The topology map shown in Figure 142 has been filtered to display only switches in the **Top > SIM > Lab_HP** folder.

Figure 142: *Filtered Map View*

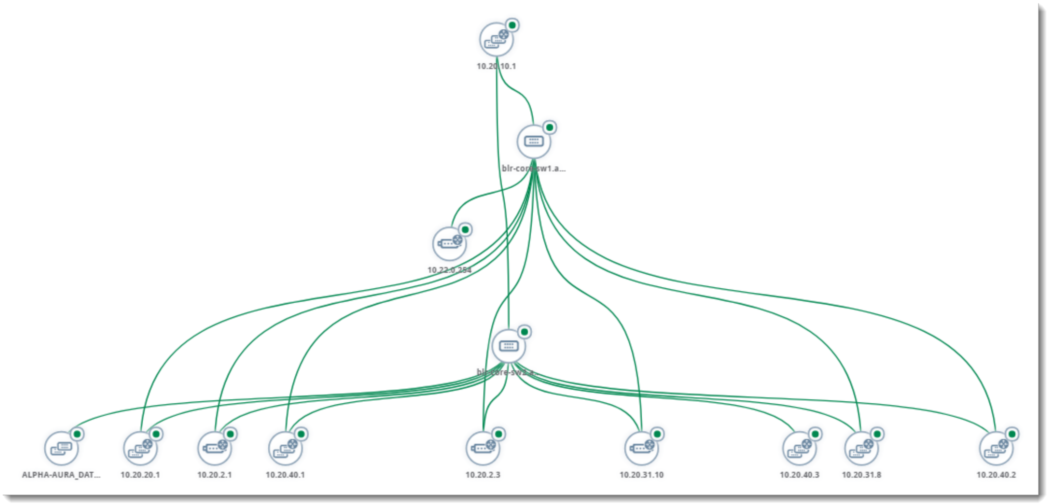


Table 97: *Device Icons*

	switch
	Switch (L2)
	Stack switch (L2)
	Switch router (L3 Switch)
	Stack switch (L3)
	Router
	AP

Set the Root Node

You might want to change the root node that Topology places at the top of the topology map. If you have a network which is separated from another network, you can set a root node on each island.

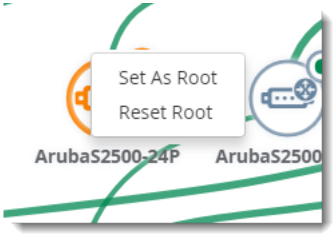
NOTE

When you set the root node, Topology saves the root node in a browser cache so that anyone with access to the OV3600 server can view the root node from any client browser.

To change the root node:

1. Locate the device in the topology map.
2. Select **Actions** from the task pane.
3. Highlight the node in the map, then click **Actions** in the task pane.
4. Select **Set As Root**. Topology highlights the node and updates the map to show the new root node. Changes can be made by selecting **Reset Root Nodes**.

Figure 143: *Setting the Root Node*



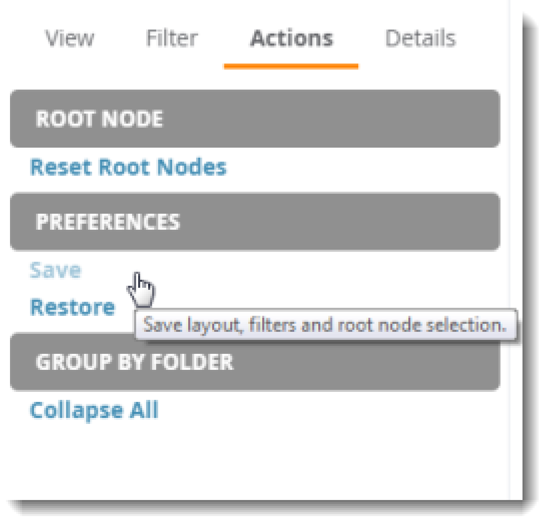
Saving Your Preferences

After changing your layout, filters, or root node, you can save your custom map.

To save your preferences:

1. Select a layout, filter, or root node.
2. Select **Actions** from the task pane.
3. Locate the Preferences section, then select **Save**. Clicking **Restore** applies your last saved preferences for layout, filters, and root nodes.

Figure 144: *Saving Your Preferences*



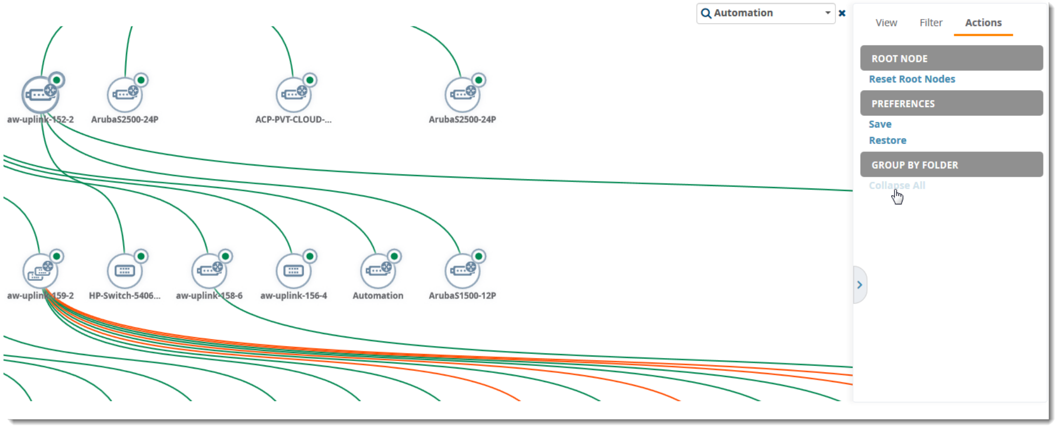
Collapsing the View

If you manage a large number of network devices, you can collapse all devices in the topology map. When displaying a collapsed view, Topology groups all devices by OV3600 folders and organizes them in a folder hierarchy. By default, OV3600 displays networks with more than 200 devices in collapsed view.

To collapse the topology map:

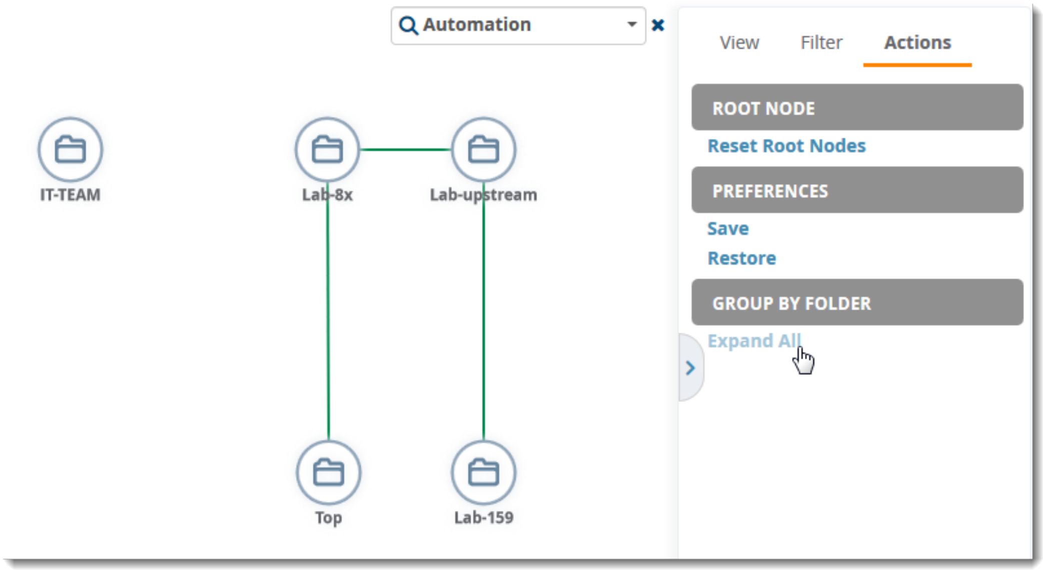
1. In the task pane, click **Actions**.
2. Select **Collapse All**. The devices collapse to folder level.

Figure 145: *Collapsing the View*



When you are in collapsed view, if you choose **Expand All**, Topology expands all nodes and redistributes them in the topology map.

Figure 146: *Expanding the View*



NOTE

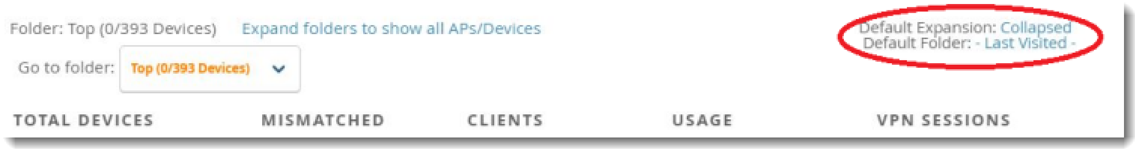
You can also double click a node to expand all or collapse the view.

Changing the Default Expansion

User preferences defined on the **Devices > List** page affect the way OV3600 displays the network in the topology map. The default expansion is collapsed and based on the folder level you last visited. If your view is collapsed, you will only see devices from that folder level.

To change the default expansion:

1. Navigate to **Devices > List**, then select **Expanded** from the **Default Expansion** drop-down menu.



Folder: Top (0/393 Devices) Expand folders to show all APs/Devices

Go to folder: Top (0/393 Devices)

Default Expansion: Collapsed
Default Folder: - Last Visited -

2. Go back to Topology. The topology map displays the network in expanded view.

Checking the Status of Your Network

The colored icons show device status, number of rogues, CPU and memory utilization, and bandwidth usage. Green generally means everything is good, yellow is average, and orange requires your attention.

Device Status

Colored circles in the topology map and colored arrows in the tooltip or Details tab indicate that:

🟢 (next to the device icon) there are no alerts or detected rogues.

🟠 (next to the device icon) there are 1 to 2 alerts and no detected rogues.

🔴 (next to the device icon) there are at least 2 alerts or 1 or more detected rogues.

↑ the device is up.

↓ the device is down.

Health Status

Colored circles in the tooltip or Detail tab, or colored link lines in the topology map indicate that:

🟢 more than 25% memory is available and less than 75% CPU is used.

🟠 (more than 15% memory is available and less than 85% CPU is used.

🔴 less than 15% memory is available and more than 85% CPU is used.

— less than 70 Mbps bandwidth is used.

— between 70 and 90 Mbps bandwidth is used.

Link Status

Colored link lines in the topology map indicate that:

— the link is up.

— the link is down.

Taking Action from Quick Links

Topology provides access to monitoring information from quick links in tooltips and device details in the right pane.

View Tooltips

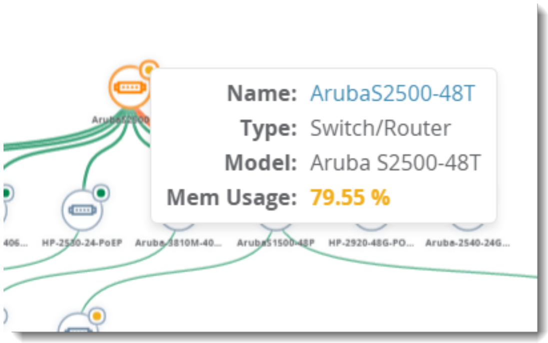
Tooltips provide quick links to the monitoring page for the device or the switch interface. Tooltips also display potential problems on a device. Alerts are colored orange in the tooltip.

To view tooltips, hover your mouse over:

- A node, which is represented by the device icon in the topology map.
- The link, which is the represented by the line between two switches.
- The link count, which is represented as a number alongside the link between two switches.

In Figure 147, the tooltip for a node shows you the name of the device, device type, model, and a health alert.

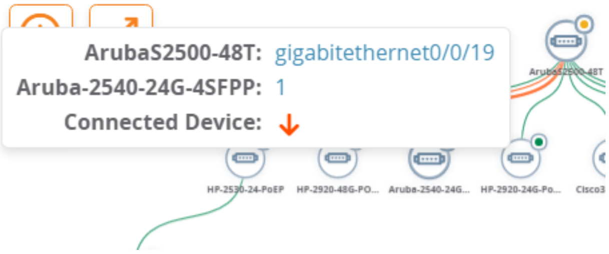
Figure 147: *Tooltip for a Node*



Name: ArubaS2500-48T
Type: Switch/Router
Model: Aruba S2500-48T
Mem Usage: 79.55 %

In Figure 148, the tooltip for a network link shows an alert for a down device. You can click the hyperlinks to troubleshoot the problem.

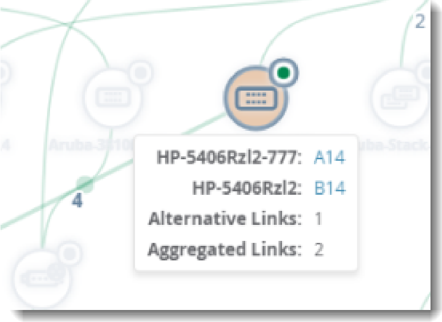
Figure 148: *Tooltip for a Link*



ArubaS2500-48T: gigabitethernet0/0/19
Aruba-2540-24G-4SFPP: 1
Connected Device: ↓

In Figure 149, the green link circle indicates that the link is aggregated; the link count indicates that there are 4 logical links, of which are 2 individual links and 2 aggregated links.

Figure 149: *Tooltip for an Aggregated Link*

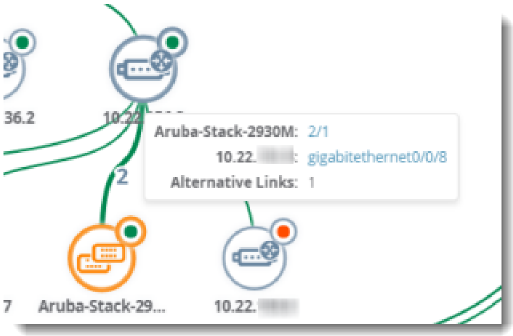


HP-5406Rzl2-777: A14
HP-5406Rzl2: B14
Alternative Links: 1
Aggregated Links: 2

The tooltip also shows whether the redundant links between tree members are dynamic, between 2 peers that support LACP, or aggregated, between 2 peers that support HP_LA. In Figure 149, "alternative link" refers to the number of non-aggregated redundant links. If you point your mouse over the link count, the tooltip provides a hyperlink to the switch interface monitoring page.

Figure 150 shows the tooltip for stack member. You can access monitoring pages from the hyperlinks in the tooltip.

Figure 150: *Tooltip for a Stack Member*



Aruba-Stack-2930M: 2/1
10.22.[redacted]: gigabitethernet0/0/8
Alternative Links: 1

Viewing Device and Stack Membership Details

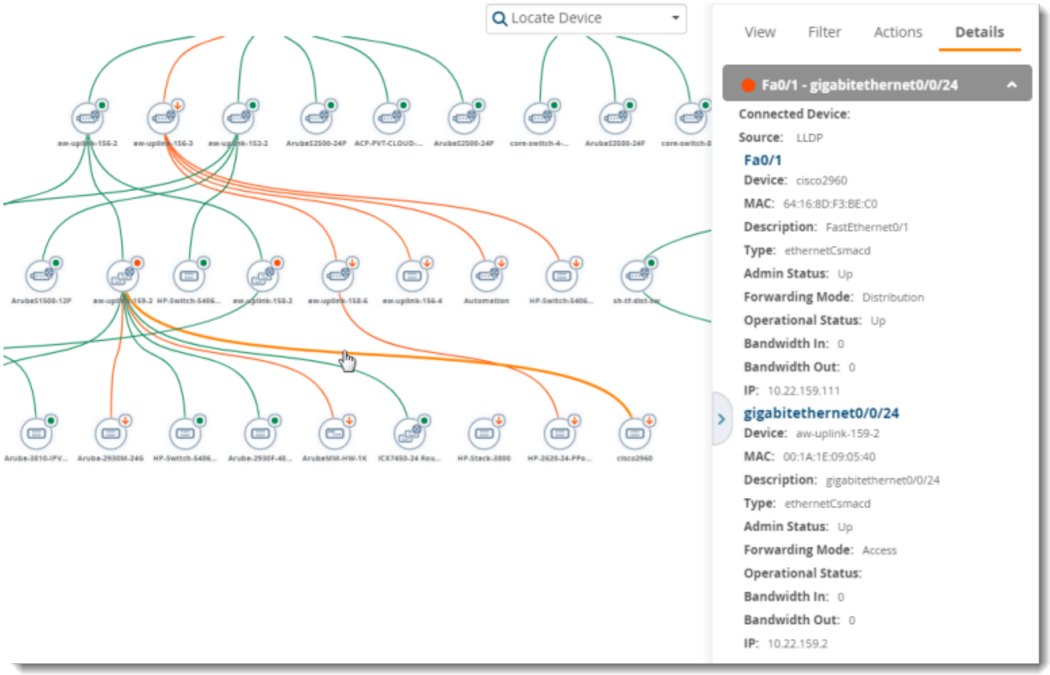
The **Details** task pane provides information, health and status indicators, and quick links to monitoring pages.

To view device and stack membership details:

- Search for a device or switch stack
- Click the node in the map
- Click a connection in the map

In Figure 151, you can see that the health of the network connection, represented as an orange line in the topology map, is critical. Thicker lines represent multiple links between devices. By clicking on the links to the switch ports, you can troubleshoot further.

Figure 151: *Connected Devices and Switch Interface Details*

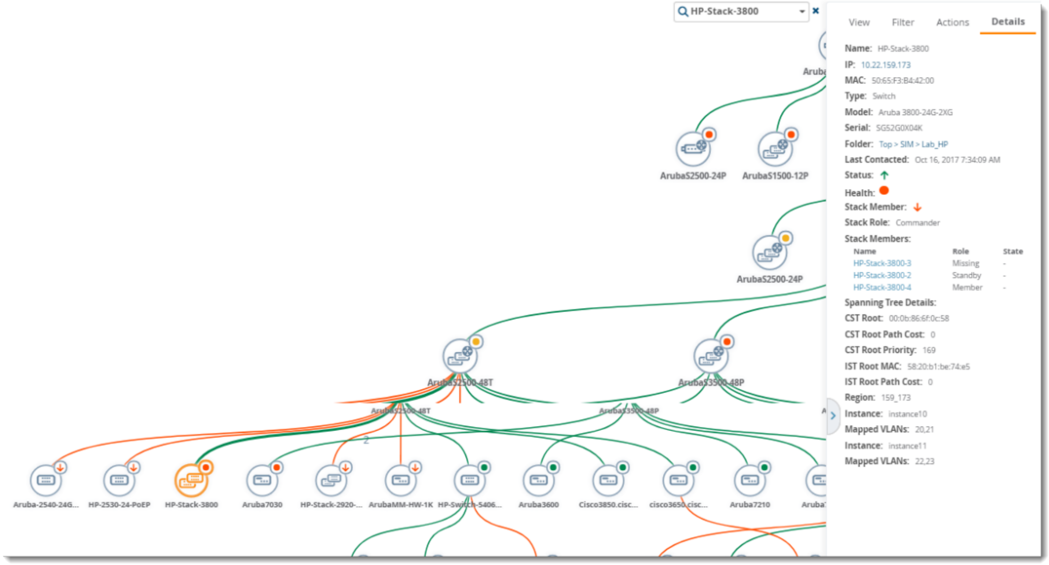


● Fa0/1 - gigabitethernet0/0/24

Connected Device:
Source: LLDP
Fa0/1
Device: cisco2960
MAC: 64:16:8D:F3:BE:C0
Description: FastEthernet0/1
Type: ethernetCsmacd
Admin Status: Up
Forwarding Mode: Distribution
Operational Status: Up
Bandwidth In: 0
Bandwidth Out: 0
IP: 10.22.159.111
gigabitethernet0/0/24
Device: aw-uplink-159-2
MAC: 00:1A:1E:09:05:40
Description: gigabitethernet0/0/24
Type: ethernetCsmacd
Admin Status: Up
Forwarding Mode: Access
Operational Status:
Bandwidth In: 0
Bandwidth Out: 0
IP: 10.22.159.2

In Figure 152, you can see information about all members in the stack commanded by the switch that is highlighted in orange on the map. The health of the network connection, represented as an orange circle in the **Details** task pane, alerts you to critical status. By clicking on the links to the stack members or folder, you can manage a stack member.

Figure 152: *Stack Member Details*



Name: HP-Stack-3800
IP: 10.22.159.173
MAC: 50:65:F3:B4:42:00
Type: Switch
Model: Aruba 3800-24G-2XG
Serial: SG52G0X04K
Folder: Top > SIM > Lab_HP
Last Contacted: Oct 16, 2017 7:34:09 AM
Status: ↑
Health: ●
Stack Member: ↓
Stack Role: Commander
Stack Members:

Name	Role	State
HP-Stack-3800-3	Missing	-
HP-Stack-3800-2	Standby	-
HP-Stack-3800-4	Member	-

Spanning Tree Details:
CST Root: 00:0b:86:6f:0c:58
CST Root Path Cost: 0
CST Root Priority: 169
IST Root MAC: 58:20:b1:be:74:e5
IST Root Path Cost: 0
Region: 159_173
Instance: instance10
Mapped VLANs: 20,21
Instance: instance11
Mapped VLANs: 22,23

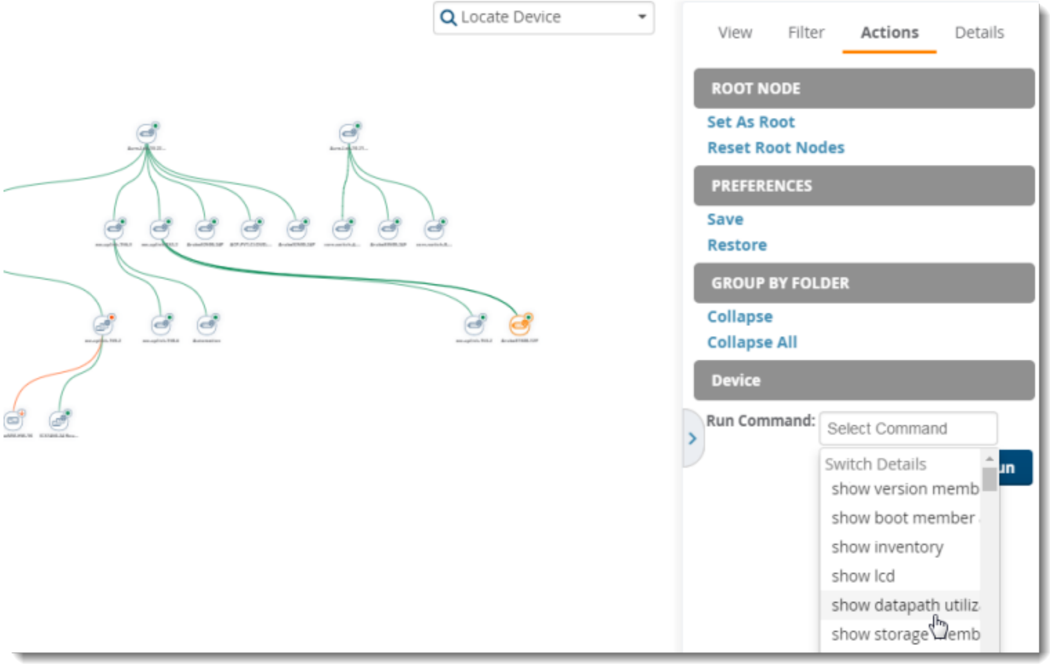
Running a Command

In addition to running a command from the monitoring page for a device, you can run a command directly from the topology map. The commands available depend on which device you select. So, if you select a switch, the commands you can choose from in the task pane are switch-related.

To run a command from the topology map:

1. Click a node in the map.
2. Select **Actions** from the task pane.
3. Locate the Device section, then select a CLI command from the Run Command menu.

Figure 153: *Selecting a Command to Run on a Device*



This section contains the following topics describing individual device configuration within device groups:

- "Moving a Device from Monitor Only to Manage Read/Write Mode" on page 208
- "Configuring Device Settings" on page 209
- "Adding a Maintenance Window for a Device" on page 217
- "Configuring Device Interfaces for Switches" on page 218
- "Individual Device Support and Firmware Upgrades" on page 219

While most device configuration settings can be efficiently managed by OV3600 at a Group level, certain settings must be managed at the individual device level. For example, because devices within a Group are often contiguous with one another, and have overlapping coverage areas, it makes sense to manage these devices individually to avoid RF interference.

NOTE

Any changes made at an individual device level will automatically override Group level settings.

OV3600 automatically saves the last 10 device configurations for reference and compliance purposes. Archived device configurations are linked on the **Devices > Device Configuration** page and identified by name. By default, configuration is tracked by the date and time it was created; device configurations are also archived by date.

It is not possible to push archived configurations to devices, but archived configurations can be compared to the current configuration, the desired configuration, or to other archived configurations using the drop-down menus on the **Devices > Device Configuration** page. This applies to startup or running configuration files.

Compare two configurations to highlight the specific lines that are mismatched. The Device Configuration page provides links to OV3600 pages where any mismatched settings can be configured.

Moving a Device from Monitor Only to Manage Read/Write Mode

You can move the device to **Manage Read/Write** mode after you have verified any configuration mismatches on the **Devices > Device Configuration** page, or you have confirmed that the device configuration status is **Good** on the **Devices > List** page.

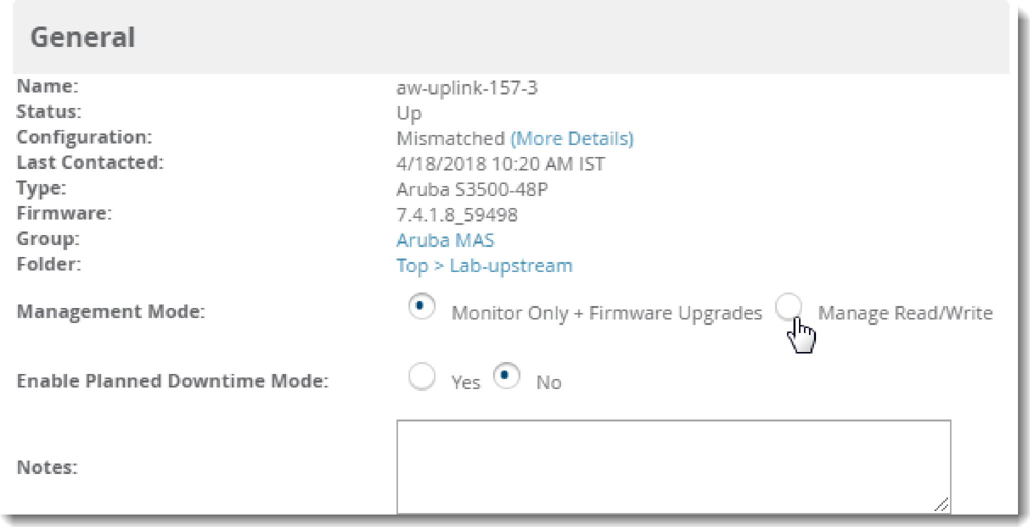
NOTE

You can set multiple devices into Planned Maintenance Mode in the **Modify Devices** link on an AP list page. For more information, refer to "Modifying Multiple Devices" on page 115.

To move a device to **Manage Read/Write** mode:

1. Go to the **Devices > List** page, then right-click on the device and select **Manage** to open the Manage page.
2. From the the **General** area, select **Manage Read/Write**, as shown in Figure 154.

Figure 154: *Selecting the Management Mode*



General

Name: aw-uplink-157-3
Status: Up
Configuration: Mismatched (More Details)
Last Contacted: 4/18/2018 10:20 AM IST
Type: Aruba S3500-48P
Firmware: 7.4.1.8_59498
Group: Aruba MAS
Folder: Top > Lab-upstream

Management Mode: ● Monitor Only + Firmware Upgrades ○ Manage Read/Write

Enable Planned Downtime Mode: ○ Yes ● No

Notes:

3. Scroll down, then select **Save and Apply**.
4. Click **Confirm Edit** on the confirmation page to retain these settings and push the configuration to the device.
5. For device configuration changes that require the device to reboot, use the **Schedule** function to push the changes at a time when WLAN users will not be affected.

NOTE

Use the **Enable Planned Maintenance Mode** field in **Devices > Manage > General** to put this device into planned maintenance. During the maintenance mode, no AP Down triggers will be deployed on these devices. Users will not be able to delete folders that contain devices in Planned Maintenance. The devices in Planned Maintenance will show the Up status, but will not be tracked in historical graphs and logs as Up. You can set multiple devices into Planned Maintenance Mode in the **Modify Devices** link on an AP list page. For more information, refer to "Modifying Multiple Devices" on page 115.

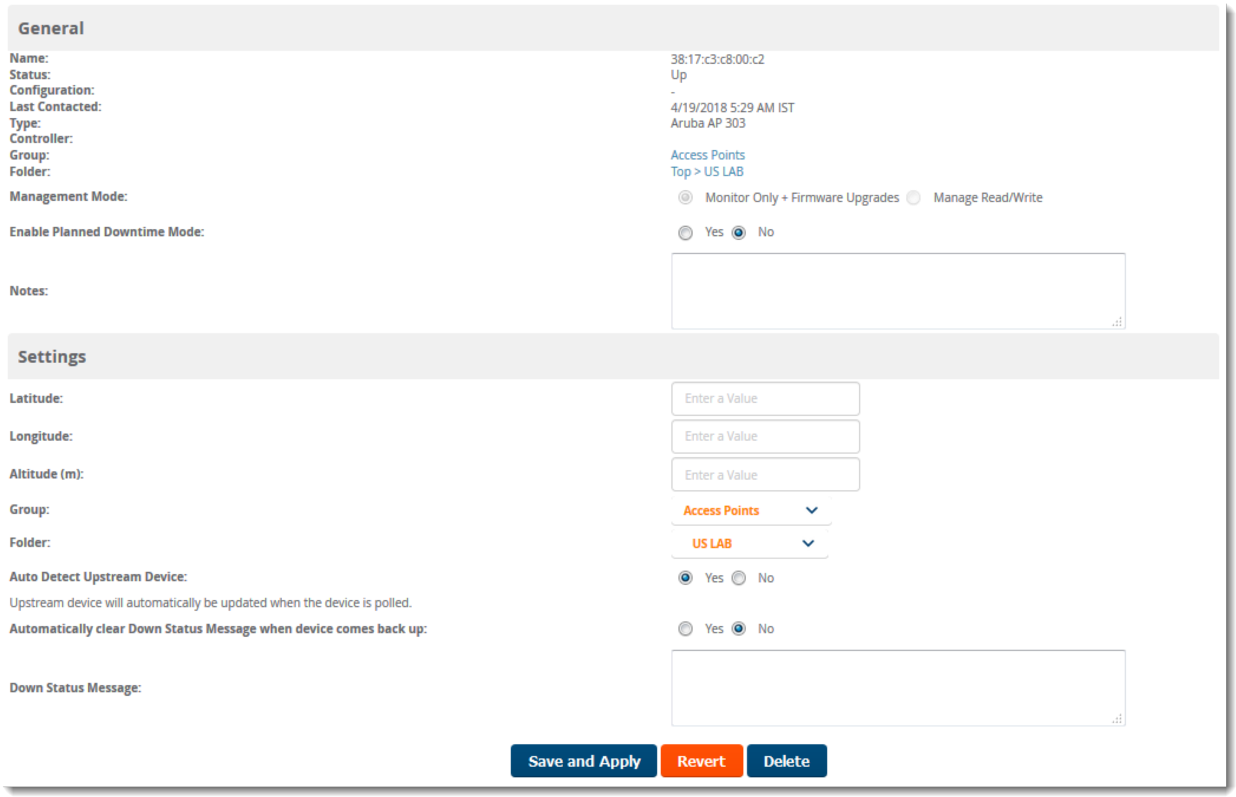
Configuring Device Settings

The device settings on the Management page variy depending on the type of device you select. If any changes are scheduled for a device, you can view them in a **Scheduled Changes** section at the top of the page and click the Job link to access to the **System > Configuration Change Job Detail** page.

To configure device settings:

1. Navigate to **Devices > List** , then right click the device and select **Manage** from the shortcut menu to access the Management page. Figure 155 shows a Management page for an AP.

Figure 155: *Example of a Management Page for an AP*



General

Name:	38:17:c3:c8:00:c2
Status:	Up
Configuration:	-
Last Contacted:	4/19/2018 5:29 AM IST
Type:	Aruba AP 303
Controller:	
Group:	Access Points
Folder:	Top > US LAB
Management Mode:	● Monitor Only + Firmware Upgrades ○ Manage Read/Write
Enable Planned Downtime Mode:	○ Yes ● No
Notes:	

Settings

Latitude:	Enter a Value
Longitude:	Enter a Value
Altitude (m):	Enter a Value
Group:	Access Points
Folder:	US LAB
Auto Detect Upstream Device:	● Yes ○ No
Upstream device will automatically be updated when the device is polled.	
Automatically clear Down Status Message when device comes back up:	○ Yes ● No
Down Status Message:	

2. Locate the **General** section for information about the device's current status.

Table 98 describes the fields, information, and settings on the Management page.

Table 98: *Devices > Manage > General Fields and Descriptions*

Field	Description
Name	Displays the name currently set on the device.
Status	Displays the current status of a device. If a device is **Up**, then OV3600 is able to ping it and fetch SNMP information from the device. If the device is listed **Down** then OV3600 is either unable to ping the device or unable to read the necessary SNMP information from the device.
Configuration	Displays the current configuration status of the device. To update the status, select **Audit** on the **Devices > Device Configuration** page.
Last Contacted	Displays the last time OV3600 successfully contacted the device.
Type	Displays the device type.
Controller	Links to the switch that is monitoring this device. **NOTE:** This field is visible for APs.
Firmware	Shows the device firmware version. **NOTE:** This field is visible for controllers and switches.

Table 98: *Devices > Manage > General Fields and Descriptions (Continued)*

Field	Description
Group	Links to the **Group > Monitoring** page for the device.
Template	Displays the name of the group template currently configuring the device. This also displays a link to the **Groups > Template** page. **NOTE:** This field is only visible for APs that are managed by templates.
Folder	Displays the name of the folder containing the device. Also displays a link to the **Devices > List** page for the folder.
Management Mode	Displays the current management mode of the device. No changes are made to the device when it is in **Monitor Only** mode. OV3600 pushes configurations and makes changes to a device when it is in **Manage Read/Write** mode.
Enable Planned Maintenance Mode	Put this device into planned maintenance. During the maintenance mode, no device Down triggers will be deployed on these devices. Users will not be able to delete folders that contain devices in Planned Maintenance. The devices in Planned Maintenance will show the Up status, but will not be tracked in historical graphs and logs as Up. You can set multiple devices into Planned Maintenance Mode in the **Modify Devices** link on a device list page.
Notes	Provides a free-form text field to describe device information.

3. Review and provide the following information in the **Settings** area. Devices with dual radios display radio-specific settings in the Slot A and Slot B area. If a device is dual-radio capable but only has one device installed, OV3600 manages that device as if it were a single slot device.

NOTE

Devices from different vendors have different RF settings and capabilities. The fields in the **Settings** section of the **Devices > Manage** page are context-sensitive and only present the information relevant for the particular device vendor and model.

Table 99 describes field settings, default values, and information for the **Settings** section of this page.

Table 99: *Devices > Manage > Settings Fields and Default Values*

Setting	Default	Device Type	Description
Name	None	All	User-configurable name for the device (max. 20 characters)
Domain Name	None	IOS	Field populated upon initial device discovery or upon refreshing settings. Enable this option from **OV3600 Setup > Network** page to display this field on the **Devices > Manage** page, with fully-qualified domain names for IOS APs. This field is used in conjunction with **Domain** variable in IOS templates.
Mesh ID	None	Mesh	Text field for entering the Mesh ID.
Timezone	None	Instant	Drop-down menu for specifying the controller timezone.

Table 99: *Devices > Manage > Settings Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
Syslog Server	None	Instant	Text field for specifying the a syslog server for the controller.
RADIUS Server	None	Instant	Text field for specifying the a RADIUS server for the controller.
RF Band Selection	All	Instant	Drop-down menu for specifying the RF Band on the controller.
Location	Read from the device	All	The SNMP location set on the device.
Latitude	None	All	Text field for entering the latitude of the device. The latitude is used with the Google Earth integration.
Longitude	None	All	Text field for entering the longitude of the device. The longitude is used with the Google Earth integration.
Altitude (meters)	None	All	Text field for entering the altitude of the device when known. This setting is used with the Google Earth integration. Specify altitude in meters.
Group	Default Group	All	Drop-down menu that can be used to assign the device to another Group.
Folder	Top	All	Drop-down menu that can be used to assign the device to another Group.
Auto Detect Upstream Device	Yes	All	Selecting **Yes** enables automatic detection of upstream device, which is automatically updated when the device is polled. Selecting **No** displays a drop-down menu of upstream devices.
Automatically clear Down Status Message when device comes back up	None	All	Whether the message entered in the **Down Status Message** field should be removed after the device returns to the Up status.
Down Status Message	None	All	Enter a text message that provides information to be provided if the device goes down.
Organization	Read from Device	Instant	The Organization string of the OAW-IAP.
Alcatel-Lucent AP Group	default	All	Specifies the Alcatel-Lucent AP Group in which this devices resides.

Table 99: *Devices > Manage > Settings Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
Administrative Status	Enable	All	Enables or disables administrative mode for the device.
Mode	Local	All	Designates the mode in which the device should operate. Options include the following: ● Local ● H-REAP ● Monitor ● Rogue Detector ● Sniffer

4. Complete additional settings on the **Devices > Manage** page, to include H-REAP, certificates, radio settings, and network settings. Table 100 describes many of the possible fields.

NOTE

For complete listing and discussion of settings applicable only to *Alcatel-Lucent* devices, see the Alcatel-Lucent *Device Configuration Guide*.

Table 100: *Additional Settings*

Setting	Default	Device Type	Description
Mesh Mode	Mesh AP	Mesh Devices	Drop-down menu specifies the mesh role for the AP as shown: ● **Mesh AP** —The AP will act like a mesh client. It will use other APs as its uplink to the network. ● **Portal AP** —The AP will become a portal AP. It will use a wired connection as its uplink to the network and serve it over the radio to other APs. ● **Remote Portal AP** —The AP will become a remote portal AP. It will use a wireless connection as its uplink to the network and serve it over the radio to other APs. ● **None** —The AP will act like a standard AP. It will not perform meshing functions.
Mesh Mobility	Static	Mesh Devices	Select **Static** if the AP is static, as in the case of a device mounted on a light pole or in the ceiling. Select **Roaming** if the AP is mobile. Two examples would be an AP mounted in a police car or utility truck.

Table 100: *Additional Settings (Continued)*

Setting	Default	Device Type	Description
Receive Antenna	Diversity	Cisco	Drop-down menu for the receive antenna provides three options: **Diversity** —Device will use the antenna that receives the best signal. If the device has two fixed (non-removable) antennas, the **Diversity** setting should be used for both receive and transmit antennas. **Right** —If your device has removable antennas and you install a high-gain antenna on the device's right connector (the connector on the right side when viewing the back panel of the device), use this setting for receive and transmit. **Left** —If your device has removable antennas and you install a high-gain antenna on the device's left connector, use this setting for both receive and transmit.
Transmit Antenna	Diversity	Cisco	See description in **Receive Antenna** above.
Antenna Diversity	Primary Only	Symbol 4131	Drop-down menu provides the following options: **Full Diversity**—The device receives information on the antenna with the best signal strength and quality. The device transmits on the antenna from which it last received information. **Primary Only**—The device transmits and receives on the primary antenna only. Secondary Only: The device transmits and receives on the secondary antenna only. **Rx Diversity**—The device receives information on the antenna with the best signal strength and quality. The device transmits information on the primary antenna only.
Transmit Power Reduction	0	Proxim	Transmit Power Reduction determines the device's transmit power. The max transmit power is reduced by the number of decibels specified.

Table 100: *Additional Settings (Continued)*

Setting	Default	Device Type	Description
Channel	6	All	Represents the device's current RF channel setting. The number relates to the center frequency output by the device's RF synthesizer. Contiguous devices should be set to different channels to minimize 'crosstalk,' which occurs when the signals from APs overlap and interfere with each other. This RF interference negatively influences WLAN performance. 802.11b's 2.4-GHz range has a total bandwidth of 80-MHz, separated into 11 center channels. Of these channels, only 3 are non-overlapping (1, 6, and 11). In the United States, most organizations use only these non-overlapping channels.
Transmit Power Level	Highest power level supported by the radio in the regulatory domain (country)	Cisco, Symbol, Proxim AP-600, AP-700, AP-2000 (802.11g)	Determines the power level of radio transmission. Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device. You can increase the coverage radius of the access point by increasing the Transmit Power Level. However, while this increases the zone of coverage, it also makes it more likely that the device will interfere with neighboring devices. Supported values are: **Cisco (100mW, 50mW, 30mW, 20mW, 5mW, 1mW) Symbol (Full or 50mW, 30mW, 15mW, 5mW, 1mW)**
Radio Enabled	Yes	All	The Radio Enabled option allows you to disable the radio's ability to transmit or receive data while still maintaining Ethernet connectivity to the network. OV3600 will still monitor the Ethernet page and ensure the device stays online. Customers typically use this option to temporarily disable wireless access in particular locations. This setting can be scheduled at a device level or Group level. **NOTE:** You cannot disable radios unless rogue scanning is disabled in **Groups > Radio**.
Use DHCP	Yes	All	If enabled, the device will be assigned a new IP address using DHCP. If disabled, the device will use a static IP address. For improved security and manageability, disable DHCP and using static IP addresses.

Table 100: *Additional Settings (Continued)*

Setting	Default	Device Type	Description
LAN IP	None	All	The IP Address of the device Ethernet interface. If One-to-One NAT is enabled, OV3600 will communicate with the device on a different address (the IP Address defined in the **Device Communication** section). If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.
Subnet Mask	None	All	Provides the IP subnet mask to identify the sub-network so the IP address can be recognized on the LAN. If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.
Gateway	None	All	The IP address of the default internet gateway. If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.

5. Locate the **Template Options** area on the **Devices > Manage** page.

NOTE

This section only appears for IOS APs, Symbol devices, and Alcatel-Lucent switches in groups with Alcatel-Lucent GUI Config disabled.

Table 101 describes field settings, default values, and additional information for this page.

Table 101: *Devices > Manage > Template Options Fields and Default Values*

Setting	Default	Device Type	Description
WDS Role	Client	Cisco IOS Wireless LAN Controllers only	Set the WDS role for this device. Select Master for the WDS master APs and Client for the WDS Client. Once this is done you can use the %if wds_role= % to push the client, master, or backup lines to appropriate WDS APs.
SSL Certificate	None	Cisco IOS	OV3600 will read the SSL Certificate off of the device when it comes UP in OV3600. The information in this field will defines what will be used in place of %certificate%.
Extra Device Commands	None	Cisco IOS	Defines the lines that will replace the %ap_include_1% variable in the IOS template. This field allows for unique commands to be run on individual APs. If you have any settings that are unique per device like a MOTD you can set them here.
switch_command	None	Cisco Catalyst switches	Defines lines included for each of the members in the stack. This field appears only on the master's **Manage** page. The information in this field will determine what is used in place of the %switch_command% variable.

6. For Cisco WLC devices, go to the interfaces section of the **Devices > Manage** page. Select **Add new Interface** to add another controller interface, or select the **pencil** icon to edit an existing controller interface. Table 102 describes the settings and default values. For detailed descriptions of Cisco WLC devices supported by OV3600, refer to the Cisco WLC product documentation.

Table 102: *Devices > Manage > Interface Fields and Descriptions for Cisco WLC Devices*

Field	Default	Description
Name	None	The name of the interface on the controller.
VLAN ID	None	The VLAN ID for the interface on the controller.
Port	None	The port on the controller to access the interface.
IP Address	None	The IP address of the controller.
Subnet Mask	None	The subnet mask for the controller.
Gateway	None	The controller's gateway.
Primary and Secondary DHCP Servers	None	The DHCP servers for the controller.
Guest LAN	Disabled	Indicates a guest LAN.
Quarantine VLAN ID	Disabled	Enabled indicates it is a quarantine VLAN; used only for H-REAP-associated clients.
Dynamic Device Management	Enabled	When enabled, makes the interface an AP-manager interface. Cisco calls this feature Dynamic AP Management.

Adding a Maintenance Window for a Device

When you add a maintenance window for a device, OV3600 changes the management mode to **Manage Read/Write** and stops polling or monitoring the device.

OV3600 will push the last saved configuration to the device, regardless of any pending changes to the group it belongs to or its device settings. Ensure all device configurations stored in OV3600 are saved before you proceed.

NOTE

It is recommended you change the management mode to **Planned Downtime** before you change the maintenance window to prevent the device from entering **Manage Read/Write** mode. OV3600 continues monitoring these device while you configure the maintenance window.

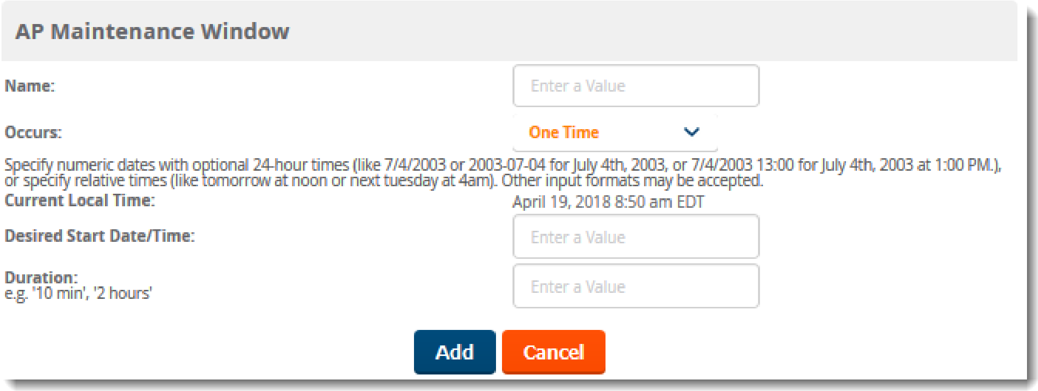
NOTE

You can also use the **Modify Devices** link to add or delete maintenance windows on multiple devices at once. This feature can also be used from the Master Console to set maintenance windows for multiple OV3600 servers.

To add a maintenance window:

1. Navigate to **Devices > List** , then right click the device and select **Manage** from the shortcut menu to access the Management page.
2. Scroll down the Management page to the **Maintenance Windows** section.
3. Click **Add**.

Figure 156: *Adding a Maintenance Window for a Device*


AP Maintenance Window

Name: Enter a Value

Occurs: One Time

Specify numeric dates with optional 24-hour times (like 7/4/2003 or 2003-07-04 for July 4th, 2003, or 7/4/2003 13:00 for July 4th, 2003 at 1:00 PM.), or specify relative times (like tomorrow at noon or next tuesday at 4am). Other input formats may be accepted.

Current Local Time: April 19, 2018 8:50 am EDT

Desired Start Date/Time: Enter a Value

Duration: e.g. '10 min', '2 hours' Enter a Value

Add Cancel

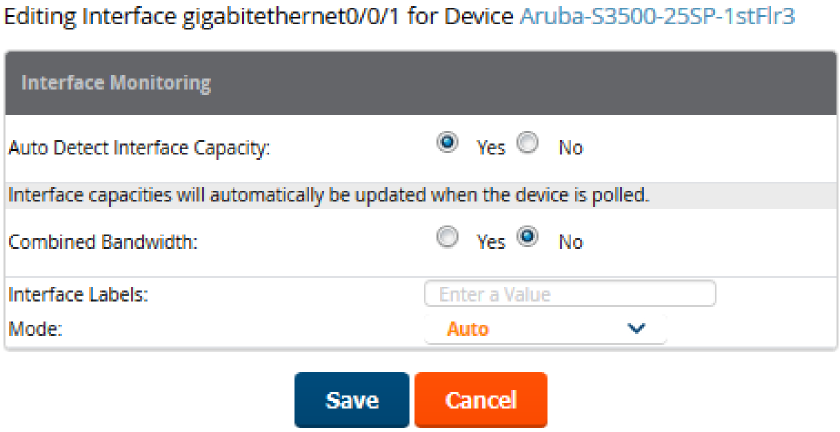
4. Enter a name for the maintenance window.
5. Select the frequency of the maintenance window.
6. Enter the start time and the duration of the maintenance window.
7. Click **Add**.

Configuring Device Interfaces for Switches

New physical and virtual interfaces are discovered using SNMP polling. SNMP/HTTP discovery scanning is the primary method for discovering devices on your network, including rogue devices. Enable this scanning method from the **Device Setup > Discover** page.

You can configure interface settings individually or in groups. For individual settings, select the pencil icon next the interface name in **AP/Devices > Interfaces**. This takes you to the **Interface Monitoring** window which may a slightly different appearance than Figure 157, depending on the device type, and whether you are configuring a physical or virtual interface.

Figure 157: *Editing a Switch Interface*


Editing Interface gigabitethernet0/0/1 for Device Aruba-S3500-25SP-1stFlr3

Interface Monitoring

Auto Detect Interface Capacity: ● Yes ○ No

Interface capacities will automatically be updated when the device is polled.

Combined Bandwidth: ○ Yes ● No

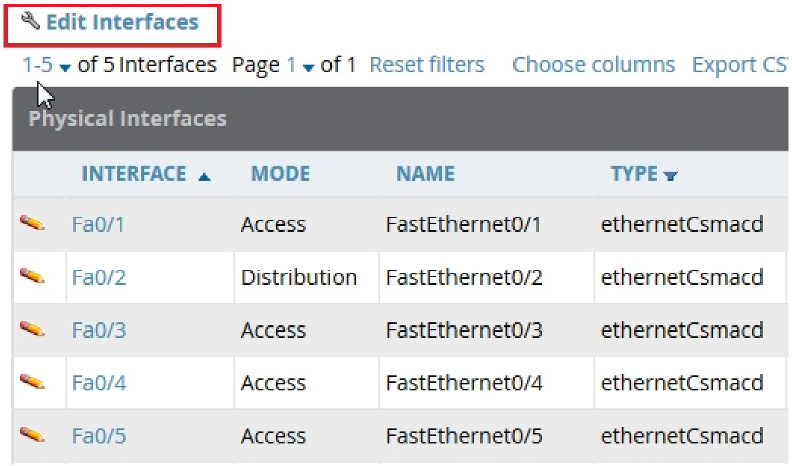
Interface Labels: Enter a Value

Mode: Auto

Save Cancel

To configure interfaces as a group, select **Edit Interfaces** above the Physical or Virtual Interfaces table as shown in Figure 158.

Figure 158: *Edit Multiple Interfaces*



Edit Interfaces

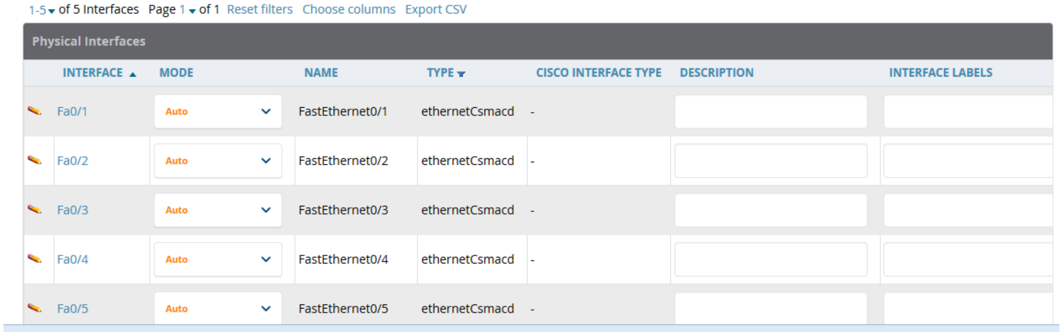
1-5 ▾ of 5 Interfaces Page 1 ▾ of 1 Reset filters Choose columns Export CS

Physical Interfaces

	INTERFACE ▲	MODE	NAME	TYPE ▾
✎	Fa0/1	Access	FastEthernet0/1	ethernetCsmacd
✎	Fa0/2	Distribution	FastEthernet0/2	ethernetCsmacd
✎	Fa0/3	Access	FastEthernet0/3	ethernetCsmacd
✎	Fa0/4	Access	FastEthernet0/4	ethernetCsmacd
✎	Fa0/5	Access	FastEthernet0/5	ethernetCsmacd

You will remain on the same page, but will have the option to make changes to the most commonly edited settings in batch mode, as shown in Figure 159.

Figure 159: *Multiple Interface Editing Page Illustration*



1-5 ▾ of 5 Interfaces Page 1 ▾ of 1 Reset filters Choose columns Export CSV

Physical Interfaces

	INTERFACE ▲	MODE	NAME	TYPE ▾	CISCO INTERFACE TYPE	DESCRIPTION	INTERFACE LABELS
✎	Fa0/1	Auto ▾	FastEthernet0/1	ethernetCsmacd	-		
✎	Fa0/2	Auto ▾	FastEthernet0/2	ethernetCsmacd	-		
✎	Fa0/3	Auto ▾	FastEthernet0/3	ethernetCsmacd	-		
✎	Fa0/4	Auto ▾	FastEthernet0/4	ethernetCsmacd	-		
✎	Fa0/5	Auto ▾	FastEthernet0/5	ethernetCsmacd	-		

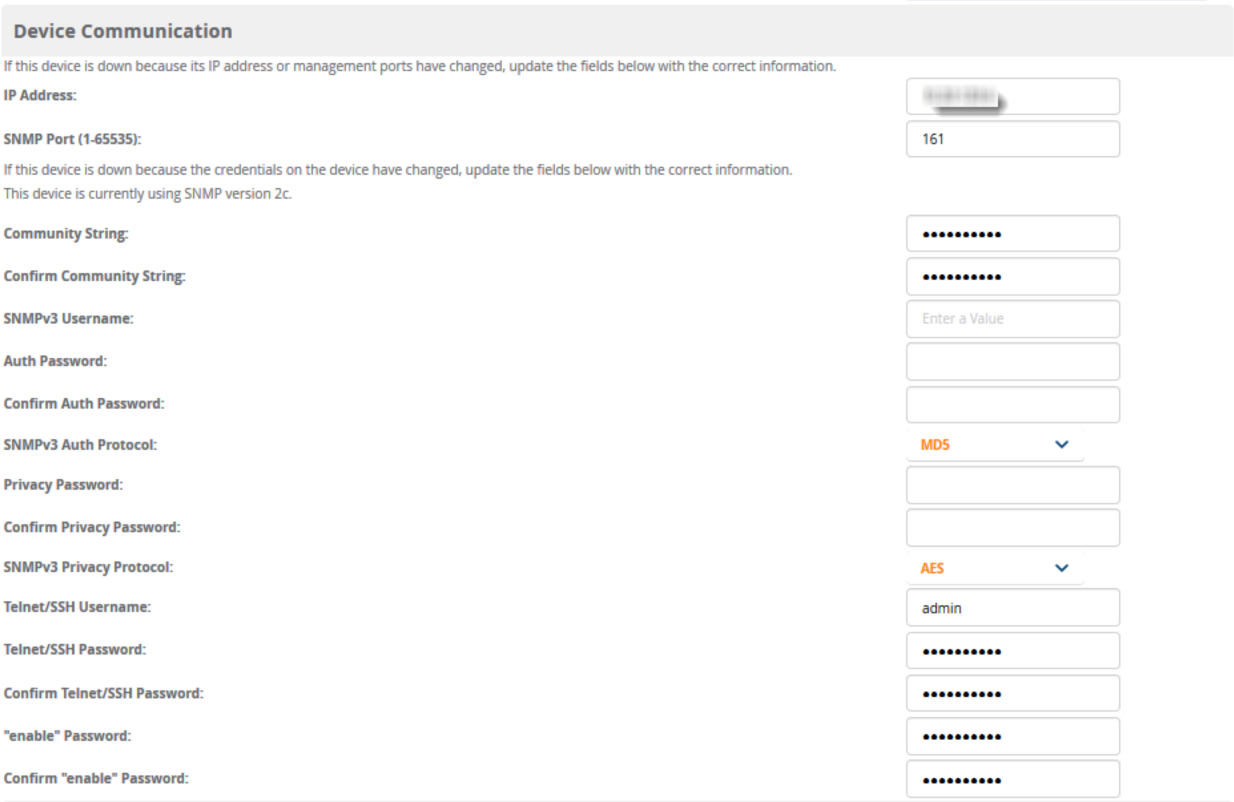
OV3600 assembles the entire running configuration using templates and your modifications to these pages. For a more detailed discussion on templates, see "Creating and Using Templates" on page 223.

Individual Device Support and Firmware Upgrades

Perform the following steps to configure device-level communication settings. The available device communication fields will vary, depending on the device brand and model.

1. Locate the **Device Communication** area on the **Devices > Manage** page.
2. Enter the credentials to be used to manage the device. Figure 160 illustrates this page.

Figure 160: *Devices > Manage > Device Communication*



Device Communication

If this device is down because its IP address or management ports have changed, update the fields below with the correct information.

IP Address:	[redacted]
SNMP Port (1-65535):	161

If this device is down because the credentials on the device have changed, update the fields below with the correct information.
This device is currently using SNMP version 2c.

Community String:	••••••••••
Confirm Community String:	••••••••••
SNMPv3 Username:	Enter a Value
Auth Password:	
Confirm Auth Password:	
SNMPv3 Auth Protocol:	MD5
Privacy Password:	
Confirm Privacy Password:	
SNMPv3 Privacy Protocol:	AES
Telnet/SSH Username:	admin
Telnet/SSH Password:	••••••••••
Confirm Telnet/SSH Password:	••••••••••
"enable" Password:	••••••••••
Confirm "enable" Password:	••••••••••

3. Enter and confirm the appropriate **Auth Password** and **Privacy Password**.
4. Enter the appropriate SSH and Telnet credentials if you are configuring Dell, Aruba Networks, Alcatel-Lucent or any Cisco device except Cisco WLAN controllers.
5. Select **Apply**, then **Confirm Edit** to apply the changes now.

NOTE

Some device configuration changes might require a system reboot, in which case you might schedule these changes to occur when users will not be affected.

Click **Update Firmware** at the bottom right of the page to upgrade the device's firmware. This button is not available if your device is in Monitor Only mode. The **Update Firmware** button only appears if the OV3600 Administrator has enabled **Allow firmware upgrades in monitor-only mode** on the **OV3600 Setup > General** page, *and* you are looking at an **Devices > Manage** page for a controller or autonomous AP that supports firmware upgrades in OV3600. See the Supported Infrastructure Devices document on the **Home > Documentation** page for a list of the OV3600-supported devices that can perform firmware upgrades. In most cases, you cannot upgrade firmware directly on thin APs.

Figure 161 illustrates the page that opens and Table 103 describes the settings and default values.

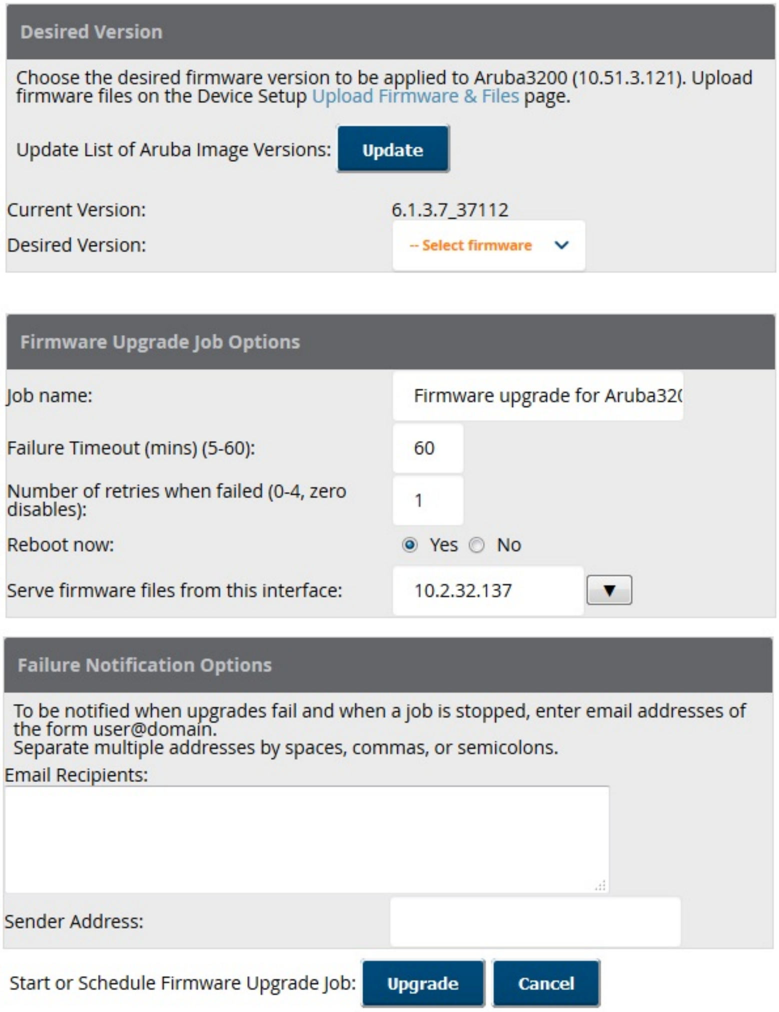
NOTE

Note that for Alcatel-Lucent firmware upgrades, OV3600 does not check whether a device is in **Master** or **Local** configuration, and it does not schedule rebooting after the upgrade. OV3600 users should consult Alcatel-Lucent's best practices for firmware upgrades and plan their upgrades using OV3600 accordingly.

Table 103: *Update Firmware Fields and Default Values*

Setting	Default	Description
Desired Version	None	Specifies the firmware to be used in the upgrade. Firmware can be added to this drop-down menu on the **Device Setup > Upload Firmware & Files** page.
Job Name	None	Sets a user-defined name for the upgrade job. Use a meaningful and descriptive name.
Use /safe flag for Cisco IOS firmware upgrade command	No	Enables or disables the /safe flag when upgrading IOS APs. The **/safe** flag must be disabled on older APs for the firmware file to fit in flash memory.
Email Recipients	None	Displays a list of email addresses that should receive alert emails if a firmware upgrade fails.
Sender Address	None	Displays the **From** address in the alert email.

Figure 161: *Devices > Manage Firmware Upgrades*



Desired Version

Choose the desired firmware version to be applied to Aruba3200 (10.51.3.121). Upload firmware files on the Device Setup Upload Firmware & Files page.

Update List of Aruba Image Versions: Update

Current Version: 6.1.3.7_37112

Desired Version: -- Select firmware

Firmware Upgrade Job Options

Job name: Firmware upgrade for Aruba32(

Failure Timeout (mins) (5-60): 60

Number of retries when failed (0-4, zero disables): 1

Reboot now: ● Yes ○ No

Serve firmware files from this interface: 10.2.32.137 ▼

Failure Notification Options

To be notified when upgrades fail and when a job is stopped, enter email addresses of the form user@domain.
Separate multiple addresses by spaces, commas, or semicolons.

Email Recipients:

Sender Address:

Start or Schedule Firmware Upgrade Job: Upgrade Cancel

Initiating a firmware upgrade will change the **Firmware Status** column for the device to Pending in **Devices > List**. You can review the status of all recent firmware upgrade jobs in **System > Firmware Upgrade Jobs**.

Chapter 6
Creating and Using Templates

This section provides an overview and several tasks supporting the use of device configuration templates in OV3600, and contains the following topics:

- "Group Templates" on page 223
- "Viewing and Adding Templates" on page 225
- "Configuring General Template Files and Variables" on page 229
- "Configuring Templates for Alcatel-Lucent Instant" on page 234
- "Configuring Templates for AirMesh" on page 236
- "Configuring Cisco IOS Templates" on page 236
- "Configuring Cisco Catalyst Switch Templates" on page 238
- "Configuring Symbol Controller / HPE WESM Templates" on page 238
- "Configuring a Global Template" on page 240

Group Templates

Supported Device Templates

Templates are helpful configuration tools that allow OV3600 to manage virtually all device settings. A template uses variables to adjust for minor configuration differences between devices.

The **Groups > Templates** configuration page allows you to create configuration templates for the following types of devices:

- Dell Networking W-Series
- Aruba
- Alcatel-Lucent

NOTE

Use the graphical Alcatel-Lucent config feature in support of Alcatel-Lucent devices, particularly for AOS-W 3.3.2.x and later. Refer to the *OmniVista 3600 Air Manager 8.2.7.1 Controller Configuration Guide* for additional information.

- Cisco Aironet IOS autonomous APs
- Cisco Catalyst switches
- HP ProCurve 530 and WeSM controllers
- Nomadix
- Symbol
- Trapeze
  - 3Com
  - Nortel
  - Enterasys

It is also possible to create local templates in a subscriber group—using global groups does not mean that global templates are mandatory

Template Variables

Variables in templates configure device-specific properties, such as name, IP address and channel. Variables can also be used to configure group-level properties, such as SSID and RADIUS server, which may differ from one group to the next. The OV3600 template understands many variables including the following:

- `%allowed_aps%`
- `%ams_identity%`
- `%antenna_receive%`
- `%antenna_transmit%`
- `%ap_include_1%` through `%ap_include_10%`
- `%ca_cert_checksum%`
- `%cck_power%`
- `%certificate%`
- `%cert_psk%`
- `%channel%`
- `%channel_width%`
- `%chassis_id%`
- `%clock_timezone%`
- `%contact%`
- `%controller_ip%`
- `%custom_variable_1% through %custom_variable_10%`
- `%domain%`
- `%enabled%`
- `%gateway%`
- `%guid%`
- `%hostname%`
- `%if interface=Dot11Radio0%`
- `%if interface=Dot11Radio1%`
- `%if ip=dhcp%`
- `%if ip=static%`
- `%if radio_type=a%`
- `%if radio_type=an%`
- `%if radio_type=b%`
- `%if radio_type=bgn%`
- `%if radio_type=g%`
- `%if wds_role=backup%`
- `%if wds_role=client%`
- `%if wds_role=master%`
- `%ip_address%`
- `%ip_address_a%`
- `%ip_address_b%`
- `%ip_address_c%`
- `%manager_ip_address%`
- `%master_ip%`
- `%netmask%`
- `%ofdmpower%`
- `%organization%`

- `%password%`
- `%power%`
- `%radius_server_ip%`
- `%rf_band%`
- `%server_cert_checkstum%`
- `%syslocation%`
- `%syslog_server%`

The variable settings correspond to device-specific values on the **Devices > Manage** configuration page for the specific AP that is getting configured.

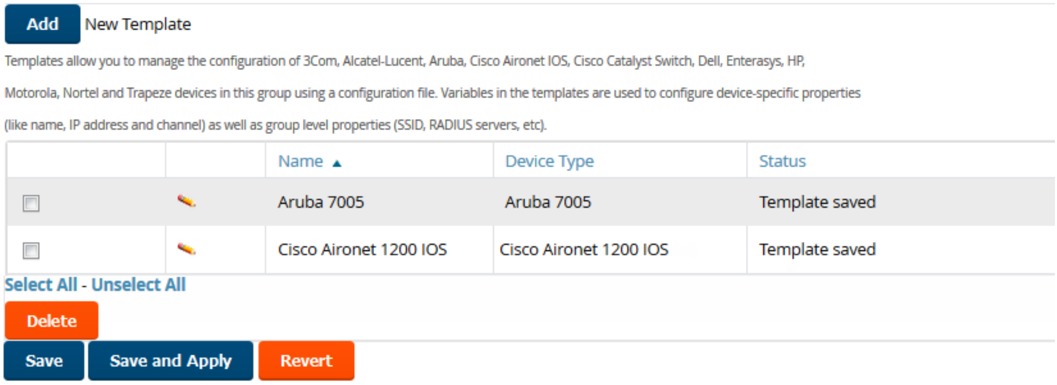
> NOTE
>
> Changes made on the other **Group** pages (Radio, Security, VLANs, SSIDs, and so forth) are not applied to any APs that are configured by templates.

Viewing and Adding Templates

Perform these steps to display, add, or edit templates.

1. Go to the **Groups > List** page, and select a group for which to add or edit templates. This can be a new group, created with the **Add** button, or you can edit an existing group by selecting the corresponding pencil icon. The **Groups > Basic** page for that group appears. Additional information about adding and editing groups is described in "Using Device Groups" on page 72.
2. From the OV3600 navigation pane, select **Templates**. The **Templates** page appears. Figure 162 illustrates the **Groups > Templates** configuration page.

Figure 162: *Groups > Templates Page Illustration for a Sample Device Group*



Templates allow you to manage the configuration of 3Com, Alcatel-Lucent, Aruba, Cisco Aironet IOS, Cisco Catalyst Switch, Dell, Enterasys, HP, Motorola, Nortel and Trapeze devices in this group using a configuration file. Variables in the templates are used to configure device-specific properties (like name, IP address and channel) as well as group level properties (SSID, RADIUS servers, etc).

		Name ▲	Device Type	Status
□	✎	Aruba 7005	Aruba 7005	Template saved
□	✎	Cisco Aironet 1200 IOS	Cisco Aironet 1200 IOS	Template saved

Table 104 describes the columns in this image.

Table 104: *Groups > Templates Fields and Default Values*

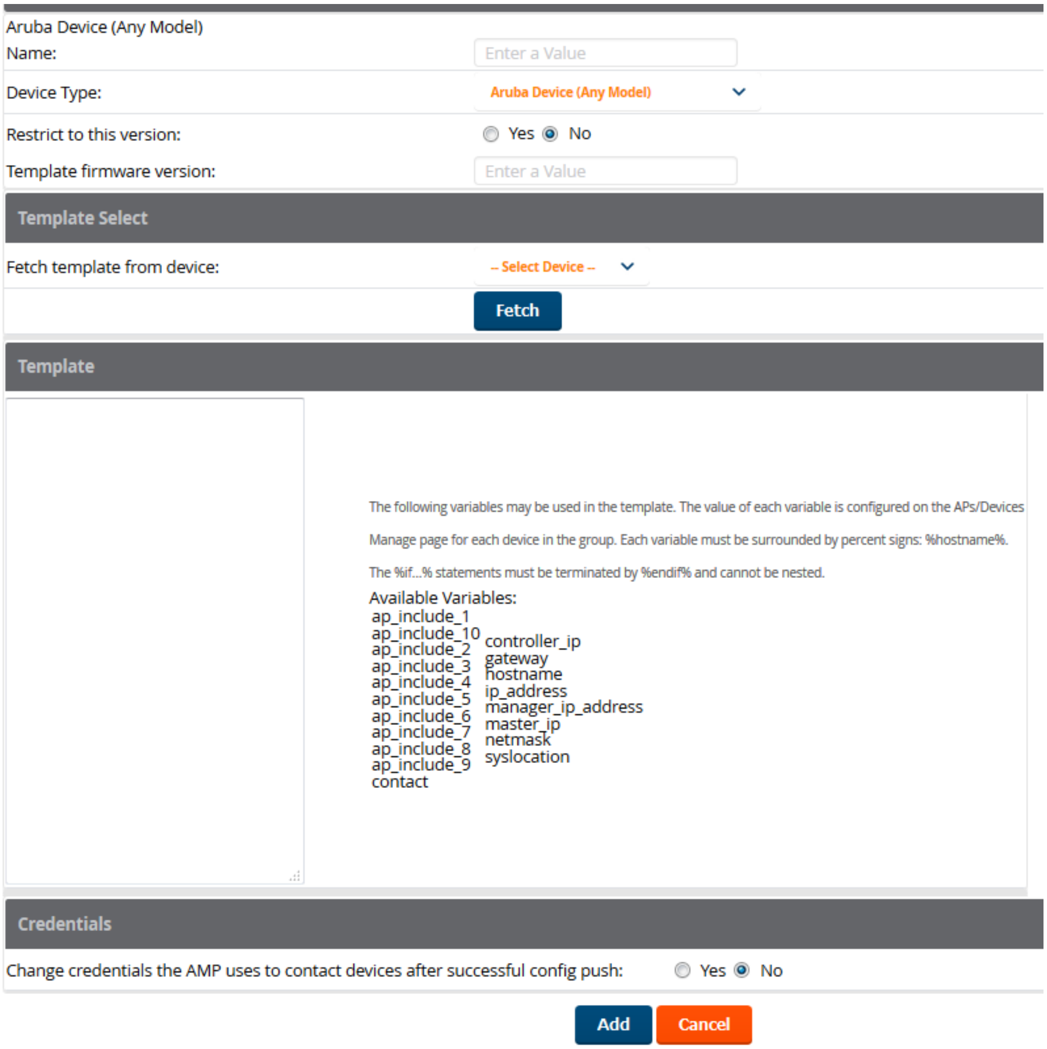
Setting	Description
Notes	When applicable, this section lists devices that are active on the network with no template available for the respective firmware. Select the link from this note to launch the **Add Template** configuration page for that device.
Name	Displays the template name.

Table 104: *Groups > Templates Fields and Default Values (Continued)*

Setting	Description
Device Type	Displays the template that applies to APs or devices of the specified type. If **(Any Model)** is selected for a vendor, then the template applies to all models from that vendor that do not have a version-specific template defined. If there are two templates that might apply to a device, the template with the most restrictions takes precedence.
Status	Displays the status of the template.
Fetch Date	Sets the date that the template was originally fetched from a device.
Version Restriction	Designates that the template only applies to APs running the version of firmware specified. If the restriction is **None**, then the template applies to all the devices of the specified type in the group. If there are two templates that might apply to a device the template with the most restrictions takes precedence. If there is a template that matches a devices firmware it will be used instead of a template that does not have a version restriction.

3. To create a new template and add it to the OV3600 template inventory, go to the **Groups > List** page, and select the group name. The **Details** page appears.
4. Select **Templates**, and then **Add**.
5. Complete the configurations illustrated in Figure 163.

Figure 163: *Groups > Templates > Add Template Page Illustration*



Aruba Device (Any Model)

Name: Enter a Value

Device Type: Aruba Device (Any Model)

Restrict to this version: ○ Yes ● No

Template firmware version: Enter a Value

Template Select

Fetch template from device: -- Select Device --

Template

The following variables may be used in the template. The value of each variable is configured on the APs/Devices Manage page for each device in the group. Each variable must be surrounded by percent signs: %hostname%.

The %if...% statements must be terminated by %endif% and cannot be nested.

Available Variables:

ap_include_1	
ap_include_10	controller_ip
ap_include_2	gateway
ap_include_3	hostname
ap_include_4	ip_address
ap_include_5	manager_ip_address
ap_include_6	master_ip
ap_include_7	netmask
ap_include_8	syslocation
ap_include_9	
contact	

Credentials

Change credentials the AMP uses to contact devices after successful config push: ○ Yes ● No

The settings for the **Add a Template** page are described in Table 105. Note that the fields can vary based on the Group.

Table 105: *Groups > Templates > Add Template Fields and Default Values*

Setting	Default	Description
Use Global Template	No	Uses a global template that has been previously configured on the **Groups > Templates** configuration page. Available templates will appear in the drop-down menu. If **Yes** is selected you can also configure global template variables. For Symbol devices you can select the groups of thin APs to which the template should be applied. For more information about global templates, see "Configuring a Global Template" on page 240.
Name	None	Defines the template display name.

Table 105: *Groups > Templates > Add Template Fields and Default Values (Continued)*

Setting	Default	Description
AP Type	Cisco IOS (Any Model)	Determines that the template applies to APs or devices of the specified type. If **Cisco IOS (Any Model)** is selected, the template applies to all IOS APs that do not have a version specific template specified.
Reboot APs After Configuration Changes	No	Determines reboot when OV3600 applies the template, copied from the new configuration file to the startup configuration file on the AP. If **No** is selected, OV3600 uses the AP to merge the startup and running configurations. If **Yes** is selected, the configuration is copied to the startup configuration file and the AP is rebooted. This field is only visible for some devices.
Restrict to this version	No	Restricts the template to APs of the specified firmware version. If **Yes** is selected, the template only applies to APs on the version of firmware specified in the **Template Firmware Version** field.
Template firmware version	None	Designates that the template only applies to APs running the version of firmware specified.
Fetch Template from Device	None	Selects an AP from which to fetch a configuration. The configuration will be turned into a template with basic AP specific settings like channel and power turned into variables. The variables are filled with the data on the **Devices > Manage** page for each AP.
Template Variables	None	Add variables to be used in the template for the group. Refer to "Configuring General Template Files and Variables" on page 229 for more information.
Group Template Variables		Add variables to be used for a Group Template.
Thin AP Groups		Configure a template for selected Thin AP groups.
AP Template		Specify template variables specifically for APs.
Change credentials the OV3600 uses to contact devices after successful config push:	No	Specify whether to change the credentials that OV3600 uses to contact devices after the configuration has been pushed. If this option is enabled, then new credential information fields display.
Community String	None	If the template is updating the community strings on the AP, enter the new community string OV3600 should use here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
Telnet/SSH Username	None	If the template is updating the Telnet/SSH user name on the AP, enter the new user name OV3600 should use here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.

Table 105: *Groups > Templates > Add Template Fields and Default Values (Continued)*

Setting	Default	Description
Telnet/SSH Password	None	If the template is updating the Telnet/SSH password on the AP, enter the new Telnet/SSH password OV3600 should use here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
enable Password	None	If the template is updating the enable password on the AP, enter the new enable password OV3600 should use here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Username	None	If the template is updating the SNMPv3 user name on the AP, enter the new SNMP user name here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
Auth Password	None	If the template is updating the SNMPv3 auth password on the AP, enter the new SNMP user name password here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Auth Protocol	MD5	Specifies the SNMPv3 auth protocol, either **MD5** or **SHA-1**.
Privacy Password	None	If the template is updating the Privacy Password on the AP, enter the new password here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Privacy Protocol	DES	Specifies the SNMPv3 Privacy protocol as either **DES** or **AES**. This option is not available for all devices.

Configuring General Template Files and Variables

This section describes the most general aspects of configuring AP device templates and the most common variables:

- "Configuring General Templates" on page 229
- "Using Template Syntax" on page 231, including the following sections:
  - "Using AP-Specific Variables" on page 231
  - "Using Directives to Eliminate Reporting of Configuration Mismatches" on page 231
  - "Using Conditional Variables in Templates" on page 232
  - "Using Substitution Variables in Templates" on page 233

Configuring General Templates

To prevent configuration changes from being applied to APs until you are sure you have the correct configuration, work with a small group of access points that are in Monitor Only mode until you are familiar with the template configuration process.

To configure templates within a group:

1. Select a group to configure, then select an AP from the group to serve as a *model* AP for the others in the group. Your selection should be configured with all the desired settings. If any APs in the group have two radios, select a model AP that has two radios and that both are configured properly.
2. Go to **Groups > Templates**, then select **Add** to add a new template.
3. Select the type of device that will be configured by this template.
4. Select the model AP from the drop-down list, and select **Fetch**.
5. OV3600 automatically attempts to replace some values from the configuration of that AP with *variables* to enable AP-specific options to be set on an AP-by-AP basis. Refer to "Using Template Syntax" on page 231.

   These variables are always encapsulated between % signs. On the right side of the configuration page is the **Additional Variables** section. This section lists all available variables for your template. Variables that are in use in a template are green, while variables that are not yet in use are black. Verify these substitutions to ensure that all of the settings that you believe should be managed on an AP-by-AP basis are labeled as variables in this fashion. If you believe that any AP-level settings are not marked correctly, please contact Alcatel-Lucent customer support before proceeding.
6. Specify the device types for the template. The templates only apply to devices of the specified type.
   - Specify whether OV3600 should reboot the devices after a configuration push. If the **Reboot Devices after Configuration Changes** option is selected, then OV3600 instructs the AP to copy the configuration from OV3600 to the startup configuration file of the AP and reboot the AP.
   - If the **Reboot Devices after Configuration Changes** option is not selected, then OV3600 instructs the AP to copy the configuration to the startup configuration file and then tell the AP to copy the startup configuration file to the running configuration file.
   - Use the **reboot** option when there are changes requiring reboot to take effect, for example, removing a new SSID from a Cisco IOS device. Copying the configuration from startup configuration file to running configuration file merges the two configurations and can cause undesired configuration lines to remain active on the AP.
7. Restrict the template to apply only to the specified version of firmware. If the template should only apply to a specific version of firmware, select **Yes** and enter the firmware version in the **Template Firmware Version** text field.
8. Select **Save and Apply** to push the configuration to all of the devices in the group. If the devices are in Monitor-only mode (which is recommended while you are crafting changes to a template or creating a new one), then OV3600 will audit the devices and compare their current configuration to the one defined in the template.

NOTE

If you set the reboot flag to **No**, then some changes could result in configuration mismatches until the AP is rebooted.

For example, changing the SSID on Cisco IOS APs requires the AP to be rebooted. Two other settings that require the AP to be rebooted for configuration change are Logging and NTP. A configuration mismatch results if the AP is not rebooted.

If logging and NTP service are not required according to the Group configuration, but are enabled on the AP, you would see a configuration file mismatch as follows if the AP is not rebooted:

IOS Configuration File Template

```
…
(no logging queue-limit)
…
```

Device Configuration File on Devices > Device Configuration Page

```
…
```

```
    line con 0
    line vty 5 15
actual logging 10.51.2.1
actual logging 10.51.2.5
actual logging facility local6
actual logging queue-limit 100
actual logging trap debugging
    no service pad
actual ntp clock-period 2861929
actual ntp server 209.172.117.194
    radius-server attribute 32 include-in-access-req format %h
…
```

9. Once the template is correct and all mismatches are verified on the **Devices > Device Configuration** page, navigate to **Groups > Monitor** and click ✎ at the right corner of the device list to select the devices to change the management mode to Manage Read/Write. The AP pulls the new startup configuration file from OV3600. For more information, see "Setting the Management Mode" on page 127.

> NOTE
>
> You can set the management mode for individual devices from the **Devices > Manage** configuration page. For more information, see "Moving a Device from Monitor Only to Manage Read/Write Mode" on page 208.

Using Template Syntax

Template syntax is comprised of the following components, described in this section:

- "Using AP-Specific Variables" on page 231
- "Using Directives to Eliminate Reporting of Configuration Mismatches" on page 231
- "Using Conditional Variables in Templates" on page 232
- "Using Substitution Variables in Templates" on page 233

Using AP-Specific Variables

When a template is applied to an AP, all variables are replaced with the corresponding settings from the **Devices > Manage** configuration page. This enables AP-specific settings (such as Channel) to be managed effectively on an AP-by-AP basis. The list of used and available variables appears on the template detail configuration page. Variables are always encapsulated between % signs. The following example illustrates this usage:

```
hostname %hostname%
…
interface Dot11Radio0
…
  power local cck %CCK_POWER%
  power local ofdm %OFDM_POWER%
  channel %CHANNEL%
…
```

The `hostname` line sets the AP hostname to the hostname stored in OV3600.

The `power` lines set the power local `cck` and `ofdm` values to the numerical values that are stored in OV3600.

Using Directives to Eliminate Reporting of Configuration Mismatches

OV3600 is designed to audit AP configurations to ensure that the actual configuration of the access point exactly matches the Group template. When a configuration mismatch is detected, OV3600 generates an automatic alert and flags the AP as having a **Mismatched** configuration status on the user page.

However, when using the templates configuration function, there will be times when the running-config file and the startup-config file do not match under normal circumstances. For example, the `ntp clock-period` setting is almost never identical in the running-config file and the startup-config file. You can use directives such as

<ignore_and_do_not_push> to customize the template to keep OV3600 from reporting mismatches for this type of variance.

OV3600 provides two types of directives that can be used within a template to control how OV3600 constructs the startup-config file to send to each AP and whether it reports variances between the running-config file and the startup-config file as "configuration mismatches.” Lines enclosed in <push_and_exclude> are included in the AP startup-config file but OV3600 ignores them when verifying configurations. Lines enclosed in <ignore_and_do_not_push> cause OV3600 to ignore those lines during configuration verification.

Ignore_and_do_not_push Command

The ignore and do not push directive should typically be used when a value cannot be configured on the device, but always appears in the running-config file. Lines enclosed in the ignore and do not push directive will not be included in the startup-config file that is copied to each AP.

When OV3600 is comparing the running-config file to the startup-config file for configuration verification, it will ignore any lines in the running-config file that start with the text within the directive. Lines belonging to an ignored and unpushed line, the lines immediately below the line and indented, are ignored as well. In the example below, if you were to bracket the NTP server, the NTP clock period would behave as if it were bracketed because it belongs with or is associated with the NTP server line.

The line <ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push> will cause lines starting with "ntp clock-period" to be ignored. However, the line <ignore_and_do_not_push>ntp </ignore_and_do_not_push> causes all lines starting with "ntp" to be ignored, so it is important to be as specific as possible.

Push_and_exclude Command

Instead of using the full tags you may use the parenthesis shorthand, (substring). The push and exclude directive is used to push commands to the AP that will not appear in the running-config file. For example, some **no** commands that are used to remove SSIDs or remove configuration parameters do not appear in the running-config file of a device. A command inside the push and exclude directive are included in the startup-config file pushed to a device, but OV3600 excludes them when calculating and reporting configuration mismatches.

The opening tag may have leading spaces.

Below are some examples of using directives:

```
…
line con 0
 </push_and_exclude>no stopbits</push_and_exclude>
line vty 5 15
!
ntp server 209.172.117.194
<ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push>
end
```

Using Conditional Variables in Templates

Conditional variables allow lines in the template to be applied only to access points where the enclosed commands will be applicable and not to any other access points within the Group. For example, if a group of APs consists of dual-radio Cisco 1200 devices (802.11a/b) and single-radio Cisco 1100 (802.11b) devices, it is necessary to make commands related to the 802.11a device in the 1200 APs conditional. Conditional variables are listed in the table below.

The syntax for conditional variables is as follows, and syntax components are described in Table 106:

```
%if variable=value%
…
%endif%
```

Table 106: *Conditional Variable Syntax Components*

Variable	Values	Meaning
interface	Dot11Radio0	2.4GHz radio module is installed
	Dot11Radio1	5GHz external radio module is installed
radio_type	a	Installed 5GHz radio module is 802.11a
	b	Installed 2.4GHz radio module is 802.11b only
	g	Installed 2.4GHz radio module is 802.11g capable
wds_role	backup	The WDS role of the AP is the value selected in the drop down menu on the **Devices > Manage** configuration page for the device.
	client	
	master	
IP	Static	IP address of the device is set statically on the AP Manage configuration page.
	DHCP	IP address of the device is set dynamically using DHCP

Using Substitution Variables in Templates

Substitution variables are used to set AP-specific values on each AP in the group. It is obviously not desirable to set the IP address, hostname, and channel to the same values on every AP within a Group. The variables in Table 107 are substituted with values specified on each access point's **Devices > Manage** configuration page within the OV3600 User page.

Sometimes, the running-config file on the AP does not include the command for one of these variables because the value is set to the default. For example, when the **transmission power** is set to maximum (the default), the line **power local maximum** will not appear in the AP running-config file, although it will appear in the startup-config file. OV3600 would typically detect and flag this variance between the running-config file and startup-config file as a configuration mismatch. To prevent OV3600 from reporting a configuration mismatch between the desired startup-config file and the running-config file on the AP, OV3600 suppresses the lines in the desired configuration when auditing the AP configuration (similar to the way OV3600 suppresses lines enclosed in parentheses, which is explained below). A list of the default values that causes lines to be suppressed when reporting configuration mismatches is shown in Table 107.

Table 107: *Substitution Variables in Templates*

Variable	Meaning	Command	Suppressed Default
hostname	Name	hostname %hostname%	-
channel	Channel	channel %channel%	-

Table 107: *Substitution Variables in Templates (Continued)*

Variable	Meaning	Command	Suppressed Default
ip_address netmask	IP address Subnet mask	ip address %ip_address% %netmask% or ip address dhcp ...	-
gateway	Gateway	ip default-gateway %gateway%	-
antenna_ receive	Receive antenna	antenna receive %antenna_ receive%	diversity
antenna_transmit	Transmit antenna	antenna transmit %antenna_ transmit%	diversity
cck_power	802.11g radio module CCK power level	power local cck %cck_power%	maximum
ofdm_power	802.11g radio module OFDM power level	power local ofdm %ofdm_ power%	maximum
power	802.11a and 802.11b radio module power level	power local %power%	maximum
location	The location of the SNMP server.	snmp-server location %location%	-
contact	The SNMP server contact.	snmp-server contact %contact%	-
certificate	The SSL Certificate used by the AP	%certificate%	-
ap include	The AP include fields allow for configurable variables. Any lines placed in the AP Include field on the **Devices > Manage** configuration page replace this variable.	%ap_include_1% through %ap_include_10%	-
chassis id	serial number of the device	%chassis_id%	-
domain	dns-domain of the device	%domain%	-
interfaces	Interfaces of the device	%interfaces%	-

Configuring Templates for Alcatel-Lucent Instant

The first Instant network that is added to OV3600 automatically includes the default configuration that is used as a template to provision other Instant networks. Refer to the documentation that accompanies Alcatel-Lucent Instant for more information.

NOTE

Be sure that the default configuration is validated and has been pre-tested in a non-production environment prior to applying it to a production network. Any changes that are made to this configuration will follow the same process each time and will be applied to other Instant networks as described in this document.

OV3600 enables you to control Instant configuration settings via the **Groups > Templates** configuration page. A sample configuration is provided below.

```
virtual-controller-country US
virtual-controller-key %guid%
virtual-controller-ip %ip_address_a_b_c%.3
name %hostname%
%if organization%
organization %organization%
%endif%
syslog-server 216.31.249.235
syslog-level debug
terminal-access
clock timezone Pacific-Time -08 00
rf-band 5.0
ams-ip %manager_ip_address%
ams-key %password%
allow-new-aps
%allowed_aps%
snmp-server engine-id undefined
arm
 wide-bands 5ghz
 min-tx-power 18
 max-tx-power 127
 band-steering-mode prefer-5ghz
 air-time-fairness-mode fair-access
syslog-level warn ap-debug
syslog-level warn network
syslog-level warn security
syslog-level warn system
syslog-level warn user
syslog-level warn user-debug
syslog-level warn wireless
mgmt-user admin 446f8a8ddacdb735dd42a9873a2e80e2
wlan ssid-profile remote-node-guest
 index 0
 type employee
 essid %ssid%
 wpa-passphrase a804e1744c137371943bdeed410e720a58eca75717ff714b
 opmode wpa2-psk-aes
 rf-band all
 captive-portal disable
 dtim-period 1
 inactivity-timeout 1000
 broadcast-filter none
enet-vlan guest
wlan external-captive-portal
 server localhost
 port 80
 url "/"
 auth-text "%venue%"
ids classification
ids
 wireless-containment none
```

Configuring Templates for AirMesh

AirMesh devices can be configured using templates in OV3600. OV3600 automatically adds a template for the first AirMesh AP in a group. The configurations are pushed using CLI commands. The sample code below includes Mesh configuration options.

```
mesh
 mesh-id %mesh_id%
 %preferred_link%
 neighbor-list-type %neighbor_list_type%
  authentication open key-management wpa2
    psk ascii 5d4f50485e4f5048ed1da60b85f2784d6bbf16442fdcbfc06aeb4460d98263f5
 neighbor-list
  %neighbor_list%
service avt
  %avt_ingress_interface%
  %avt_ingress_ip%
  buffer_time 200
  mode %avt_mode%
```

NOTE

OV3600 displays a warning if AirMesh APs attempting to either upgrade or push configurations lack the necessary write permissions.

Configuring Cisco IOS Templates

Cisco IOS access points have hundreds of configurable settings. OV3600 enables you to control them via the **Groups > Templates** configuration page. This page defines the startup-config file of the devices rather than using the OV3600 normal **Group** configuration pages. OV3600 no longer supports making changes for these devices via the browser-based page, but rather uses templates to configure all settings, including settings that were controlled formerly on the OV3600 Group configuration pages. Perform these steps to configure a Cisco IOS Template for use with one or more groups, and the associated devices.

This section includes the following topics:

- "Applying Startup-config Files" on page 236
- "WDS Settings in Templates" on page 237
- "SCP Required Settings in Templates" on page 237
- "Supporting Multiple Radio Types via a Single IOS Template" on page 237
- "Configuring Single and Dual-Radio APs via a Single IOS Template" on page 238

Applying Startup-config Files

Each of the APs in the Group copies its unique startup-config file from OV3600 via TFTP or SCP.

- If the **Reboot Devices after Configuration Changes** option is selected, then OV3600 instructs the AP to copy the configuration from OV3600 to the startup-config file of the AP and reboot the AP.
- If the **Reboot Devices after Configuration Changes** option is not selected, then OV3600 instructs the AP to copy the configuration to the startup-config file and then tell the AP to copy the startup config file to the running-config file. Use the reboot option when possible. Copying the configuration from startup to running merges the two configurations and can cause undesired configuration lines to remain active on the AP.

NOTE

Changes made on the standard OV3600 Group configuration pages, to include Basic, Radio, Security, VLANs, and so forth, are not applied to any template-based APs.

WDS Settings in Templates

A group template supports Cisco WDS settings. APs functioning in a WDS environment communicate with the Cisco WLSE via a WDS master. IOS APs can function in Master or Slave mode. Slave APs report their rogue findings to the WDS Master (AP or WLSM which reports the data back to the WLSE. On the **Devices > Manage** configuration page, select the proper role for the AP in the WDS Role drop down menu.

The following example sets an AP as a WDS Slave with the following lines:

```
%if wds_role=client%
wlccp ap user name wlse password 7 XXXXXXXXXX
%endif%
```

The following example sets an AP as a WDS Master with the following lines:

```
%if wds_role=master%
aaa authentication login method_wds group wds
aaa group server radius wds server
10.2.25.162 auth-port 1645 acct-port 1646
wlccp authentication-server infrastructure method_wds
wlccp wds priority 200 interface BVI1
wlccp ap user name wlse password 7 095B421A1C
%endif%
```

The following example sets an AP as a WDS Master Backup with the following lines:

```
%if wds_role=backup%
aaa authentication login method_wds group wds
aaa group server radius wds server
10.2.25.162 auth-port 1645 acct-port 1646
wlccp authentication-server infrastructure method_wds
wlccp wds priority 250 interface BVI1
wlccp ap user name wlse password 7 095B421A1C
%endif%
```

SCP Required Settings in Templates

A few things must be set up before enabling SCP on the **Groups > Basic** configuration page. The credentials used by OV3600 to login to the AP must have level 15 privileges. Without them, OV3600 is not able to communicate with the AP via SCP. The line "`aaa authorization exec default local`" must be in the APs configuration file and the AP must have the SCP server enabled. These three settings correspond to the following lines in the AP's configuration file:

```
user name Cisco privilege 15 password 7 0802455D0A16
aaa authorization exec default local
ip scp server enable
```

The `user name` line is a guideline and will vary based on the user name being set, in this case Cisco, and the password and encoding type, in this case 0802455D0A16 and 7 respectively.

These values can be set on a group wide level using Templates and TFTP. Once these lines are set, SCP can be enabled on the **Groups > Basic** configuration page without problems.

Supporting Multiple Radio Types via a Single IOS Template

Some lines in an IOS configuration file should only apply to 802.11g vs. 802.11b. For instance, lines related to speed rates that mention rates above 11.0Mb/s do not work for 802.11b radios that cannot support these speeds. Use the "`%IF` *`variable=value`*`%` … `%ENDIF%`" construct to allow a single IOS configuration template to configure APs with different radio types within the same Group as illustrated below:

```
interface Dot11Radio0
…
%IF radio_type=g%
```

```
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
%ENDIF%
%IF radio_type=b%
speed basic-1.0 2.0 5.5 11.0
%ENDIF%
%IF radio_type=g%
power local cck %CCK_POWER%
power local ofdm %OFDM_POWER%
%ENDIF%
…
```

Configuring Single and Dual-Radio APs via a Single IOS Template

To configure single and dual-radio APs using the same IOS config template, you can use the interface variable within the %IF...% construct. The below example illustrates this usage:

```
%IF interface=Dot11Radio1%
interface Dot11Radio1
 bridge-group 1
 bridge-group 1 block-unknown-source
 bridge-group 1 spanning-disabled
 bridge-group 1 subscriber-loop-control
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 no ip address
 no ip route-cache
 rts threshold 2312
 speed basic-6.0 basic-9.0 basic-12.0 basic-18.0 basic-24.0 36.0 48.0 54.0
 ssid decibel-ios-a
   authentication open
   guest-mode
   station-role root
      %ENDIF%
```

Configuring Cisco Catalyst Switch Templates

Cisco Catalyst Switch templates are configured much like Cisco IOS templates with the addition of the `interfaces` and `switch_command` (for stacked switches) variables. Interfaces can be configured on the Device Interface pages, as shown in "Configuring Device Interfaces for Switches" on page 218. You can import interface information as described in this section or by fetching a template from that device, as described in "Configuring General Templates" on page 229.

Just one template is used for any type of Cisco IOS device, and another is used for any type of Catalyst Switch regardless of individual model.

Configuring Symbol Controller / HPE WESM Templates

This section describes the configuration of templates for Symbol controllers and HPE WESM devices.

Symbol switches (RFS x000, 5100 and 2000) can be configured in OV3600 using templates. OV3600 supports Symbol thin AP firmware upgrades from the controller's manage page.

A sample running-configuration file template is provided in this topic for reference. A template can be fetched from a model device using the Cisco IOS device procedure described in "Configuring Cisco IOS Templates" on page 236. Cisco IOS template directives such as **ignore_and_do_not_push** can also be applied to Symbol templates.

Certain parameters such as `hostname` and `location` are turned into variables with the `%` tags so that device-specific values can be read from the individual manage pages and inserted into the template. They are listed in Available Variable boxes on the right-hand side of the template fields.

Certain settings have integrated variables, including **alp-license** and **adoption-preference-id**. The radio preamble has been template-integrated as well. An option on the **Group > Templates** page reboots the device after pushing a configuration to it.

A sample Symbol controller partial template is included below for reference.

```
!
! configuration of RFS4000 version 4.2.1.0-005R
!
version 1.4
!
!
aaa authentication login default local none
service prompt crash-info
!
network-element-id RFS4000
!
user name admin password 1 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
user name admin privilege  superuser
user name operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
access-list 100 permit ip 192.168.0.0/24 any rule-precedence 10
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst configuration
 name My Name
!
ip dns-server-forward
wwan auth-type chap
no bridge multiple-spanning-tree enable bridge-forward
country-code us
aap-ipfilter-list no port 3333 plz
aap-ipfilter-list no port 3333 tcp plz
 deny tcp src-start-ip 0.0.0.0 src-end-ip 255.255.255.255 dst-start-ip 0.0.0.0 dst-end-ip
255.255.255.255 dst-start-port 3333 dst-end-port 3334 rule 1
%redundancy_config%
logging buffered 4
logging console 4
snmp-server engineid netsnmp 6b8b45674b30f176
snmp-server location %location%
snmp-server contact %contact%
snmp-server sysname %hostname%
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5 0x1aa491f4ca7c55df0f57801bece9044c
snmp-server user snmpmanager v3 encrypted auth md5 0x1aa491f4ca7c55df0f57801bece9044c
snmp-server user snmpoperator v3 encrypted auth md5 0xb03b1ebfa0e3d02f50e2b1c092ab7c9f
```

A sample Symbol Smart RF template is provided below for reference:

```
radio %radio_index% radio-mac %radio_mac%
%if radio_type=11a%
  radio %radio_index% coverage-rate  18
%endif%
%if radio_type=11an%
  radio %radio_index% coverage-rate  18
%endif%
```

```
%if radio_type=11b%
  radio %radio_index% coverage-rate  5p5
%endif%
%if radio_type=11bg%
  radio %radio_index% coverage-rate  6
%endif%
%if radio_type=11bgn%
  radio %radio_index% coverage-rate  18
%endif%
```

A sample Symbol thin AP template is provided below for reference and for the formatting of `if` statements.

```
radio add %radio_index% %lan_mac% %radio_type% %ap_type%
 radio %radio_index% radio-number %radio_number%
 radio %radio_index% description %description%
 %if radio_type=11a%
 radio %radio_index% speed  basic6 9 basic12 18 basic24 36 48 54
 radio %radio_index% antenna-mode primary
 radio %radio_index% self-heal-offset 1
 radio %radio_index% beacon-interval 99
 radio %radio_index% rts-threshold 2345
 radio %radio_index% max-mobile-units 25
 radio %radio_index% admission-control voice max-perc 76
 radio %radio_index% admission-control voice res-roam-perc 11
 radio %radio_index% admission-control voice max-mus 101
 radio %radio_index% admission-control voice max-roamed-mus 11
 %endif%
 %if radio_type=11an%
 radio %radio_index% speed  basic11a 9 18 36 48 54 mcs 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
 %endif%
 %if radio_type=11b%
 radio %radio_index% speed  basic1 basic2 basic5p5 basic11
 %endif%
 %if radio_type=11bg%
 radio %radio_index% speed  basic1 basic2 basic5p5 6 9 basic11 12 18 24 36 48 54
 radio %radio_index% on-channel-scan
 radio %radio_index% adoption-pref-id 7
 radio %radio_index% enhanced-beacon-table
 radio %radio_index% enhanced-probe-table
 %endif%
 %if radio_type=11bgn%
 radio %radio_index% speed  basic11b2 6 9 12 18 24 36 48 54 mcs
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
 %endif%
 radio %radio_index% channel-power indoor %channel% %transmit_power% %channel_attribute%
 %detector%
%adoption_pref_id%
 radio %radio_index% enhanced-beacon-table
 radio %radio_index% on-channel-scan
%ap_include_4%
```

Configuring a Global Template

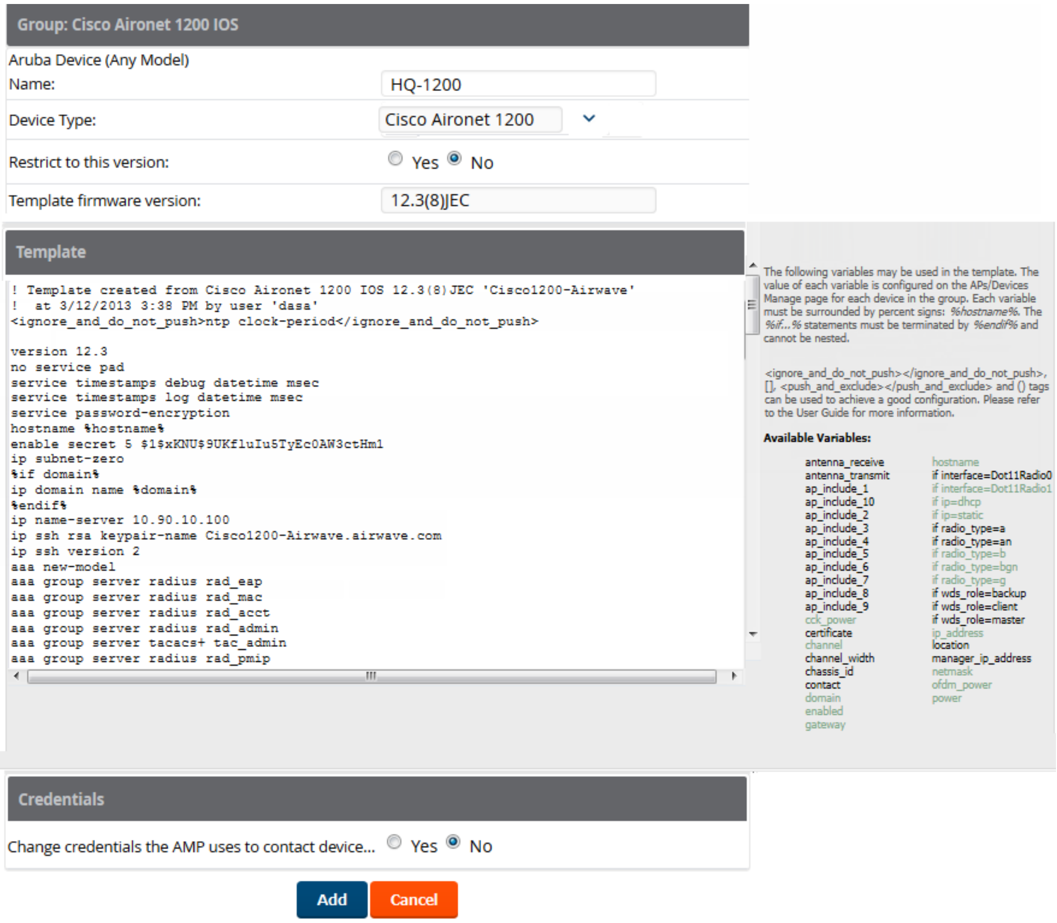
Global templates allow OV3600 users to define a single template in a global group that can be used to manage APs in subscriber groups. They turn settings like group RADIUS servers and encryption keys into variables that can be configured on a per-group basis.

Perform the following steps to create a global template, or to view or edit an existing global template:

1. Go to the **Group > Templates** configuration page for the global group that owns it.
2. Select **Add** to add a new template, or select the **pencil** icon next to an existing template to edit it.

3. Examine the configurations illustrated in Figure 164.

Figure 164: *Group > Templates > Add Page Illustration*



Group: Cisco Aironet 1200 IOS

Aruba Device (Any Model)

Name: HQ-1200

Device Type: Cisco Aironet 1200

Restrict to this version: ○ Yes ● No

Template firmware version: 12.3(8)JEC

Template

```
! Template created from Cisco Aironet 1200 IOS 12.3(8)JEC 'Cisco1200-Airwave'
!  at 3/12/2013 3:38 PM by user 'dasa'
<ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push>

version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname %hostname%
enable secret 5 $1$xKNU$9UKfluIu5TyEc0AW3ctHm1
ip subnet-zero
%if domain%
ip domain name %domain%
%endif%
ip name-server 10.90.10.100
ip ssh rsa keypair-name Cisco1200-Airwave.airwave.com
ip ssh version 2
aaa new-model
aaa group server radius rad_eap
aaa group server radius rad_mac
aaa group server radius rad_acct
aaa group server radius rad_admin
aaa group server tacacs+ tac_admin
aaa group server radius rad_pmip
```

The following variables may be used in the template. The value of each variable is configured on the APs/Devices Manage page for each device in the group. Each variable must be surrounded by percent signs: *%hostname%*. The *%if...%* statements must be terminated by *%endif%* and cannot be nested.

<ignore_and_do_not_push></ignore_and_do_not_push>, [], <push_and_exclude></push_and_exclude> and () tags can be used to achieve a good configuration. Please refer to the User Guide for more information.

Available Variables:

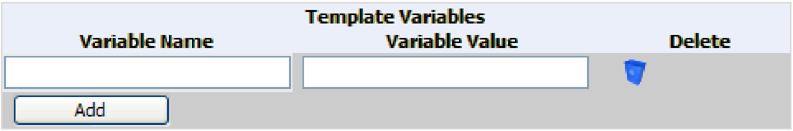
antenna_receive
antenna_transmit
ap_include_1
ap_include_10
ap_include_2
ap_include_3
ap_include_4
ap_include_5
ap_include_6
ap_include_7
ap_include_8
ap_include_9
cck_power
certificate
channel
channel_width
chassis_id
contact
domain
enabled
gateway
hostname
if interface=Dot11Radio0
if interface=Dot11Radio1
if ip=dhcp
if ip=static
if radio_type=a
if radio_type=an
if radio_type=b
if radio_type=bgn
if radio_type=g
if wds_role=backup
if wds_role=client
if wds_role=master
ip_address
location
manager_ip_address
netmask
ofdm_power
power

Credentials

Change credentials the AMP uses to contact device... ○ Yes ● No

4. Use the drop-down menu to select a device from which to build the global template and click the **Fetch** button. The menus are populated with all devices that are contained in any group that subscribes to the global group. The fetched configuration populates the template field. Global template variables can be configured with the **Add** button in the **Template Variables** box, illustrated in Figure 165.

Figure 165: *Template Variables Illustration*



The variable name cannot have any spaces or non-alphanumeric characters. The initial variable value entered is the default value, but can be changed on a per-group basis later. You can also populate global template variables by uploading a CSV file (see below).

5. Once you have configured your global template, select **Add**. You are taken to a confirmation configuration page where you can review your changes.

6. If you want to add the global template, select **Apply Changes Now**. If you do not want to add the template, select **Cancel and Discard Changes**. Canceling from the confirmation configuration page causes the template and all of the template variables to be lost.

7. Once you have added a new global template, you can use a CSV upload option to configure global template variables. Go to the **Groups > Templates** configuration page and select the **CSV** upload icon for the template. The CSV file must contain columns for **Group Name** and **Variable Name**. All fields must be completed.
   - **Group Name**—the name of the subscriber group that you wish to update.
   - **Variable Name**—the name of the group template variable you wish to update.
   - **Variable Value**—the value to set.

   For example, for a global template with a variable called "ssid_1", the CSV file might resemble what follows:

   ```
   Group Name, ssid_1
   Subscriber 1, Value 0
   ```

8. Once you have defined and saved a global template, it is available for use by any local group that subscribes to the global group. Go to the **Groups > Template** configuration page for the local group and select the pencil icon next to the global template in the list.
9. To make template changes, go to the **Groups > Template** configuration page for the global group and select the **pencil** icon next to the template you wish to edit. Note that you cannot edit the template itself from the subscriber group's **Groups > Templates** tab.
10. If group template variables have been defined, you are able to edit the value for the group on the **Groups > Templates > Add** configuration page in the **Group Template Variables** box. For Symbol devices, you are also able to define the template per group of APs.

Chapter 7 Using RAPIDS

This chapter provides an overview to rogue device and IDS event detection, alerting, and analysis using RAPIDS, and contains the following sections:

Introduction to RAPIDS

Rogue device detection is a core component of wireless security. With RAPIDS rules engine and containment options, you can create a detailed definition of what constitutes a rogue device, and quickly act on a rogue AP for investigation, restrictive action, or both. Once rogue devices are discovered, RAPIDS alerts your security team of the possible threat and provides essential information needed to locate and manage the threat.

RAPIDS discovers unauthorized devices in your WLAN network in the following ways:

- Over the Air using your existing enterprise APs.
- On the Wire
  - Polling routers and switches to identify, classify, and locate unknown APs
  - Using the switch’s wired discovery information
  - Using HTTP and SNMP scanning

NOTE

To set up a scan, refer to "How to Set Up Device Discovery" on page 120.

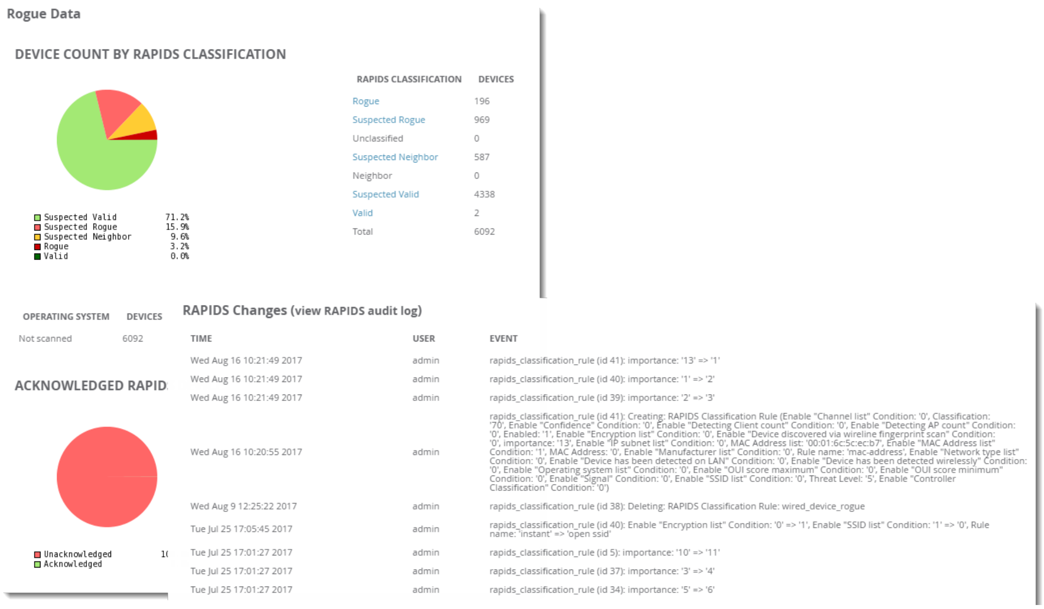
Furthermore, RAPIDS integrates with external intrusion detection systems (IDS), as follows:

- **Alcatel-Lucent WIP**—Wireless Intrusion Protection (WIP) module integrates wireless intrusion protection into the mobile edge infrastructure. The WIP module provides wired and wireless AP detection, classification and containment; detects DoS and impersonation attacks; and prevents client and network intrusions.
- **Cisco WLSE** (1100 and 1200 IOS)—OV3600 fetches rogue information from the HTTP interface and gets new AP information from SOAP API. This system provides wireless discovery information rather than rogue detection information.
- **AirMagnet Enterprise**—Retrieves a list of managed APs from OV3600.
- **AirDefense**—Uses the OV3600 XML API to keep its list of managed devices up to date.
- **WildPackets OmniPeek**—Retrieves a list of managed APs from OV3600.

Viewing RAPIDS Summary

The **RAPIDS > Overview** page displays pie charts and device counts by RAPIDS classifications (see Figure 166). Clicking the hyperlinks opens the RAPIDS list for the selected classification.

Figure 166: *RAPIDS > Overview Page*



Rogue Data

DEVICE COUNT BY RAPIDS CLASSIFICATION

RAPIDS CLASSIFICATION	DEVICES
Rogue	196
Suspected Rogue	969
Unclassified	0
Suspected Neighbor	587
Neighbor	0
Suspected Valid	4338
Valid	2
Total	6092

OPERATING SYSTEM	DEVICES
Not scanned	6092

ACKNOWLEDGED RAPID

RAPIDS Changes (view RAPIDS audit log)

TIME	USER	EVENT
Wed Aug 16 10:21:49 2017	admin	rapids_classification_rule (id 41): importance: '13' => '1'
Wed Aug 16 10:21:49 2017	admin	rapids_classification_rule (id 40): importance: '1' => '2'
Wed Aug 16 10:21:49 2017	admin	rapids_classification_rule (id 39): importance: '2' => '3'
Wed Aug 16 10:20:55 2017	admin	rapids_classification_rule (id 41): Creating: RAPIDS Classification Rule (Enable "Channel list" Condition: '0', Classification: '70', Enable "Confidence" Condition: '0', Enable "Detecting Client count" Condition: '0', Enable "Detecting AP count" Condition: '0', Enabled: '1', Enable "Encryption list" Condition: '0', Enable "Device discovered via wireline fingerprint scan" Condition: '0', importance: '13', Enable "IP subnet list" Condition: '0', MAC Address list: '00:01:6c:5c:ec:b7', Enable "MAC Address list" Condition: '1', MAC Address: '0', Enable "Manufacturer list" Condition: '0', Rule name: 'mac-address', Enable "Network type list" Condition: '0', Enable "Device has been detected on LAN" Condition: '0', Enable "Device has been detected wirelessly" Condition: '0', Enable "Operating system list" Condition: '0', Enable "OUI score maximum" Condition: '0', Enable "OUI score minimum" Condition: '0', Enable "Signal" Condition: '0', Enable "SSID list" Condition: '0', Threat Level: '5', Enable "Controller Classification" Condition: '0')
Wed Aug 9 12:25:22 2017	admin	rapids_classification_rule (id 38): Deleting: RAPIDS Classification Rule: wired_device_rogue
Tue Jul 25 17:05:45 2017	admin	rapids_classification_rule (id 40): Enable "Encryption list" Condition: '0' => '1', Enable "SSID list" Condition: '1' => '0', Rule name: 'instant' => 'open ssid'
Tue Jul 25 17:01:27 2017	admin	rapids_classification_rule (id 5): importance: '10' => '11'
Tue Jul 25 17:01:27 2017	admin	rapids_classification_rule (id 37): importance: '3' => '4'
Tue Jul 25 17:01:27 2017	admin	rapids_classification_rule (id 34): importance: '5' => '6'

Table 108 defines the summary information that appears on the page.

Table 108: *RAPIDS > Overview Fields and Descriptions*

Summary	Description
Device Count by RAPIDS Classification	A pie chart of rogue device percentages by RAPIDS classification.
RAPIDS Classification	A summary list with details of the statistics depicted in the Device Count by RAPIDS Classification pie chart. Click the linked classification name to be taken to a filtered rogue list.
RAPIDS Devices by OS	A pie chart of RAPIDS percentages by the detected operating system.
Operating System	Detected operating systems represented in this summary listing. Click on the linked Operating System name to see the rogues list filtered by that classification. OS scans can be run manually or enabled to run automatically on the **RAPIDS > Setup** page.
Acknowledged RAPIDS Devices	A color coded pie chart comparing the number of acknowledged devices to the unacknowledged devices.
RAPIDS Changes	Tracks every change made to RAPIDS including changes to rules, manual classification, and components on the **RAPIDS > Setup** page. A link at the top of the list directs you to the **RAPIDS > Audit Log** page.

Setting Up RAPIDS

The **RAPIDS > Setup** page allows you to configure your OV3600 server for RAPIDS. Complete the settings on this page as desired, and select **Save**. Most of the settings are internal to the way that OV3600 will process rogues.

Refer to the following sections:

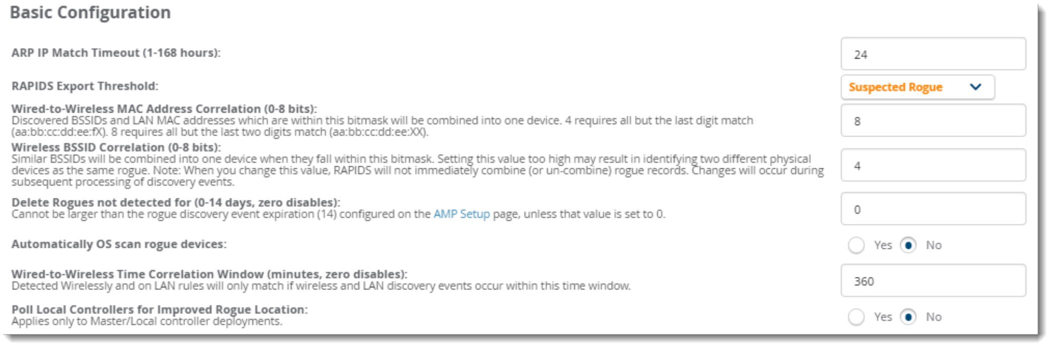
- "RAPIDS Setup" on page 245
- "Additional Settings" on page 248

RAPIDS Setup

Basic Configuration

On the **RAPIDS > Setup** page, the **Basic Configuration** section allows you to define RAPIDS behavior settings.

Figure 167: *Basic Configuration Settings*



Basic Configuration

ARP IP Match Timeout (1-168 hours): 24

RAPIDS Export Threshold: Suspected Rogue

Wired-to-Wireless MAC Address Correlation (0-8 bits):
Discovered BSSIDs and LAN MAC addresses which are within this bitmask will be combined into one device. 4 requires all but the last digit match (aa:bb:cc:dd:ee:fX). 8 requires all but the last two digits match (aa:bb:cc:dd:ee:XX).
8

Wireless BSSID Correlation (0-8 bits):
Similar BSSIDs will be combined into one device when they fall within this bitmask. Setting this value too high may result in identifying two different physical devices as the same rogue. Note: When you change this value, RAPIDS will not immediately combine (or un-combine) rogue records. Changes will occur during subsequent processing of discovery events.
4

Delete Rogues not detected for (0-14 days, zero disables):
Cannot be larger than the rogue discovery event expiration (14) configured on the AMP Setup page, unless that value is set to 0.
0

Automatically OS scan rogue devices: ○ Yes ● No

Wired-to-Wireless Time Correlation Window (minutes, zero disables):
Detected Wirelessly and on LAN rules will only match if wireless and LAN discovery events occur within this time window.
360

Poll Local Controllers for Improved Rogue Location:
Applies only to Master/Local controller deployments.
○ Yes ● No

Table 109: *RAPIDS > Setup > Basic Configuration Fields and Default Values*

Field	Default	Description
ARP IP Match Timeout (1-168 hours)	24	If you have routers and switches on OV3600, and it's scanning them for ARP tables, this can assign a rogue IP address information. This timeout specifies how recent that information needs to be for the IP address to be considered valid. Note that the default ARP poll period is long (several hours).
RAPIDS Export Threshold	Suspected Rogue	Exported rogues will be sent to VisualRF for location calculation.
Wired-to-Wireless MAC Address Correlation (0-8 bits)	4	Discovered BSSIDs and LAN MAC addresses which are within this bitmask will be combined into one device. 4 requires all but the last digit match (aa:bb:cc:dd:ee:fX). 8 requires all but the last two digits match (aa:bb:cc:dd:ee:XX).
Wireless BSSID Correlation (0-8 bits)	4	Similar BSSIDs will be combined into one device when they fall within this bitmask. Setting this value too high may result in identifying two different physical devices as the same rogue. **NOTE:** When you change this value, RAPIDS will not immediately combine (or un-combine) rogue records. Changes will occur during subsequent processing of discovery events.

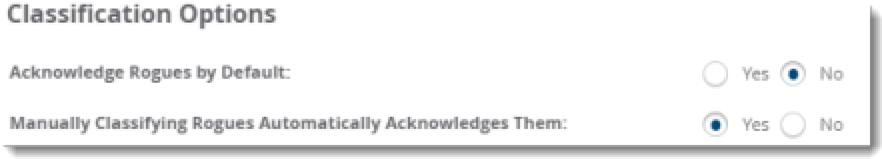
Table 109: *RAPIDS > Setup > Basic Configuration Fields and Default Values (Continued)*

Field	Default	Description
Delete Rogues not detected for (0-30 days, zero disables):	N/A	This value cannot be larger than the rogue discovery event expiration (30) configured on the OV3600 Setup page, unless that value is set to **0**.
Automatically OS scan rogue devices	No	Whether to scan the operating system of rogues. Enabling this feature will cause RAPIDS to perform an OS scan when it gets in IP address for a rogue device. The OS scan will be run when a rogue gets an IP address for the first time or if the IP address changes.
Wired-to-Wireless Time Correlation Window (minutes, zero disables):	360	Specify a time frame for wired and wireless correlation. RAPIDS discovery events detected wirelessly and on LAN will only match if the wireless and LAN discovery events occur during this timeframe.

Classification Options

The classification option settings determine how OV3600 acknowledges rogues and classifies them.

Figure 168: *Classification Options*



Classification Options

Acknowledge Rogues by Default: ○ Yes ● No

Manually Classifying Rogues Automatically Acknowledges Them: ● Yes ○ No

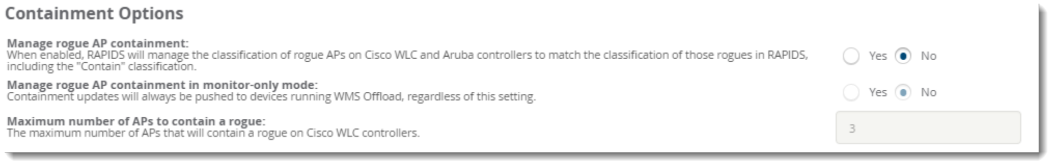
Table 110: *RAPIDS > Setup > Classification Options Fields and Default Values*

Field	Default	Description
Acknowledge Rogues by Default	No	Sets RAPIDS to acknowledge rogue devices upon initial detection, prior to their classification.
Manually Classifying Rogues Automatically Acknowledges them	Yes	Defines whether acknowledgment happens automatically whenever a rogue device receives a manual classification.

Containment Options

Using RAPIDS, OV3600 can shield rogue devices from associating to Cisco WLC controllers (versions 4.2.114 and later), and Alcatel-Lucent switches (running AOS-W versions 3.x and later). OV3600 will alert you to the appearance of the rogue device and identify any mismatch between switch configuration and the desired configuration.

Figure 169: *Containment Options*



Containment Options

Manage rogue AP containment:
When enabled, RAPIDS will manage the classification of rogue APs on Cisco WLC and Aruba controllers to match the classification of those rogues in RAPIDS, including the "Contain" classification. ○ Yes ● No

Manage rogue AP containment in monitor-only mode:
Containment updates will always be pushed to devices running WMS Offload, regardless of this setting. ○ Yes ● No

Maximum number of APs to contain a rogue:
The maximum number of APs that will contain a rogue on Cisco WLC controllers. 3

NOTE

WMS Offload is not required to manage containment in OV3600.

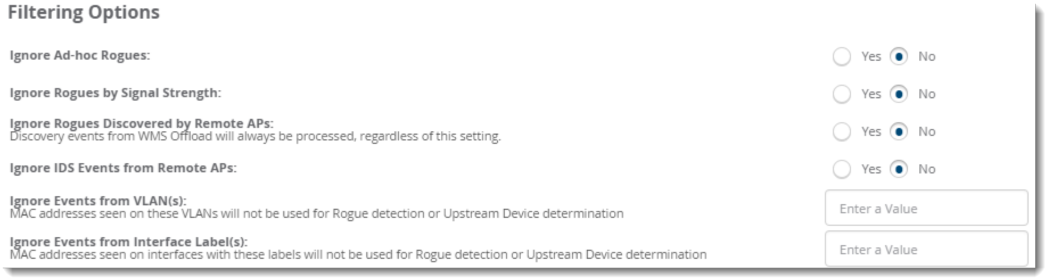
Table 111: *RAPIDS > Setup > Containment Options Fields and Default Values*

Field	Default	Description
Manage rogue AP containment	No	Specifies whether RAPIDS will manage the classification of rogue APs on Cisco WLC and Alcatel-Lucent controllers to match the classification of those rogues in RAPIDS. This includes the "Contained" classification. If this setting is enabled, then the **Maximum number of APs to contain a rogue** setting can be configured. Similarly, if this is enabled, then the Contained Rogue option will appear in the classification drop down menu when you add a new classification rule. (See "Viewing and Configuring RAPIDS Rules" on page 250 for more information.)
Manage rogue AP containment in monitor-only mode	No	Specify whether rogue AP containment can be performed in monitor-only mode. Note that containment updates will always be pushed to devices that are running WMS Offload, regardless of this setting.
Maximum number of APs to contain a rogue	N/A	If **Manage rogue AP containment** is enabled, then specify the maximum number of APs that can contain a rogue on Cisco WLC controllers.

Filtering Options

Filtered rogues are dropped from the system before they are processed through the rules engine. This can speed up overall performance but will eliminate all visibility into these types of devices.

Figure 170: *Filtering Settings*



Filtering Options

Ignore Ad-hoc Rogues: ○ Yes ● No

Ignore Rogues by Signal Strength: ○ Yes ● No

Ignore Rogues Discovered by Remote APs:
Discovery events from WMS Offload will always be processed, regardless of this setting. ○ Yes ● No

Ignore IDS Events from Remote APs: ○ Yes ● No

Ignore Events from VLAN(s):
MAC addresses seen on these VLANs will not be used for Rogue detection or Upstream Device determination — Enter a Value

Ignore Events from Interface Label(s):
MAC addresses seen on interfaces with these labels will not be used for Rogue detection or Upstream Device determination — Enter a Value

Table 112: *RAPIDS > Setup > Filtering Options Fields and Default Values*

Field	Default	Description
Ignore Ad-hoc rogues	No	Filters rogues according to ad-hoc status.
Ignore Rogues by Signal Strength	No	Filters rogues according to signal strength. Since anything below the established threshold will be ignored and possibly dangerous, best practices is to keep this setting disabled. Instead, incorporate signal strength into the classification rules on the **RAPIDS > Rules** page.
Ignore Rogues Discovered by Remote APs	No	Filters rogues according to the remote AP that discovers them. Enabling this option causes OV3600 to drop all rogue discovery information coming from remote APs.

Table 112: *RAPIDS > Setup > Filtering Options Fields and Default Values (Continued)*

Field	Default	Description
Ignore IDS Events from Remote APs	No	Filters IDS Events discovered by remote APs.
Ignore Events from VLAN(s)	N/A	Specify a VLAN or list of VLANs to be ignored when a wired rogue discovery event occurs. MAC addresses that appear on these VLANs will not be used for rogue detection or upstream device determination.
Ignore Events from Interface Label(s)	N/A	Specify an interface or list of interfaces to be ignored when a wired rogue discovery event occurs. MAC addresses that appear on these interface labels will not be used for rogue detection or upstream device determination.

Additional Settings

Use the **OV3600 Setup > Roles > Add/Edit Role** page to define the ability to use RAPIDS by user role. Refer to "Creating OV3600 User Roles" on page 39.

Defining RAPIDS Rules

The **RAPIDS > Rules** page is one of the core components of RAPIDS. This feature allows you to define rules by which any detected device on the network is classified.

This section describes how to define, use, and monitor RAPIDS rules, provides examples of such rules, and demonstrates how they are helpful.

This section contains the following topics:

- "switch Classification with WMS Offload" on page 248
- "Device OUI Score" on page 249
- "Rogue Device Threat Level" on page 249
- "Viewing and Configuring RAPIDS Rules" on page 250
- "Recommended RAPIDS Rules " on page 254
- "Using RAPIDS Rules with Additional OV3600 Functions" on page 254

switch Classification with WMS Offload

This classification method is supported only when WMS offload is enabled on Alcatel-Lucent WLAN switches. switch classification of this type remains distinct from RAPIDS classification. WLAN switches feed wireless device information to OV3600, which OV3600 then processes. OV3600 then pushes the WMS classification to all of the AOS-W switches that are WMS-offload enabled.

WMS Offload ensures that a particular BSSID has the same classification on all of the switches. WMS Offload removes some load from master switches and feeds '`connected-to-lan`' information to the RAPIDS classification engine. RAPIDS classifications and switch classifications are separate and often are not synchronized.

NOTE

RAPIDS classification is not pushed to the devices.

The following table compares how default classification may differ between OV3600 and Alcatel-Lucent AOS-W for scenarios involving WMS Offload.

Table 113: *Rogue Device Classification Matrix*

OV3600	AOS-W (ARM)
Unclassified (default state)	Unknown
Rogue	Rogue
Suspected Neighbor	Interfering
Neighbor	Known Interfering
Valid	Valid
Contained Rogue	DOS

For additional information about WMS Offload, refer to the *OmniVista 3600 Air Manager 8.2.7.1 Best Practices Guide* on the **Home > Documentation** page.

Device OUI Score

The Organizationally Unique Identifier (OUI) score is based on the LAN MAC address of a device. RAPIDS can be configured to poll your routers and switches for the bridge forwarding tables. RAPIDS then takes the MAC addresses from those tables and runs them through a proprietary database to derive the OUI score. The OUI score of each device is viewable from each rogue's detail page. Table 114 provides list the OUI scores definitions.

Table 114: *Device OUI Scores*

Score	Description
Score of 1	Indicates any device on the network; this is the lowest threat level on the network.
Score of 2	Indicates any device in which the OUI belongs to a manufacturer that produces wireless (802.11) equipment.
Score of 3	Indicates that the OUI matches a block that contains APs from vendors in the Enterprise and small office/ small home market.
Score of 4	Indicates that the OUI matches a block that belonged to a manufacturer that produces small office/ small home access points.

Rogue Device Threat Level

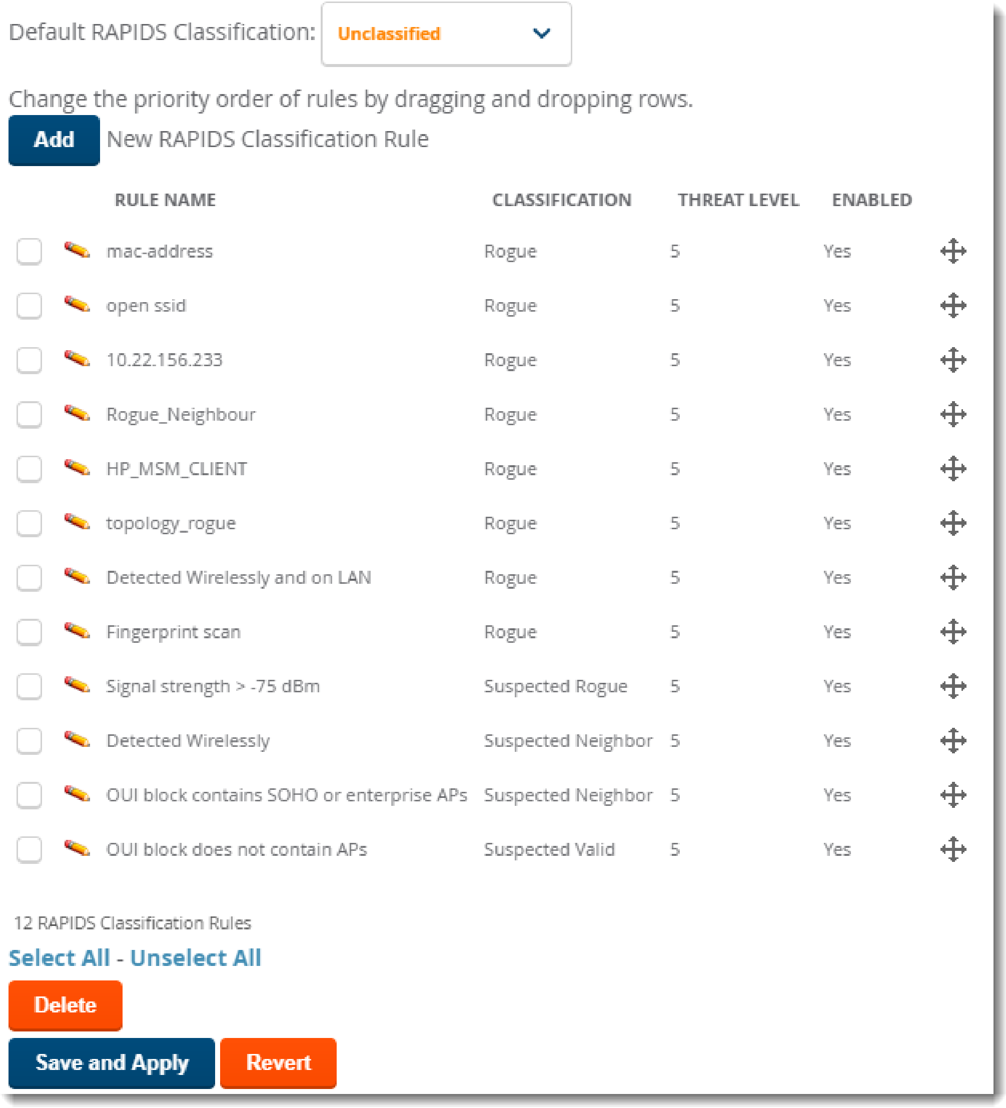
The threat level classification adds granularity for each general RAPIDS classification. Devices of the same classification can have differing threat scores based on the classifying rule, ranging from 1 to 10 with a default value of **5**. This classification process can help identify the greater threat. Alerts can be defined and sorted by threat level.

Threat level and classification are both assigned to a device when a device matches a rule. Once classified, a device's classification and threat level change only if it is classified by a new rule or is manually changed. Threats levels can be manually defined on the **RAPIDS > Detail** page when the RAPIDS classification is manually overridden or you can edit the rule to have a higher threat level.

Viewing and Configuring RAPIDS Rules

OV3600 displays RAPIDS rules on the **RAPIDS > Rules** page (Figure 171). By default, rogues that don't match any rules are unclassified, but you can set the default classification using the Default RAPIDS Classification drop-down menu at the top of the page.

Figure 171: *RAPIDS > Rules Page*



Default RAPIDS Classification: Unclassified

Change the priority order of rules by dragging and dropping rows.

Add New RAPIDS Classification Rule

		RULE NAME	CLASSIFICATION	THREAT LEVEL	ENABLED	
□	✎	mac-address	Rogue	5	Yes	✥
□	✎	open ssid	Rogue	5	Yes	✥
□	✎	10.22.156.233	Rogue	5	Yes	✥
□	✎	Rogue_Neighbour	Rogue	5	Yes	✥
□	✎	HP_MSM_CLIENT	Rogue	5	Yes	✥
□	✎	topology_rogue	Rogue	5	Yes	✥
□	✎	Detected Wirelessly and on LAN	Rogue	5	Yes	✥
□	✎	Fingerprint scan	Rogue	5	Yes	✥
□	✎	Signal strength > -75 dBm	Suspected Rogue	5	Yes	✥
□	✎	Detected Wirelessly	Suspected Neighbor	5	Yes	✥
□	✎	OUI block contains SOHO or enterprise APs	Suspected Neighbor	5	Yes	✥
□	✎	OUI block does not contain APs	Suspected Valid	5	Yes	✥

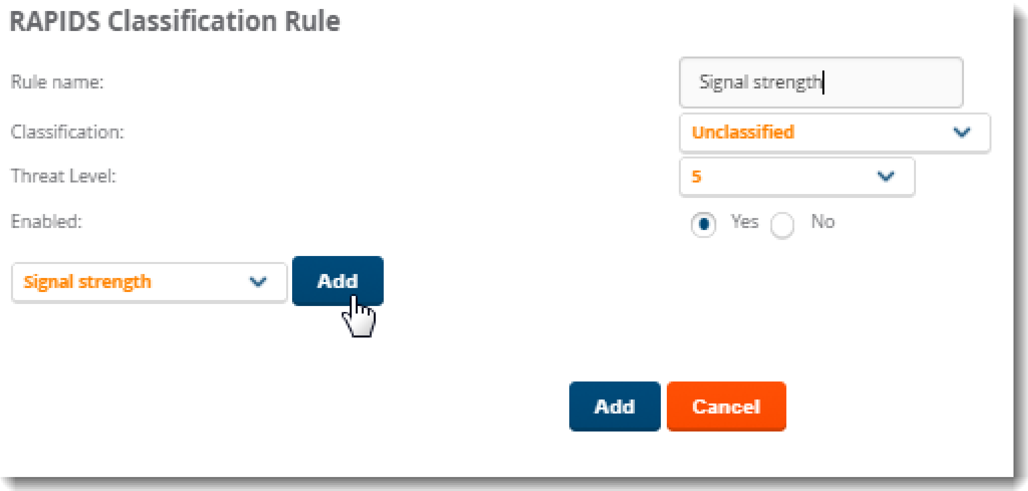
12 RAPIDS Classification Rules

Select All - Unselect All

To create a new RAPIDS classification rule:

1. Navigate to **RAPIDS > Rules**, then select the **Add**.
2. Enter a name for this RAPIDS classification rule. Rule names should describe your rule's core purpose.
3. Select the classification that a device will receive if rules are met.
4. Select the threat level for the rogue device. See "Rogue Device Threat Level" on page 249 for additional information.
5. Select a rule from the drop-down menu, then click **Add**. Rule conditions become available for you to configure.

Figure 172: *Adding a Rule Condition*



RAPIDS Classification Rule

Rule name: Signal strength

Classification: Unclassified

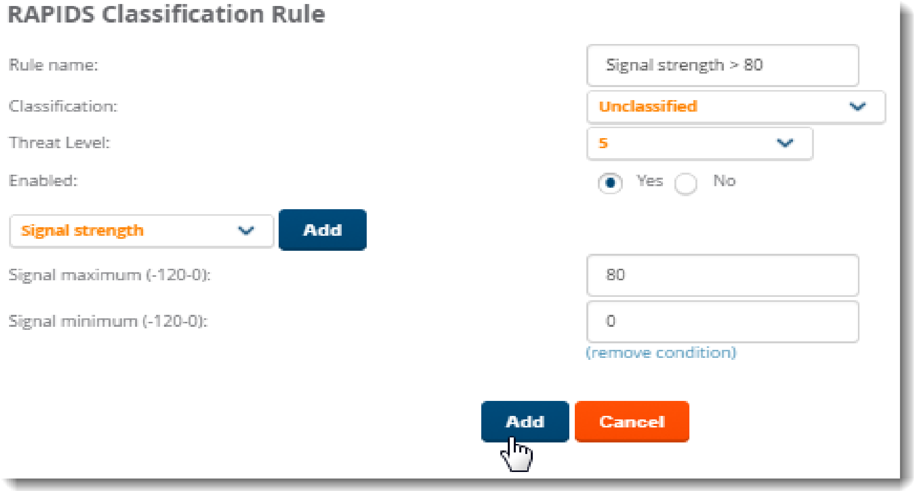
Threat Level: 5

Enabled: ● Yes ○ No

Signal strength

6. Repeat Step 5 to create additional rule conditions. Figure 173 shows a condition being created for a maximum signal strength of 80 dBm
7. Click **Add** at the bottom of the page.

Figure 173: *Creating a Rule for Signal Strength*



RAPIDS Classification Rule

Rule name: Signal strength > 80

Classification: Unclassified

Threat Level: 5

Enabled: ● Yes ○ No

Signal strength

Signal maximum (-120-0): 80

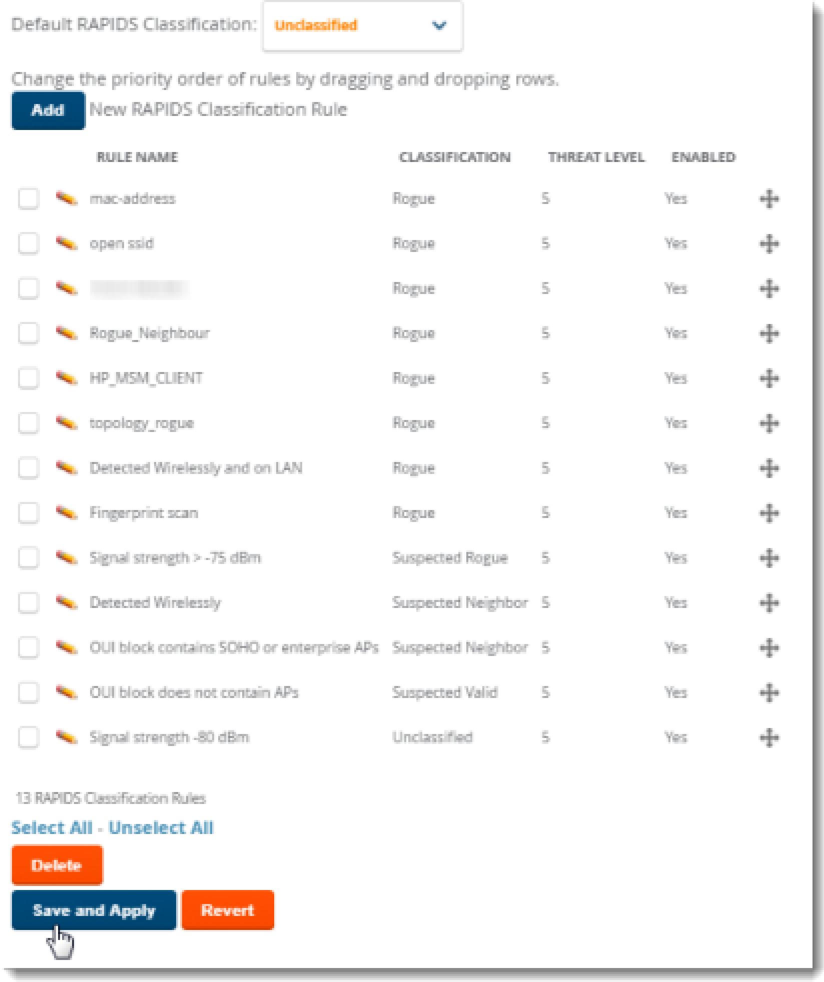
Signal minimum (-120-0): 0

(remove condition)

OV3600 displays the newly created rule on the Rules page.

Figure 174:

Figure 175: *Newly Created Signal Strength Rule*



Default RAPIDS Classification: Unclassified

Change the priority order of rules by dragging and dropping rows.

Add New RAPIDS Classification Rule

	RULE NAME	CLASSIFICATION	THREAT LEVEL	ENABLED
□	mac-address	Rogue	5	Yes
□	open ssid	Rogue	5	Yes
□	[redacted]	Rogue	5	Yes
□	Rogue_Neighbour	Rogue	5	Yes
□	HP_MSM_CLIENT	Rogue	5	Yes
□	topology_rogue	Rogue	5	Yes
□	Detected Wirelessly and on LAN	Rogue	5	Yes
□	Fingerprint scan	Rogue	5	Yes
□	Signal strength > -75 dBm	Suspected Rogue	5	Yes
□	Detected Wirelessly	Suspected Neighbor	5	Yes
□	OUI block contains SOHO or enterprise APs	Suspected Neighbor	5	Yes
□	OUI block does not contain APs	Suspected Valid	5	Yes
□	Signal strength -80 dBm	Unclassified	5	Yes

13 RAPIDS Classification Rules

Select All - Unselect All

8. Click **Save and Apply** to have the new rule take effect.

RAPIDS Classification Rule Properties

Table 115 defines the properties that you can add to a RAPIDS classification rule.

Table 115: *Rule Properties*

Option	Description
Wireless Properties	
Detected on WLAN	Classifies based on how the rogue is detected on the wireless LAN.
Detecting AP Count	Classifies based on the number of managed devices that can hear the rogue. Enter a numeric value and select **At Least** or **At Most**.
Encryption	Classifies based on the rogue matching a specified encryption method. Note that you can select **no encryption** with a rule that says **Encryption does not match WEP or better.**

Table 115: *Rule Properties (Continued)*

Option	Description
Network type	Rogue is running on the selected network type, either **Ad-hoc** or **Infrastructure**.
Signal Strength	Rogue matches signal strength parameters. Specify a minimum and maximum value in dBm.
SSID	Classifies the rogue when it matches or does not match the specified string for the SSID or a specified regular expression. **NOTE:** For SSID matching functions, OV3600 processes only alpha-numeric characters and the asterisk wildcard character (*****). OV3600 ignores all other non-alpha-numeric characters. For example, the string of **`ethersphere-*`** matches the SSID of **`ethersphere-wpa2`** but also the SSID of **`ethersphere_this_is_an_example`** (without any dashes).
Channel	Rogue matches a specified Channel number. Enter channel numbers in the valid format to match rogue devices.
Detected Client Count	Classifies based on the number of valid clients.
Wireline Properties	
Detected on LAN	Rogue is detected on the wired network. Select **Yes** or **No**.
Fingerprint Scan	Rogue matches fingerprint parameters.
IP Address	Rogue matches a specified IP address or subnet. Enter IP address or subnet information as explained by the fields.
OUI Score	Rogue matches manufacturer OUI criteria. You can specify minimum and maximum OUI score settings from two drop-down lists. Select **remove** to remove one or both criteria, as desired.
Operating System	Rogue matches OS criteria. Specify matching or non-matching OS criteria as prompted by the fields.
Wireless/Wireline Properties	
Manufacturer	Rogue matches the manufacturer information of the rogue device. Specify matching or non-matching manufacturer criteria.
MAC Address	Rogue matches the MAC address. Specify matching or non-matching address criteria, or use a wildcard (*) for partial matches.
Alcatel-Lucent switch Properties	
Controller Classification	Rogue matches the specified controller classification.
Confidence	Rogue falls within a specified minimum and maximum confidence level, ranging from 1 to 100.

Deleting or Editing a Rule

To delete a rule:

1. Go to the **RAPIDS > Rules** page.
2. Select the check box next to the rule you want to delete, and click **Delete**. Or, click ✎ to apply changes to a rule, then click **Save**.

Changing the Rule Priority

To change the sequence in which rules apply to any rogue device, drag and drop the rule to a new position in the rules sequence.

Recommended RAPIDS Rules

- **If Any Device Has Your SSID, then Classify as Rogue**

  The only devices broadcasting your corporate SSID should be devices that you are aware of and are managed by OV3600. Rogue devices often broadcast your official SSID in an attempt to get access to your users, or to trick your users into providing their authentication credentials. Devices with your SSID generally pose a severe threat. This rule helps to discover, flag, and emphasize such a device for prompt response on your part.
- **If Any Device Has Your SSID and is Not an Ad-Hoc Network Type, then Classify as Rogue**

  This rule classifies a device as a rogue when the SSID for a given device is your SSID and is not an Ad-Hoc device. Windows XP automatically tries to create an Ad-hoc network if it can not find the SSID for which it is searching. This means that user's laptops on your network may appear as Ad-Hoc devices that are broadcasting your SSID. If this happens too frequently, you can restrict the rule to apply to non-ad-hoc devices.
- **If More Than Four APs Have Discovered a Device, then Classify as Rogue**

  By default, OV3600 tries to use Signal Strength to determine if a device is on your premises. Hearing device count is another metric that can be used.

  The important concept in this scenario is that legitimate neighboring devices are only heard by a few APs on the edge of your network. Devices that are heard by a large number of your APs are likely to be in the heart of your campus. This rule works best for scenarios in large campuses or that occupy an entire building. For additional rules that may help you in your specific network scenario, contact Alcatel-Lucent support.

Using RAPIDS Rules with Additional OV3600 Functions

Rules that you configure on the **RAPIDS > Rules** page establish an important way of processing rogue devices on your network, and flagging them for attention as required. Such devices appear on the following pages in OV3600, with additional information:

- **RAPIDS > List**—Lists rogue devices as classified by rules.
- **RAPIDS > Rules**—Displays the rules that classify rogue devices.
- **RAPIDS > Overview**—Displays general rogue device count and statistical information.
- **System > Triggers**—Displays triggers that are currently configured, including any triggers that have been defined for rogue events.
- **Reports > Definitions**—Allows you to run New Rogue Devices Report with custom settings.
- **VisualRF**—Displays physical location information for rogue devices.

Viewing Rogues

There are several ways to view rogue devices, listed by rogue classification.

To view the list of rogue devices:

- Click the rogue count in the header statistics at the top of the OV3600 WebUI.

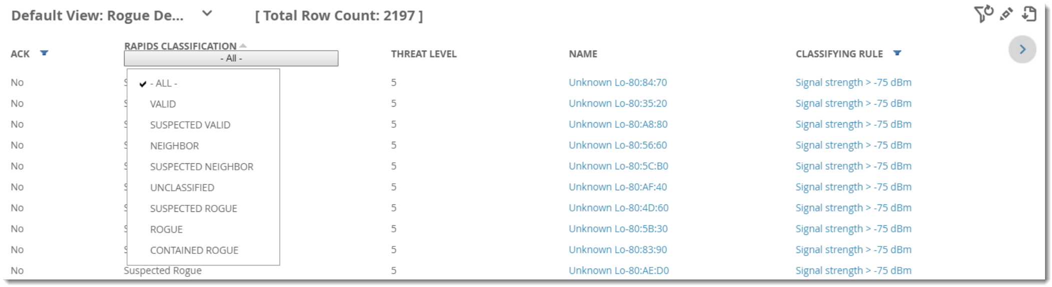
- Go to **RAPIDS > Overview**, then click the RAPIDS classification link.
- Go to **RAPIDS > List** and select a RAPIDS classification from the drop-down menu, as shown in Figure 176.

You can sort the table columns by selecting the column head. Most columns can be filtered by clicking the funnel icon ▼ . The hyperlinks on this page open additional pages for RAPIDS configuration or device processing.

Predefined, Default Views for Rogue Devices

OV3600 displays a default view for rogue devices on the **RAPIDS > List** page. Default views have predefined columns that cannot be modified.

Figure 176: *Predefined, Default Views for Rogue Devices*



Default View: Rogue De... [Total Row Count: 2197]

ACK	RAPIDS CLASSIFICATION	THREAT LEVEL	NAME	CLASSIFYING RULE
No		5	Unknown Lo-80:84:70	Signal strength > -75 dBm
No		5	Unknown Lo-80:35:20	Signal strength > -75 dBm
No		5	Unknown Lo-80:A8:80	Signal strength > -75 dBm
No		5	Unknown Lo-80:56:60	Signal strength > -75 dBm
No		5	Unknown Lo-80:5C:B0	Signal strength > -75 dBm
No		5	Unknown Lo-80:AF:40	Signal strength > -75 dBm
No		5	Unknown Lo-80:4D:60	Signal strength > -75 dBm
No		5	Unknown Lo-80:5B:30	Signal strength > -75 dBm
No		5	Unknown Lo-80:83:90	Signal strength > -75 dBm
No	Suspected Rogue	5	Unknown Lo-80:AE:D0	Signal strength > -75 dBm

Table 116 describes the information displayed in the default view.

Table 116: *Default View for Rogue Devices*

Column	Description
Ack	Displays whether or not the rogue device has been acknowledged. Devices can be acknowledged manually or you can configure RAPIDS so that manually classifying rogues will automatically acknowledges them. Additionally, devices can be acknowledged by using **Modify Devices** link at the top of the **RAPIDS > List** page. Rogues should be acknowledged when the OV3600 user has investigated them and determined that they are not a threat (see "RAPIDS Setup" on page 245).
RAPIDS Classification	Displays the RAPIDS classification of the discovered device, including: valid, suspected valid, neighbor, suspected neighbor, unclassified, suspected rogue, rogue, and contained rogue. RAPIDS classifies the discovered devices based on rules that you customize on the **RAPIDS > Rules** page (see "Defining RAPIDS Rules" on page 248).
Threat Level	This field displays the numeric threat level of the device, in a range from 1 to 10. The definition of threat level is configurable, as described in "Rogue Device Threat Level" on page 249. The threat level is also supported with Triggers (see "Using the System Pages" on page 263).
Name	Displays the alpha-numeric name of the rogue device, as known. By default, OV3600 assigns each rogue device a name derived from the OUI vendor and the final six digits of the MAC address. Clicking the linked name will redirect you to the **RAPIDS > Detail** page for that rogue device. Refer to "Overview of the RAPIDS > Detail Page" on page 258.
Classifying Rule	Displays the RAPIDS Rule that classified the rogue device (see "Viewing and Configuring RAPIDS Rules" on page 250).

Table 116: *Default View for Rogue Devices (Continued)*

Column	Description
Controller Classification	Displays the classification of the device based on the controller's hard-coded rules. **NOTE:** This column is hidden unless **Offload WMS Database** is enabled by at least one group on the **Groups > Basic** page.
Detecting APs	Displays the number of AP devices that have wirelessly detected the rogue device. A designation of **heard** implies the device was heard over the air.
First Discovering AP	Displays when a rogue was first seen. You can sort on this field to decide whether to be concerned with the rogue.
Last Discovering AP	Displays the most recent AP to discover the rogue device. The device name in this column is taken from the device name in OV3600. Click the linked device name to be redirected to the **Devices > Monitor** page for that AP.

Filtered Views for Rogue Devices

You can create a new view, or edit and copy a view, and save the view to access information you frequently use.

For more information on filtering data from your view, see "Creating Filtered Views" on page 132.

Table 117: *Additional Columns for Custom Views*

Column	Description
Ack	Displays whether or not the rogue device has been acknowledged. Devices can be acknowledged manually or you can configure RAPIDS so that manually classifying rogues will automatically acknowledges them. Additionally, devices can be acknowledged by using **Modify Devices** link at the top of the **RAPIDS > List** page. Rogues should be acknowledged when the OV3600 user has investigated them and determined that they are not a threat (see "RAPIDS Setup" on page 245).
Ch	Indicates the most recent RF channel on which the rogue was detected. **NOTE:** The rogue can be detected on more than one channel if it contains more than one radio.
Classifying Rule	Displays the RAPIDS Rule that classified the rogue device (see "Viewing and Configuring RAPIDS Rules" on page 250).
Confidence	The confidence level of the suspected rogue. How confidence is calculated varies based on the version of AOS-W. When an AOS-Wswitch sees evidence that a device might be on the wire, it will up the confidence level. If AOS-W is completely certain that it is on the wire, it gets classified as a rogue.
Controller Classification	Displays the classification of the device based on the controller's hard-coded rules. **NOTE:** This column is hidden unless **Offload WMS Database** is enabled by at least one group on the **Groups > Basic** page.
Current Associations	The number of current rogue client associations to this device.
Detecting APs	Displays the number of AP devices that have wirelessly detected the rogue device. A designation of **heard** implies the device was heard over the air.

Table 117: *Additional Columns for Custom Views (Continued)*

Column	Description
Encryption Type	Displays the encryption that is used by the device. Possible contents of this field include the following encryption types: - **Open**—No encryption - **WEP**—Wired Equivalent Privacy - **WPA**—Wi-Fi Protected Access Generally, this field alone does not provide enough information to determine if a device is a rogue, but it is a useful attribute. If a rogue is not running any encryption method, you have a wider security hole than with an AP that is using encryption.
First Discovering Time	Displays the time the rogue was first discovered.
Floor Coordinates	Displays the x and y coordinates taken from VisualRF for rogues.
IP Address	Displays the IP address of the rogue device. The IP address data comes from fingerprint scans or ARP polling of routers and switches.
LAN MAC Address	The LAN MAC address of the rogue device.
LAN Vendor	Indicates the LAN vendor of the rogue device, when known.
Last Discovering AP	Displays the most recent AP to discover the rogue device. The device name in this column is taken from the device name in OV3600. Click the linked device name to be redirected to the **Devices > Monitor** page for that AP.
Location	If the rogue has been placed in VisualRF, this column will display the name of the floor plan the rogue is on as a link to the VisualRF Floor Plan View page.
Max Associations	The highest number of rogue client associations ever detected at one time.
Model	Displays the model of rogue device, if known. This is determined with a fingerprint scan, and this information may not always be available.
Network Type	Displays the type of network in which the rogue is present, for example: - **Ad-hoc**—This type of network usually indicates that the rogue is a laptop that attempts to create a network with neighboring laptops, and is less likely to be a threat. - **AP**—This type of network usually indicates an infrastructure network, for example. This may be more of a threat. - **Unknown**—The network type is not known.
Notes	Indicates any notes about the rogue device that may have been added.
OS	This field displays the OS of the device, as known. OS is the result of a running an OS port scan on a device. An IP addresses is required to run an OS scan. The OS reported here is based on the results of the scan.
Port	Indicates the physical port of the switch or router where the rogue was last seen.

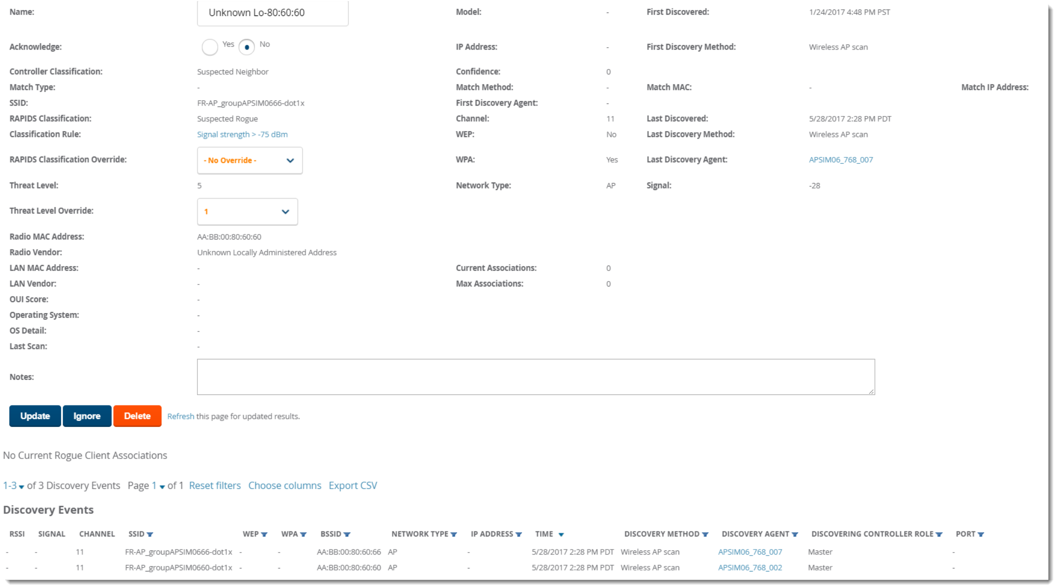
Table 117: *Additional Columns for Custom Views (Continued)*

Column	Description
Radio MAC Address	Displays the MAC address for the radio device, when known.
Radio Vendor	Indicates the radio vendor of the rogue device, when known.
RSSI	Displays the signal strength in dBm. In OV3600, the signal strength is a calculation based on RSSI measurements received in the radio signal from the AP. This RSSI data is relative and varies by AP.
Signal	Displays the strongest signal strength detected for the rogue device.
SSID	Displays the most recent SSID that was heard from the rogue device.
Switch/Router	Displays the switch or router where the device's LAN MAC address was last seen.
Threat Level	This field displays the numeric threat level of the device, in a range from 1 to 10. The definition of threat level is configurable, as described in "Rogue Device Threat Level" on page 249. The threat level is also supported with Triggers (see "Using the System Pages" on page 263).
Wired	Displays whether the rogue device has been discovered on one of your wired networks by polling routers/switches, your SNMP/HTTP scans, or Alcatel-Lucent WIP information. This column displays **Yes** or is blank if wired information was not detected.
WMS Classification AP	The AP that provided the information used to classify the device. Click the linked device name to be redirected to the **Devices > Monitor** page for that AP.
WMS Classification Date	The date that WMS set the classification.

Overview of the RAPIDS > Detail Page

Clicking a hyperlink in the **Name** column on the **RAPIDS > List** page opens a detailed view for the selected device (Figure 177).

Figure 177: *RAPIDS > Detail Page*



Name: Unknown Lo-80:60:60

Acknowledge: ○ Yes ● No

Controller Classification: Suspected Neighbor

Match Type: -

SSID: FR-AP_groupAPSIM0666-dot1x

RAPIDS Classification: Suspected Rogue

Classification Rule: Signal strength > -75 dBm

RAPIDS Classification Override: - No Override -

Threat Level: 5

Threat Level Override: 1

Radio MAC Address: AA:BB:00:80:60:60

Radio Vendor: Unknown Locally Administered Address

LAN MAC Address: -

LAN Vendor: -

OUI Score: -

Operating System: -

OS Detail: -

Last Scan: -

Notes:

Model: -

IP Address: -

Confidence: 0

Match Method: -

First Discovery Agent: -

Channel: 11

WEP: No

WPA: Yes

Network Type: AP

Current Associations: 0

Max Associations: 0

First Discovered: 1/24/2017 4:48 PM PST

First Discovery Method: Wireless AP scan

Match MAC: -

Match IP Address:

Last Discovered: 5/28/2017 2:28 PM PDT

Last Discovery Method: Wireless AP scan

Last Discovery Agent: APSIM06_768_007

Signal: -28

Refresh this page for updated results.

No Current Rogue Client Associations

1-3 of 3 Discovery Events Page 1 of 1 Reset filters Choose columns Export CSV

Discovery Events

RSSI	SIGNAL	CHANNEL	SSID	WEP	WPA	BSSID	NETWORK TYPE	IP ADDRESS	TIME	DISCOVERY METHOD	DISCOVERY AGENT	DISCOVERING CONTROLLER ROLE	PORT
-	-	11	FR-AP_groupAPSIM0666-dot1x	-	-	AA:BB:00:80:60:66	AP	-	5/28/2017 2:28 PM PDT	Wireless AP scan	APSIM06_768_007	Master	-
-	-	11	FR-AP_groupAPSIM0660-dot1x	-	-	AA:BB:00:80:60:60	AP	-	5/28/2017 2:28 PM PDT	Wireless AP scan	APSIM06_768_002	Master	-

Important Considerations

Keep in mind the following considerations when working with rogue devices:

- Users with the role of **Admin** can see all rogue AP devices.
- Users with roles limited by folder can see a rogue AP if there is at least one discovering device that they can see.
- Active rogue clients associated with this AP are listed in the **Current Rogue Client Associations** table. Selecting a linked MAC address will take you to the **Clients > Client Detail** page, where you can view fingerprinting and device details.
- Discovery events displayed are from APs that you can see on the network. There may be additional discovery events that remain hidden to certain user roles.
- Each rogue device frequently has multiple discovery methods, all of which are listed.
- VisualRF uses the heard signal information to calculate the physical location of the device.
- If the device is seen on the wire, RAPIDS reports the switch and port for easy isolation.
- If you find that the rogue belongs to a neighboring business, for example, you can override the classification to a neighbor and acknowledge the device. Otherwise, it is strongly recommended that you extract the device from your building and delete the rogue device from your system. If you delete a rogue, you will be notified the next time it is discovered.

Filter the Device Data

You can use filters to narrow results or work with large amounts of data.

To filter the device data:

- Use global filtering options on the **RAPIDS > Setup** page to filter rogue devices according to signal strength, ad-hoc status, and discovered by remote APs.
- Click ▼ to filter columns in the **Discovery Events** table .

Update Rogue Devices

In addition to updating the **Name** and **Notes** fields to identify the AP and document its location, you can:

1. Select the **Identify OS for Suspected Rogues** option if an IP address is available to obtain operating system information using an nmap scan. Note that if you are running wireline security software on your network, it may identify your OV3600 as a threat, which you can ignore.
2. Select the **Ignore** button if the rogue device is to be ignored. Ignored devices will not trigger alerts if they are rediscovered or reclassified.
3. Select the **Delete** button if the rogue device is to be removed from OV3600 processing.

Viewing Ignored Rogue Devices

The **RAPIDS > List** page allows you to view ignored rogues—devices that have been removed from the rogue count displayed by OV3600. Such devices do not trigger alerts and do not display on lists of rogue devices. To display ignored rogue devices, select **View Ignored Rogues** at the bottom left of the page.

Once a classification that has rogue devices is chosen from the drop-down menu, a detailed table displays all known information.

Using RAPIDS Workflow to Process Rogue Devices

One suggested workflow for using RAPIDS is as follows:

- Start from the **RAPIDS > List** page. Sort the devices on this page based on classification type. Begin with Rogue APs, working your way through the devices listed.
- Select **Modify Devices**, then select all devices that have an IP address and select **Identify OS**. OV3600 performs a port scan on the device and attempts to determine the operating system. (See "Setting Up RAPIDS" on page 245.)

  You should investigate devices running an embedded Linux OS installation. The OS scan can help identify false positives and isolate some devices that should receive the most attention.
- Find the port and switch at which the device is located and shut down the port or follow wiring to the device.
- To manage the rogue, remove it from the network and acknowledge the rogue record. If you want to allow it on the network, classify the device as valid and update with notes that describe it.

NOTE

Not all rogue discovery methods will have all information required for resolution. For example, the switch/router information, port, or IP address are found only through switch or router polling. Furthermore, RSSI, signal, channel, SSID, WEP, or network type information only appear through wireless scanning. Such information can vary according to the device type that performs the scan.

Score Override

On the **RAPIDS > Score Override** page you can change the OUI scores that are given to MAC addresses detected during scans of bridge forwarding tables on routers or switches. Figure 178, Figure 179, and Table 118 illustrate and describe RAPIDS Score Override. Perform these steps to create a score override.

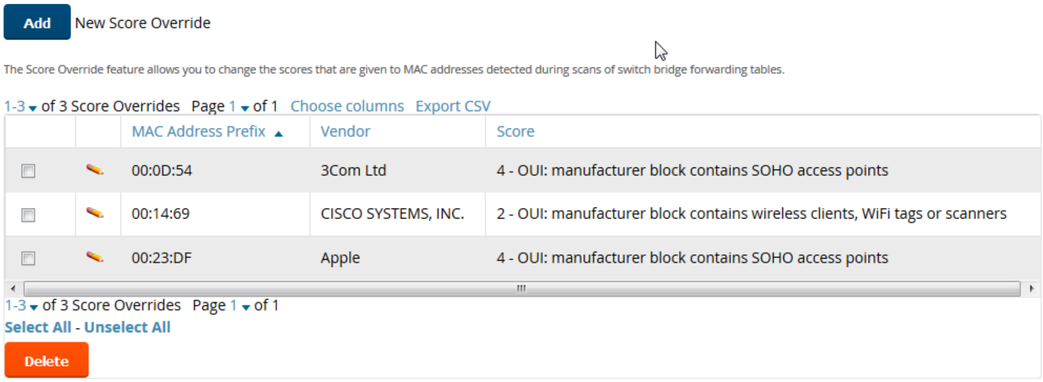
Once a new score is assigned, all devices with the specified MAC address prefix receive the new score.

NOTE

Note that re-scoring a MAC Address Prefix poses a security risk. The block has received its score for a reason. Any devices that fall within this block receive the new score.

1. Navigate to the **RAPIDS > Score Override** page. This page lists all existing overrides if they have been created.

Figure 178: *RAPIDS > Score Override Page*



Add New Score Override

The Score Override feature allows you to change the scores that are given to MAC addresses detected during scans of switch bridge forwarding tables.

1-3 ▾ of 3 Score Overrides Page 1 ▾ of 1 Choose columns Export CSV

		MAC Address Prefix ▲	Vendor	Score
□	✎	00:0D:54	3Com Ltd	4 - OUI: manufacturer block contains SOHO access points
□	✎	00:14:69	CISCO SYSTEMS, INC.	2 - OUI: manufacturer block contains wireless clients, WiFi tags or scanners
□	✎	00:23:DF	Apple	4 - OUI: manufacturer block contains SOHO access points

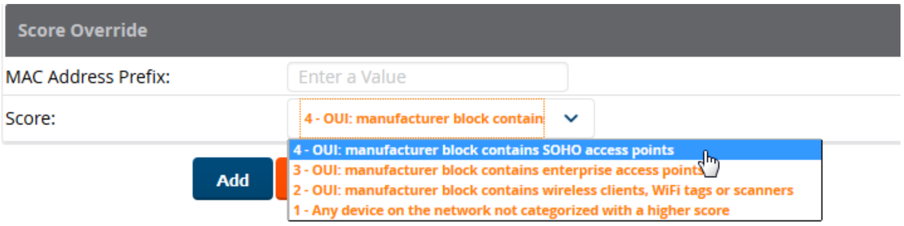
1-3 ▾ of 3 Score Overrides Page 1 ▾ of 1

Select All - Unselect All

Delete

2. Click **Add** to create a new override or select the pencil icon next to an existing override to edit that override. The **Score Override** add or edit page appears (Figure 179).

Figure 179: *Add/Edit Score Override Page*



Score Override

MAC Address Prefix: Enter a Value

Score: 4 - OUI: manufacturer block contain

4 - OUI: manufacturer block contains SOHO access points
3 - OUI: manufacturer block contains enterprise access points
2 - OUI: manufacturer block contains wireless clients, WiFi tags or scanners
1 - Any device on the network not categorized with a higher score
Add

Table 118: *RAPIDS > Add/Edit Score Override Page Fields*

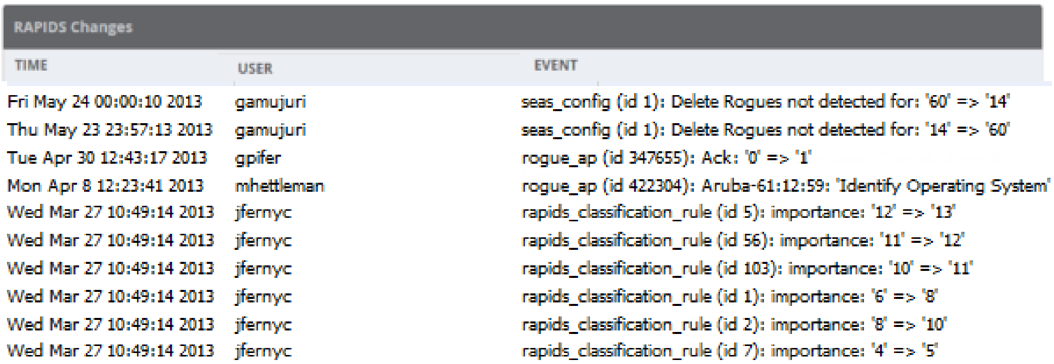
Field	Description
MAC Address Prefix	Use this field to define the OUI prefix to be re-scored.
Score	Use this field to set the score that a device, with the specified MAC address prefix, will receive.

3. Enter in the six-digit MAC prefix for which to define a score, and select the desired score. Once the new score has been saved, all detected devices with that prefix receive the new score.
4. Click **Add** to create the new override, or click **Save** to retain changes to an existing override. The new or revised override appears on the **RAPIDS > Score Override** page.
5. To remove any override, select that override in the check box, and then click the **Delete** button.

Using the Audit Log

The Audit Log is a record of any changes made to the RAPIDS rules, setup page, and manual changes to specific rogues. This allows you to see how something is changes, when it changed, and who made the alteration. The Audit Log can be found at **RAPIDS > Audit Log**. For more information, see Figure 180.

Figure 180: *Audit Log Page Illustration*



RAPIDS Changes

TIME	USER	EVENT
Fri May 24 00:00:10 2013	gamujuri	seas_config (id 1): Delete Rogues not detected for: '60' => '14'
Thu May 23 23:57:13 2013	gamujuri	seas_config (id 1): Delete Rogues not detected for: '14' => '60'
Tue Apr 30 12:43:17 2013	gpifer	rogue_ap (id 347655): Ack: '0' => '1'
Mon Apr 8 12:23:41 2013	mhettleman	rogue_ap (id 422304): Aruba-61:12:59: 'Identify Operating System'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 5): importance: '12' => '13'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 56): importance: '11' => '12'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 103): importance: '10' => '11'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 1): importance: '6' => '8'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 2): importance: '8' => '10'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 7): importance: '4' => '5'

Additional Resources

The following OV3600 tools support RAPIDS:

- **System Triggers and Alerts**—Triggers and Alerts that are associated with rogue devices follow the classification-based system described in this chapter. For additional information about triggers that support rogue device detection, see to Creating New Triggers.
- **Reports**—The **New Rogue Devices Report** displays summary and detail information about all rogues first discovered in a given time period. For more information, see "Using the New Rogue Devices Report" on page 341.

For additional security-related features and functions, see the following topics in this guide.

- "Configuring Security for Device Groups" on page 86
- "Configuring Cisco WLC Security Parameters and Functions" on page 105
- "Configuring SSIDs and VLANs for Device Groups" on page 92
- "Using the System Pages" on page 263

Chapter 8

Performing Daily Administration in OV3600

Daily WLAN administration often entails network monitoring, supporting WLAN and OV3600 users, and monitoring OV3600 system operations.

This chapter includes the following sections:

- "Using the System Pages" on page 263
- "Backing Up Your Data" on page 279
- "Managing Mobile Devices with SOTI MobiControl and OV3600 " on page 285
- "About the Home Page" on page 286
- "Logging out of OV3600" on page 313

Using the System Pages

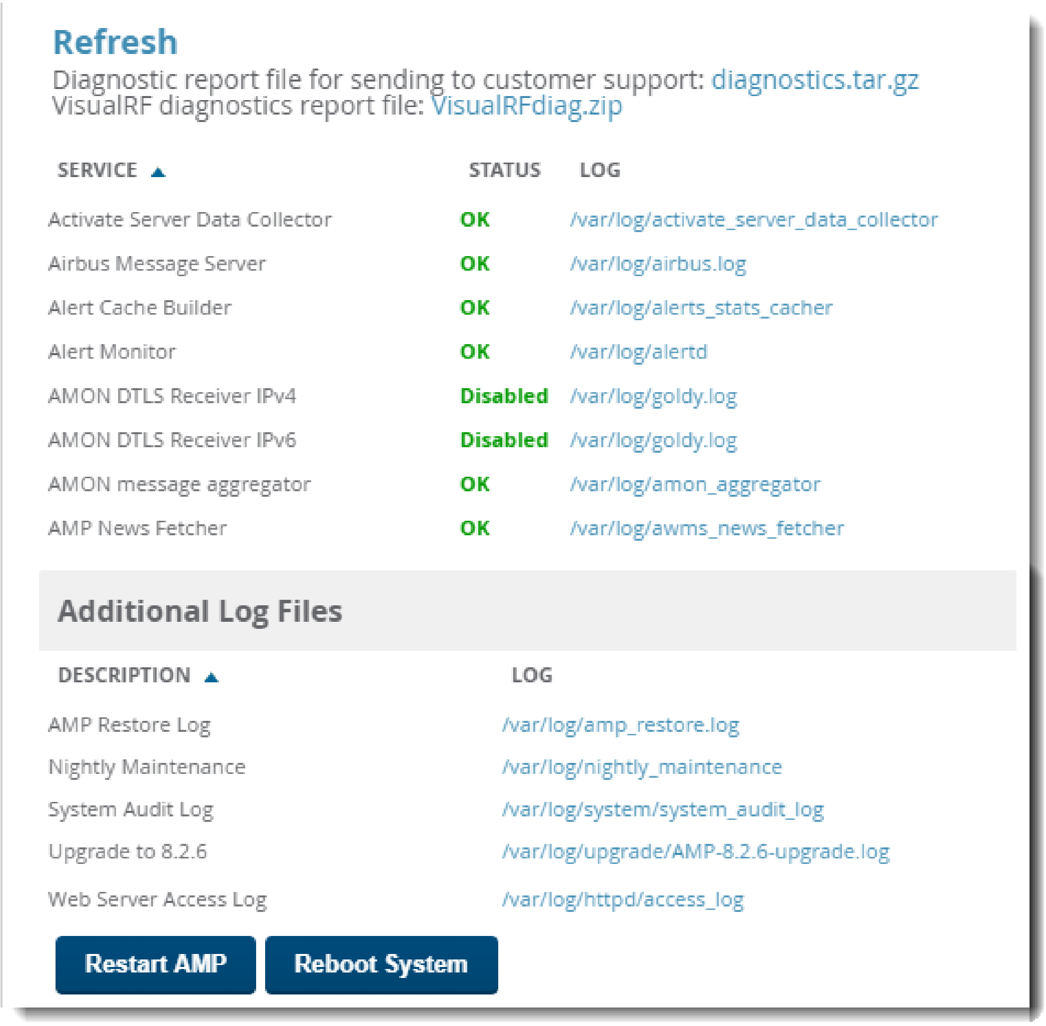
The **System** pages provide a centralized location for system-wide OV3600 data and settings. System pages let you view things like syslog messages and OV3600 events, set triggers, respond to alerts, manage configuration jobs, and monitor system performance.

Checking the Status of OV3600 Services

AirWave records information about the services and puts them into log files that are available on the **System > Status** page. You can also access other OV3600 logs on the **System > Download Log Files** page. For information, see "Downloading Log Files" on page 1.

Figure 181 shows an example of the System Status page. Green status descriptions indicate everything is OK or disabled. If you see status descriptions in red, contact Alcatel-Lucent support for help troubleshooting the service which is down.

Figure 181: *System Status Page*



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

SERVICE ▲	STATUS	LOG
Activate Server Data Collector	OK	/var/log/activate_server_data_collector
Airbus Message Server	OK	/var/log/airbus.log
Alert Cache Builder	OK	/var/log/alerts_stats_cacher
Alert Monitor	OK	/var/log/alertd
AMON DTLS Receiver IPv4	Disabled	/var/log/goldy.log
AMON DTLS Receiver IPv6	Disabled	/var/log/goldy.log
AMON message aggregator	OK	/var/log/amon_aggregator
AMP News Fetcher	OK	/var/log/awms_news_fetcher

Additional Log Files

DESCRIPTION ▲	LOG
AMP Restore Log	/var/log/amp_restore.log
Nightly Maintenance	/var/log/nightly_maintenance
System Audit Log	/var/log/system/system_audit_log
Upgrade to 8.2.6	/var/log/upgrade/AMP-8.2.6-upgrade.log
Web Server Access Log	/var/log/httpd/access_log

In addition to viewing service status and downloading log files, you can:

- Click **Refresh** at the top of the page to update system status.
- Click the blue **diagnostics.tar.gz** link at the top of the page to get diagnostic reports and logs, or the **VisualRF.diag.zip** link to get VisualRF diagnostic information. Both will help customer support troubleshoot and solve problems.
- Click **Restart OV3600** to restart OV3600 services without power cycling the server or reloading the OS.
- Click **Reboot System** to power cycle your OV3600 remotely.

Important OV3600 Logs

Table 119 describes some of the most important OV3600 logs. You can download additional logs from the /var/log and /tmp directories using SSH. If Alcatel-Lucent support engineers request these additional logs. you'll get instructions on how to retrieve the logs.

Table 119: *Important AirWave Logs*

Service	Log	Description
Alcatel-Lucent Device HTTPS Handler	device_https_ handler	Logs switch ZTP activities.
Client Monitor Worker	async_logger_ client	Logs device monitoring checks.
Configuration Server	config_pusher	Logs errors in pushing configuration to devices.
Database	pgsql	Logs database activity.
Postfix Mail Server	maillog	Applies in cases where emailed reports or alerts do not arrive at the intended recipient's address.
RADIUS Accounting Server	radius	Displays error messages associated with RADIUS accounting.
VisualRF Engine	visualrf.log	Details errors and messages associated with the VisualRF application.
Web Server	error_log	Reports problems with the web server. Also linked from the internal server error page that displays on the web page; send this log to Alcatel-Lucent support whenever reporting an internal server error.

Viewing Device Events

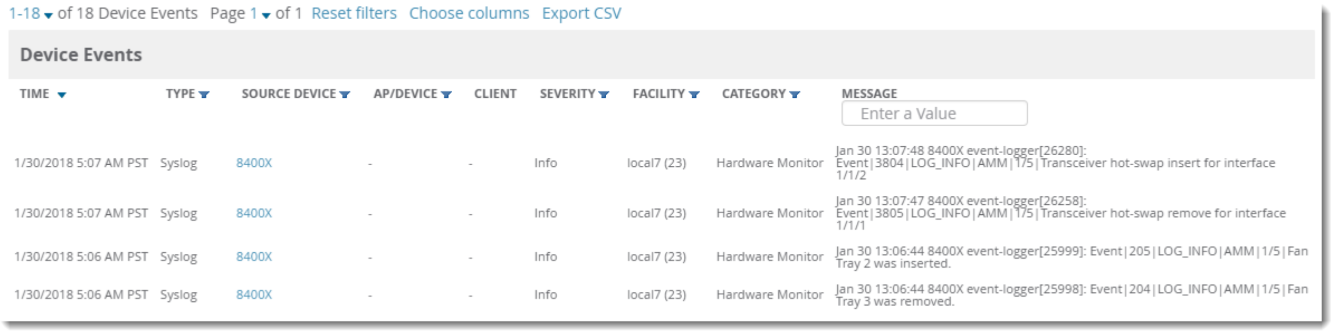
Admins can use the **System > Syslog & Traps** page to review all syslog messages and SNMP traps that OV3600 receives from the trigger type **Device Event**. For more information about triggers, see "Viewing Triggers" on page 1.

NOTE

Starting with OV3600 8.2.6, you can set critical thresholds to alert when there are hardware failures on the Alcatel-Lucent 8400 and 8320 switches. By default, OV3600 enables the trigger when you upgrade to or install OV3600 8.2.6.

Figure 182 shows an example of events for the Alcatel-Lucent 8400 Switch.

Figure 182: *Viewing Device Events*



1-18 of 18 Device Events Page 1 of 1 Reset filters Choose columns Export CSV

Device Events

TIME	TYPE	SOURCE DEVICE	AP/DEVICE	CLIENT	SEVERITY	FACILITY	CATEGORY	MESSAGE
								Enter a Value
1/30/2018 5:07 AM PST	Syslog	8400X	-	-	Info	local7 (23)	Hardware Monitor	Jan 30 13:07:48 8400X event-logger[26280]: Event|3804|LOG_INFO|AMM|1/5|Transceiver hot-swap insert for interface 1/1/2
1/30/2018 5:07 AM PST	Syslog	8400X	-	-	Info	local7 (23)	Hardware Monitor	Jan 30 13:07:47 8400X event-logger[26258]: Event|3805|LOG_INFO|AMM|1/5|Transceiver hot-swap remove for interface 1/1/1
1/30/2018 5:06 AM PST	Syslog	8400X	-	-	Info	local7 (23)	Hardware Monitor	Jan 30 13:06:44 8400X event-logger[25999]: Event|205|LOG_INFO|AMM|1/5|Fan Tray 2 was inserted.
1/30/2018 5:06 AM PST	Syslog	8400X	-	-	Info	local7 (23)	Hardware Monitor	Jan 30 13:06:44 8400X event-logger[25998]: Event|204|LOG_INFO|AMM|1/5|Fan Tray 3 was removed.

Here are some of the details about the device events you can view from the Syslog & Traps page:

- Time. The time the device event occurred.
- Type. The type can be syslog or SNMP trap.

- Source Device. The name of the device that sent the message. This field provides a link to the device monitoring page if you have visibility to the device, or it can be empty if OV3600 can't correlate the source IP address.
- AP/Device. This field provides a link to the device monitoring page for a device other than the source device if it correlates data contained in the message (by LAN MAC, BSSID, or IP Address) and you have visibility to the device.
- Client. The user's MAC address, if found in the message. This field provides a link to the client page if you have visibility to the user's AP, or it can be empty.
- Severity. The event severity can be emergency, alert, critical, bug, error, warning, notice, or info.
- Facility. The facility is obtained from part of the syslog spec, which is the logical source of the message. From controllers, the facility will always be one of local0 to local7. You can configure on the controller which facility you want to use in the messages when sending syslog messages to a receiver.
- Category. For SNMP traps, the category can be hardware, IDS, client security, AP security, AP status, software, or rogue detection. For Syslog messages, a category is based on the process name on the controller that sent the syslog message. Categories for traps and syslog messages only works for events from anAlcatel-Lucentswitch.
- Message. The raw trap message includes the AP MAC Address, time sent, and other information. For syslog messages, OV3600 doesn't display the numbers at the beginning of the message that indicate the severity and facility. For SNMP traps, OV3600 tries to translate them into human-readable format. OV3600 won't receive processed SNMP traps into the Device Event framework if the OV3600 doesn't have the MIB file to translate the trap.

> Syslog messages also appear in the **Devices > Monitor** page for switches and in **Clients > Client Detail** pages under the **Association History** section.

You can filter most columns by clicking ▼ , and you can filter the messages after you enter a text into the **Search** field, as shown in Figure 182.

To change the historical data retention period, go to **OV3600 Setup > General** and update the **Device Events (Syslog, Traps)** field.

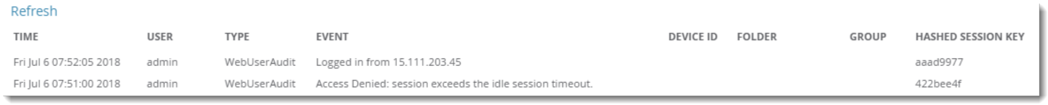
Using the Event Log

The system event log lets you troubleshoot recent OV3600 events, such as APs coming up and down, services restarting, and most OV3600-related errors.

OV3600 also audits activity committed by the Web or CLI so that you can analyze when a particular change might have occurred, especially for a shared system that multiple people can access.

In Figure 183, the system even log shows that OV3600 audited the web session initiated by the admin user and ended the web session because of inactivity.

Figure 183: ***System > Event Log***



TIME	USER	TYPE	EVENT	DEVICE ID	FOLDER	GROUP	HASHED SESSION KEY
Fri Jul 6 07:52:05 2018	admin	WebUserAudit	Logged in from 15.111.203.45				aaad9977
Fri Jul 6 07:51:00 2018	admin	WebUserAudit	Access Denied: session exceeds the idle session timeout.				422bee4f

Table 120 describes the page components.

Table 120: *Event Log Fields*

Column	Description
Time	Date and time of the event.
User	The OV3600 user that triggered the event. When OV3600 itself is responsible, **System** is displayed.
Type	Displays the Type of event recorded, which is one of four types, as follows: - **Device**—An event localized to one specific device. - **Group**—A group-wide event. - **System**—A system-wide event. - **NMS**—An event triggered by an NMS server. (See "Integrating NMS Servers" on page 66 for more info.) - **Alert**—If a trigger is configured to report to the log, an **Alert** type event will be logged here. - **WebUserAudit**—Logging of actions performed from the AMP web interface. - **CLIUserAudit**—Logging of actions performed from the AMP CLI menu interface.
Event	The event that OV3600 observed. This information can be useful for debugging, user tracking, and change tracking.
Device ID	If the event is a Device event, then this column shows the device ID.
Folder	If the event is a Device event, this column shows the folder where the device resides.
Group	If the event is a Device event, this column shows the Group in which the device resides.
Hashed Session Key	Displays a partial of hash of the randomly generated key used for secure connections to help identify the session since users can have multiple sessions. **NOTE:** You can restrict the session from **AMP Setup > Authentication**.

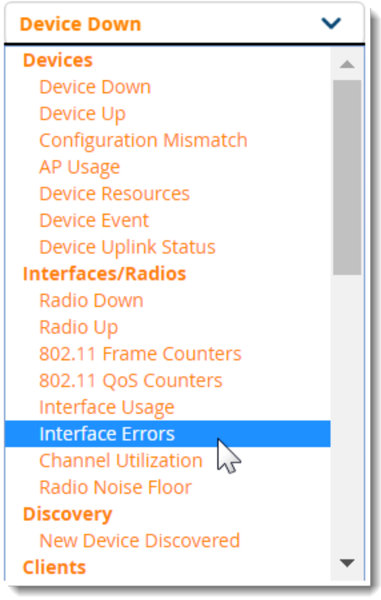
Creating New Triggers

OV3600 monitors key aspects of your network performance. When certain conditions or parameters arise that are outside of normal bounds, AirWave triggers alerts that enable you to address problems, often before users have a chance to report them.

To create a trigger:

1. Navigate to **System > Triggers**, then click **Add**.
2. Select the type of trigger from the drop down menu.

Figure 184: *Selecting the Type of Trigger*



3. Select the severity level.
4. Select whether OV3600 matches all or any trigger conditions, then click **Add**. In many cases, you must configure at least on condition setting. For more information about trigger conditions, see "Types of Triggers" on page 268.
5. Configure the trigger restrictions:
   - Folder. Limits the trigger to apply to devices in the selected folder.
   - Include Subfolders. Limits the trigger to apply to devices in the selected folder and subfolders.
   - Group. Limits the trigger to apply to devices in the selected group.

   Selecting folder and group applies the trigger to the intersection of devices in both group and folder.
6. Enter alert notifications, including a note that will be included with the alert. This note will appear with the alert on the **System > Alerts** page. Alert notification settings include:
   - Email. Enter the sender and recipient email addresses.
   - NMS. Choose one or more of the pre-defined trap destinations, which are configured on the **OV3600 Setup >NMS** page. This option is available if an NMS server has been added to OV3600.
   - Logged Alert Visibility. Choose how this trigger is distributed. The trigger can distributed according to how is it generated (triggering agent), or by the role with which it is associated.
   - Suppress Until Acknowledged. Choose whether the trigger requires manual, administrative acknowledgment to gain visibility. If **No**, a new alert will be created every time the trigger criteria are met. If **Yes**, an alert will only be received the first time the criteria is met. A new alert for the device is not created until the initial one is acknowledged.
7. Click **Add** to save the trigger. The trigger appears the next time you go to the **System > Triggers** page.

Types of Triggers

The following sections provide information about the triggers and condition settings you can apply to each one.

- "Device Triggers " on page 269
- "Interface and Radio Triggers" on page 271
- "Discovery Trigger" on page 273
- "Client Triggers" on page 273

- "RADIUS Authentication Triggers" on page 275
- "RADIUS Accounting Triggers" on page 275
- "IDS Event Triggers" on page 275
- "Health Triggers" on page 276

Device Triggers

To set a trigger for devices, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the device triggers described in Table 121

For more information on creating a device trigger for hardware errors, see "Triggers for hardware monitoring" on page 270. For more information on creating a device trigger for switch clusters, see "Triggers for switch Cluster Monitoring" on page 271

Table 121: *Device Triggers*

Name	Description and Conditions
Device Down	This type of trigger activates when an authorized, monitored AP has failed to respond to SNMP queries from OV3600. To set the conditions for this trigger type, select **Add** in the **Conditions** section. Complete the conditions with the **Option**, **Condition**, and **Value** drop-down menus. The conditions establish the device type. Multiple conditions can apply to this type of trigger. The Device Down trigger can be configured to send alerts for thin APs when the controller is down; this behavior is turned off by default. Triggers with the **Minutes Down** condition enabled will compare the amount of time an AP has been down to the value (in minutes) set for the condition. When the **Limit by number of down events** is enabled, you can set the number of down events that activate the trigger, as well as the duration of the time window to be measured. OV3600 will then count the number of times that the device has gone from Up to Down in the specified span of time and display this in the Device Down alert.
Device Up	This trigger type activates when an authorized, previously down AP is now responding to SNMP queries. To set the conditions for this trigger type, select **Add** in the **Conditions** section.
Configuration Mismatch	This trigger type activates when the actual configuration on the AP does not match the defined **Group** configuration policy. To set the conditions for this trigger type, select **Add** in the **Conditions** section.
AP Usage	Activates when the total bandwidth through the device has exceeded a predefined threshold for more than a specified period (such as more than 1500 Kbps for more than 120 seconds). You can also select bandwidth direction and page/radio. Selecting this type displays the following new fields in the **Type** section. Define these settings. ● **Alert if AP Usage >= (Kbps)**—This threshold establishes a device-specific bandwidth policy, not a bandwidth policy on the network as a whole. ● **Usage Direction**—Choose **In**, **Out**, or **Combined**. This bandwidth is monitored on the device itself, not on the network as a whole. ● **Severity** - Specify the severity type for the trigger. ● **Duration** - Specify the time frame for the trigger.
Device Resources	This type of trigger indicates that the CPU or memory utilization for a device (including router or switch) has exceeded a defined percentage for a specified period of time.

Table 121: *Device Triggers (Continued)*

Name	Description and Conditions
Device Event	This trigger is used for alerting based on SNMP traps and syslog messages, which are displayed in **System > Syslogs & Traps**, **Devices > Monitor** for affected devices, and in **Clients > Client Detail.** The conditions supported are: ● **Event Contents** (case insensitive substring matches on message content) ● **Event Type** (syslog or trap) ● **Syslog Severity**: Emergency, Alert, Critical, Bug, Error, Warning, Notice, or Info ● Syslog Category ● **SNMP Trap Category**: Hardware, IDS, Client Security, AP Security, AP Status, Software, or Rogue Detection ● **Syslog Category** **NOTE:** During the process of upgrading or installation for non-Master Console/Failover OV3600s, OV3600 creates two default trigger definitions for Device Events: ● SNMP Trap Category of **Hardware** or **Software** ● Event Type is **Syslog** and **Syslog Severity** >= **Critical** For help creating these triggers, see "Triggers for hardware monitoring" on page 270
Device Uplink Status	This trigger deploys whenever a RAP's active uplink changes from Ethernet to USB or vice versa. The corresponding events are captured in a RAP's **Devices > Monitor** page.
switch Cluster Trigger	This trigger informs you when the controllers present in the cluster are reaching AP capacity, client capacity, and how much bandwidth usage (total traffic in and out) is reaching the threshold. For help creating these triggers, see "Triggers for switch Cluster Monitoring" on page 271.

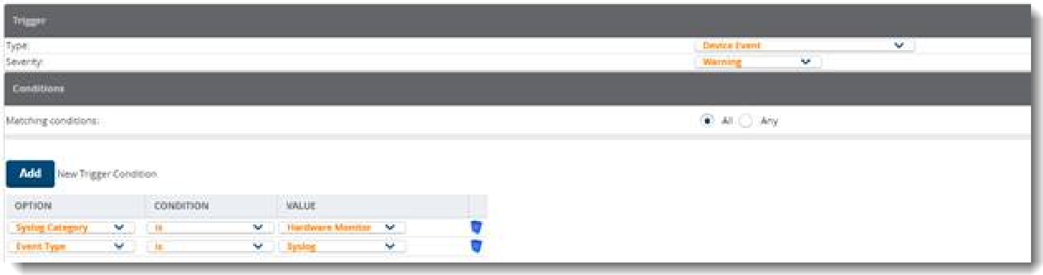
Triggers for hardware monitoring

OV3600 provides triggers that alert you to hardware failures to your APs, Alcatel-Lucent switches, and hardware components.

To create a trigger for device hardware failures:

1. Navigate to the **System > Triggers** page, then select Device Event for the trigger type.
2. Select the event severity: Normal, Warning, Minor, Major, or Critical.
3. Click **Add** to create the trigger conditions shown in Figure 185.

Figure 185: *Example Hardware Monitoring Trigger Conditions*



Trigger

Type: Device Event

Severity: Warning

Conditions

Matching conditions: ● All ○ Any

Add New Trigger Condition

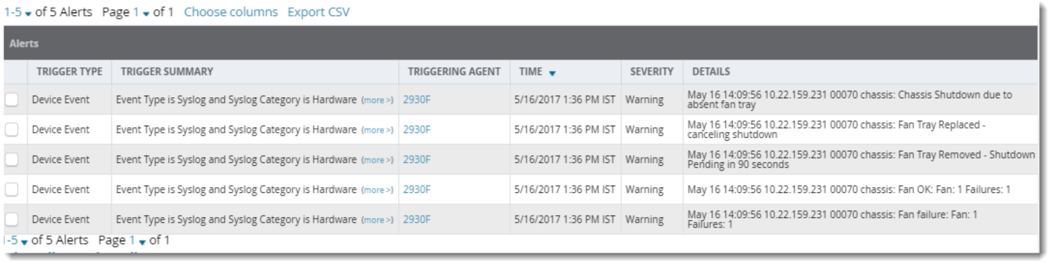
OPTION	CONDITION	VALUE
Syslog Category	is	Hardware Monitor
Event Type	is	Syslog

4. Configure the switch for sending syslog messages:

```
HP-Switch-5406Rzl2(config)# logging facility syslog
HP-Switch-5406Rzl2(config)# logging <Airwave _IP>
```

The hardware triggers display in the Triggers table, as shown in Figure 186.

Figure 186: *Hardware Triggers*



1-5 ▾ of 5 Alerts Page 1 ▾ of 1 Choose columns Export CSV

Alerts

	TRIGGER TYPE	TRIGGER SUMMARY	TRIGGERING AGENT	TIME ▾	SEVERITY	DETAILS
□	Device Event	Event Type is Syslog and Syslog Category is Hardware (more >)	2930F	5/16/2017 1:36 PM IST	Warning	May 16 14:09:56 10.22.159.231 00070 chassis: Chassis Shutdown due to absent fan tray
□	Device Event	Event Type is Syslog and Syslog Category is Hardware (more >)	2930F	5/16/2017 1:36 PM IST	Warning	May 16 14:09:56 10.22.159.231 00070 chassis: Fan Tray Replaced - canceling shutdown
□	Device Event	Event Type is Syslog and Syslog Category is Hardware (more >)	2930F	5/16/2017 1:36 PM IST	Warning	May 16 14:09:56 10.22.159.231 00070 chassis: Fan Tray Removed - Shutdown Pending in 90 seconds
□	Device Event	Event Type is Syslog and Syslog Category is Hardware (more >)	2930F	5/16/2017 1:36 PM IST	Warning	May 16 14:09:56 10.22.159.231 00070 chassis: Fan OK: Fan: 1 Failures: 1
□	Device Event	Event Type is Syslog and Syslog Category is Hardware (more >)	2930F	5/16/2017 1:36 PM IST	Warning	May 16 14:09:56 10.22.159.231 00070 chassis: Fan failure: Fan: 1 Failures: 1

1-5 ▾ of 5 Alerts Page 1 ▾ of 1

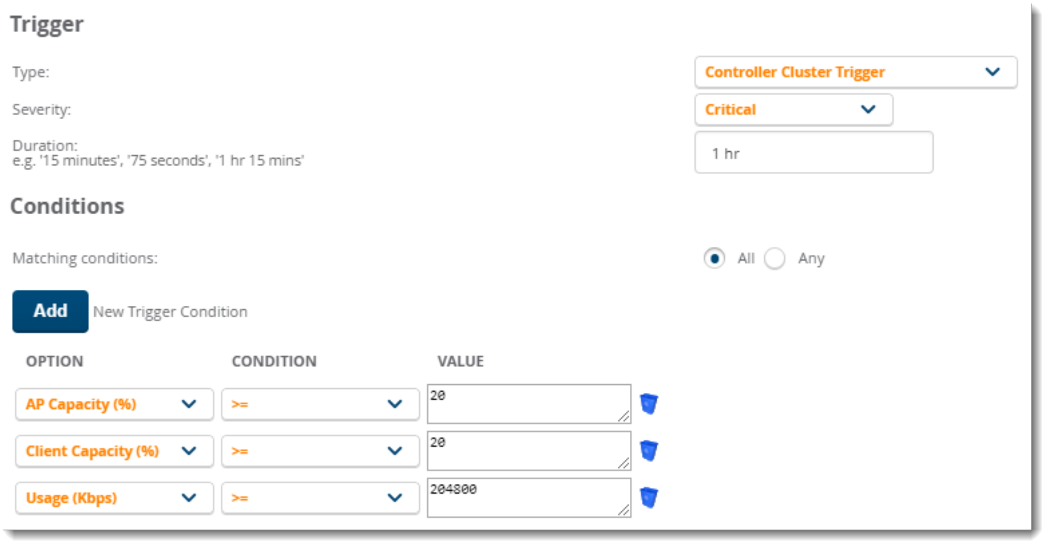
Triggers for switch Cluster Monitoring

You can set critical thresholds to inform you of when maximum throughput or AP and client capacities are being reached.

To create a trigger for switch clusters:

1. Navigate to the **System > Triggers** page, then create trigger as a device event.
2. Select the event severity: Normal, Warning, Minor, Major, or Critical.
3. Click **Add** to create trigger conditions as shown in Figure 187.

Figure 187: *Example switch Cluster Trigger Conditions*



Trigger

Type: Controller Cluster Trigger

Severity: Critical

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

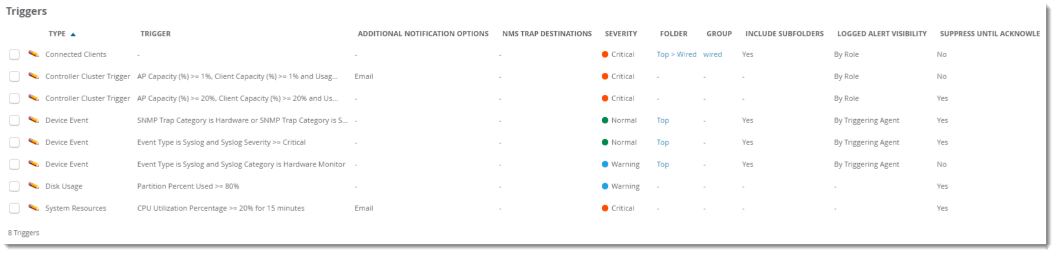
Conditions

Matching conditions: ● All ○ Any

OPTION	CONDITION	VALUE
AP Capacity (%)	>=	20
Client Capacity (%)	>=	20
Usage (Kbps)	>=	204800

4. Click **Add** to save the trigger. The switch cluster trigger displays in the Triggers table, as shown in Figure 188.

Figure 188: ***switch Cluster Trigger***



Triggers

	TYPE ▲	TRIGGER	ADDITIONAL NOTIFICATION OPTIONS	NMS TRAP DESTINATIONS	SEVERITY	FOLDER	GROUP	INCLUDE SUBFOLDERS	LOGGED ALERT VISIBILITY	SUPPRESS UNTIL ACKNOWLE
□	Connected Clients	-	-	-	● Critical	Top > Wired	wired	Yes	By Role	No
□	Controller Cluster Trigger	AP Capacity (%) >= 1%, Client Capacity (%) >= 1% and Usag...	Email	-	● Critical	-	-	-	By Role	No
□	Controller Cluster Trigger	AP Capacity (%) >= 20%, Client Capacity (%) >= 20% and Us...	-	-	● Critical	-	-	-	By Role	Yes
□	Device Event	SNMP Trap Category is Hardware or SNMP Trap Category is S...	-	-	● Normal	Top	-	Yes	By Triggering Agent	Yes
□	Device Event	Event Type is Syslog and Syslog Severity >= Critical	-	-	● Normal	Top	-	Yes	By Triggering Agent	Yes
□	Device Event	Event Type is Syslog and Syslog Category is Hardware Monitor	-	-	● Warning	Top	-	Yes	By Triggering Agent	No
□	Disk Usage	Partition Percent Used >= 80%	-	-	● Warning	-	-	-	-	Yes
□	System Resources	CPU Utilization Percentage >= 20% for 15 minutes	Email	-	● Critical	-	-	-	-	Yes

8 Triggers

Interface and Radio Triggers

To set a trigger for interfaces and radios on monitored devices, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the interface or radio triggers described in Table 122.

For more information on creating a new trigger, see "Creating New Triggers" on page 267.

Table 122: *Interface and Radio Triggers*

Name	Description and Conditions
Radio Down	Indicates that a device’s radio is down on the network. Once you choose this trigger type, select **Add New Trigger Condition** to create at least one condition. **This type** requires that a radio capability be set as a condition. The **Value** drop-down menu supports several condition options.
Radio Up	Indicates that a device’s radio is up on the network. Once you choose this trigger type, select **Add New Trigger Condition** to create at least one condition. **This type** requires that a radio capability be set as a condition. The **Value** drop-down menu supports several condition options.
802.11 Frame Counters	Enables monitoring of traffic levels. There are multiple rate-related parameters for which you define conditions including ACK Failures, Retry Rate, and Rx Fragment Rate. See the **Option** drop-down menu in the **Conditions** section of the trigger page for a complete list of parameters. Select **Add New Trigger Condition** to access these settings. Define at least one condition for this trigger type.
802.11 QoS Counters	Enables monitoring of Quality of Service (QoS) parameters on the network, according to traffic type. The rate of different parameters includes ACK Failures, Duplicated Frames and Transmitted Fragments. See the drop-down field menu in the conditions section of the trigger page for a complete list of parameters. Select **Add New Trigger Condition** to access these settings. Define at least one condition for this trigger type.
Interface Usage	Interface labels defined on the trigger page will be used to set up triggers on one or more interfaces and/or radios. Available conditions are **Device Type**, **Interface Description**, **Interface Label**, **Interface Mode**, **Interface Speed In (Mbps)**, **Interface Speed Out (Mbps)**, **Interface Type**, and **Radio Type**.
Interface Errors	Indicates that errors have occurred while transmitting and receiving traffic over the selected interface, device, or interface label. Available conditions are **Device Type**, **Interface Errors Combined (%)**, **Interface Errors In (%)**, **Interface Errors Out (%)**, **Interface Label**, **Interface Mode**, **Interface Name**, and **Interface Type**. For information about creating these triggers, see "Triggers for Interface Errors" on page 272.
Channel Utilization	Indicates that channel utilization has crossed particular thresholds. Available conditions are **Interference (%)**, **Radio Type**, **Time Busy (%)**, **Time Receiving (%)**, and **Time Transmitting (%)**.
Radio Noise Floor	Indicates that the Noise Floor dBM has exceeded a certain value for a specified period of time.

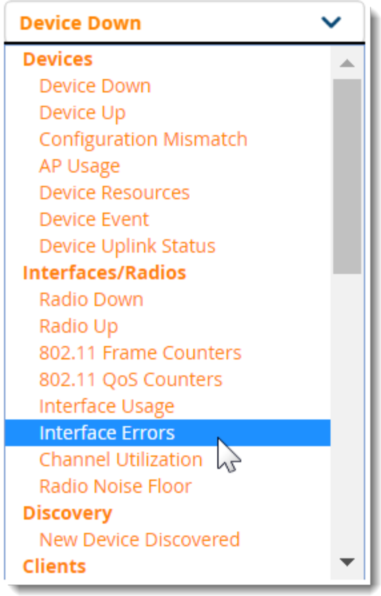
Triggers for Interface Errors

You can create alerts to help you monitor interface errors by setting criticial thresholds depending on the interface type.

To create a trigger for interface errors:

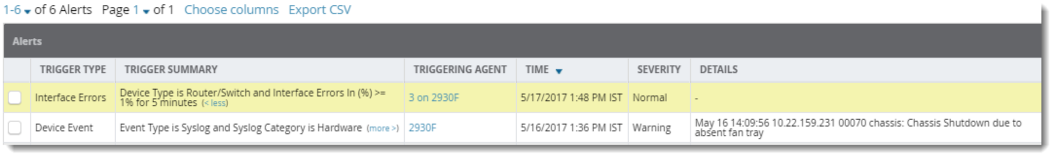
1. Navigate to **System > Triggers**, select **Interface Errors** from the list, as shown in Figure 189.

Figure 189: *Selecting the Interface Error Trigger*



2. Apply match conditions. Figure 190 shows an alert for a switch interface that is showing 1% or more input errors for 5 minutes.

Figure 190: *Interface Errors Trigger*



1-6 of 6 Alerts Page 1 of 1 Choose columns Export CSV

Alerts

	TRIGGER TYPE	TRIGGER SUMMARY	TRIGGERING AGENT	TIME	SEVERITY	DETAILS
□	Interface Errors	Device Type is Router/Switch and Interface Errors In (%) >= 1% for 5 minutes (< less)	3 on 2930F	5/17/2017 1:48 PM IST	Normal	-
□	Device Event	Event Type is Syslog and Syslog Category is Hardware (more >)	2930F	5/16/2017 1:36 PM IST	Warning	May 16 14:09:56 10.22.159.231 00070 chassis: Chassis Shutdown due to absent fan tray

Discovery Trigger

To set a discovery trigger, click the **Type** drop-down list on the **System** > **Triggers** > **Add** page and select the New Device Discovered trigger. Table 123 describes the trigger.

For more information on creating a new trigger, see "Creating New Triggers" on page 267.

Table 123: *Discovery Trigger*

Name	Description and Conditions
New Device Discovered	This trigger type flags the discovery of a new AP, router, or switch connected to the network (an device that OV3600 can monitor and configure). Once you choose this trigger type, select **Add New Trigger Condition** to specify a **Device Type** (Access Point, Controller, Remote AP, or Router/Switch)

Client Triggers

To set a user-related trigger for clients, click the **Type** drop-down list on the **System** > **Triggers** > **Add** page and select one of the client triggers described in Table 124.

For more information on creating a new trigger, see "Creating New Triggers" on page 267.

Table 124: *Client Triggers*

Name	Description and Conditions
New Client	This trigger type indicates a new user has associated to a device within a defined set of groups or folders. A Filter on connection mode field appears to allow you to filter by **Wired** or **Wireless** clients. Note that the **New Client** trigger type does not require the configuration of any condition settings, so the **Condition** section disappears.
Connected Clients	This trigger type indicates a device (based on an input list of MAC addresses) has associated to the wireless network. It is required to define one or more MAC addresses with the field that appears.
Client Count	Activates when a device, Radio/Interface, or BSSID reaches a user-count threshold for more than a specified period (such as more than 10 users associated for more than 60 seconds).
Client Usage	This trigger type indicates that the sustained rate of bandwidth used by an individual user has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 1500 Kbps for more than 120 seconds). Once you choose this trigger type, select **Add New Trigger Condition** to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger. The **Value** field requires that you input a numerical figure for kilobits per second (Kbps).
New VPN User	This trigger type indicates a new VPN user has associated to a device within a defined set of groups or folders. Note that the **New VPN User** trigger type does not require the configuration of any condition settings, so the **Condition** section disappears.
Connected VPN Users	This trigger type indicates a VPN device (based on an input list of MAC addresses) has associated to the VPN network. It is required to define one or more VPN user names with the field that appears.
VPN Session Usage	This trigger type indicates that the sustained rate of bandwidth used in an individual VPN session has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 1500 Kbps for more than 120 seconds). Once you choose this trigger type, select **Add New Trigger Condition** to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger. The **Value** field requires that you input a numerical figure for kilobits per second (Kbps).
Inactive Tag	This trigger type flags events in which an RFID tag has not been reported back to OV3600 by a controller for more than a certain number of hours. This trigger can be used to help identify inventory that might be lost or stolen. Set the time duration for this trigger type if not already completed.
IPv4 Link-Local Addresses	When enabled, this trigger checks whether the total count of self-assigned IP addresses has crossed a set threshold for clients within a selected folder or group. The alert deployed by this trigger includes a link to search for IP addresses containing 169.254.x.x.
Client Goodput	This trigger type indicates that the goodput for an individual client has exceeded a predefined threshold. Available conditions are Usage Kbps (combined), Usage Kbps (in), and Usage Kbps (out).

Table 124: *Client Triggers (Continued)*

Name	Description and Conditions
Client Speed	This trigger type indicates that the speed for an individual client has exceeded a predefined threshold. The available condition for this trigger is Speed Mbps.

RADIUS Authentication Triggers

To set a trigger for RADIUS authentication issues, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the RADIUS authentication triggers described in Table 125.

For more information on creating a new trigger, see "Creating New Triggers" on page 267.

Table 125: *RADIUS Authentication Triggers*

Name	Description and Conditions
Client RADIUS Authentication Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a user. The **Option**, **Condition**, and **Value** fields allow you to define the number of authentication issues per client that will trigger an issue.
Device RADIUS Authentication Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a device. The **Option**, **Condition**, and **Value** fields allow you to define the number of authentication issues per device that will trigger an issue.
Total RADIUS Authentication Issues	This trigger sets the threshold for the maximum number of failures before an alert is issued for both users and devices.

RADIUS Accounting Triggers

To set a trigger for RADIUS accounting issues, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the RADIUS accounting triggers described in Table 126.

For more information on creating a new trigger, see "Creating New Triggers" on page 267.

Table 126: *RADIUS Authentication Triggers*

Name	Description and Conditions
Client RADIUS Accounting Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a user. The **Option**, **Condition**, and **Value** fields allow you to define the number of accounting issues per client that will trigger an issue.
Device RADIUS Accounting Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a device. The **Option**, **Condition**, and **Value** fields allow you to define the number of accounting issues per device that will trigger an issue.
Total RADIUS Accounting Issues	This trigger sets the threshold for the maximum number of failures before an alert is issued for both users and devices.

IDS Event Triggers

To set a trigger for Intrusion Detection System (IDS) events, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the IDS event triggers described in Table 127.

For more information on creating a new trigger, see "Creating New Triggers" on page 267.

Table 127: *IDS Event Triggers*

Name	Description and Conditions
Device IDS Events	This trigger type is based on the number of IDS events has exceeded the threshold specified as Count in the Condition within the period of time specified in seconds in Duration. Alerts can also be generated for traps based on name, category or severity. Select **Add New Trigger Condition**to specify the count characteristics that trigger an IDS alert.
Rogue Device Classified	This trigger type indicates that a device has been discovered with the specified Rogue Score. Ad-hoc devices can be excluded automatically from this trigger by selecting **Yes**. See "Using RAPIDS" on page 243 for more information on score definitions and discovery methods. Once you choose this trigger type, select **Add New Trigger Condition** to create one or more conditions. A condition for this trigger enables you to specify the nature of the rogue device in multiple ways.
Client on Rogue AP	This trigger type indicates that a client has associated to a rogue AP. Available conditions include rogue classification, and whether the client is valid.

Health Triggers

To set a trigger for OV3600 server health issues, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the health triggers described in Table 128.

For more information on creating a new trigger, see "Creating New Triggers" on page 267.

Table 128: *Health Triggers*

Name	Description and Conditions
Disk Usage	This trigger type is based on the disk usage of OV3600. This type of trigger indicates that disk usage for the OV3600 server has met or surpassed a defined threshold. Select **Add New Trigger Condition** to specify the disk usage characteristics that trigger an alert. Set one of these triggers at **90%** so you receive a warning before OV3600 suffers performance degradation due to lack of disk space.
System Resources	For the System Resources trigger, you must configure at least one matching condition before you save the new trigger. The available matching conditions are **CPU Utilization Percentage**, **Disk I/O Utilization Percentage**, and **Memory Utilization Percentage**.

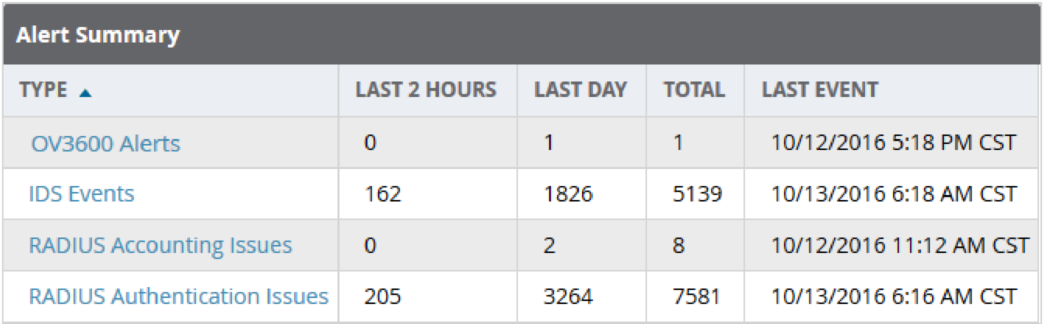
About Alerts

OV3600 displays summary information about alerts, including the alert type and how many times an event occurred over the past 2 hours and the last 24 hours, in table that is available from the following WebUI pages:

- **Devices > List**
- **Devices > Monitor**
- **Groups > Monitor**
- **Home > Overview**
- **Clients > Connected or Client Detail**
- **System > Alerts** . For more information, see "Viewing System Alerts" on page 277.

When you click the hyperlinks in the **Type** column, a detailed view for the selected type of alert opens.

Figure 191: *Alert Summary*



Alert Summary

TYPE ▲	LAST 2 HOURS	LAST DAY	TOTAL	LAST EVENT
OV3600 Alerts	0	1	1	10/12/2016 5:18 PM CST
IDS Events	162	1826	5139	10/13/2016 6:18 AM CST
RADIUS Accounting Issues	0	2	8	10/12/2016 11:12 AM CST
RADIUS Authentication Issues	205	3264	7581	10/13/2016 6:16 AM CST

Information about **AMP Alerts** include:

- Trigger Type: Name of the OV3600 Alert trigger
- Trigger Summary: Description of the OV3600 Alert trigger
- Triggering Agent: MAC address of the device that triggered the alert
- Severity: Alert severity level
- Time: Timestamp for the alert

Information about **IDS Events** include:

- Severity: Event severity level
- Category: IDS category for the event
- Scope: Indicates of the scope of the IDS event impacts an *AP*, *Client or AP*, *Client* or *Probe*.
- Attack: Name of the IDS Event
- Detail: Details about the IDS Event type, if available
- Attacker: MAC address of the device that triggered the IDS event
- Target: MAC address of the device that was the target of the IDS attack
- Time: Timestamp for the event

Information about **RADIUS Accounting Issues** and **RADIUS Authentication Issues** include:

- Event: Name of the RADIUS event
- Username: user name of the device that triggered the event
- Client MAC Address: MAC address of the client that triggered the event
- Client IP address: IP address of the client that triggered the event
- AP/Device: AP or device to which the client is associated
- BSSID: BSSID of the AP radio
- Radio: PHY type of the AP radio (e.g., 802.11a, 802.11ac, etc.)
- switch: Name of the switch to which the device is associated
- RADIUS Server/RADIUS IP: Server name and IP address of the RADIUS server
- Time: Timestamp for the event

Viewing System Alerts

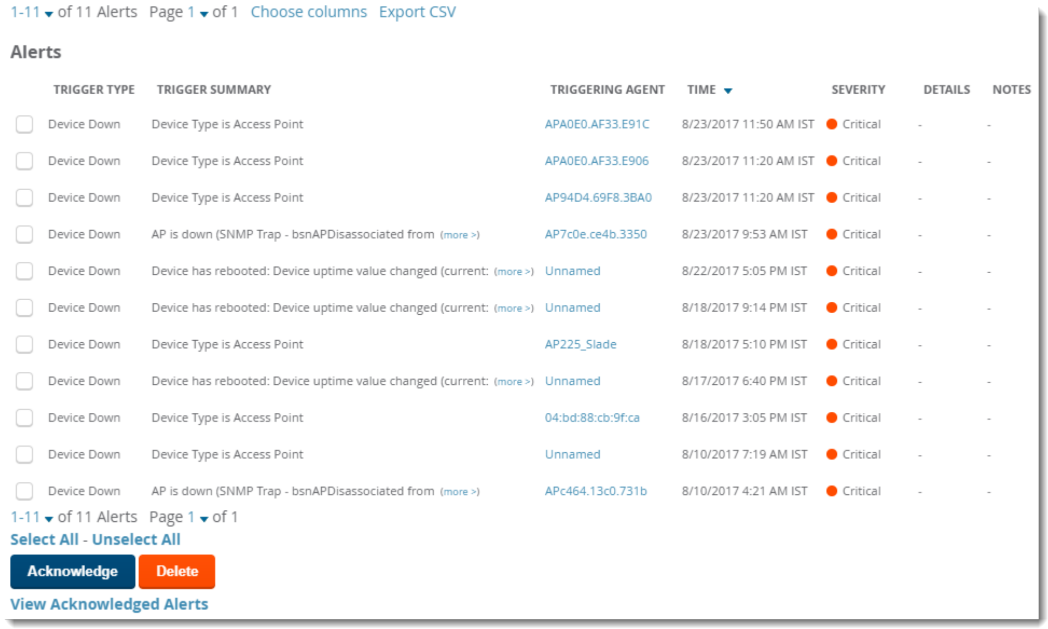
The top header of each OV3600 WebUI page provides direct links to alerts and severe alerts. You can also navigate to **System > Alerts** to view these alerts and acknowledge or delete them.

You can identify alerts by color-coded icons. For example, alerts with high severity are red and warnings are blue. shows critical alerts colored orange.

NOTE

For information about setting the severe alert threshold, see "Setting Severe Alert Warning Behavior" on page 311.

Figure 192: *System Alerts Page*



1-11 ▾ of 11 Alerts Page 1 ▾ of 1 Choose columns Export CSV

Alerts

	TRIGGER TYPE	TRIGGER SUMMARY	TRIGGERING AGENT	TIME ▾	SEVERITY	DETAILS	NOTES
□	Device Down	Device Type is Access Point	APA0E0.AF33.E91C	8/23/2017 11:50 AM IST	● Critical	-	-
□	Device Down	Device Type is Access Point	APA0E0.AF33.E906	8/23/2017 11:20 AM IST	● Critical	-	-
□	Device Down	Device Type is Access Point	AP94D4.69F8.3BA0	8/23/2017 11:20 AM IST	● Critical	-	-
□	Device Down	AP is down (SNMP Trap - bsnAPDisassociated from (more >)	AP7c0e.ce4b.3350	8/23/2017 9:53 AM IST	● Critical	-	-
□	Device Down	Device has rebooted: Device uptime value changed (current: (more >)	Unnamed	8/22/2017 5:05 PM IST	● Critical	-	-
□	Device Down	Device has rebooted: Device uptime value changed (current: (more >)	Unnamed	8/18/2017 9:14 PM IST	● Critical	-	-
□	Device Down	Device Type is Access Point	AP225_Slade	8/18/2017 5:10 PM IST	● Critical	-	-
□	Device Down	Device has rebooted: Device uptime value changed (current: (more >)	Unnamed	8/17/2017 6:40 PM IST	● Critical	-	-
□	Device Down	Device Type is Access Point	04:bd:88:cb:9f:ca	8/16/2017 3:05 PM IST	● Critical	-	-
□	Device Down	Device Type is Access Point	Unnamed	8/10/2017 7:19 AM IST	● Critical	-	-
□	Device Down	AP is down (SNMP Trap - bsnAPDisassociated from (more >)	APc464.13c0.731b	8/10/2017 4:21 AM IST	● Critical	-	-

1-11 ▾ of 11 Alerts Page 1 ▾ of 1

The **System > Alerts** page displays the information described in Table 129.

Table 129: *System > Alerts Fields and Default Settings*

Field	Description
Trigger Type	Displays and sorts triggers by the type of trigger.
Trigger Summary	Provides an additional summary information related to the trigger.
Triggering Agent	Lists the name of the AP that generated the trigger. Select the name to display its **Devices > Manage** page.
Time	Displays the date and time the trigger was generated.
Severity	Displays the severity code associated with that trigger
Details	Displays additional details for alerts.
Notes	Displays any notes that you have added.

Delivering Triggered Alerts

OV3600 uses Postfix to deliver alerts and reports via email because it provides a high level of security and queues email locally until delivery. If OV3600 is located behind a firewall, preventing it from sending email directly to a specified recipient, use the following procedures to forward email to a smarthost.

1. Add the following line to /etc/postfix/main.cf:

   ```
   relayhost = [mail.example.com]
   ```

   where mail.example.com is the IP address or hostname of your smarthost

2. Run `service postfix restart`.

3. Send a test message to an email address:

```
Mail -v user@example.com
Subject: test mail
.
CC:
```

4. Press **Enter**.
5. Check the mail log to ensure mail was sent:

```
tail -f /var/log/maillog
```

Responding to Alerts

Once you have viewed an alert, you may take one of the following courses of action:

- Leave it in active status if it is unresolved. The alert remains on the **New Alerts** list until you acknowledge or delete it. If an alert already exists, the trigger for that AP or user does not create another alert until the existing alert has been acknowledged or deleted.
- Move the alert to the Alert Log by selecting it and selecting **Acknowledge**. You can see all logged alerts by selecting the **View logged alerts** link at the top of the **System > Alerts** page. Select the **Alerts** link to return to the list of new alerts.
- Delete the alert by selecting it from the list and clicking the **Delete** button.

Backing Up Your Data

OV3600 creates nightly archives of all relational data, statistical data, and log files. This occurs by default at 4:15 AM, but is configurable on the **OV3600 Setup > General** page under **Nightly Maintenance Time**.

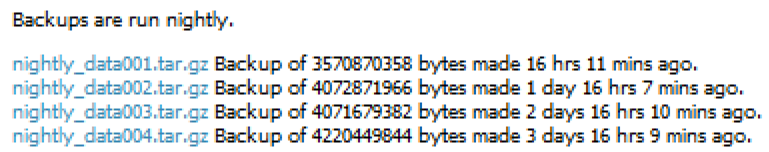
Although OV3600 only keeps the last four sets of archives, the archives can be downloaded manually or automatically off-site for more extensive backup strategies. OV3600 creates one data backup file each night. The data backup file contains all of the device and group information as well as historical data and system files, including IP address, NTP information, mail relay hosts, and other OV3600 settings.

For information about running a backup and restoring from a backup, see "AMP Command Line Interface" on page 396.

Viewing and Downloading Backups

To view current OV3600 backup files, go to the **System > Backups** page. Figure 193 illustrates this page.

Figure 193: *System > Backups* *Page Illustration*



Backups are run nightly.

nightly_data001.tar.gz Backup of 3570870358 bytes made 16 hrs 11 mins ago.
nightly_data002.tar.gz Backup of 4072871966 bytes made 1 day 16 hrs 7 mins ago.
nightly_data003.tar.gz Backup of 4071679382 bytes made 2 days 16 hrs 10 mins ago.
nightly_data004.tar.gz Backup of 4220449844 bytes made 3 days 16 hrs 9 mins ago.

To download a backup file, select the filename URL and the **File Download** pop up page appears.

Regularly save the data backup file to another machine or media. This process can be automated easily with a nightly script.

NOTE

Nightly maintenance and ov3600_backup scripts back up the full OV3600 data and save the file as nightly_data00[1-4].tar.gz. In previous OV3600 versions, the scripts created both config backup and data backup files. In order to restore the OV3600 data, it is only necessary to have most recent data backup file, and OV3600 no longer uses or supports the config backup file, effective as of OV3600 6.3.2.

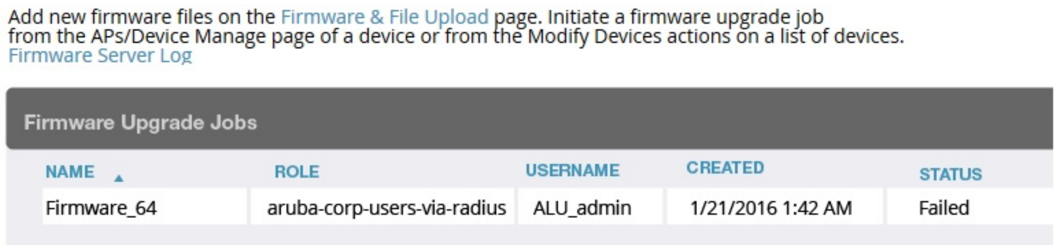
Using the System > Firmware Upgrade Jobs Page

The **System > Firmware Upgrade Jobs** page displays a list of recent firmware upgrade jobs that have been initiated in the **Devices > Manage** page or **Modify Devices** page for a controller or autonomous AP that supports firmware upgrades in OV3600.

Successful upgrade jobs are not archived on this page -- generally you visit this page to review failed or pending firmware upgrade jobs.

Users with the **AP/Device Manager** role and higher can view this page. Audit-only users cannot view this page or tab.

Figure 194: *System > Firmware Upgrade Jobs Page Illustration*



Add new firmware files on the Firmware & File Upload page. Initiate a firmware upgrade job from the APs/Device Manage page of a device or from the Modify Devices actions on a list of devices.
Firmware Server Log

Firmware Upgrade Jobs

NAME ▲	ROLE	USERNAME	CREATED	STATUS
Firmware_64	aruba-corp-users-via-radius	ALU_admin	1/21/2016 1:42 AM	Failed

You can perform the following operations on this page:

- To restart failed firmware upgrade jobs, select the check boxes next to the rows you want to restart and select the **Restart Failed Jobs** button.
- To stop a pending upgrade job and remove it from the list, select the **Cancel and Delete Jobs** button.
- Use additional links on the page as shortcuts to the **Device Setup > Upload Firmware & Files** page, or the complete raw text of the Firmware Server Log
- To view additional details about an individual upgrade job including the devices being upgraded, select the name of an upgrade job from the Name column to go to the **System > Firmware Upgrade Job Detail** page, illustrated in .

  From here you can click the device name to go to its **Devices > Monitor** page, or the link under **Firmware File** column to go to the **Device Setup > Upload Firmware & Files** page.

Refer also to "Uploading Firmware and Files" on page 55.

Using the System > Configuration Change Jobs Page

Schedule configuration change jobs are summarized in the **Scheduled Events** table on the **System > Configuration Change Jobs** page, illustrated in Figure 195. Select a AP or group in the **Device** or **Group** columns in this table to go to the monitoring page for that device or group. Select a folder in the **Folder** columns to go to the **AP's/Devices > List** page for that folder.

To edit an existing configuration change job:

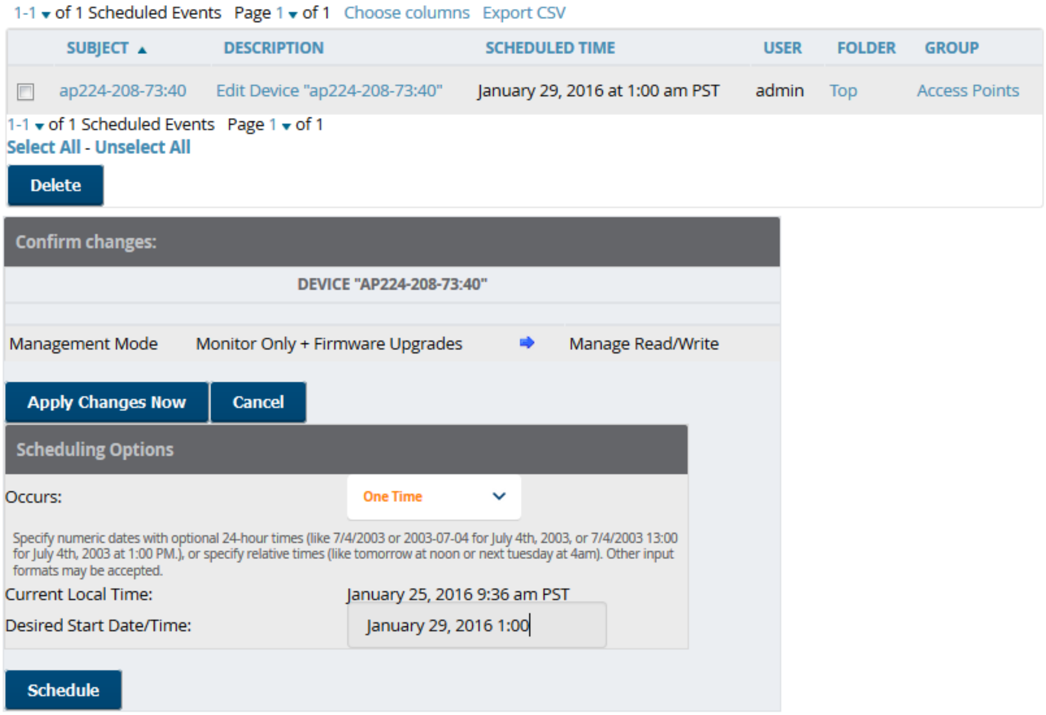
1. Click the description of a change job in the **Description** column of the **Scheduled Events** table. The **System > Configuration Change Job Detail** window opens.
2. On the **System > Configuration Change Job Detail** window you can choose to run the job immediately by selecting **Apply Changes Now**, to reschedule the job by selecting **Schedule**, **Delete** the job, or **Cancel** the job edit.

Select the linked AP or group name under the **Subject** column to go to its monitoring page.

3. Select the linked group and folder names under **Folder** or **Group** to go to the AP's folder or group page.

4. Scheduled configuration change jobs will also appear on the **Manage** page for an AP or the **Monitoring** page for a group.

Figure 195: *System > Configuration Change Jobs and System > Configuration Change Jobs Detail*



1-1 ▾ of 1 Scheduled Events Page 1 ▾ of 1 Choose columns Export CSV

	SUBJECT ▲	DESCRIPTION	SCHEDULED TIME	USER	FOLDER	GROUP
□	ap224-208-73:40	Edit Device "ap224-208-73:40"	January 29, 2016 at 1:00 am PST	admin	Top	Access Points

1-1 ▾ of 1 Scheduled Events Page 1 ▾ of 1

Select All - Unselect All

Confirm changes:

DEVICE "AP224-208-73:40"

Management Mode	Monitor Only + Firmware Upgrades	➡	Manage Read/Write

Scheduling Options

Occurs: One Time

Specify numeric dates with optional 24-hour times (like 7/4/2003 or 2003-07-04 for July 4th, 2003, or 7/4/2003 13:00 for July 4th, 2003 at 1:00 PM.), or specify relative times (like tomorrow at noon or next tuesday at 4am). Other input formats may be accepted.

Current Local Time: January 25, 2016 9:36 am PST

Desired Start Date/Time: January 29, 2016 1:00

Using the System > Performance Page

The **System > Performance** page displays basic OV3600 hardware information as well as resource usage over time. OV3600 logs performance statistics such as load average, memory and swap data every minute.

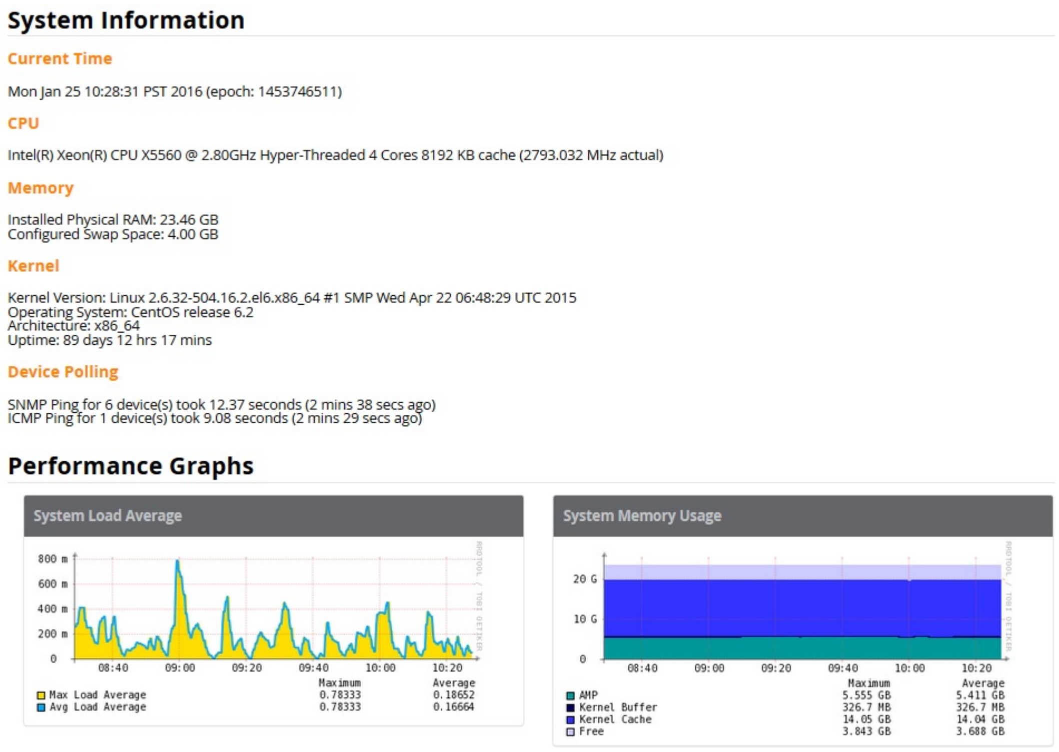
The historical logging is useful to determine the best usable polling period and track the health of OV3600 over time.

The page is divided into the following sections:

- System Information
- Performance Graphs
- AMON Statistics
- Redis Statistics
- Database Statistics
- Disk Space

Figure 196 illustrates this page, and Table 130 describes fields and information displayed.

Figure 196: *System > Performance Page Illustration (Partial Screen)*



System Information

Current Time

Mon Jan 25 10:28:31 PST 2016 (epoch: 1453746511)

CPU

Intel(R) Xeon(R) CPU X5560 @ 2.80GHz Hyper-Threaded 4 Cores 8192 KB cache (2793.032 MHz actual)

Memory

Installed Physical RAM: 23.46 GB
Configured Swap Space: 4.00 GB

Kernel

Kernel Version: Linux 2.6.32-504.16.2.el6.x86_64 #1 SMP Wed Apr 22 06:48:29 UTC 2015
Operating System: CentOS release 6.2
Architecture: x86_64
Uptime: 89 days 12 hrs 17 mins

Device Polling

SNMP Ping for 6 device(s) took 12.37 seconds (2 mins 38 secs ago)
ICMP Ping for 1 device(s) took 9.08 seconds (2 mins 29 secs ago)

Performance Graphs

System Load Average

```
                      Maximum    Average
■ Max Load Average    0.78333    0.18652
■ Avg Load Average    0.78333    0.16664
```

System Memory Usage

```
                      Maximum    Average
■ AMP                 5.555 GB   5.411 GB
■ Kernel Buffer       326.7 MB   326.7 MB
■ Kernel Cache        14.05 GB   14.04 GB
□ Free                3.843 GB   3.688 GB
```

Table 130: *System > Performance Page Fields and Graphs*

Field	Description
System Information	
Current Time	Displays the current time on the OV3600 server.
CPU(s)	Basic CPU information as reported by the operating system.
Memory	The amount of physical RAM and Swap space seen by the operating system. Refer to the *OmniVista 3600 Air Manager Server Sizing Guide* for hardware requirements.
Kernel	The version of the Linux kernel running on the box.
Device Polling	Displays some AP/Device polling statistics.
Performance Graphs	
System Load Average	The number of jobs currently waiting to be processed. Load is a rough metric that will tell you how busy a server is. A typical OV3600 load is around 2-3 times the number of CPU cores you have in your system. A constant load of 4x to 5x is cause for concern. A load above 6x is a serious issue and will probably result in OV3600 becoming unusable. To lower the load average, try increasing a few polling periods in the **Groups > Basic** page.

Table 130: *System > Performance Page Fields and Graphs (Continued)*

Field	Description
System Memory Usage	The amount of RAM that is currently used broken down by usage. It is normal for OV3600 to have very little free RAM. Linux automatically allocates all free RAM as cache and buffer. If the kernel needs additional RAM for process it will dynamically take it from the cache and buffer.
System Disk Throughput	The rate of reading and writing from and to the disk in bytes per second.
System Swap Usage	The amount of Swap memory used by OV3600. Swap is used when there is no more free physical RAM. A large performance penalty is paid when swap is used. If your OV3600 consistently uses swap, you should consider installing additional RAM.
System Disk IOPs	The number of disk reads and writes per second.
System Disk Outstanding I/O Requests	The average number of outstanding I/O requests (queue depth). If it's high, it means that I/O requests (disk reads/writes) aren't being serviced as fast as they're being asked for.
System Disk Utilization	The amount of data read from the disk and written to the disk.
System CPU Utilization	The percentage of CPU that has been used by the user and the system as well as the amount that was idle.
Process Counts by Service	This breaks down network usage based on Web server, database, OV3600 Service, and VisualRF processes.
Average Delay Time by Queue Type	This shows the queue time for Async logger clients and RAPIDS processing.
I/O Throughput by Worker/by Service	Displays reads and writes for workers (OV3600 services, database, VisualRF, web server, RRD tool and AWRRD tool) and for services (OV3600, VisualRF and web server).
CPU Utilization by Worker/by Service	Displays reads and writes for workers (OV3600 services, database, VisualRF, web server, RRD tool and AWRRD tool) and for services (OV3600, VisualRF and web server).
System Network Usage	All traffic in and out measured in bits per second of your primary network interface (Eth0 being the most common).
Usage by Protocol	Displays the amount of traffic used by Telnet, HTTPS and SNMP used by your primary network interface (Eth0 being the most common).
AMON	Displays the number of AMON packet traffic used by your network over the last two hours, day, week, month, and year.
SNMP Traps	Displays the number of SNMP Trap packets in your network over the last two hours, day, week, month, and year

Table 130: *System > Performance Page Fields and Graphs (Continued)*

Field	Description
Legacy SNMP Fetcher Requests	The number of SNMP get and walk requests per second performed by the legacy (v1 and v3) SNMP fetcher.
Legacy SNMP Fetcher Responses	The number of SNMP OIDs received per second performed by the legacy (v1 and v3) SNMP fetcher.
High Performance SNMP Fetcher Requests	The number of SNMP get and walk requests per second performed by the high performance SNMP (v2c) fetcher.
High Performance SNMP Fetcher Responses	The number of SNMP OIDs received per second performed by the high performance SNMP (v2c) fetcher.
Redis Statistics	
Redis Activity	Use this chart under the supervision of Alcatel-Lucent support to troubleshoot Redis activity. Click any point in the chart to view Redis activity over the past day, week, month or year.
Redis Used Memory	Use this chart under the supervision of Alcatel-Lucent support to troubleshoot Redis memory issues. Click any point in the chart to view the total number of bytes used by the Redis process over the past day, week, month or year.
Redis Keyspace	Use this chart under the supervision of Alcatel-Lucent support to troubleshoot Redis keys. Click any point in the chart to view Redis Key usage over the past day, week, month or year.
Database Statistics	
Top 5 Tables (by row count)	The five largest tables in OV3600. Degraded performance has been noticed for in some cases for tables over 200,000 rows. Decreasing the length of time client data is stored on the OV3600 page is recommended if a user/client table exceeds 250,000 rows.
Database Table Scans	The number of database table scans performed by the database.
Database Row Activity	The number of insertions, deletions and updates performed to the database.
Database Transaction Activity	The number of commits and rollbacks performed by the database.
Disk Space	
Disk Space	Pie charts that display the amount of used and free hard drive space for each partition. If a drive reaches over 80% full, you may want to lower the **Historical Data Retention** settings on the **OV3600 Setup > General** page or consider additional drive space.

There are several initial steps that you can take to troubleshoot OV3600 performance problems, including slow page loads and timeout errors. Initial troubleshooting steps would include the following:

- Increasing the polling period settings on the **Groups > Basic** page.
- Increasing the polling period time for groups with routers and switches.

- Adding additional memory to the server. Please consult the sizing information in the latest edition of the *OmniVista 3600 Air Manager Server Sizing Guide* or contact Alcatel-Lucent support for the latest recommendations.

Managing Mobile Devices with SOTI MobiControl and OV3600

Overview of SOTI MobiControl

SOTI MobiControl, the mobile device management platform for Windows Mobile, Apple, and Android devices, has been integrated into OV3600 to provide direct access to the MobiControl Web Console.

MobiControl runs on your Mobile Device Manager (MDM) server. This server provisions mobile devices to configure connectivity settings, enforce security policies, restore lost data, and other administrative services. Information gathered from mobile devices can include policy breaches, data consumption, and existing configuration settings.

Refer to the following for additional information:

- "Prerequisites for Using MobiControl with OV3600" on page 285
- "Adding a Mobile Device Management Server for MobiControl" on page 285
- "Accessing MobiControl from the Clients > Client Detail Page " on page 286

Prerequisites for Using MobiControl with OV3600

In order to use the MobiControl integration in OV3600, the following is required:

- An OV3600 running version 7.2.3 or later
- An MDM server with SOTI MobiControl Console 8.0x
- A client device that is:
  - associated with WLAN infrastructure managed by the OV3600 server running 7.2.3 or later
  - being actively managed by the SOTI MobiControl server

For more information about setting up MobiControl, please see http://www.soti.net/mc/help/.

In order to use SOTI MobiControl from within OV3600, you must first add your MDM server and designate it as a MobiControl.

Adding a Mobile Device Management Server for MobiControl

1. To add an MDM server to OV3600, navigate to **OV3600 Setup > MDM Server** and click **Add**. Complete the fields on this page. Table 131 describes the settings and default values:

Table 131: *OV3600 Setup > MDM Server > Add Fields and Descriptions*

Field	Description
Hostname/IP Address	The address or DNS hostname configured for your MobiControl Web Console.
Protocol	Whether HTTP or HTTPS is to be used when polling the MDM server. The port on which to connect to the MDM server is inferred from the protocol: with HTTP, OV3600 will connect to port 80 of the SOTI server; with HTTPS, OV3600 will connect to port 443.

Table 131: *OV3600 Setup > MDM Server > Add Fields and Descriptions (Continued)*

Field	Description
URL Context	The URL context appended to the server URL to build the URL when connecting with the SOTI server. For MobiControl v8.0x the default URL Context is MobiControlWeb. For MobiControl v8.5x the default URL Context is MobiControl.
Enabled	Whether this server can be polled by OV3600. Make sure it is set to **Yes**.
Username/Password	The login credentials for accessing the web console of the MobiControl system.
Polling Period	The frequency in which OV3600 polls the MDM server. The default is 5 minutes.

2. When finished, select **Add.**

The list page for the MDM server also displays:

- **Last Contacted –** The last time OV3600 was able to contact the MDM server.
- **Errors** – Issues, if any, encountered during the last contact.

During each polling period, OV3600 will obtain a list of all device IDs and their WLAN MAC addresses. The information about device OS, device OS Detail, Manufacturer, Model, Name are retrieved from MobiControl and populated to the **Clients > Client Detail** page for supported mobile devices. A **View device in SOTI MobiControl** link provides direct access to the MobiControl Web Console for additional details about the device. MobiControl information overrides data obtained from AOS-W switches running 6.0 or later.

Accessing MobiControl from the Clients > Client Detail Page

In order to access the MobiControl web console for a SOTI-managed mobile device from within OV3600, follow these steps:

1. Navigate to a page that lists clients. This can include:
   - **Clients > Connected** or **Clients > All**
   - Search results that display user MAC addresses
2. Select the MAC address in the **Clients** list table. The **Clients > Client Detail** page displays.
3. Under the Classification field, select the **View device in SOTI MobiControl** link. A new window will display the MobiControl Web Console for this device.

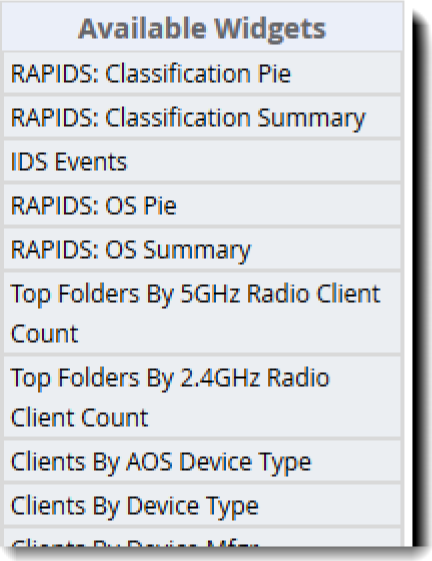
About the Home Page

The **Home** page provides access to customizable dashboards, where you can monitor the health of your network services, mobile app usage, RF issues, UCC traffic, application traffic, Clarity data, and the topology map. It is also where you can access product documentation, manage OV3600 licenses, and customize your user information and search preferences.

Customizing the Dashboard

You can customize the dashboard so you see only what you want in your reports with widgets. Figure 197 shows an example of available widgets that you can use.

Figure 197: *Example of Some Available Widgets*



Available Widgets

RAPIDS: Classification Pie

RAPIDS: Classification Summary

IDS Events

RAPIDS: OS Pie

RAPIDS: OS Summary

Top Folders By 5GHz Radio Client Count

Top Folders By 2.4GHz Radio Client Count

Clients By AOS Device Type

Clients By Device Type

To customize the dashboard:

1. Navigate to **Home > Overview**, then click ⚙ at the upper-right corner of the page.
2. Drag and drop widgets from the **Available Widgets** list and an open space on the dashboard within gridlines. The widget label turns orange if you place it over occupied space.
3. Click **Save**.

Available Widgets

When a widget is enabled, the information that displays can vary based on the user's permission level. Certain roles can limit the top folder that a user sees.

Table 132 describes all the widgets.

Table 132: *Available Widgets*

Widget	Description
Client/Usage Graphs	The **Client** graph is enabled by default and, by default, shows the maximum number of attached clients over the last two hours. Select the **Show All** link to view more specific client information on the graph, such as the total and average clients for a specific SSID, the maximum VPN sessions, etc. The available check boxes within this graph are determined by the SSIDs that OV3600 is aware of from polling the device. The **Usage** graph is enabled by default and, by default, shows the average bits-per-second in/out information and average VPN in/out information. Select the **Show All** link to view usage information for specific SSIDs. The available checkboxes within this graph are determined by the SSIDs that OV3600 is aware of from polling the device. The information in these graphs is color coded to match the selected check boxes.

Table 132: *Available Widgets (Continued)*

Widget	Description
Monitoring and Configuration Pie Charts	The **Monitoring Status** pie chart shows the percentage of total devices that are up and the number and percentage of devices that are currently down. Clicking within this pie chart takes you to the **Devices > Down** page. The **Configuration Compliance** pie chart shows the percentage of devices that are mismatched, good, unknown, and those with auditing disabled. It also provides a summary of the total number of devices that are mismatched. Clicking within this pie chart takes you to the **Devices > Mismatch** page. These pie charts are enabled by default.
Alert Summary	The **Alert Summary** table is enabled by default and provides the number of OV3600 alerts, IDS events, and RADIUS authentication issues over the last 2 hours, the last 24 hours, and the total since the last OV3600 server reboot. ● Click on **OV3600Alerts** to drill down to more detailed alert information. This information displays in the current page. You can return to the **Alert Summary** graph by selecting the **Home Overview** link. ● Click on **IDS Events** to drill to more detailed event information. This link takes you to the **RAPIDS > IDS Events** page. ● Click on **RADIUS Authentication Issues** to drill to more detailed RADIUS authentication information. This information displays in the current page. You can return to the **Alert Summary** graph by selecting the **Home Overview** link.
Quick Links	The **Quick Links** section is enabled by default. This section provides the user with easy navigation to a specific folder, group, report, or common task.
RAPIDS: Acknowledged	The **Acknowledged RAPIDS Devices** pie chart shows the percentage of acknowledged and unacknowledged RAPIDS that the user has visibility into. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Ignored rogues, however, are not included in this chart. This chart also displays on the **RAPIDS > Overview** page.
RAPIDS: Classification Pie	The **RAPIDS: Classification Pie** shows the percentage of devices classified as Valid, Suspected Neighbor, Suspected Valid, Suspected Rogue, Rogue, and Neighbor that are attached to OV3600. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Ignored rogues, however, are not included in this chart. This pie chart can also be viewed on the **RAPIDS > Overview** page.

Table 132: *Available Widgets (Continued)*

Widget	Description
RAPIDS: Classification Summary	The **RAPIDS: Classification Summary** table shows the number of devices classified as Valid, Suspected Valid, Neighbor, Suspected Neighbor, Suspected Rogue, Rogue, and Unclassified that are attached to OV3600. In addition, contained rogue information will appear if **Manage rogue AP containment** is set to **Yes** on the **RAPIDS > Setup** page. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Note that ignored rogues are not included in this chart. This table can also be viewed on the **RAPIDS > Overview** page.
IDS Events	The **IDS Events** table shows the number and type of attacks logged by the intrusion detection system over the last 2 hours, the last 24 hours, and the total since the last OV3600 server reboot. This is the same table that displays on the **RAPIDS > Overview** page.
RAPIDS: OS Pie	The **RAPIDS: OSPie** chart shows the top 9 rogue devices by OS, Others, Unknown, and Not Scanned. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Note that ignored rogues are not included in this chart. This pie chart can also be viewed on the **RAPIDS > Overview** page.
RAPIDS: OS Summary	The **RAPIDS: OS Summary** table shows the top 9 rogue devices by OS, Others, Unknown, and Not Scanned. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Note that ignored rogues are not included in this chart. This table can also be viewed on the **RAPIDS > Overview** page.
Top Folders By AP Usage	This chart lists the folders and the number of APs in each folder whose usage is greater than the cutoff (or usage threshold). The cutoff represents 75% of the maximum usage, where the maximum usage is the AP with the highest usage regardless of the folder in which it resides. The cutoff value is displayed within the title, and this value can vary. The chart takes into account approved APs with radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Folders By A Radio Channel Usage	This chart shows the folders and the number of 802.11a radios (5GHz) in each folder whose channel usage is greater than the cutoff (or usage threshold) as measured by Mbps. This cutoff is on the on the **OV3600 Setup > General** page using the **Configure Channel Busy Threshold** option. If this option is not configured, then the cutoff is 75% of the 'maximum,' where the 'maximum' refers to the AP that has the highest usage regardless of the folder in which it resides. The cutoff value is displayed within the title, and this value can vary. This chart takes into account approved APs with 'A' radios based on the last 24 hours. In addition, this chart is updated every hour.

Table 132: *Available Widgets (Continued)*

Widget	Description
Top Folders By BG Radio Channel Usage	This chart shows the folders and the number of 802.11b/g radios (2.4GHz) in each folder whose channel usage is greater than the cutoff (or usage threshold) as measured by Mbps. This cutoff is on the on the **OV3600 Setup > General** page using the **Configure Channel Busy Threshold** option. If this option is not configured, then the cutoff is 75% of the 'maximum,' where the 'maximum' refers to the AP that has the highest usage regardless of the folder in which it resides. The cutoff value is displayed within the title, and this value can vary. This chart takes into account approved APs with 'BG' radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Folders By A Radio Client Count	This chart shows the folders and the number of 802.11a radios (5GHz) in each folder whose client count is greater than the cutoff. The cutoff represents 75% of the 'maximum,' where the 'maximum' is the radio that has the highest client count regardless of the folder. The cutoff value is displayed within the title and can vary. This chart takes into account approved APs with A radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Folders By BG Radio Client Count	This chart shows the folders and the number of 802.11b/g radios (2.4GHz) in each folder whose client count is greater than the cutoff. The cutoff represents 75% of the 'maximum,' where the 'maximum' is the radio that has the highest client count regardless of the folder. The cutoff value is displayed within the title and can vary. This chart takes into account approved APs with BG radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Clients By Total Traffic	The widget looks at currently connected clients as well has client historical information over the past 24 hours and then displays the top 10 clients with the must usage. You can click on a MAC address to view more information about any of the clients that display on this table. This table is updated every hour.
Clients By AOS Device Type	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the AOS device type.
Clients By Device Type	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the device type (such as a specific operating system or smart phone type).
Clients By Device Mfgr	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the client manufacturer.
Clients By Device Model	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the device model (such as the smart phone type).
Clients By Mfgr & Model	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the client manufacturer and model.

Table 132: *Available Widgets (Continued)*

Widget	Description
Clients By Device OS	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the device operating system (such as Windows or Android).
Clients By Device OS Detail	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the device operating system version (such as Windows NT 6.1).
Clients By Network Vendor	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on each device's network interface vendor.
Client Signal Distribution	The **Client Signal Distribution** chart shows the number of attached devices that have a signal quality within a set of ranges.

4.

Adding Widgets

You can change the widgets on this page by clicking ⚙ in the upper-right corner of the **Home > Overview** page.

To add a widget:

1. Select a widget from the **Available Widgets** list, then drag the widget across to the right side of the page.
2. Place the widget in an open space within the gridlines. The widget label turns orange if you place it over occupied space.
3. Click **Save**.

Available Widgets

Table 133 describes the list of available widgets along with a description for each. Note that when a widget is enabled, the information that displays can vary based on the user's permission level. Certain roles, for example, limit the top folder that a user can view.

Table 133: *Available Widgets*

Widget	Description
Client/Usage Graphs	The **Client** graph is enabled by default and, by default, shows the maximum number of attached clients over the last two hours. Select the **Show All** link to view more specific client information on the graph, such as the total and average clients for a specific SSID, the maximum VPN sessions, etc. The available check boxes within this graph are determined by the SSIDs that OV3600 is aware of from polling the device. The **Usage** graph is enabled by default and, by default, shows the average bits-per-second in/out information and average VPN in/out information. Select the **Show All** link to view usage information for specific SSIDs. The available checkboxes within this graph are determined by the SSIDs that OV3600 is aware of from polling the device. The information in these graphs is color coded to match the selected check boxes.
Monitoring and Configuration Pie Charts	The **Monitoring Status** pie chart shows the percentage of total devices that are up and the number and percentage of devices that are currently down. Clicking within this pie chart takes you to the **Devices > Down** page. The **Configuration Compliance** pie chart shows the percentage of devices that are mismatched, good, unknown, and those with auditing disabled. It also provides a summary of the total number of devices that are mismatched. Clicking within this pie chart takes you to the **Devices > Mismatch** page. These pie charts are enabled by default.
Alert Summary	The **Alert Summary** table is enabled by default and provides the number of OV3600 alerts, IDS events, and RADIUS authentication issues over the last 2 hours, the last 24 hours, and the total since the last OV3600 server reboot. ● Click on **OV3600 Alerts** to drill down to more detailed alert information. This information displays in the current page. You can return to the **Alert Summary** graph by selecting the **Home Overview** link. ● Click on **IDS Events** to drill to more detailed event information. This link takes you to the **RAPIDS > IDS Events** page. ● Click on **RADIUS Authentication Issues** to drill to more detailed RADIUS authentication information. This information displays in the current page. You can return to the **Alert Summary** graph by selecting the **Home Overview** link.
Quick Links	The **Quick Links** section is enabled by default. This section provides the user with easy navigation to a specific folder, group, report, or common task.
RAPIDS: Acknowledged	The **Acknowledged RAPIDS Devices** pie chart shows the percentage of acknowledged and unacknowledged RAPIDS that the user has visibility into. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Ignored rogues, however, are not included in this chart. This chart also displays on the **RAPIDS > Overview** page.

Table 133: *Available Widgets (Continued)*

Widget	Description
RAPIDS: Classification Pie	The **RAPIDS: Classification Pie** shows the percentage of devices classified as Valid, Suspected Neighbor, Suspected Valid, Suspected Rogue, Rogue, and Neighbor that are attached to OV3600. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Ignored rogues, however, are not included in this chart. This pie chart can also be viewed on the **RAPIDS > Overview** page.
RAPIDS: Classification Summary	The **RAPIDS: Classification Summary** table shows the number of devices classified as Valid, Suspected Valid, Neighbor, Suspected Neighbor, Suspected Rogue, Rogue, and Unclassified that are attached to OV3600. In addition, contained rogue information will appear if **Manage rogue AP containment** is set to **Yes** on the **RAPIDS > Setup** page. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Note that ignored rogues are not included in this chart. This table can also be viewed on the **RAPIDS > Overview** page.
IDS Events	The **IDS Events** table shows the number and type of attacks logged by the intrusion detection system over the last 2 hours, the last 24 hours, and the total since the last OV3600 server reboot. This is the same table that displays on the **RAPIDS > Overview** page.
RAPIDS: OS Pie	The **RAPIDS: OS Pie** chart shows the top 9 rogue devices by OS, Others, Unknown, and Not Scanned. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Note that ignored rogues are not included in this chart. This pie chart can also be viewed on the **RAPIDS > Overview** page.
RAPIDS: OS Summary	The **RAPIDS: OS Summary** table shows the top 9 rogue devices by OS, Others, Unknown, and Not Scanned. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Note that ignored rogues are not included in this chart. This table can also be viewed on the **RAPIDS > Overview** page.
Top Folders By AP Usage	This chart lists the folders and the number of APs in each folder whose usage is greater than the cutoff (or usage threshold). The cutoff represents 75% of the maximum usage, where the maximum usage is the AP with the highest usage regardless of the folder in which it resides. The cutoff value is displayed within the title, and this value can vary. The chart takes into account approved APs with radios based on the last 24 hours. In addition, this chart is updated every hour.

Table 133: *Available Widgets (Continued)*

Widget	Description
Top Folders By A Radio Channel Usage	This chart shows the folders and the number of 802.11a radios (5GHz) in each folder whose channel usage is greater than the cutoff (or usage threshold) as measured by Mbps. This cutoff is on the on the **OV3600 Setup > General** page using the **Configure Channel Busy Threshold** option. If this option is not configured, then the cutoff is 75% of the 'maximum,' where the 'maximum' refers to the AP that has the highest usage regardless of the folder in which it resides. The cutoff value is displayed within the title, and this value can vary. This chart takes into account approved APs with 'A' radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Folders By BG Radio Channel Usage	This chart shows the folders and the number of 802.11b/g radios (2.4GHz) in each folder whose channel usage is greater than the cutoff (or usage threshold) as measured by Mbps. This cutoff is on the on the **OV3600 Setup > General** page using the **Configure Channel Busy Threshold** option. If this option is not configured, then the cutoff is 75% of the 'maximum,' where the 'maximum' refers to the AP that has the highest usage regardless of the folder in which it resides. The cutoff value is displayed within the title, and this value can vary. This chart takes into account approved APs with 'BG' radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Folders By A Radio Client Count	This chart shows the folders and the number of 802.11a radios (5GHz) in each folder whose client count is greater than the cutoff. The cutoff represents 75% of the 'maximum,' where the 'maximum' is the radio that has the highest client count regardless of the folder. The cutoff value is displayed within the title and can vary. This chart takes into account approved APs with A radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Folders By BG Radio Client Count	This chart shows the folders and the number of 802.11b/g radios (2.4GHz) in each folder whose client count is greater than the cutoff. The cutoff represents 75% of the 'maximum,' where the 'maximum' is the radio that has the highest client count regardless of the folder. The cutoff value is displayed within the title and can vary. This chart takes into account approved APs with BG radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Clients By Total Traffic	The widget looks at currently connected clients as well has client historical information over the past 24 hours and then displays the top 10 clients with the must usage. You can click on a MAC address to view more information about any of the clients that display on this table. This table is updated every hour.
Clients By AOS Device Type	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the AOS device type.
Clients By Device Type	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the device type (such as a specific operating system or smart phone type).

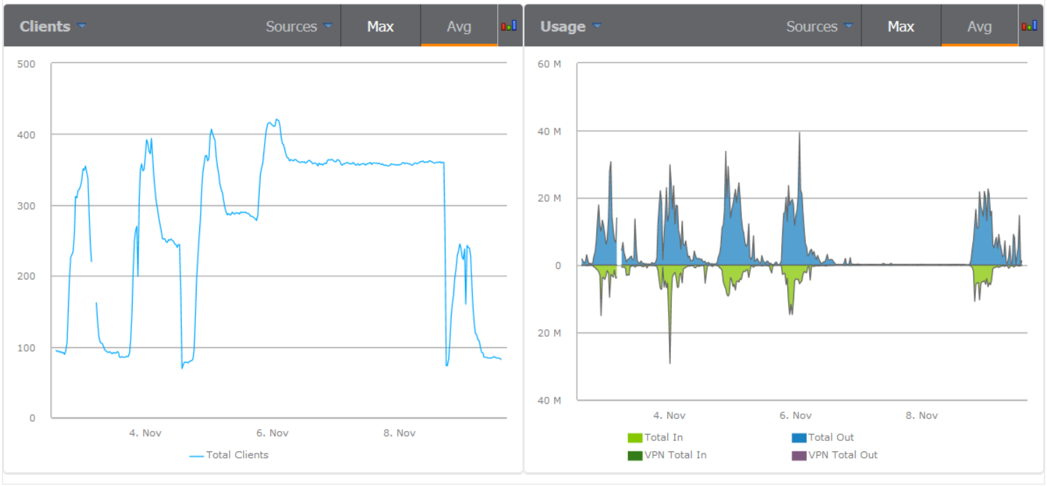
Table 133: *Available Widgets (Continued)*

Widget	Description
Clients By Device Mfgr	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the client manufacturer.
Clients By Device Model	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the device model (such as the smart phone type).
Clients By Mfgr & Model	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the client manufacturer and model.
Clients By Device OS	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the device operating system (such as Windows or Android).
Clients By Device OS Detail	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on the device operating system version (such as Windows NT 6.1).
Clients By Network Vendor	This pie chart shows the percentage of clients that have attached to OV3600 over the last 24 hours based on each device's network interface vendor.
Client Signal Distribution	The **Client Signal Distribution** chart shows the number of attached devices that have a signal quality within a set of ranges.

Defining Graph Display Preferences

Many of the graphs in OV3600 are Highcharts, which allow you to adjust the graph settings attributes as shown in Figure 198.

Figure 198: *Interactive Graphs on the* ***Home*** **>** ***Overview*** *Page*



Highcharts are built with JavaScript, so the graphs can run directly through your browser without the need for additional client-side plugins. This makes it possible to view your OV3600 charts on a mobile device.

These charts can be used and customized as follows.

- A Time Range selector in the upper right portion of the charts (including pop-up charts) allows you to select a common or a custom date range for your data. The preconfigured ranges for OV3600 charts are current 2 hours, 1 day, 1 week, and 1 year.
- Drop-down menus are available for viewing client and usage for specific SSIDs and/or all SSIDs. A search field is available to help you quickly find a specific WLAN.

  You can select up to six options from each drop-down menu. Once selected, each option will appear in the color-coded legend below the chart. Clicking on an option in this legend will disable or enable that information in the graph. Note that even if an option is disabled from viewing in the graph, that option will still remain in the legend until you deselect it from the drop-down menu.
- Max and Avg options allow you to change the chart view to show the maximum or average client and usage information.
- Plot points display within the chart at varying intervals, depending on the selected time range. Tooltips and a plot line appear as you hover over each plot point, showing you the detailed information for that specific time.
- Click on any chart to view a pop-up version. In this version, you can easily zoom in on a range of data by using your mouse to drag a rectangle in the chart. While you are zoomed in, a **Reset zoom** button appears, enabling you to return to the original view. The pop-up charts also include a legend that displays the Last, Min, Max, and Avg values for the selected graph.
- Some charts include a drop-down option next to the graph title. For example, on the **Devices > Monitor** page for Radio Statistics, you can select the drop-down beside the graph title to view a graph for Client, Usage, Radio Channel, Radio Noise, Radio Power, Radio Errors, and 802.11 Counters information. In prior versions of OV3600, these graphs appeared as separate tabs.

Monitoring Your Network Health

To view your overall network health, navigate to **Home > Overview**. The top header of the page displays the status of your network, while the navigation pane on the left side of the page allows you to navigate through the OV3600 WebUI.

Table 134 describes the sections and graphs that appear in the Overview page.

Table 134: *Home > Overview Sections and Charts*

Section	Description
Graphs	You can select the following graphs to display: ● Clients. This graph shows a summary of the number of users on the network during a specified period of time. By default, OV3600 displays the maximum number of users. To display a list of data series that this graph can display, such as the user count by SSID, select **Show All** . Or, clear the **Max Clients** or **Avg Clients** check boxes to change the display. ● Client Health. This graph shows the percentage of clients with good, fair, and poor health. The client health metric displayed in these charts is the efficiency at which that AP transmits downstream traffic to a particular client. AirWave compares the amount of time the AP spends transmitting call data to a client to the amount of time that would be required under ideal conditions (at the maximum Rx rate supported by client, with no data retries) to calculate this metric. To view the new graph from the Home page, select **Client Health** from the **Clients** menu. ● Usage. This adjustable chart displays bandwidth data over time. To remove bandwidth in or out from the graphical display, clear the check box for **Avg Bits Per SecondIn** or **Out**. To display details for specific devices, select **Show All** and select the devices to be included in the graphical bandwidth summary chart. To view historical graphs in a new window, select the three-bar icon on the upper right of the chart.
Folder Overview	This table displays statistics for AirWave folders and provides shortcuts to monitoring pages for the OV3600 folders.
Monitoring Status	This pie chart shows the percentage of all devices that are up and down on the network. To review devices that are down, select **Down** in the legend or the chart, and the **Devices > Down** page displays.
Configuration Compliance	The pie chart displays all known device configuration status on the network. Devices are classified as **Good**, **Unknown**, **Mismatched,** or **Audit Disabled**. Select the **Mismatched** link to see the **Devices > Mismatched** page.
Alert Summary	This section displays all known and current alerts configured and enabled in the **System > Alerts** page (refer to "Creating New Triggers" on page 267). Alerts can be sorted using the column headers (**Type**, **Last 2 Hours**, **Last Day**, **Total**, or **Last Event**). The **Alert Summary** field displays the following alerts: ● OV3600 Alerts ● IDS Events ● RADIUS Accounting Issues ● RADIUS Authentication Issues

Table 134: *Home > Overview Sections and Charts (Continued)*

Section	Description
Quick Links	The **Quick Links** section provides drop-down menus that enable you to move to the most common and frequently used pages in OV3600 as follows: ● **Go to folder**—This menu lists all folders defined in OV3600 from the **Devices List** page. See "Using Device Folders" on page 134. ● **Go to group**—This menu lists all groups defined in OV3600, and enables you to display information for any or all of them. Use the **Groups** pages to edit, add, or delete groups that appear in this section. See "Using Device Groups" on page 72. ● **View Latest Reports**—OV3600 supports creating custom reports or viewing the latest daily version of any report. Select any report type to display the daily version. See "Creating, Running, and Sending Reports" on page 315. ● **Common Tasks**—This menu lists quick links to the most heavily used task-oriented pages in OV3600, to include the following: ■ **Configure Alert Thresholds**—This link takes you to the **System > Triggers** page. See "Viewing Triggers" on page 1. ■ **Configure Default Credentials**—This link takes you to the **Device Setup > Communication** page. See "Configuring Communication Settings for Discovered Devices" on page 53. ■ **Discover New Devices on Your Network**—This link takes you to the **Device Setup > Discover** page. See "Discovering, Adding, and Auditing Devices " on page 120. ■ **Supported Devices and Features**—This link displays a PDF that summarizes all supported devices and features in chart format for OV3600. ■ **Upload Device Firmware**—This link displays the **Device Setup > Upload Firmware & Files & Files Upload** page. See "Uploading Firmware and Files" on page 55. ■ **View Event Log**—This link displays the **System > Event Log** page. See "Using the Event Log" on page 266.

Monitoring Application Traffic

The **Home > Traffic Analysis** page displays mobile app usage and performance statistics to network administrators. Non-admin users can view information for the devices and folders to which they have access.

To switch among table, chart, and graph widgets:

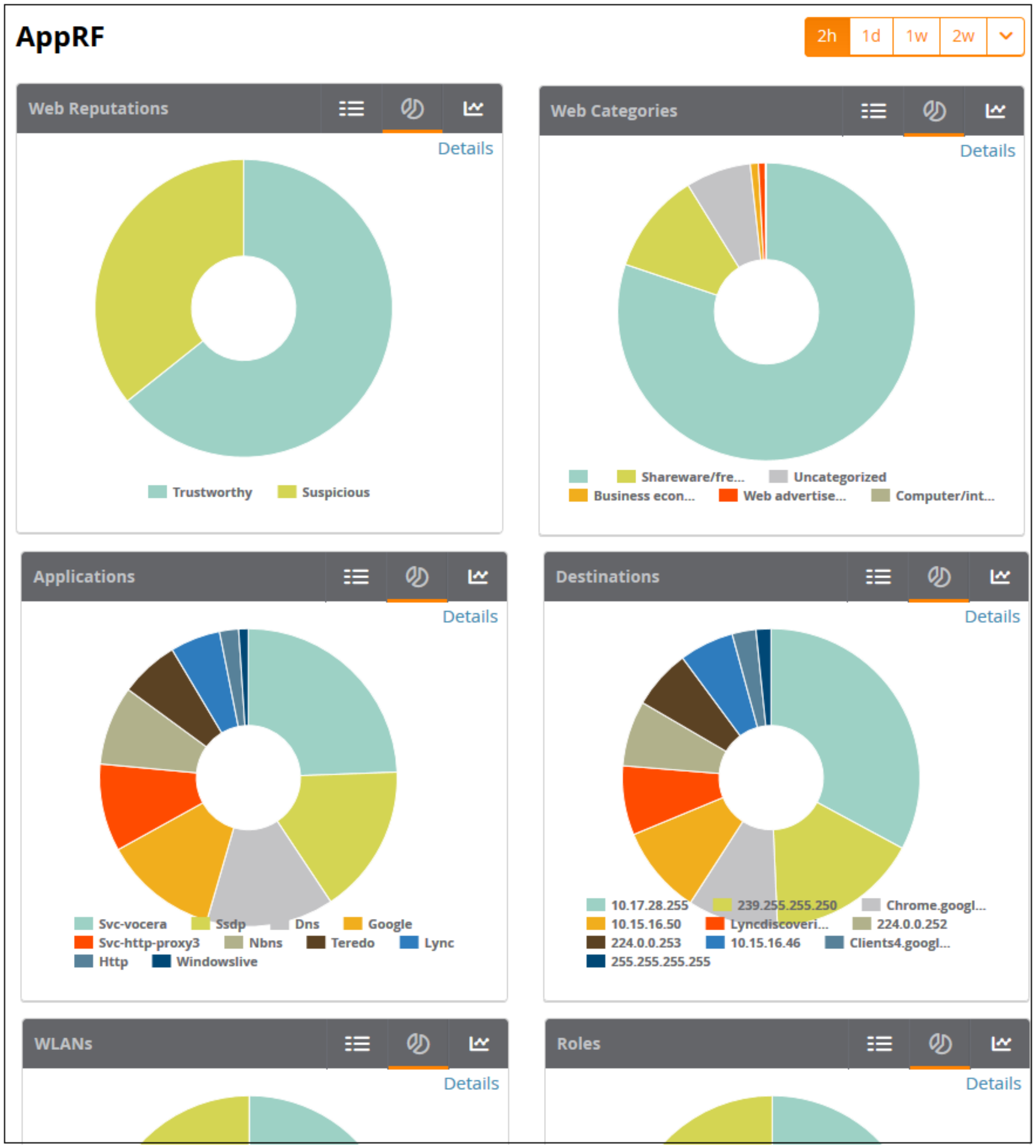
- Click ☰ to view usage data in a table. Categories vary for each widget. For example, the categories for application are Social Media, Torrent, Chat Protocols, Games, Web Development Tools, Ad Blocker.
- Click ◔ to view the percent usage of each category in a donut chart. Hover your mouse above each section of the chart to view the category name and usage, in KB and percentage (%).
- Click 📈 to view a graph of usage (in MB) over time.

When you click the Details link in the bottom right corner of each widget, a pop-up window opens with the following information:

- **Category**: Name of the user
- **Bytes**: Total usage in bytes (MB)
- **Packets**: Total number of packets transmitted/received
- **Web Reputation**: Web reputation, indicating the safety of the site
- **Web Category**: Website type
- **Destination**: Number of destinations reached through the given category
- **User Role**: Number of roles assigned to the user
- **Devices**: Number of devices connected to the given category
- **User Name**: Name of the user
- **Device MAC**: MAC address of the user

- **WLANs**: Number of WLANs to which the user is connected

Figure 199: *Traffic Analysis Dashboard*



Using the UCC Dashboard

The UCC dashboard in OV3600 displays charts that show UCC trends to network administrators. Non-admin users can view information for the devices and folders to which they have access.

Viewing Call Details

You can view call details by clicking the **Call Details** link at the lower-left of each graph. Information, such as the operating system of the client device, protocol used to complete the call, and connectivity type are all displayed in the table view. In support of AOS-W 6.5 and 8.2, you can also see who provides the UCC service for WiFi calls.

You can look for any device issues that are detected during the call in the **End-to-End Quality** field, or network quality issues in the **Mean Opinion Score (MOS)** field. The MOS is updated after a call has ended.

By default, the data in this table is displayed by the call start time, with the most recent call at the top of the list.

To change how the data is displayed, do any of the following:

- Click the column heading to sort the data.
- Click ▼ at the top of column headings to filter the data.
- Click the Show link to add parameters like Protocol to the table view.

Tips for Filtering Calls

If you want to reduce the amount of calls that appear as unknown, you can filter the results by call types. When you select **Voice**, the UCC dashboard shows only voice calls and conference calls. When you select **Others**, any other type of call, such as video and desktop sharing, is reported.

The UCC dashboard also displays calls based on the end-to-end call quality. When you select **WLAN**, information displayed is based on the UCC score of the calls.

NOTE

If Heuristics is enabled in OV3600 and there is no end-to-end call quality information, OV3600 will display information based on UCC call quality (see "Additional OV3600 Services" on page 30).

Viewing UCC Charts, Graphs, and Tables

OV3600 aggregates UCC call data and presents them in charts, graphs, and tables. Hovering over the charts displays details about the highlighted section of that chart.

Call Quality

Call quality is measured by a metric called the UCC score. This metric takes into account delay, jitter, and packet loss. OV3600 obtains these metrics from RTCP messages sent from the client (if the client is capable of sending them). For audio calls, OV3600 obtains these metrics from the Alcatel-Lucent AP that inspects the RTP flows.

The following table describes the UCC scores and quality indications.

Table 135: *UCC Quality Levels*

UCC Score	Quality Indication
71 or greater	Good quality seen by the network
31 to 70	Fair quality seen by the network
0 to 30	Poor quality seen by the network

To view call quality information, click the following hyperlinks:

- Trend. This chart shows the number of calls with good, fair, or poor client health over the selected time period.
- Distribution. This graph shows the relative proportions of calls with each quality type.
- APs. This chart shows information about APs that supported poor quality calls.
- Folder. This table view shows all folders that carried calls and, for each folder, the percentage of calls that were rated poorly by UCC.

Quality Correlation

These graphs display the correlation between call quality and client health. The client health metric displayed is the efficiency at which that AP transmits downstream traffic to a particular client. OV3600 determines this value by comparing the amount of time the AP spends transmitting call data to a client to the amount of time that would be required under ideal conditions at the maximum Rx rate supported by client, without data retries.

For example, a client health metric of 100% means the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25%

means the AP is taking four times longer than the ideal transmission time, or is sending 3 extra transmissions to that client for every packet.

To view quality correlation information, click one of the following hyperlinks:

- Trend. This chart shows the number of calls with good, fair, or poor client health over the selected time period.
- Scatterplot. This chart shows a historical view of the call quality and client health of each individual call. To view call details for a specific client, click on a call session (see "Viewing End-to-End Call Details" on page 301).
- Connectivity. This table view shows the number of calls of each quality level (good, fair, poor, and unknown) by connectivity type (wired to Wi-Fi, wired to external, wired to wired, Wi-Fi conference, Wi-Fi to external, and Wi-Fi to Wi-Fi).

Call Volume

To view call volume information, click one of the following hyperlinks:

- Trend. This graph and table displays the number of calls made during the selected time period using a UCC application, such as SIP, Lync, and FaceTime.
- APs. This graph displays the names of the APs that supported these calls.

Devices

These graphs display information about the calls made by different device types, such as Windows 7, Mac OS X, iPhone, or Android devices.

- Trend. This graph show the numbers of calls by each platform type over the selected time period.
- Distribution. This chart shows the relative proportion of calls that originated form each device type.
- Quality. This graph shows the numbers of calls at each quality level made by each device type.

Viewing End-to-End Call Details

For an end-to-end view about a call, go to **Home > UCC > Call Quality > Call Details** and click the magnifying glass icon in the **Details** column. Overall client health is rated good, fair, or poor (see "Quality Correlation" on page 300 for information about the UCC score).

Client information, such as a description of the client device, the signal-to-noise (SNR) ratio for the call on the client's connection, speaker and microphone glitch rate, and transaction rates, are provided in this table view.

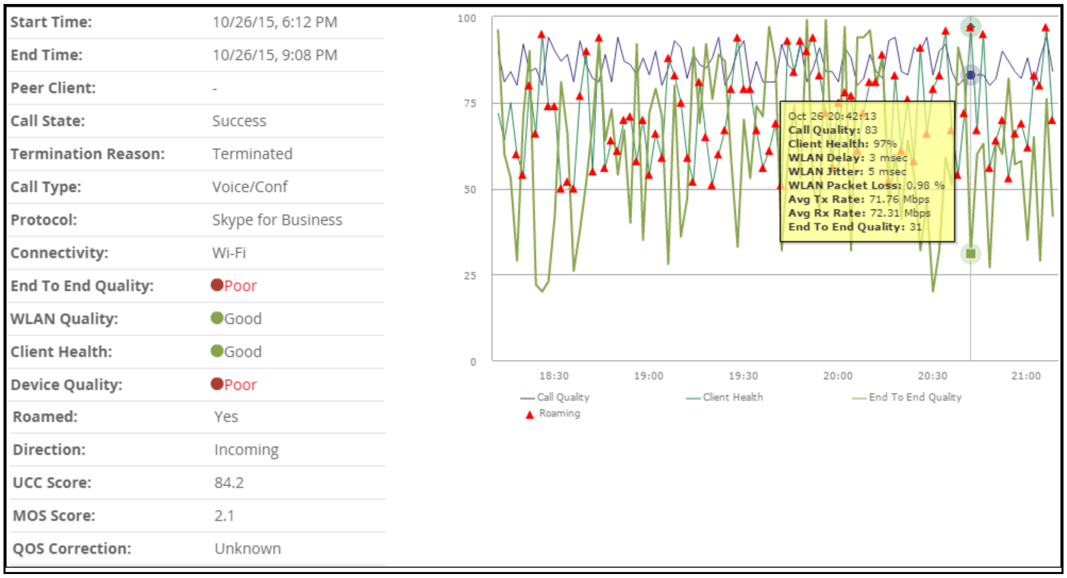
Table 136: *AP Details*

Column Name	Description
AP Type	The type of AP to which the client is connected.
Radio Name	The AP's radio being used for the call (802.11bgn or 802.11ac)
Radio MAC	The AP radio's MAC address.
Concurrent Poor Calls	The number of poor calls occurring simultaneously with the call being viewed.
Channel	The channel used for the call.
Channel Utilization	The used channel's utilization as a percentage.
Channel Interference	The interference impacting the used channel as a percentage.

Get Call Summary

Use the **Summary** tab to see more call details and a graph displaying the quality of the call as it progressed. Hovering over the graph displays a snap-shot of the call at two-minute intervals, which can help you identify when changes occurred during the call.

Figure 200: *Call Summary Information*



Start Time:	10/26/15, 6:12 PM
End Time:	10/26/15, 9:08 PM
Peer Client:	-
Call State:	Success
Termination Reason:	Terminated
Call Type:	Voice/Conf
Protocol:	Skype for Business
Connectivity:	Wi-Fi
End To End Quality:	🟥Poor
WLAN Quality:	🟩Good
Client Health:	🟩Good
Device Quality:	🟥Poor
Roamed:	Yes
Direction:	Incoming
UCC Score:	84.2
MOS Score:	2.1
QOS Correction:	Unknown

Oct 26 20:42:13
Call Quality: 83
Client Health: 97%
WLAN Delay: 3 msec
WLAN Jitter: 5 msec
WLAN Packet Loss: 0.98 %
Avg Tx Rate: 71.76 Mbps
Avg Rx Rate: 72.31 Mbps
End To End Quality: 31

To view more details about a call, click the **More** link at the lower right of the Summary tab.

- Microphone Details. This information about the client's microphone includes manufacturer and model, the capture device driver, glitch rate, and audio microphone error.
- WLAN. This information repeats some of that shown on the End-to-End tab, in addition to WLAN delay, jitter, and packet loss.
- End To End. This information, about the connection between the caller and receiver, includes MOS, delay, jitter, packet loss, and burst gap details.
- End Point Details. This information about the device used by the caller includes IP address, Wi-Fi device driver, CPU details, and OS.
- Speaker Details. This information describes the type of speaker used by the caller.

For a granular look at a specific call, click the Details Tab. It shows the same information found on the Summary tab in table divided into two-minute intervals.

Using the UCC Report

The UCC report provides an overall look at UCC activity on your network in the specified time period. This information is displayed in a series of tables representing the top connectivity types, call types, application types, device types, folders, APs, and clients with the highest percentage of poor quality calls.

Table 137: *UCC Report Fields*

Field	Description
Quality Metric	The metric used to determine the quality of calls.

Table 137: *UCC Report Fields (Continued)*

Field	Description
Connectivity Type	The type of connection used to complete VoIP calls: ● Wi-Fi to Conference. Conference call connectivity between wireless, wired, and desktop-shared devices. ● Wi-Fi to External. Call connectivity between wireless devices to other devices on an external network. ● Wi-Fi to Wi-Fi. Call connectivity between wireless devices within the same network. ● Wired to Wi-Fi. Call connectivity between wired and wireless devices within the same network. ● Wired to External. Call connectivity between wired devices to other devices on an external network. ● Wired to Wired. Call connectivity between wired devices on the same network.
Call Type	The type of call, such as voice or video.
Application Type	The software application used to complete a call.
Device Type	The client device used to complete a call. The device type is displayed as the device's operating system.
% of Poor Calls	The percentage of poor calls completed on the specified metric such as device type, application type, etc.
Poor Calls	The number of poor calls completed on the specified metric such as device type, application type, etc.
Total Calls	The total number of calls completed on the specified metric such as device type, application type, etc.
Folders	The device folder from which calls were completed.
APs	The APs that carried calls.
Clients	The clients who completed calls. This is displayed by MAC address and user name.
% of Poor Calls by MOS Score	The percentage of poor calls completed by a folder, AP, or client based on the MOS Score.
% of Poor Calls by UCC Score	The percentage of poor calls completed by a folder, AP, or client based on the UCC Score.
Average Client Health (Poor Calls)	The average client health when completing a call.
Total Calls	Total number of calls from a folder, AP, or client.
Total Call Time	Total call time of all calls from a folder, AP, or client.

Viewing RF Performance

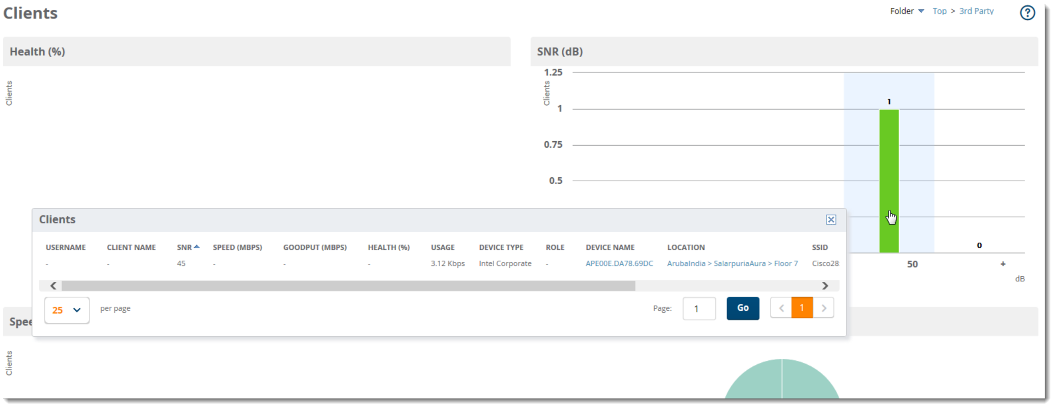
OV3600 helps you identify clients with low SNR rates, health, speed, and goodput, putting the data in interactive RF performance graphs on the Clients page. You can find these graphs by navigating to **Home > RF Performance**.

From the Clients page , you can do the following:

- In the upper-right corner of the page, select a folder from the drop-down menu to narrow down the results. Keep in mind that folder-level permissions are assigned to user roles. Find more information about "Creating OV3600 User Roles" on page 39 and "Using Device Folders" on page 134.

- In any graph, click on a value is to view the Clients table, or click the hyperlinks in the Clients table to access shortcuts to monitoring pages and, if available, VisualRF floor plans (Figure 201).
- In the Client page, you can click the client name link to go to the **Clients > Diagnostics** page. Find more information about "Troubleshooting Client Issues" on page 189.

Figure 201: *Accessing the Clients Table*



Clients

USERNAME	CLIENT NAME	SNR ▲	SPEED (MBPS)	GOODPUT (MBPS)	HEALTH (%)	USAGE	DEVICE TYPE	ROLE	DEVICE NAME	LOCATION	SSID
-	-	45	-	-	-	3.12 Kbps	Intel Corporate	-	APE00E.DA78.69DC	ArubaIndia > SalarpuriaAura > Floor 7	Cisco28

Speed and goodput graphs are available for Alcatel-Lucent devices that support AMON, and health graphs are available for switches running AOS-W 6.3 or later.

Viewing RF Capacity

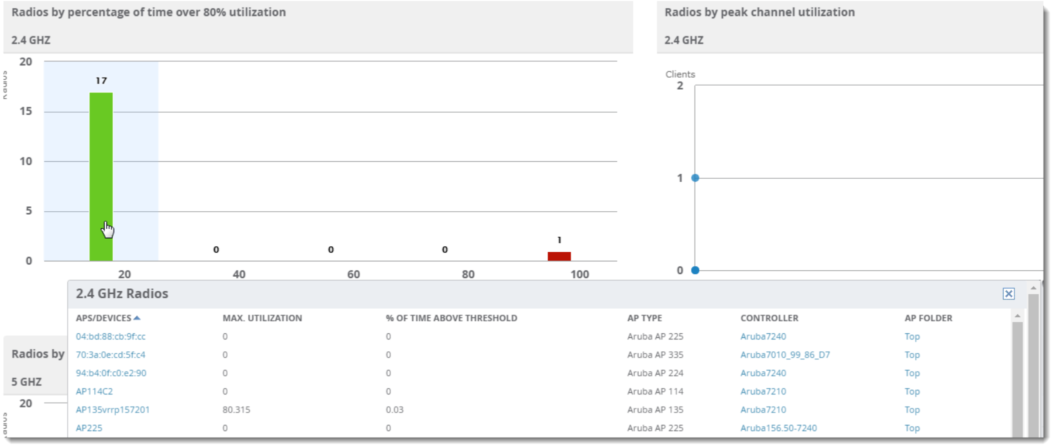
OV3600 summarizes radio and channel utilization information for network traffic in the last week and puts the data in interactive RF capacity graphs on the Radios page. You can find these graphs by navigating to **Home > RF Capacity**. These graphs refresh after nightly maintenance completes. The process goes over all the radios and determines the maximum client count and maximum channel utilization for each radio.

The Radios page is available to only Admin users.

OV3600 displays two sets of data for 2.4 GHz and 5 GHz channels:

- Radios by percentage of time over 80% utilization. These graphs show the percent of the time that the radios are above the threshold during the day when in use. OV3600 determines the normal usage time based on stored utilization samples. Values in red indicate that these radios are above the threshold 75 to 100% of the time. You might want to investigate these radios to see if you need to upgrade them or add additional APs to this location. The information on this graph is collected every 24 hours, after nightly maintenance, and includes data from the last week. You can click on a bar in this graph to view details in a pop-up window (see Figure 202).

Figure 202: *Accessing Device Details for Radios*

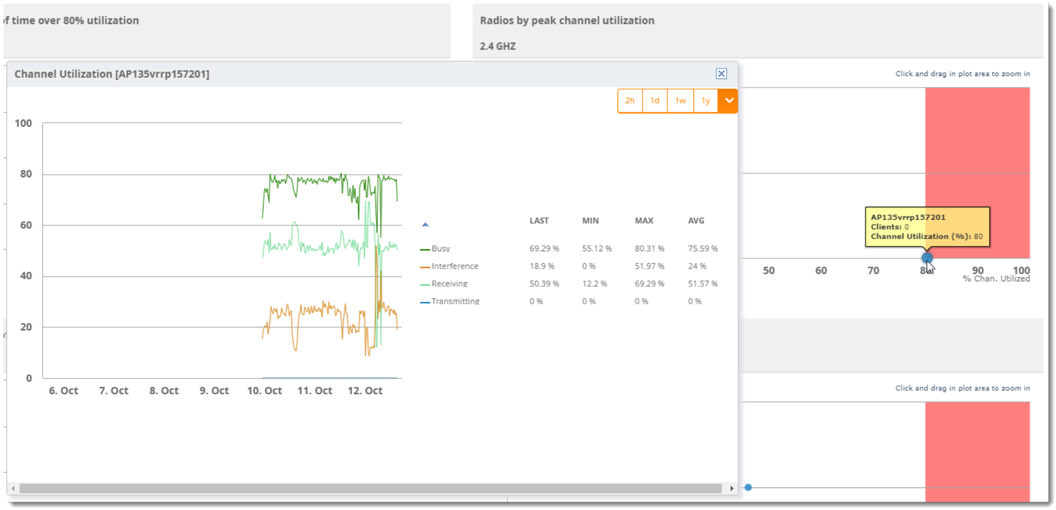

Radios by percentage of time over 80% utilization
2.4 GHZ
20
15
10
5
0
17
0
0
0
1
20
40
60
80
100
Radios by peak channel utilization
2.4 GHZ
Clients
2
1
0
Radios by
5 GHZ
20

2.4 GHz Radios

APS/DEVICES ▲	MAX. UTILIZATION	% OF TIME ABOVE THRESHOLD	AP TYPE	CONTROLLER	AP FOLDER
04:bd:88:cb:9f:cc	0	0	Aruba AP 225	Aruba7240	Top
70:3a:0e:cd:5f:c4	0	0	Aruba AP 335	Aruba7010_99_86_D7	Top
94:b4:0f:c0:e2:90	0	0	Aruba AP 224	Aruba7240	Top
AP114C2	0	0	Aruba AP 114	Aruba7210	Top
AP135vrrp157201	80.315	0.03	Aruba AP 135	Aruba7210	Top
AP225	0	0	Aruba AP 225	Aruba156.50-7240	Top

- Radios by peak channel utilization. This graph shows the total number of clients connected to radios and corresponding radios connected during peak channel utilization. Data collection occurs every 24 hours, after nightly maintenance, and OV3600 includes utilization data from the last week in this graph. You can click plot points, which represent radios, to view historical utilization information for the last two hours, day, week, year, or view a custom time range in a pop-up window (see Figure 203).

Figure 203: *Accessing the Channel Utilization Details for a Radio*


f time over 80% utilization
Radios by peak channel utilization
2.4 GHZ
Channel Utilization [AP135vrrp157201]
2h
1d
1w
1y
100
80
60
40
20
0
6. Oct
7. Oct
8. Oct
9. Oct
10. Oct
11. Oct
12. Oct
Click and drag in plot area to zoom in
AP135vrrp157201
Clients: 0
Channel Utilization (%): 80
50
60
70
80
90
100
% Chan. Utilized
Click and drag in plot area to zoom in

▲	LAST	MIN	MAX	AVG
Busy	69.29 %	55.12 %	80.31 %	75.59 %
Interference	18.9 %	0 %	51.97 %	24 %
Receiving	50.39 %	12.2 %	69.29 %	51.57 %
Transmitting	0 %	0 %	0 %	0 %

Viewing Network Deviations

The **Home > Network Deviations** page provides graphs that track your network's Client and Usage information and draw attention to unusual network usage patterns. These graphs can show you, for example, if heavy network traffic is occurring during off hours, or they can be used to detect the time(s) of day when your network traffic peaks.

By default, the graph lines display, in five-minute intervals, the previous 2 hours of client and usage information for the current day of the week averaged out over the last 40 weeks. The shaded area indicates the standard deviation, which defaults to 1. So, for example, if you launch this page at 9:00 am on a Friday, then a 2-hour graph will show the current and average number of connected clients and usage between 7:00 AM and 9:00 AM on all Fridays over the last 40 weeks, with plot points showing the number of clients for every five minutes. You can also select/drag a set of plot points to zoom in and view a more precise time range. Click the **Reset zoom** button to return to the specified time range. You can change the time range of the graphs to 4 hours, 8 hours, or 1 day using the time-range options in the upper-right corner of this page, and OV3600 will remember the new setting the next time the page is launched.

The left graph shows client information - specifically the current and average number of clients over the last 40 weeks during the selected time range. The right graphs show usage information - specifically the current and average incoming and outgoing bits-per-second over the last 40 weeks during the selected time range. The shaded/gray color within the graphs indicates the standard deviation. Any blue lines (Avg Clients, Avg Out Usage) or green lines (Avg In Usage) that appear outside of the shaded/gray area can be considered deviation points because the value does not come within the range of the calculated standard deviation.

NOTE

This operation can consume a significant amount of CPU capacity as it parses through large amounts of data. Larger deployments you may have to wait up to a minute before seeing the initial graph plot points. In addition, this page does not automatically refresh, rather it refreshes each time this page is selected and/or each time you click Refresh. As a result, if you click this page, navigate away, and then return to this page, the page will begin to load again. If your network includes a large amount of data, then a best practice is to open this page in a new tab before navigating to another page. In this case, the Network Deviations page will continue to load while you continue to work in OV3600.

Figure 204: *Home > Network Deviations page*

The first time this page is launched, the graphs will display information for all devices in the Top folder. To specify a different folder, simply select one from the folder drop down in the upper-right corner, and then refresh the page. OV3600 will remember the new setting the next time that the page is launched.

By default, the graphs display average and standard deviation information for the current time over the last 40 weeks. Click the **gear icon** in the upper right corner to change these defaults. OV3600 will remember the new setting the next time that the page is launched.

NOTE

The **Thresholds** button is disabled while the page is loading. The **Folder** drop down is disabled until the first plot points display.

Figure 205: *Network Deviations Threshold*

How Standard Deviation is Calculated

Plot lines may or may not display outside of the shaded, standard deviation range depending on the SD value specified from Thresholds button. Refer to the following example to review the way that standard deviation is calculated.

Standard Deviation Example

Assumptions:

- Mean: 5
- Standard Deviation: 2

```
SD(1):
-------
1*SD +- Mean
1*2 +- 5
2 +- 5
Normal Range: 3 - 7

SD(2):
-------
2*SD +- Mean
2*2 +- 5
4 +- 5
Normal Range: 1 - 9

SD(3):
-------
3*SD +- Mean
```

```
3*2 +- 5
6 +- 5
Normal Range: 0 - 11 (-1 is not considered, so 0 is taken)
```

Given the information above, if the Average Client Count over the last 40 weeks is 5, then this is not an anomaly (deviation) for any SD value. On the other hand, if at one point the client count was 8, then this would be an anomaly for SD1, whose normal client range is from 3-7. The plot point would appear outside of the shaded area when the standard deviation is set to 1, but it would be normal from a standard deviation of 2 or 3.

Accessing OV3600 Documentation

The **Home > Documentation** page provides easy access to all relevant OV3600 documentation. All of the documents on this page are hosted locally by your OV3600 server. The PDF files can be viewed by any PDF viewer, and the HTML files can be viewed in any supported browser.

If you have any questions that are not answered by the documentation, please contact Alcatel-Lucent support.

Licensing in OV3600

You can view current licenses, verify your license count, and add new licenses from the **License** page. When you add switches to a stack, one OV3600 license covers the switch stack.

Adding licenses

To add a license:

1. Open the email containing your license key, and select and copy the text of that license.
2. From the **Home > License** page, click **Add**. A pop up window opens.
3. Paste the text of the license into the pop up window, and click **Add**. The Alcatel-Lucent End-User License Agreement appears.
4. Review the license agreement, then click **I Accept**. The newly added license displays in the License table.

Viewing licenses

You can click in the license table to view a pop up that shows details of any license key.

Table 138: *License Table Fields and Descriptions*

Field	Description
Organization	Displays the organization listed on your license key.
Product	This product description is read directly from the license key.
Package	Displays the license type. For example, this could be a license for an enterprise OV3600 server, or a smaller license to support additional devices.
Type	Shows whether the license is for a Master Console, an AirWave server, or a failover server.
Device Count	Number of devices supported by the license.
IP Address	IP address of the OV3600 server using the license. This address is read directly from the license key.

Table 138: *License Table Fields and Descriptions (Continued)*

Field	Description
Days Remaining	Remaining number of days on a trial license.
Expiration Date	Expiration date of the temporary or evaluation license.
Valid	Indicates that the license is valid and active.

Configuring License Expiration Email Notifications

For licenses with an expiration date, the administrator can configure email messages to notify specified parties of when a license is set to expire. OV3600 sends an expiration notification email six months, three months, one month, and one week prior to expiration. Additionally, the email lists time remain for each expiring license installed on the OV3600 server. This feature is disabled by default.

To configure Expiry Notifications:

1. Navigate to **Home > License > Expiry Notification Settings**.
2. Check the **Receive Email Notifications** check box to enable.
3. Insert any number of email addresses separated by spaces, commas, or semicolons.
4. Click **Save**.

Configuring User Information and Customizing the WebUI

You can update your user information and customize what you see in the OV3600 in the WebUI from the User Info page (see Figure 206).

Configure Your User Information

To configure your user information:

1. Navigate to **Home > User Info**.
2. In the **User Information** section, enter the following information :
   - **Name**—Enter the ID by which you log into and operate in OV3600.
   - **Email Address**—Enter the email address to be used for alerts, triggers, and additional OV3600 functions that support an email address.
   - **Phone**—Enter the area code and phone number, if desired.
   - **Notes**—Enter any additional text-based information that helps other OV3600 users or administrators to understand the functions, roles, or other rights of the user being created.

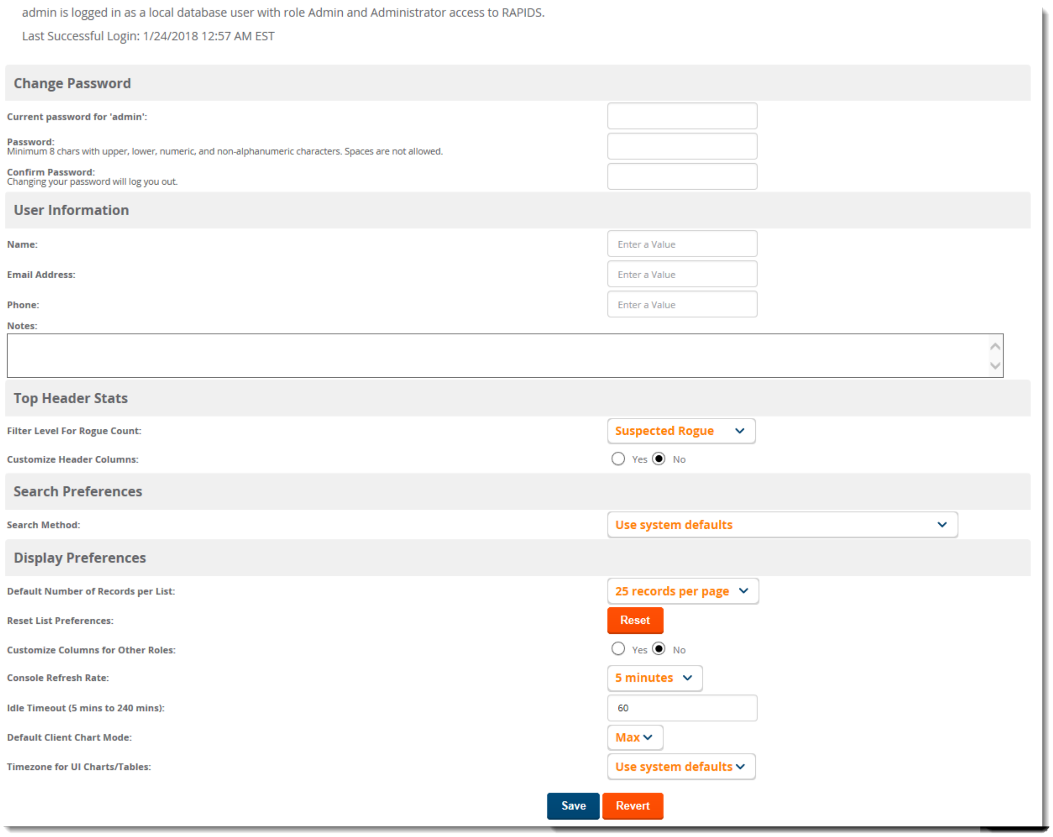
Customizing the WebUI

You can customize your top header statistics, search preferences, and display preferences.

To configure what you see in the OV3600 WebUI:

1. Navigate to **Home > User Info**.
2. Complete the information described in Table 139.

Figure 206: *User Info Page*



admin is logged in as a local database user with role Admin and Administrator access to RAPIDS.

Last Successful Login: 1/24/2018 12:57 AM EST

Change Password

Current password for 'admin':	
Password: Minimum 8 chars with upper, lower, numeric, and non-alphanumeric characters. Spaces are not allowed.	
Confirm Password: Changing your password will log you out.	

User Information

Name:	Enter a Value
Email Address:	Enter a Value
Phone:	Enter a Value
Notes:	

Top Header Stats

Filter Level For Rogue Count:	Suspected Rogue
Customize Header Columns:	○ Yes ● No

Search Preferences

Search Method:	Use system defaults

Display Preferences

Default Number of Records per List:	25 records per page
Reset List Preferences:	Reset
Customize Columns for Other Roles:	○ Yes ● No
Console Refresh Rate:	5 minutes
Idle Timeout (5 mins to 240 mins):	60
Default Client Chart Mode:	Max
Timezone for UI Charts/Tables:	Use system defaults

Table 139: *Home > User Info Fields and Descriptions*

Field	Description
Top Header Stats	
Filter Level For Rogue Count	Specifies the minimum classification that will cause a device to be included in the rogue count header information. More about the classifications can be found in "switch Classification with WMS Offload" on page 248.
Customize Header Columns	Enables/disables the ability to control which statistics hyperlinks (also known as Top Header Stats) are displayed at the top of every OV3600 screen.
Stats	Select the specific data you would like to see in the Top Header Stats. Refer to the "Status Section" topic in the *OmniVista 3600 Air Manager 8.2.7.1 Installation Guide*. **Note**: This field only appears if you selected **Yes** in the previous field.
Severe Alert Threshold	Configures the minimum severity of an alert to be included in the Severe Alerts count. See "Setting Severe Alert Warning Behavior" on page 311 for details. **Note:** The severe alerts count header info will only be displayed if 'Severe Alerts' is selected in the **Stats** section above and if a severe alert exists. **Note**: This field only appears if you selected **Yes** in the **Customize Header Columns** field.

Table 139: *Home > User Info Fields and Descriptions (Continued)*

Field	Description
Include Device Types	Configures the types of devices that should be included in the header stats. If a device type is not selected then it will not be included in the header stats. **Note:** This field only appears if you selected **Yes** in **Customize Header Columns**.
Search Preferences	
Search Method	Specify one of the following search methods: - Use System Defaults: The Search Method will be based on the system-wide configuration setting. This method is configured on the **OV3600 Setup > General** page.Active clients + all devices: This looks at all active clients (not historical) and all devices. This search is not case-sensitive. - Active clients + historical clients (exact match) + all devices: Commonly referred to as Quick Search, this looks at all active and historical clients and all devices. This search is not case-sensitive. The results of this search display in a pop up window rather than on the **Home > Search** page. This pop up window includes top-level navigation that allows you to filter the results based on Clients, APs, Controllers, and Switches. - Active clients + all categories: This looks at all active clients (not historical) and all categories. This search is not case-sensitive. - Active clients + all categories (exact match): This looks at all active clients (not historical) and all categories. This search returns only matches that are exactly as typed (IP, user name, device name, etc). This search is case-sensitive for all searched fields. - Active + historical clients + all categories: This looks at all active and historical clients and all categories. This search is not case-sensitive. - Active + historical clients + all categories (exact match): This looks at all active and historical clients and all categories. This search returns only matches that are exactly as typed (IP, user name, device name, etc). This search is case-sensitive for all searched fields.
Display Preferences	
Default Number of Records per List	Defines the number of rows to appear in any list by default. If a row count is manually set, it will override the default setting.
Reset List Preferences	Reset all list preferences including number of records per list, column order and hidden column information.
Customize Columns for Other Roles	Allows admin users to determine the columns that should be displayed and the order they should be displayed for specific user roles. To customize lists for other users, navigate to that list and select **Choose Columns for roles** above the list. Make the desired column changes; select the roles to update and **Save**.
Console Refresh Rate	The frequency in which lists and charts automatically refresh on a page.
Idle Timeout (5 mins to 240 mins)	Number of minutes of idle time until OV3600 automatically ends the user session. This setting only the logged-in user of this OV3600. The default is 60 minutes. To set the max idle timeout for all users of this OV3600, see "Configuring the User Login" on page 45.

Setting Severe Alert Warning Behavior

You can control the alert levels you can see on the **Alerts** top header stats link using the **Severe Alert Threshold** drop down menu located in the **Top Header Stats** section of the **Home > User Info** page. The **Severe Alert Threshold** determines the severity level that results in a Severe Alert. Specify either **Normal**, **Warning**, **Minor**, **Major**, or **Critical** as the severity alert threshold value. These threshold values are tied to triggers that are created on the **System > Triggers** page. For example, if a trigger is defined to result in a Critical alert, and if the Severe Alert Threshold here is defined as Major, then the list of Severe Alerts will include all Major and Critical alerts. Similarly, if this value is set to Normal, which is the lowest threshold, then the list of Severe Alerts will include all alerts.

When a Severe Alert exists, a new component named **Severe Alerts** will appear at the right of the **Status** field in bold red font. This field is hidden if there are no Severe Alerts. In addition, only users who are enabled for viewing Severe Alerts on the **Home > User Info** page can see severe alerts.

Using the Master Console

You can monitor multiple OV3600 servers using the Master Console. After you add the OV3600 servers to Master Console, they will be polled for basic OV3600 information.

The **Overview** page in the Master Console provides summary statistics for the entire network at a glance.

- Reports can be run from the **Master Console** to display information from multiple OV3600 stations; because such reports can be extremely large, reports can also be run as summary only so that they generate more quickly and finish as a manageable file size.
- The **Master Console** can also be used to populate group-level configuration on managed OV3600 installations using the **Global Groups** feature.
- The **Master Console** offers a display of devices that are in a **Down** or **Error** state anywhere on the network. This information is supported on **Master Console** pages that display device lists such as **Home > Overview** and **APs Devices > List**.
- The **Master Console** and **Failover** servers can be configured with a **Managed OV3600 Down** trigger that generates an alert if communication is lost to a managed or watched OV3600 station. The **Master Console** or **Failover** server can also send email or NMS notifications about the event.

NOTE

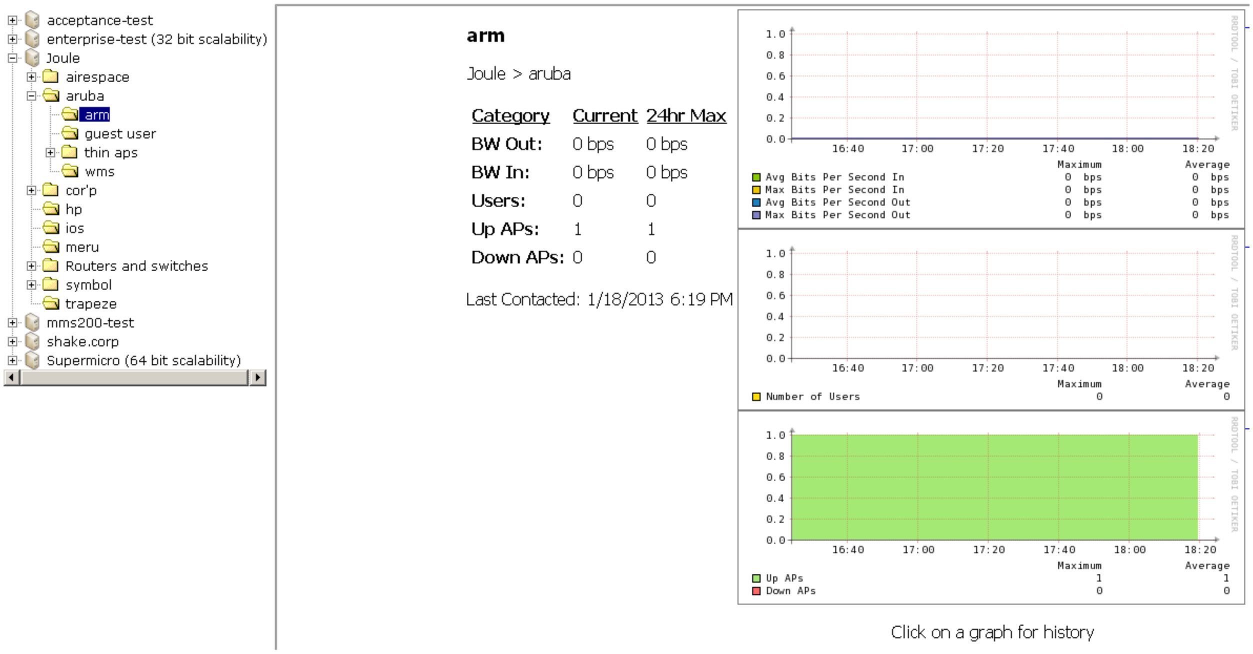
XML APIs are not supported on the Master Console.

If you have the Master Console license, you can also monitor your multiple OV3600 servers using Glass. For more information, see the *Glass 1.0.0 User Guide*.

Using the Public Portal on Master Console

The **Master Console** also contains an optional Public Portal that allows any user to view basic group-level data for each managed OV3600. This feature is disabled by default for security reasons; no OV3600 or Master Console login is required to view the public portal. The Public Portal can be enabled in **OV3600 Setup > General** in the **Master Console** section. Once enabled, a new **Portal** tab will appear to the right of the **Groups** tab . The URL of the public portal will be https://your.OV3600.name/public. When you upgrade to the latest version of OV3600, the public portal is disabled by default, regardless of the type of license.

Figure 207: *Public Portal Page Illustration*



- acceptance-test
- enterprise-test (32 bit scalability)
- Joule
  - airespace
  - aruba
    - arm
    - guest user
    - thin aps
    - wms
  - cor'p
  - hp
  - ios
  - meru
  - Routers and switches
  - symbol
  - trapeze
- mms200-test
- shake.corp
- Supermicro (64 bit scalability)

arm

Joule > aruba

Category	Current	24hr Max
BW Out:	0 bps	0 bps
BW In:	0 bps	0 bps
Users:	0	0
Up APs:	1	1
Down APs:	0	0

Last Contacted: 1/18/2013 6:19 PM

1.0
0.8
0.6
0.4
0.2
0.0
16:40
17:00
17:20
17:40
18:00
18:20
RRDTOOL / TOBI OETIKER
Maximum
Average
🟩 Avg Bits Per Second In 0 bps 0 bps
🟨 Max Bits Per Second In 0 bps 0 bps
🟦 Avg Bits Per Second Out 0 bps 0 bps
🟪 Max Bits Per Second Out 0 bps 0 bps
🟨 Number of Users 0 0
🟩 Up APs 1 1
🟥 Down APs 0 0

Click on a graph for history

The Public Portal supports configuration of the iPhone interface, which can be configured using the Master Console OV3600 page.

Adding a Managed OV3600 with the Master Console

Perform the following steps to add a managed OV3600 console.

1. Navigate to the **Home > Managed OV3600s** page.
2. Select the **pencil** icon to edit or reconfigure an existing OV3600 console, or select **Add New Managed OV3600** to create a new OV3600 console. The **Managed OV3600** page appears. Complete the settings on this page as described in Table 140.

Table 140: *Managed OV3600 fields and default values*

Field	Default	Description
Hostname / IP Address	N/A	Enter the IP address or Hostname of the OV3600 server to be managed.
Polling Enabled	Yes	Enables or disables the Master Console polling of managed OV3600 server.
Polling Period	5 minutes	Determines how frequently the Master Console polls the managed OV3600 server.
Username	N/A	The user name used by the Master Console to login to the managed OV3600 server. The user needs to be an AP/Device Manager or OV3600 Administrator.
Password (Confirm Password)	N/A	The password used by the Master Console to login to the managed OV3600 server.
HTTP Timeout (5-1000 sec)	60	Defines the timeout period used when polling the managed OV3600 server.

Table 140: *Managed OV3600 fields and default values (Continued)*

Field	Default	Description
Manage Group Configuration	No	Defines whether the Master Console can manage device groups on the managed OV3600 server.

3. When finished, select **Add** to return to the **Managed OV3600s** list page.

Using Global Groups with Master Console

To push configurations to managed groups using the OV3600 Global Groups feature, follow these steps:

1. Navigate to the Master Console's **Groups > List** page.
2. Select **Add** to add a new group, or select the name of the group to edit settings for an existing group.
3. Select the **Duplicate** icon to create a new group with identical configuration to an existing group. Groups created on the Master Console will act as Global Groups, or groups with master configurations that can be pushed out to subscriber groups on managed OV3600s. Global groups are visible to all users, so they cannot contain APs (which can be restricted based on user role).
4. Selecting the name of an existing group on the **Master Console** loads the subtabs for **Basic, Security, SSIDs, AAA Servers, Templates, Radio, Cisco WLC Config, Proxim Mesh,** and **MAC ACL** pages, if such pages and configurations are active for the devices in that group.

   These subtabs contain the same fields as the group subtabs on a monitored OV3600, but each field also has a check box. The Master Console can also configure global templates that can be used in subscriber groups. The process is the same as described in the templates chapter of the OV3600 User Guide, except that there is no process by which templates can be fetched from devices in the subscriber group on managed OV3600 servers. Instead, the template must be copied and pasted into the Master Console Global Group.

When a Global Group is pushed from the **Master Console** to subscriber groups on managed OV3600s, all settings will be static except for settings with the check box selected; for fields with check boxes selected, the value or setting can be changed on the corresponding tab for each managed group. For list pages, override options are available only on the **Add** page for each list. It will take several minutes for changes to Global Groups on the **Master Console** to be pushed to the managed OV3600 servers; make sure that the **Manage Group Configuration** option is enabled for each managed OV3600.

Once Global Groups have been configured on the **Master Console**, groups must be created or configured on the managed OV3600 servers to subscribe to a particular Global Group. To configure subscriber groups, enable **Use Global Groups** on the **Group > Basic** page of a group on a managed OV3600. Select the name of the Global Group from the drop-down menu, and then select **Save and Apply**. Note that the MC doesn't push anything when you create new subscriber groups; the copy of the Global Group already on the managed OV3600 provides the information.

Once the configuration is pushed, the non-overridden fields from the Global Group will appear on the subscriber group as static values and settings. Only fields that had the override check box selected in the Global Group will appear as fields that can be set at the level of the subscriber group. Any changes to a static field must be made on the Global Group.

The Global Groups feature can also be used without the Master Console. For more information about how this feature works, refer to the **Configuring and Using Device Groups** chapter of the OV3600 User Guide"Using Device Groups" on page 72.

Logging out of OV3600

To log out of OV3600, select the **Logout** link on the upper right hand corner of every OV3600 page.

You will be logged off automatically based on the number of minutes set in the **Idle Timeout** setting of **Home > User Info**. Refer to "Configuring the User Login" on page 45.

Chapter 9
Creating, Running, and Sending Reports

Reports in OV3600 are powerful tools for network analysis, user configuration, device optimization, and network monitoring. All reports can be printed, emailed, or exported.

What You Can Do With Reports

OV3600 includes default reports that contain one or more sections of data, (also called widgets). The most commonly used reports are the Aruba License, Device Summary, Inventory, Client Details, Traffic Analysis, and RF Health reports . You can also create a custom report by combining individual widgets from multiple report types. The default report definitions become available after you have applied a license key.

You can access these reports after they have run, through hyperlinks on the **Generated Reports** page. You might want to keep only the reports that you need and delete, or reschedule, others to optimize your disk space. For information about working with reports, see "About the Default Reports" on page 317.

OV3600 populates the default reports with pre-defined fields. Some default reports don’t span a period of time, taking snapshots of your device inventory and configurations. Commonly used reports include: inventory, configuration audit, and client sessions.

If these reports don't have the details you need, you can build a custom report with the help of widgets. By changing the restriction settings, you can isolate a folder, group, or period of time. For information about report customization, see "Creating Custom Reports" on page 348 and "Cloning Reports" on page 348.

Track licenses

- License. Use this report to track licenses on the devices in your network. The report includes the license type, quantity, percentage used, installation dates, expiration dates, and license keys. For information, see "Using the License Report" on page 317.

Improve Network Efficiency and User Experience

- Capacity Planning. Use this report to track device bandwidth capacity and throughput in groups, folders, and SSIDs. Based on interface-level activity, you can use it to analyze device capacity and performance on the network. For information, see "Using the Capacity Planning Report" on page 318.
- Memory and CPU Utilization. Use this report to view the top percentage of memory utilization and usage for devices and CPUs. You can use filters by specific devices, such as controllers, switches, and APs. For information, see "Using the Memory and CPU Utilization Report" on page 320.
- Network Usage. Use this report to track network-wide information by usage and clients. You can narrow information by groups and folders, or summarize by usage and client count for folders. For information, see "Using the Network Usage Report" on page 320.
- Port Usage. Use this report to find all the ports and switches in your network and view traffic patterns. The histogram identifies unused ports and switches. For information, see "Using the Port Usage Report" on page 322.
- RF Health. Use this report to monitor the top AP radio issues by noise, MAC/Phy errors, channel changes, transmit power changes, mode changes, and interfering devices (the last two apply only if there are ARM events). This report helps pinpoint the most problematic devices on your network, and lists the top devices by problem type. For information, see "Using the RF Health Report" on page 324.
- UCC. Use this report to monitor UCC activity on your network. This information includes the top connectivity types, call types, application types, device types, folders, APs, and clients with the highest percentage of poor quality calls. For information, see "Using the UCC Report" on page 302.

Monitor Clients and Devices

- Client Inventory. Use this report to view information about clients that connected to your network. You can use filters and match criteria to customize your report. Information reported includes include manufacturer make and model, OS summary, asset category and group, and authentication type. For information, see "Using the Client Inventory Report" on page 326.
- Client Session. Use this report to view information for each time a user connects to your network. You can use filters and match criteria to customize your report. Information reported includes MAC address, user name, role, and SSID. For information, see "Using the Client Session Report" on page 328.
- Configuration Audit. Use this report to see a network snapshot of your device configurations. You can get an inventory one device at a time, one folder at a time, or one device group at a time. The report includes hypertext links to device configuration pages. For information, see "Using the Configuration Audit Report" on page 330.
- Device Summary. Use this report to see which devices are used the most or least, as well as get an inventory of all devices. You can also use this report to establish more equal bandwidth distribution across multiple devices. For information, see "Using the Device Summary Report" on page 332.
- Device Uptime. Use this report to monitor device performance and availability. This report covers average uptimes by SNMP and ICMP protocols, device groups and folders, or SSID information. You can add time restrictions so OV3600 only generates the report during a planned maintenance period or business days. For information, see "Using the Device Uptime Report" on page 333.
- Inventory. Use this report to track all devices in your network. For example, you could use the report to find Cisco devices and break down the list by model and device type. For information, see "Using the Inventory Report" on page 334.
- Rogue Containment Audit. Use this report to see whether your rogue containments are failing. For information, see "Using the Rogue Containment Audit Report" on page 336.

Show Compliance

- PCI Compliance. Use this report to view PCI configurations and show compliance during an audit. For information, see "Using the PCI Compliance Report" on page 337.

Troubleshoot Device and Network Issues

- IDS Events. Use this report to respond to IDS events on the network involving APs or controller devices. OV3600 reports on devices that have had the most events in the prior 24 hours. The report includes hypertext links to device configuration pages. You can use filters to show IDS events for specific devices, such as controllers and APs. For information, see "Using the IDS Events Report" on page 338.
- Match Event. Use this report to track matching events that occurred on devices. For example, you could use the report to find sticky client problems and break down the information by folder, AP, and client. For information, see "Using the Match Event Report" on page 339.
- New Clients. Use this report to see new clients that OV3600 discovered on the network during the time duration of the report. Information reported includes user identifier, associated role when known, and device information. You can use filters to find specific devices and users, matching criteria, or view all information. For information, see "Using the New Clients Report" on page 339.
- New Rogue Devices. Use this report to find rogues device on your network. Before OV3600 can run the report, you must define the restrictions. For information, see "Using the New Rogue Devices Report" on page 341.
- RADIUS Authentication Issues. Use this report to find the top 10 issues with controllers, RADIUS servers, and users. The report includes the number of total failures and the first and most recent event times. For information, see "Using the RADIUS Reports" on page 343.

- RADIUS Accounting Issues. Use this report to find the top 10 issues by device, controller, RADIUS server, and client. For information, see "RADIUS Accounting Issues" on page 344.
- Rogue Clients. Use this report to track the number of valid users that connected to rogues in the specified time frame. You can filter results by rogue classification, and you can include ad-hoc devices and client details. By default, the minimum RAPIDS classification is suspected rogue, and the maximum is contained rogue. For information, see "Using the Rogue Clients Report" on page 345.
- VPN Session. Use this report to view summary or detailed information about VPN activity by sessions. You can use filters or narrow results with match criteria. You can also specify device types to include in the report. For information, see "Using the VPN Session Report" on page 347.

Sorting Reports

By default, the **Reports > Generated** page lists reports ordered by generation time. You can sort reports by any column header, or choose columns to display. Clicking the report title opens the report.

Table 141 describes each column for the **Reports > Generated** page.

Table 141: *Reports > Generated Page Fields and Descriptions*

Field	Description
Generated Time	Displays the date and time of the last time the report was run, or when the latest report is available. Selecting the link in this field displays the latest version of a given report. When the latest version of a given report is not available, this field is blank. In this case, a report can be run by selecting the report title and selecting **Run**.
Title	Displays title of the report. This is a user-configured field when creating the report.
Type	Displays the type of the report.
Subject	Displays the scope of the report, to include groups, folders, SSIDs, or any combination of these that are included in the report.
User	This displays the user who created the customized report.
Report Start	Displays the beginning of the time period covered in the report.
Report End	Displays the end of the time period covered in the report.
Role	In the **Reports definitions for other roles** section, this column indicates the roles for which additional reports are defined.

About the Default Reports

This section describes the default reports in OV3600 that run daily. You can access these reports from the **Reports > Generated** page. If you need to customize a report, see "Creating Custom Reports" on page 348.

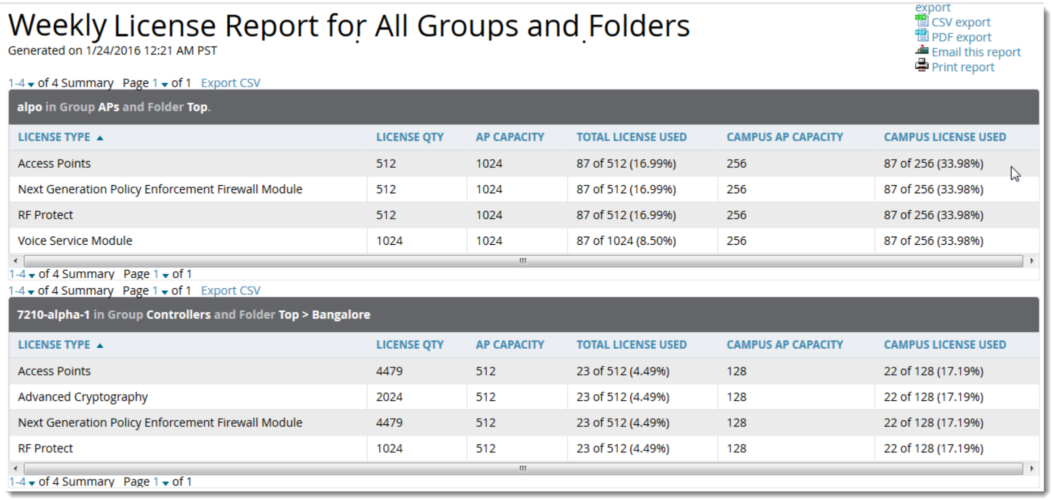
Using the License Report

The Alcatel-Lucent License Report tracks licenses on Alcatel-Lucent devices in your network. This report includes information on the type, quantity, percent used, installation date, expiration date, and the license keys.

NOTE

This report includes the built-in license count only when the installed license count is less than the license limits.

Figure 208: *Alcatel-Lucent Detail Page*



Weekly License Report for All Groups and Folders

Generated on 1/24/2016 12:21 AM PST

1-4 of 4 Summary Page 1 of 1 Export CSV

alpo in Group **APs** and Folder **Top**.

LICENSE TYPE ▲	LICENSE QTY	AP CAPACITY	TOTAL LICENSE USED	CAMPUS AP CAPACITY	CAMPUS LICENSE USED
Access Points	512	1024	87 of 512 (16.99%)	256	87 of 256 (33.98%)
Next Generation Policy Enforcement Firewall Module	512	1024	87 of 512 (16.99%)	256	87 of 256 (33.98%)
RF Protect	512	1024	87 of 512 (16.99%)	256	87 of 256 (33.98%)
Voice Service Module	1024	1024	87 of 1024 (8.50%)	256	87 of 256 (33.98%)

1-4 of 4 Summary Page 1 of 1

1-4 of 4 Summary Page 1 of 1 Export CSV

7210-alpha-1 in Group **Controllers** and Folder **Top > Bangalore**

LICENSE TYPE ▲	LICENSE QTY	AP CAPACITY	TOTAL LICENSE USED	CAMPUS AP CAPACITY	CAMPUS LICENSE USED
Access Points	4479	512	23 of 512 (4.49%)	128	22 of 128 (17.19%)
Advanced Cryptography	2024	512	23 of 512 (4.49%)	128	22 of 128 (17.19%)
Next Generation Policy Enforcement Firewall Module	4479	512	23 of 512 (4.49%)	128	22 of 128 (17.19%)
RF Protect	1024	512	23 of 512 (4.49%)	128	22 of 128 (17.19%)

1-4 of 4 Summary Page 1 of 1

Using the Capacity Planning Report

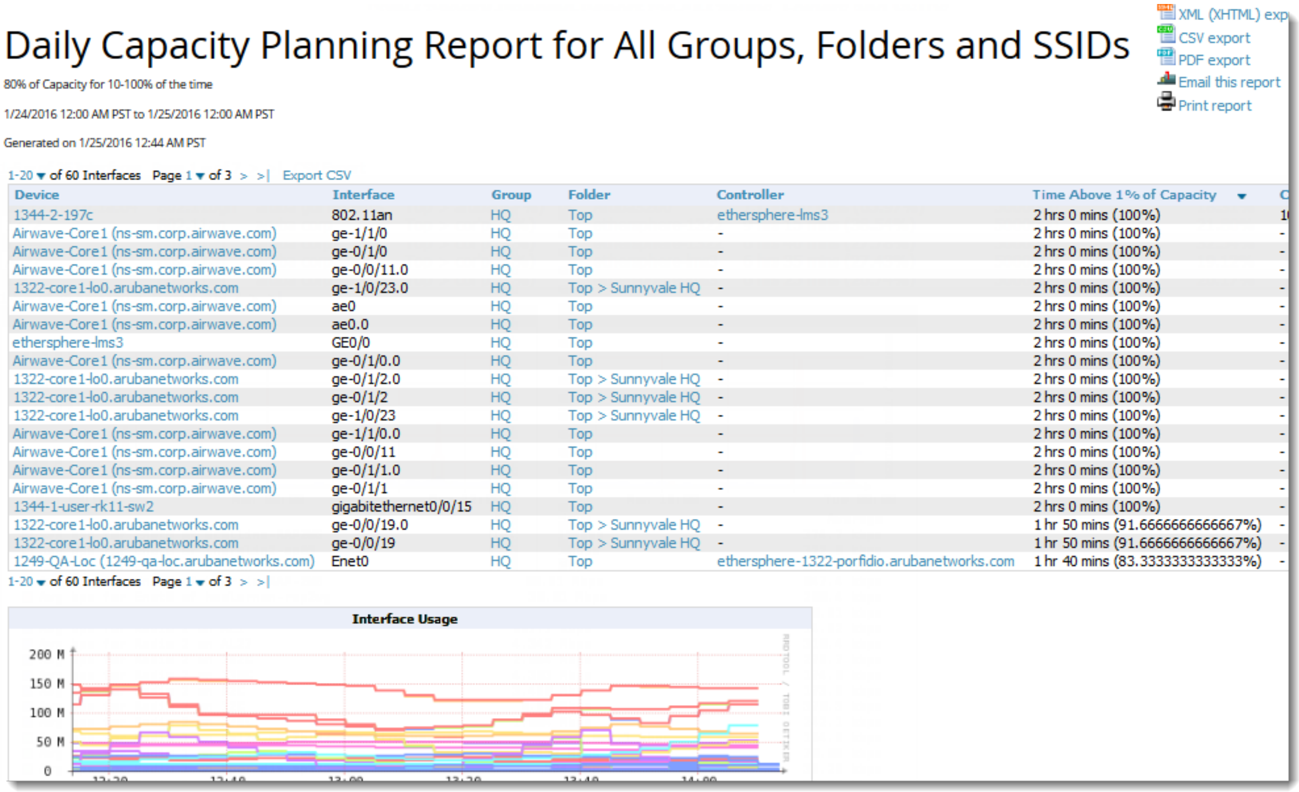
The Capacity Planning Report tracks device bandwidth capacity and throughput in device groups, folders, and SSIDs. With this report, you can achieve network efficiency and an improved user experience. For information about bandwidth information, see "Using the Network Usage Report" on page 320.

Example Custom Report

The following example creates a report looks for devices that are under-utilized. This report will search for devices over a 2-hour period that were at 1% of capacity for 5-100% of the time. Any setting omitted from this example remains the default value.

1. Navigate to **Reports > Definitions**, then click **Add New Report Definition**.
2. Enter the title, "Capacity Planning Report 1% for Group HQ".
3. Select **Capacity Planning** from the **Type** drop-down menu.
4. Select "HQ" from the **Groups** drop down menu.
5. Set the capacity threshold to 1.
6. Set the minimum time above the threshold to 5.
7. Set the maximum time above the threshold to 100.
8. Enter a 2-hour time interval for the report to run.
9. Click **Save and Run**. The report displays on the Generated Reports page when it is available, as shown in Figure 209.

Figure 209: *Capacity Planning Report*



XML (XHTML) exp
CSV export
PDF export
Email this report
Print report

Daily Capacity Planning Report for All Groups, Folders and SSIDs

80% of Capacity for 10-100% of the time

1/24/2016 12:00 AM PST to 1/25/2016 12:00 AM PST

Generated on 1/25/2016 12:44 AM PST

1-20 ▾ of 60 Interfaces Page 1 ▾ of 3 > >| Export CSV

Device	Interface	Group	Folder	Controller	Time Above 1% of Capacity ▾	C
1344-2-197c	802.11an	HQ	Top	ethersphere-lms3	2 hrs 0 mins (100%)	1
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-1/1/0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/1/0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/0/11.0	HQ	Top	-	2 hrs 0 mins (100%)	-
1322-core1-lo0.arubanetworks.com	ge-1/0/23.0	HQ	Top > Sunnyvale HQ	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ae0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ae0.0	HQ	Top	-	2 hrs 0 mins (100%)	-
ethersphere-lms3	GE0/0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/1/0.0	HQ	Top	-	2 hrs 0 mins (100%)	-
1322-core1-lo0.arubanetworks.com	ge-0/1/2.0	HQ	Top > Sunnyvale HQ	-	2 hrs 0 mins (100%)	-
1322-core1-lo0.arubanetworks.com	ge-0/1/2	HQ	Top > Sunnyvale HQ	-	2 hrs 0 mins (100%)	-
1322-core1-lo0.arubanetworks.com	ge-1/0/23	HQ	Top > Sunnyvale HQ	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-1/1/0.0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/0/11	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/1/1.0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/1/1	HQ	Top	-	2 hrs 0 mins (100%)	-
1344-1-user-rk11-sw2	gigabitethernet0/0/15	HQ	Top	-	2 hrs 0 mins (100%)	-
1322-core1-lo0.arubanetworks.com	ge-0/0/19.0	HQ	Top > Sunnyvale HQ	-	1 hr 50 mins (91.6666666666667%)	-
1322-core1-lo0.arubanetworks.com	ge-0/0/19	HQ	Top > Sunnyvale HQ	-	1 hr 50 mins (91.6666666666667%)	-
1249-QA-Loc (1249-qa-loc.arubanetworks.com)	Enet0	HQ	Top	ethersphere-1322-porfidio.arubanetworks.com	1 hr 40 mins (83.3333333333333%)	-

1-20 ▾ of 60 Interfaces Page 1 ▾ of 3 > >|

Interface Usage

Table 142 describes the fields in the Capacity Planning Report.

Table 142: *Capacity Planning Report Fields and Descriptions*

Field	Description
Device	Displays the device type or name.
Interface	Displays the type of 802.11 wireless service supported by the device.
Group	Displays the device group with which the device is associated.
Folder	Displays the folder with which the device is associated.
Controller	Displays the controller with which a device operates.
Time Above 1% of Capacity	Displays the time duration in which the device has functioned above 0% of capacity. A low percentage of use in this field may indicate that a device is under-used or poorly configured in relation to its capacity, or in relation to user needs.
Capacity Combined (b/s)	Displays the combined capacity in and out of the device, in bits-per-second.
Usage While > Threshold (Combined)	Displays the time in which a device has functioned above defined threshold capacity, both in and out.
Overall Usage (Combined)	Displays the overall usage of the device, both combined in and out traffic.

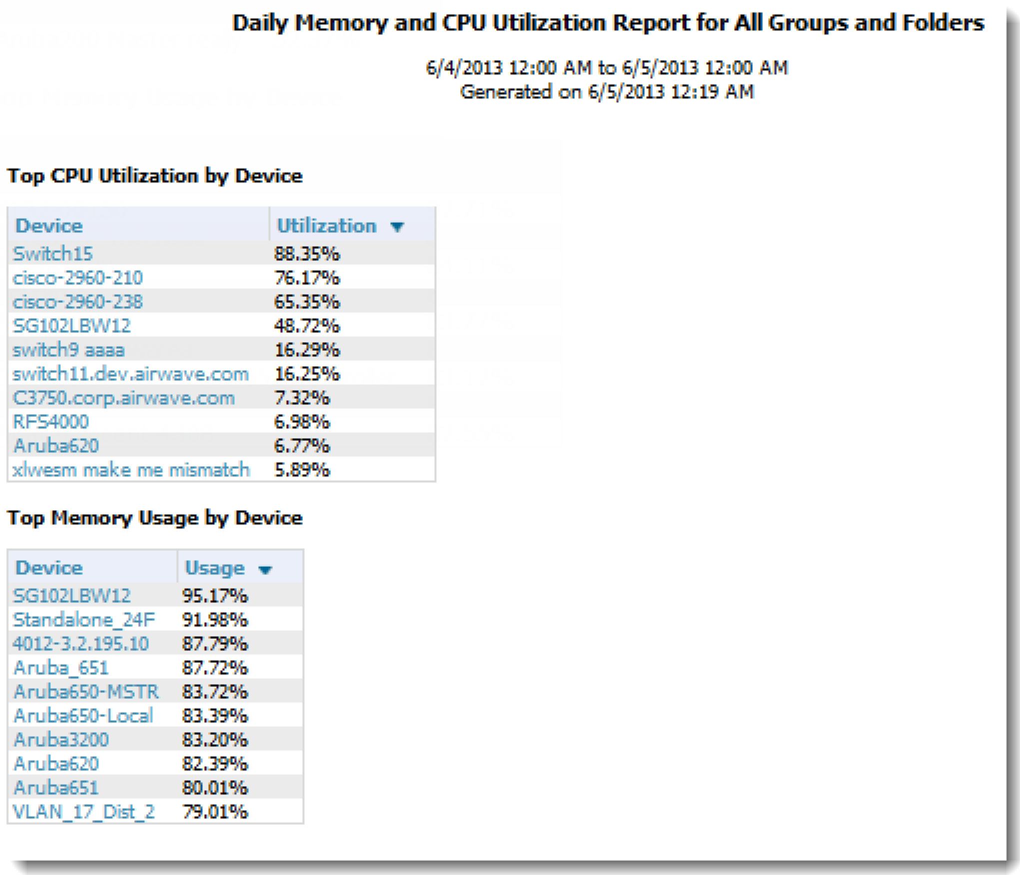
Table 142: *Capacity Planning Report Fields and Descriptions (Continued)*

Field	Description
Usage While > Threshold (in)	Displays device usage that exceeds the defined and incoming threshold capacity.
Overall Usage (In)	Displays overall device usage for incoming data.
Usage While > Threshold (Out)	Displays device usage for outgoing data that exceeds defined thresholds.
Overall Usage (Out)	Displays device usage for outgoing data.

Using the Memory and CPU Utilization Report

The Memory and CPU Utilization report, as shown in Figure 210, displays the top percentage of memory utilization and usage for devices and CPUs. You can filter this report by specific devices (controllers, APs, etc.), or to report on any number of IDS events for each specified device type.

Figure 210: *Daily Memory and CPU Usage Report*



Daily Memory and CPU Utilization Report for All Groups and Folders

6/4/2013 12:00 AM to 6/5/2013 12:00 AM
Generated on 6/5/2013 12:19 AM

Top CPU Utilization by Device

Device	Utilization ▼
Switch15	88.35%
cisco-2960-210	76.17%
cisco-2960-238	65.35%
SG102LBW12	48.72%
switch9 aaaa	16.29%
switch11.dev.airwave.com	16.25%
C3750.corp.airwave.com	7.32%
RFS4000	6.98%
Aruba620	6.77%
xlwesm make me mismatch	5.89%

Top Memory Usage by Device

Device	Usage ▼
SG102LBW12	95.17%
Standalone_24F	91.98%
4012-3.2.195.10	87.79%
Aruba_651	87.72%
Aruba650-MSTR	83.72%
Aruba650-Local	83.39%
Aruba3200	83.20%
Aruba620	82.39%
Aruba651	80.01%
VLAN_17_Dist_2	79.01%

Using the Network Usage Report

The Network Usage report, as shown in Figure 211, contains network-wide information in two categories:

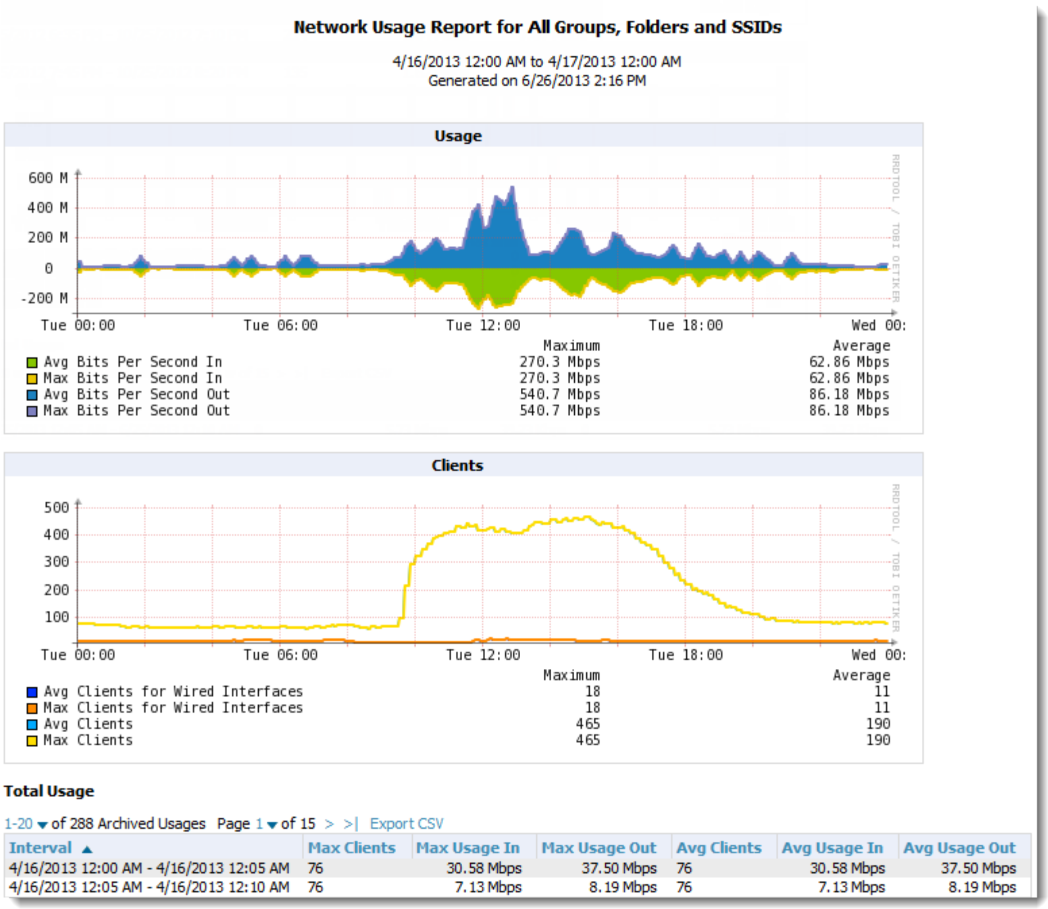
- **Usage**—maximum and average bandwidth
- **Clients**—average bandwidth in and out

This information can be broken down by Groups and Folders. It can also be summarized by Usage, Client Count, and by both for folders.

When you create this report, you can specify to view information for all or specific device types and all or specific SSIDs. You can summarize the report based on Client Count, Usage, and/or Usage and Client Count by Folder.

You can select an option to include tabular information below each graph, and then choose which columns display in the tables.

Figure 211: *Network Usage Report*



Network Usage Report for All Groups, Folders and SSIDs

4/16/2013 12:00 AM to 4/17/2013 12:00 AM
Generated on 6/26/2013 2:16 PM

	Maximum	Average
🟩 Avg Bits Per Second In	270.3 Mbps	62.86 Mbps
🟨 Max Bits Per Second In	270.3 Mbps	62.86 Mbps
🟦 Avg Bits Per Second Out	540.7 Mbps	86.18 Mbps
🟪 Max Bits Per Second Out	540.7 Mbps	86.18 Mbps

	Maximum	Average
🟦 Avg Clients for Wired Interfaces	18	11
🟧 Max Clients for Wired Interfaces	18	11
🟦 Avg Clients	465	190
🟨 Max Clients	465	190

Total Usage

1-20 ▾ of 288 Archived Usages Page 1 ▾ of 15 > >| Export CSV

Interval ▲	Max Clients	Max Usage In	Max Usage Out	Avg Clients	Avg Usage In	Avg Usage Out
4/16/2013 12:00 AM - 4/16/2013 12:05 AM	76	30.58 Mbps	37.50 Mbps	76	30.58 Mbps	37.50 Mbps
4/16/2013 12:05 AM - 4/16/2013 12:10 AM	76	7.13 Mbps	8.19 Mbps	76	7.13 Mbps	8.19 Mbps

Table 143: *Network Usage Report Fields and Descriptions*

Field	Description
Interval	This table is broken down in five-minute intervals. The Interval column describes the network usage information during these specific five minutes.
Max Clients	The maximum number of clients that were connected during this interval.
Max Usage In	Shows the maximum amount of incoming traffic on the network during this interval. This value is shown in Mbps.
Max Usage Out	Shows the maximum amount of outgoing traffic on the network during this interval. This value is shown in Mbps.

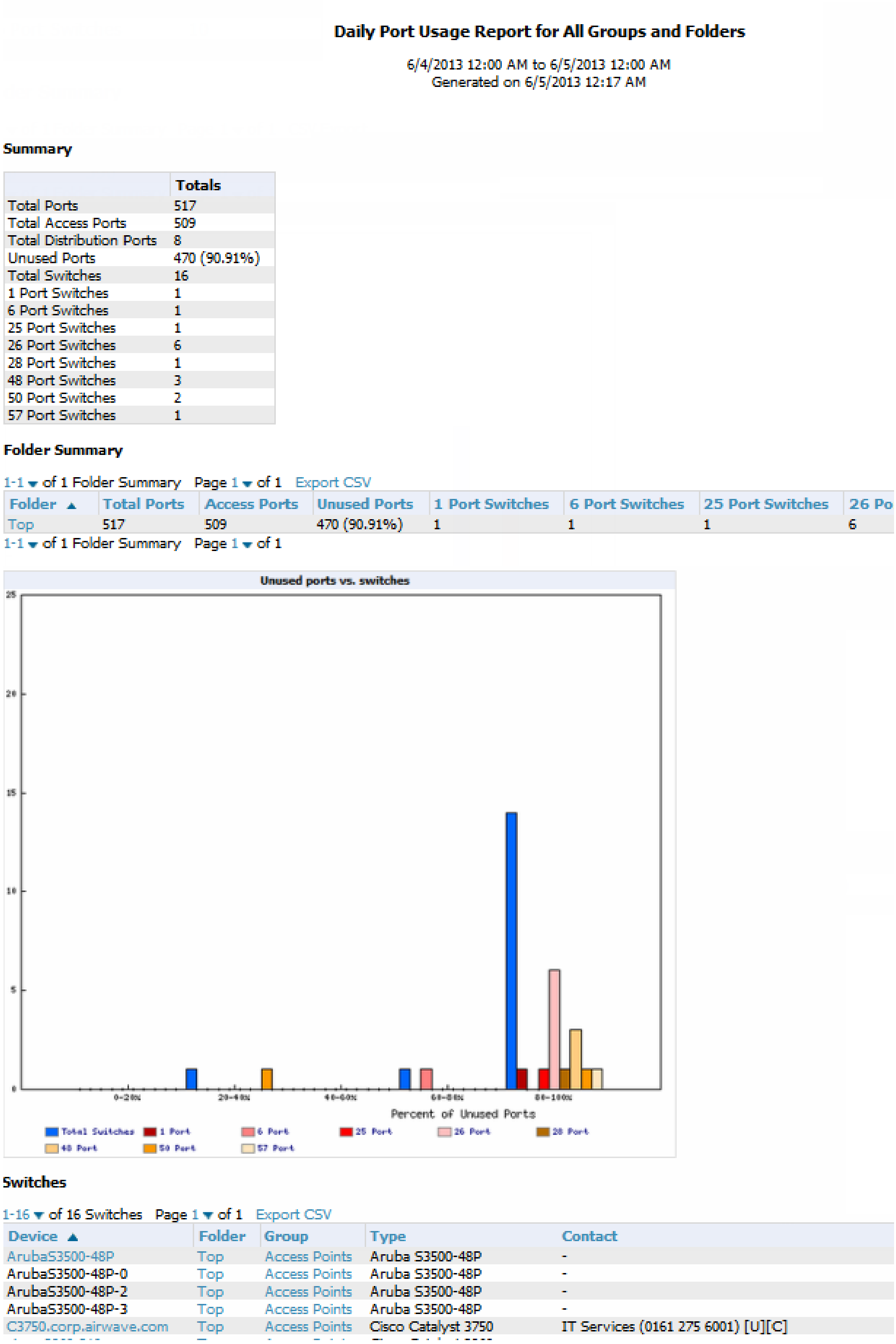
Table 143: *Network Usage Report Fields and Descriptions (Continued)*

Field	Description
Avg Clients	The average number of clients that were connected during this interval.
Avg Usage In	Shows the average amount of incoming traffic on the network during this interval. This value is shown in Mbps.
Avg Usage Out	Shows the average amount of outgoing traffic on the network during this interval. This value is shown in Mbps.

Using the Port Usage Report

The Port Usage report includes the following statistics: all the switches and ports in your network by folder, unused ports, access and distribution ports, most used switches, and most used ports. This report, as shown in Figure 212, also provides a histogram of unused ports vs. unused switches by type (access or distribution).

Figure 212: *Port Usage Report*



Daily Port Usage Report for All Groups and Folders

6/4/2013 12:00 AM to 6/5/2013 12:00 AM
Generated on 6/5/2013 12:17 AM

Summary

	Totals
Total Ports	517
Total Access Ports	509
Total Distribution Ports	8
Unused Ports	470 (90.91%)
Total Switches	16
1 Port Switches	1
6 Port Switches	1
25 Port Switches	1
26 Port Switches	6
28 Port Switches	1
48 Port Switches	3
50 Port Switches	2
57 Port Switches	1

Folder Summary

1-1 ▾ of 1 Folder Summary   Page 1 ▾ of 1   Export CSV

Folder ▲	Total Ports	Access Ports	Unused Ports	1 Port Switches	6 Port Switches	25 Port Switches	26 Po
Top	517	509	470 (90.91%)	1	1	1	6

1-1 ▾ of 1 Folder Summary   Page 1 ▾ of 1

Switches

1-16 ▾ of 16 Switches   Page 1 ▾ of 1   Export CSV

Device ▲	Folder	Group	Type	Contact
ArubaS3500-48P	Top	Access Points	Aruba S3500-48P	-
ArubaS3500-48P-0	Top	Access Points	Aruba S3500-48P	-
ArubaS3500-48P-2	Top	Access Points	Aruba S3500-48P	-
ArubaS3500-48P-3	Top	Access Points	Aruba S3500-48P	-
C3750.corp.airwave.com	Top	Access Points	Cisco Catalyst 3750	IT Services (0161 275 6001) [U][C]

Table 144 describes the fields in the Switches table that is in this report.

Table 144: *Switch Table Fields and Descriptions*

Field	Description
Device	The name of the device

Table 144: *Switch Table Fields and Descriptions (Continued)*

Field	Description
Folder/Group	The folder and group that this devices belongs to
Type	The switch type
Contact	Displays the contact info for the switch, if available
Location	Displays the location information for the switch, if available
Total Ports	The total number of ports available on the device
Access Ports	The total number of Access Ports available on the device
Unused Ports (%)	The percentage of the ports on the device that are unused
Traffic In	The amount of incoming traffic on the device
Traffic Out	The amount of outbound traffic on the device

Using the RF Health Report

The RF Health Report assists in pinpointing the most problematic devices on your network, and lists the top devices by problem type. The default RF Health report shows the max concurrent clients count per radio band.

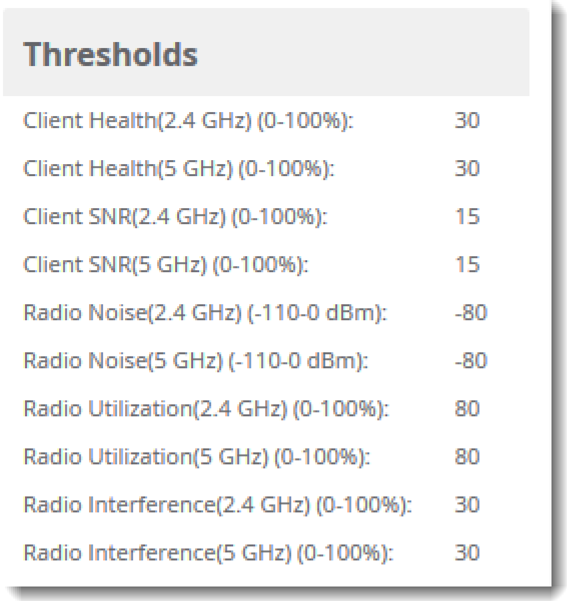
When creating a custom RF Health report, you can select the following widgets from the custom options:

- Max concurrent clients (2.4 GHz)
- Max concurrent clients (5 GHz)

From the generated report, you can open the monitoring page for the selected radio by clicking a hyperlink in the AP Name column.

Thresholds

Thresholds for the radio statistics are reported as a percentage (%) or a power measurement (dBm). For information on changing the threshold values, see "Changing Your Report Summary and Thresholds" on page 325.



Thresholds

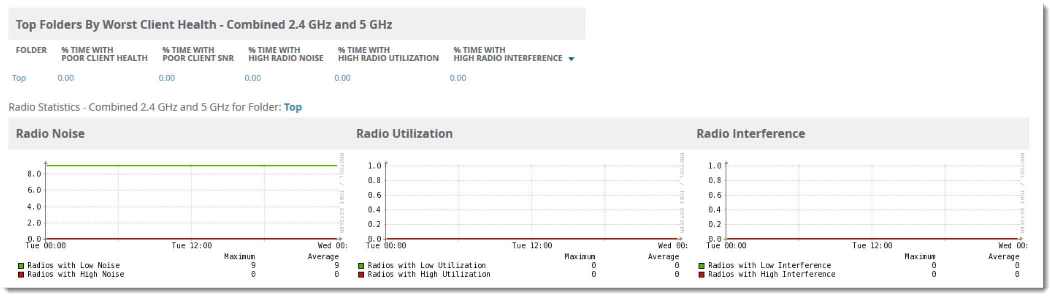
Client Health(2.4 GHz) (0-100%):	30
Client Health(5 GHz) (0-100%):	30
Client SNR(2.4 GHz) (0-100%):	15
Client SNR(5 GHz) (0-100%):	15
Radio Noise(2.4 GHz) (-110-0 dBm):	-80
Radio Noise(5 GHz) (-110-0 dBm):	-80
Radio Utilization(2.4 GHz) (0-100%):	80
Radio Utilization(5 GHz) (0-100%):	80
Radio Interference(2.4 GHz) (0-100%):	30
Radio Interference(5 GHz) (0-100%):	30

Top Folders and Radio Statistics

A report can be summarized by the following statistics:

- Top Folders By Worst Client and Radio Statistics Combined 2.4 GHz and 5 GHz
- Client and Radio Statistics by Folder - Combined 2.4 GHz and 5 GHz
- Top Folders By Worst Client and Radio Statistics 2.4 GHz
- Client and Radio Statistics by Folder - 2.4 GHz
- Top Folders By Worst Client and Radio Statistics 5 GHz
- Client and Radio Statistics by Folder - 5 GHz

The statistics displayed can be Client Health, Client SNR, Radio Noise, Radio Utilization, or Radio Interference.



Top Folders By Worst Client Health - Combined 2.4 GHz and 5 GHz

FOLDER	% TIME WITH POOR CLIENT HEALTH	% TIME WITH POOR CLIENT SNR	% TIME WITH HIGH RADIO NOISE	% TIME WITH HIGH RADIO UTILIZATION	% TIME WITH HIGH RADIO INTERFERENCE ▼
Top	0.00	0.00	0.00	0.00	0.00

Radio Statistics - Combined 2.4 GHz and 5 GHz for Folder: **Top**

Radio Noise

	Maximum	Average
🟩 Radios with Low Noise	9	9
🟥 Radios with High Noise	0	0

Radio Utilization

	Maximum	Average
🟩 Radios with Low Utilization	0	0
🟥 Radios with High Utilization	0	0

Radio Interference

	Maximum	Average
🟩 Radios with Low Interference	0	0
🟥 Radios with High Interference	0	0

Changing Your Report Summary and Thresholds

To select a new summary method:

1. Log in to OV3600.
2. Navigate to **Reports > Definitions**, then click **Add**.
3. Select **Daily RF Health Report**.
4. In the Report Restrictions area, select the **Summarize report by** options that you want.
5. Select the statistics to be displayed from the **Top Folder Sorting Column** drop-down menu.
6. Define the thresholds for your report.
7. Click **Save and Run** or **Save**.

If an RF Health Report has not been generated before, you can create it by following the instructions on the "Creating Custom Reports" on page 348 section of this chapter.

Lists of Top Radio Issues

OV3600 tracks the top AP radio issues and lists them by problems. A device will make it into the list of problems if it violates two or more thresholds. For more on the thresholds that indicate problems, refer to "Viewing the Radio Statistics Page" on page 142.)

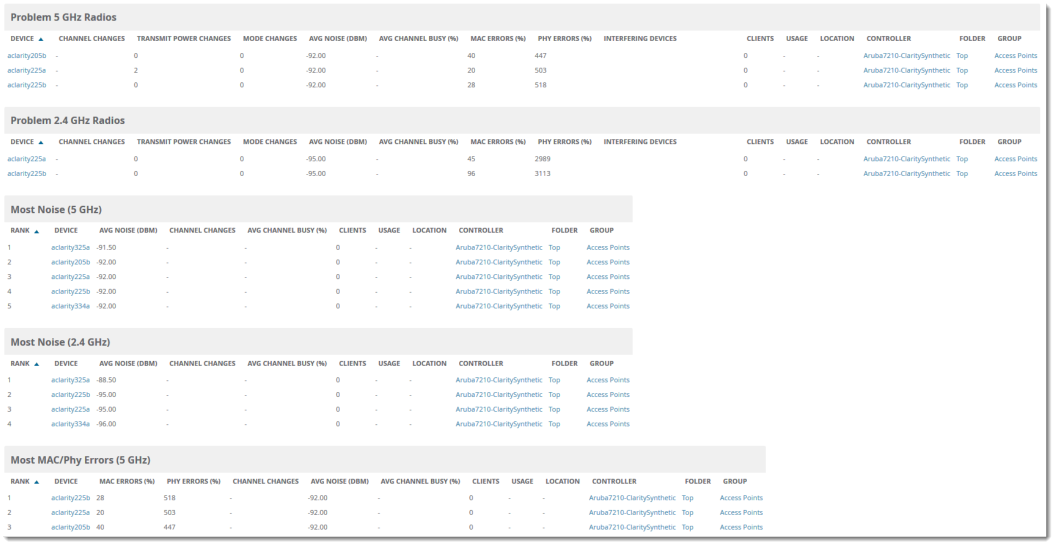
The lists for most mode changes and most interfering are available if there are ARM events.

Other lists include:

- Most or Least Utilized by Channel Usage
- Most MAC/Phy Errors
- Most Channel Changes
- Most Transmit Power Changes
- Clients with Least Goodput
- Clients with Least Speed
- Radios with Least Goodput

Figure 213 illustrates some of the lists on the Daily RF Health Report.

Figure 213: *Lists of Problems and Radio 8888 Issues*



Problem 5 GHz Radios

DEVICE ▲	CHANNEL CHANGES	TRANSMIT POWER CHANGES	MODE CHANGES	AVG NOISE (DBM)	AVG CHANNEL BUSY (%)	MAC ERRORS (%)	PHY ERRORS (%)	INTERFERING DEVICES	CLIENTS	USAGE	LOCATION	CONTROLLER	FOLDER	GROUP
aclarity205b	-	0	0	-92.00	-	40	447		0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
aclarity225a	-	2	0	-92.00	-	20	503		0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
aclarity225b	-	0	0	-92.00	-	28	518		0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points

Problem 2.4 GHz Radios

DEVICE ▲	CHANNEL CHANGES	TRANSMIT POWER CHANGES	MODE CHANGES	AVG NOISE (DBM)	AVG CHANNEL BUSY (%)	MAC ERRORS (%)	PHY ERRORS (%)	INTERFERING DEVICES	CLIENTS	USAGE	LOCATION	CONTROLLER	FOLDER	GROUP
aclarity225a	-	0	0	-95.00	-	45	2989		0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
aclarity225b	-	0	0	-95.00	-	96	3113		0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points

Most Noise (5 GHz)

RANK ▲	DEVICE	AVG NOISE (DBM)	CHANNEL CHANGES	AVG CHANNEL BUSY (%)	CLIENTS	USAGE	LOCATION	CONTROLLER	FOLDER	GROUP
1	aclarity325a	-91.50	-	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
2	aclarity205b	-92.00	-	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
3	aclarity225a	-92.00	-	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
4	aclarity225b	-92.00	-	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
5	aclarity334a	-92.00	-	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points

Most Noise (2.4 GHz)

RANK ▲	DEVICE	AVG NOISE (DBM)	CHANNEL CHANGES	AVG CHANNEL BUSY (%)	CLIENTS	USAGE	LOCATION	CONTROLLER	FOLDER	GROUP
1	aclarity325a	-88.50	-	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
2	aclarity225b	-95.00	-	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
3	aclarity225a	-95.00	-	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
4	aclarity334a	-96.00	-	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points

Most MAC/Phy Errors (5 GHz)

RANK ▲	DEVICE	MAC ERRORS (%)	PHY ERRORS (%)	CHANNEL CHANGES	AVG NOISE (DBM)	AVG CHANNEL BUSY (%)	CLIENTS	USAGE	LOCATION	CONTROLLER	FOLDER	GROUP
1	aclarity225b	28	518	-	-92.00	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
2	aclarity225a	20	503	-	-92.00	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points
3	aclarity205b	40	447	-	-92.00	-	0	-	-	Aruba7210-ClaritySynthetic	Top	Access Points

The RF Health report lists devices that are ranked and then sorted by the third column in the table. Click the blue **Device** link to access the **Devices > Monitor > Radio Statistics** page for the radio band.

NOTE

OV3600 limits data storage to 183 days, which is approximately six months, per radio. If you create an RF Health report with range of more than 183 days, the report will only include Channel Changes, Transmit Power Changes, Average Utilization, Mac/Phy Errors and Average Noise based on whatever part of the report intersects the last 183 days. Most reports have data (like bandwidth and users) that maxes out at 425 days. OV3600 validates reports so you can only run them over a 366-day duration.

Using the Client Inventory Report

The Client Inventory Report can be used for viewing information about clients that connected to you network. Similar to the Inventory Report, you can filter this report to search for specific devices (such as, "Aruba"). You can also filter this report based on the connection mode (wired or wireless).

This report also gives you the option to filter instead on specific devices and/or users. Whether viewing information for devices or clients, the report can configured to display additional options. For many of these options, you can choose to view all information or a specific set of information (Matching option). If Matching is selected, a text entry field displays. When you put your cursor in the text entry field, an additional side menu displays providing you with a list of available options that you can select.

- AOS Device Type - All or Matching
- Device Manufacturer - All or Matching
- Device Model - All or Matching
- Device Type - All or Matching
- OS Summary - All or Matching
- Steerable Clients
- Asset Category - All or Matching
- Asset Group - All or Matching
- Device Manufacturer and Model
- Device OS Detail - All or Matching
- EAP Supplicant - All or Matching
- Last Role
- Last Authentication Type
- Last Connection Mode
- Last SSID
- Network Chipset - All or Matching
- Network Driver - All or Matching
- Network Vendor

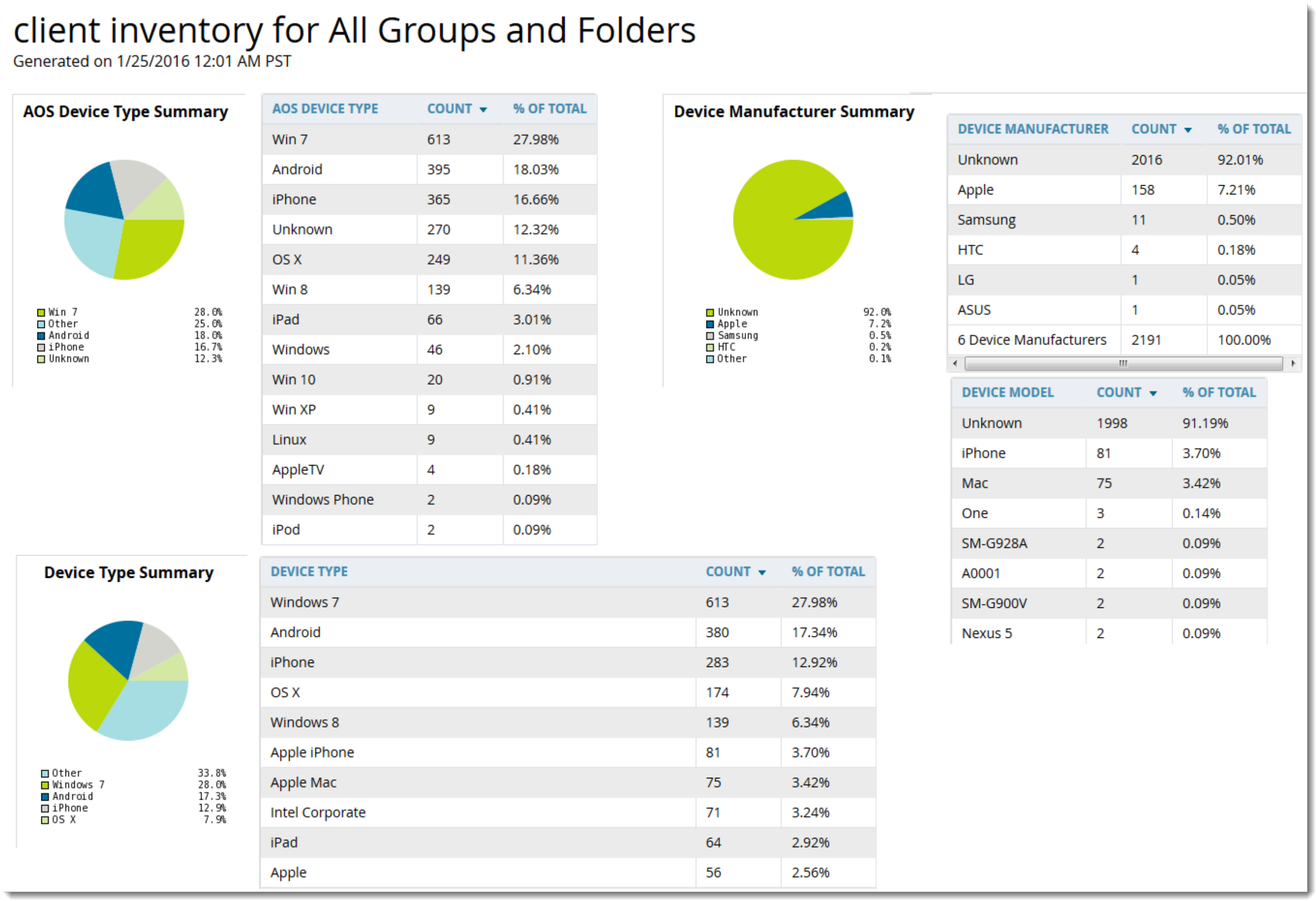
This report allows you to include details about every client, for example, the User Name, MAC Address, Role, AP Radio information, and more. Finally, you can limit this report to include devices that active or inactive at the time when this report is run.

Example Custom Report

The following example creates a summary report of Apple devices on your network. The report also displays the last connection mode and the last SSID for all devices to help determine how and where the devices are connecting.

1. Navigate to **Reports > Definitions**, then click **Add New Report Definition**.
2. Enter the title, called "Client Inventory - iPhone, iPod, iPad."
3. Select **Client Inventory** from the **Type** drop-down menu.
4. In the Summarize Report By section, select the AOS Device Type Summary, Device Type Summary, Last Connection Mode Summary, and Last SSID Summary options.
5. Specify "Matching" in the Model section for iPads, iPhones, and iPods.
6. Click **Save and Run**. The report displays on the Generated Reports page when it is available, as shown in Figure 214.

Figure 214: *Reports > Generated > Client Inventory (partial)*



client inventory for All Groups and Folders

Generated on 1/25/2016 12:01 AM PST

AOS Device Type Summary

AOS DEVICE TYPE	COUNT ▾	% OF TOTAL
Win 7	613	27.98%
Android	395	18.03%
iPhone	365	16.66%
Unknown	270	12.32%
OS X	249	11.36%
Win 8	139	6.34%
iPad	66	3.01%
Windows	46	2.10%
Win 10	20	0.91%
Win XP	9	0.41%
Linux	9	0.41%
AppleTV	4	0.18%
Windows Phone	2	0.09%
iPod	2	0.09%

Device Manufacturer Summary

DEVICE MANUFACTURER	COUNT ▾	% OF TOTAL
Unknown	2016	92.01%
Apple	158	7.21%
Samsung	11	0.50%
HTC	4	0.18%
LG	1	0.05%
ASUS	1	0.05%
6 Device Manufacturers	2191	100.00%

DEVICE MODEL	COUNT ▾	% OF TOTAL
Unknown	1998	91.19%
iPhone	81	3.70%
Mac	75	3.42%
One	3	0.14%
SM-G928A	2	0.09%
A0001	2	0.09%
SM-G900V	2	0.09%
Nexus 5	2	0.09%

Device Type Summary

DEVICE TYPE	COUNT ▾	% OF TOTAL
Windows 7	613	27.98%
Android	380	17.34%
iPhone	283	12.92%
OS X	174	7.94%
Windows 8	139	6.34%
Apple iPhone	81	3.70%
Apple Mac	75	3.42%
Intel Corporate	71	3.24%
iPad	64	2.92%
Apple	56	2.56%

The fields on this report are described in Table 145.

Table 145: *Client Inventory Report Fields and Descriptions*

Field	Description
AOS Device Type	Displays the device type or name.
Count	The total number of each device current included in the client inventory.
% of Total	The percentage of each of the devices that are included in the client inventory.
Last SSID Summary	The SSID most recently connected to by each device. This includes the total number of clients and the percentage of each of those devices that connected to the SSID.
Last Connection Mode	The most recent connection mode used by that each device .This includes the total number of clients and the percentage of each of those devices that connected for each connection mode.

Using the Client Session Report

The Client Session Report itemizes user-level activity by session, meaning any instance in which a user connects to the network. In list and chart format, this report displays session information, such as: cipher; connection mode; role; SSID or VLAN ID, top clients by total MB used; device type; asset category and group; EAP supplicant; manufacturer; model; network chipset, driver, and interface vendor; and OS.

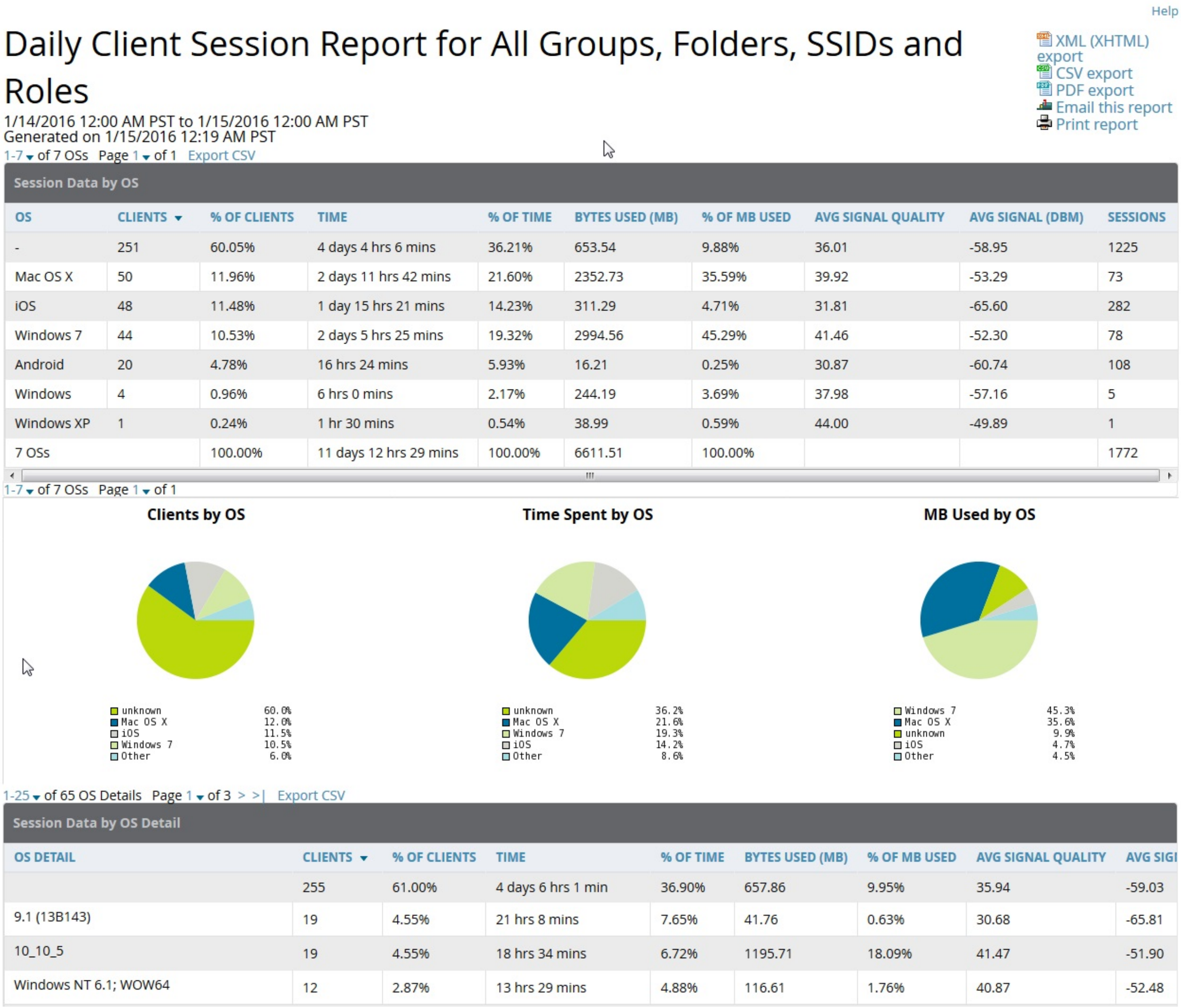
NOTE

The period of time in which the client remains connected to the network is typically calculated as a single session. However, if a client roams between APs, the periods of time the client connected to the different APs may be calculated as separate sessions.

Each report can be filtered based SSID, Device Type, Manufacturer, Model, and more.

You can specify the details that you want to include in the Sessions information, such as the MAC Address, user name, role, and SSID.

Figure 215: *Client Session Detail*



Help

Daily Client Session Report for All Groups, Folders, SSIDs and Roles

1/14/2016 12:00 AM PST to 1/15/2016 12:00 AM PST
Generated on 1/15/2016 12:19 AM PST

XML (XHTML) export
CSV export
PDF export
Email this report
Print report

1-7 ▾ of 7 OSs Page 1 ▾ of 1 Export CSV

Session Data by OS

OS	CLIENTS ▾	% OF CLIENTS	TIME	% OF TIME	BYTES USED (MB)	% OF MB USED	AVG SIGNAL QUALITY	AVG SIGNAL (DBM)	SESSIONS
-	251	60.05%	4 days 4 hrs 6 mins	36.21%	653.54	9.88%	36.01	-58.95	1225
Mac OS X	50	11.96%	2 days 11 hrs 42 mins	21.60%	2352.73	35.59%	39.92	-53.29	73
iOS	48	11.48%	1 day 15 hrs 21 mins	14.23%	311.29	4.71%	31.81	-65.60	282
Windows 7	44	10.53%	2 days 5 hrs 25 mins	19.32%	2994.56	45.29%	41.46	-52.30	78
Android	20	4.78%	16 hrs 24 mins	5.93%	16.21	0.25%	30.87	-60.74	108
Windows	4	0.96%	6 hrs 0 mins	2.17%	244.19	3.69%	37.98	-57.16	5
Windows XP	1	0.24%	1 hr 30 mins	0.54%	38.99	0.59%	44.00	-49.89	1
7 OSs		100.00%	11 days 12 hrs 29 mins	100.00%	6611.51	100.00%			1772

1-7 ▾ of 7 OSs Page 1 ▾ of 1

1-25 ▾ of 65 OS Details Page 1 ▾ of 3 > >| Export CSV

Session Data by OS Detail

OS DETAIL	CLIENTS ▾	% OF CLIENTS	TIME	% OF TIME	BYTES USED (MB)	% OF MB USED	AVG SIGNAL QUALITY	AVG SIGI
	255	61.00%	4 days 6 hrs 1 min	36.90%	657.86	9.95%	35.94	-59.03
9.1 (13B143)	19	4.55%	21 hrs 8 mins	7.65%	41.76	0.63%	30.68	-65.81
10_10_5	19	4.55%	18 hrs 34 mins	6.72%	1195.71	18.09%	41.47	-51.90
Windows NT 6.1; WOW64	12	2.87%	13 hrs 29 mins	4.88%	116.61	1.76%	40.87	-52.48

Each Client Session Report includes a Client Session Summary section. Table 146 describes the fields that display in this summary.

Table 146: *Client Session Summary Fields and Descriptions*

Field	Description
Sessions	The number of client sessions that occurred during the time range specified in this report.
Unique Clients	The number of unique clients that connected.
Guest Users	The number of guest users that connected.
Unique APs	The number of unique APs that were available.
Average session duration	The average amount of time that a client was connected during this time range. This is determined by {[disconnect time] - [connect time]}.
Total traffic (MB)	The total amount of traffic that passed through the network during this time range.
Total traffic In (MB)	The total amount of traffic that passed in the network.
Total traffic Out (MB)	The total amount of traffic that passed out of the network.
Avg traffic per session (MB)	The average amount of traffic generated by each session.
Avg traffic in per session (MB)	The average amount of traffic in generated by each session.
Avg traffic out per session (MB)	The average amount of traffic out generated by each session.
Avg traffic per client (MB)	The average amount of traffic generated by each client.
Avg traffic in per client (MB)	The average amount of traffic in generated by each client.
Avg traffic out per client (MB)	The average amount of traffic out generated by each client.
Avg bandwidth per client (Kbps)	The average client bandwidth.
Avg signal quality	The average signal quality for each session.

Using the Configuration Audit Report

The Configuration Audit Report provides a snapshot of your device configurations on the network. You can get an inventory one device at a time, one folder at a time, or one device group at a time. Reports include hypertext links to additional configuration pages.

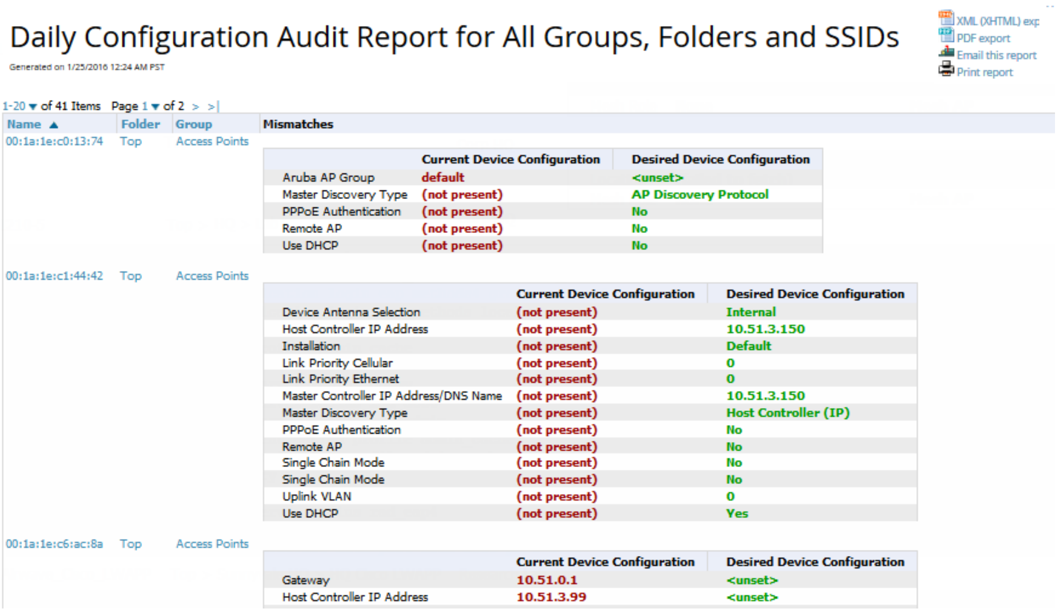
Follow these steps to view the current audit report and configure a device using this report:

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and select **Latest Configuration Audit Report** to display **Detail** device configuration information for all devices. The ensuing **Detail** report can be very large in size, and provides multiple links to additional device configuration or information display pages.

3. You can display device-specific configuration to reduce report size and to focus on a specific device. When viewing configured devices on the **Detail** page, select a device in the **Name** column. The device-specific configuration appears.
4. You can create or assign a template for a given device from the **Detail** page. Select **Add a Template** when viewing device-specific configuration information.
5. You can audit the current device configuration from the **Detail** page. Select **Audit** when viewing device-specific information.
6. You can display archived configuration about a given device from the **Detail** page. Select **Show Archived Device Configuration**.

Figure 216 and Table 147 illustrate and describe the general Configuration Audit report and related contents.

Figure 216: *Daily Configuration Audit Report Page, partial view*



Daily Configuration Audit Report for All Groups, Folders and SSIDs

Generated on 1/25/2016 12:24 AM PST

1-20 ▼ of 41 Items Page 1 ▼ of 2 > >|

Name ▲	Folder	Group	Mismatches
00:1a:1e:c0:13:74	Top	Access Points	

	Current Device Configuration	Desired Device Configuration
Aruba AP Group	default	<unset>
Master Discovery Type	(not present)	AP Discovery Protocol
PPPoE Authentication	(not present)	No
Remote AP	(not present)	No
Use DHCP	(not present)	No

Name	Folder	Group	Mismatches
00:1a:1e:c1:44:42	Top	Access Points	

	Current Device Configuration	Desired Device Configuration
Device Antenna Selection	(not present)	Internal
Host Controller IP Address	(not present)	10.51.3.150
Installation	(not present)	Default
Link Priority Cellular	(not present)	0
Link Priority Ethernet	(not present)	0
Master Controller IP Address/DNS Name	(not present)	10.51.3.150
Master Discovery Type	(not present)	Host Controller (IP)
PPPoE Authentication	(not present)	No
Remote AP	(not present)	No
Single Chain Mode	(not present)	No
Single Chain Mode	(not present)	No
Uplink VLAN	(not present)	0
Use DHCP	(not present)	Yes

Name	Folder	Group	Mismatches
00:1a:1e:c6:ac:8a	Top	Access Points	

	Current Device Configuration	Desired Device Configuration
Gateway	10.51.0.1	<unset>
Host Controller IP Address	10.51.3.99	<unset>

Table 147: *Daily Configuration Audit Report*

Field	Description
Name	Displays the device name for every device on the network. Selecting a given device name in this column allows you to display device-specific configuration.
Folder	Displays the folder in which the device is configured in OV3600. Selecting the folder name in this report displays the **Devices > List** page for additional device, folder and configuration options.
Group	Displays the group with which any given device associates. Selecting the group for a given device takes you to the **Groups > Monitor** page for that specific group, to display graphical group information, modification options, alerts, and an audit log for the related group.
Mismatches	This field displays configuration mismatch information. When a device configuration does not match ideal configuration, this field displays the ideal device settings compared to current settings.

Using the Device Summary Report

The Device Summary Report identifies devices that are the most or least used devices, and a comprehensive list of all devices. One potential use of this report is to establish more equal bandwidth distribution across multiple devices. This report contains the following five lists of devices.

- **Most Utilized by Maximum Number of Simultaneous Users**—By default, this list displays the 10 devices that support the highest numbers of users. This list provides links to additional information or configuration pages for each device to make adjustments, as desired.
- **Most Utilized by Bandwidth**—By default, this list displays the 10 devices that consistently have the highest bandwidth consumption during the time period defined for the report. This list provides links to additional information or configuration pages for each device.
- **Least Utilized by Maximum Number of Simultaneous Users**—By default, this list displays the 10 devices that are the least used, according to the number of users.
- **Least Utilized by Bandwidth**—By default, this list displays the 10 devices that are the least used, according to the bandwidth throughput.
- **Devices**—This list displays all devices in OV3600. By default it is sorted alphabetically by device name.

NOTE

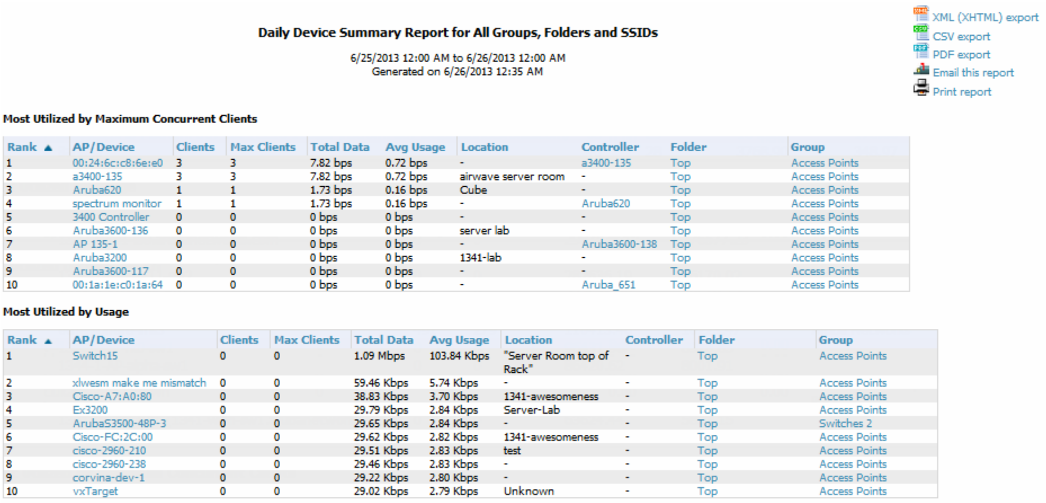
You can specify the number of devices that appear in each of the first four categories in the **Reports > Definitions > Add** page.

Any section of this report can be sorted by any of the columns. For example, you can specify a location and then sort the **Devices** list by the **Location** column to see details by location, or you can see all of the APs associated with a particular controller by sorting on the **Controller** column. If the AP name contains information about the location of the AP, you can sort by AP name.

If sorting the **Devices** list does not provide you with sufficient detail, you can specify a **Group** or **Folder** in the report **Definition** of a custom report. If you create a separate Group or Folder for each set of master and local controllers, you can generate a separate report for each Group or Folder. With this method, the summary sections of each report contain only devices from that Group or Folder.

Figure 217 and Table 148 illustrate and describe the Device Summary Report.

Figure 217: *Daily Device Summary Report Illustration (partial view)*



Daily Device Summary Report for All Groups, Folders and SSIDs

6/25/2013 12:00 AM to 6/26/2013 12:00 AM
Generated on 6/26/2013 12:35 AM

Most Utilized by Maximum Concurrent Clients

Rank ▲	AP/Device	Clients	Max Clients	Total Data	Avg Usage	Location	Controller	Folder	Group
1	00:24:6c:c8:6e:e0	3	3	7.82 bps	0.72 bps	-	a3400-135	Top	Access Points
2	a3400-135	3	3	7.82 bps	0.72 bps	airwave server room	-	Top	Access Points
3	Aruba620	1	1	1.73 bps	0.16 bps	Cube	-	Top	Access Points
4	spectrum monitor	1	1	1.73 bps	0.16 bps	-	Aruba620	Top	Access Points
5	3400 Controller	0	0	0 bps	0 bps	-	-	Top	Access Points
6	Aruba3600-136	0	0	0 bps	0 bps	server lab	-	Top	Access Points
7	AP 135-1	0	0	0 bps	0 bps	-	Aruba3600-138	Top	Access Points
8	Aruba3200	0	0	0 bps	0 bps	1341-lab	-	Top	Access Points
9	Aruba3600-117	0	0	0 bps	0 bps	-	-	Top	Access Points
10	00:1a:1e:c0:1a:64	0	0	0 bps	0 bps	-	Aruba_651	Top	Access Points

Most Utilized by Usage

Rank ▲	AP/Device	Clients	Max Clients	Total Data	Avg Usage	Location	Controller	Folder	Group
1	Switch15	0	0	1.09 Mbps	103.84 Kbps	"Server Room top of Rack"	-	Top	Access Points
2	xlwesm make me mismatch	0	0	59.46 Kbps	5.74 Kbps	-	-	Top	Access Points
3	Cisco-A7:A0:80	0	0	38.83 Kbps	3.70 Kbps	1341-awesomeness	-	Top	Access Points
4	Ex3200	0	0	29.79 Kbps	2.84 Kbps	Server-Lab	-	Top	Access Points
5	ArubaS3500-48P-3	0	0	29.65 Kbps	2.84 Kbps	-	-	Top	Switches 2
6	Cisco-FC:2C:00	0	0	29.62 Kbps	2.82 Kbps	1341-awesomeness	-	Top	Access Points
7	cisco-2960-210	0	0	29.51 Kbps	2.83 Kbps	test	-	Top	Access Points
8	cisco-2960-238	0	0	29.46 Kbps	2.83 Kbps	-	-	Top	Access Points
9	corvina-dev-1	0	0	29.22 Kbps	2.80 Kbps	-	-	Top	Access Points
10	vxTarget	0	0	29.02 Kbps	2.79 Kbps	Unknown	-	Top	Access Points

Table 148: *Daily Device Summary Report Unique Fields and Descriptions*

Field	Description
Rank	Ranks the device from 1 to 10.
AP/Device	The AP name or device MAC address.
Clients	The number of clients that were last connected to the device.
Max Clients	The highest number of clients that were connected to the device during the time/date range of the report. If a range is not specified, then this value will match the value for Clients.
Total Data	Displays the total rate of data in that traveled through device during the period of time covered by the report.
Average Usage	Displays the average rate of data in that traveled through device during the period of time covered by the report.
Location	Displays the location information if available.
Controller	The controller that the device is associated to.
Folder/Group	Displays the folder and group information for the device.

Using the Device Uptime Report

The Device Uptime Report monitors device performance and availability on the network, tracking uptime by multiple criteria to include the following:

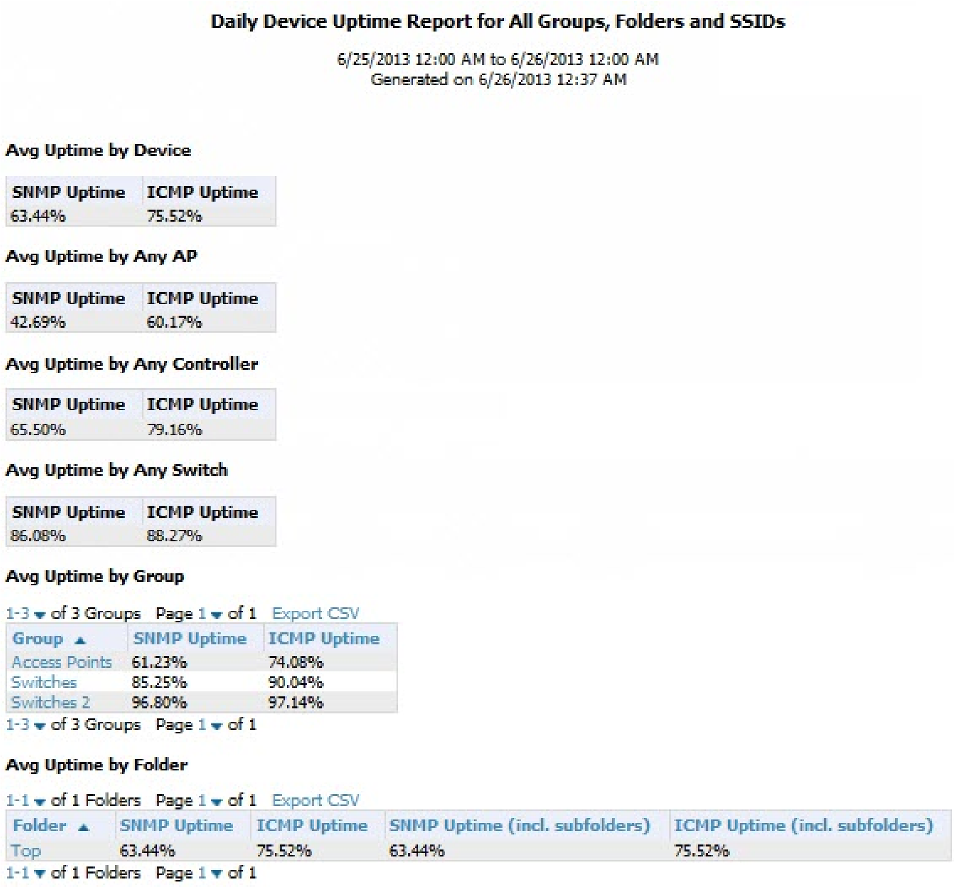
- Total average uptime by SNMP and ICMP
- Average uptime by device group
- Average uptime by device folder

You can use this report as the central starting point to improve uptime by multiple criteria. This report covers protocol-oriented, device-oriented, or SSID-oriented information. This report can help to monitor and optimize the network in multiple ways. It can demonstrate service parameters, can establish locations that have superior or problematic uptime availability, and can help with additional analysis in multiple ways. Locations, device groups, or other groupings within a network can be identified as needing attention or can be proven to have superior performance when using this report.

The Device Uptime Report contains columns that track bootstrap count (number of times the device has gone down for a firmware change), reboot count, downtime duration, and downtime duration percent. As mentioned above, you can optionally ignore device downtime during planned maintenance periods in this report, and you can restrict the report to business days only.

The Device Uptime Report is described in the image and table that follow.

Figure 218: *Device Uptime Report Illustration*



Daily Device Uptime Report for All Groups, Folders and SSIDs

6/25/2013 12:00 AM to 6/26/2013 12:00 AM
Generated on 6/26/2013 12:37 AM

Avg Uptime by Device

SNMP Uptime	ICMP Uptime
63.44%	75.52%

Avg Uptime by Any AP

SNMP Uptime	ICMP Uptime
42.69%	60.17%

Avg Uptime by Any Controller

SNMP Uptime	ICMP Uptime
65.50%	79.16%

Avg Uptime by Any Switch

SNMP Uptime	ICMP Uptime
86.08%	88.27%

Avg Uptime by Group

1-3 ▾ of 3 Groups Page 1 ▾ of 1 Export CSV

Group ▲	SNMP Uptime	ICMP Uptime
Access Points	61.23%	74.08%
Switches	85.25%	90.04%
Switches 2	96.80%	97.14%

1-3 ▾ of 3 Groups Page 1 ▾ of 1

Avg Uptime by Folder

1-1 ▾ of 1 Folders Page 1 ▾ of 1 Export CSV

Folder ▲	SNMP Uptime	ICMP Uptime	SNMP Uptime (incl. subfolders)	ICMP Uptime (incl. subfolders)
Top	63.44%	75.52%	63.44%	75.52%

1-1 ▾ of 1 Folders Page 1 ▾ of 1

Table 149: *Device Uptime Report Unique Fields and Descriptions*

Field	Description
SNMP Uptime	Displays the percentage of time the device was reachable via ICMP. OV3600 polls the device via SNMP at the rate specified on the **Groups > Basic** page.
ICMP Uptime	Displays the percentage of time the device was reachable via ICMP. If the device is reachable via SNMP it is assumed to be reachable via ICMP. OV3600 only pings the device if SNMP fails and then it pings at the SNMP polling interval rate.
Time Since Last Boot	The uptime as reported by the device at the end of the time period covered by the report.

Using the Inventory Report

The **Inventory Report** itemizes all devices on the network. The output breaks down this information by vendor, model (including firmware and bootloader), and device type.

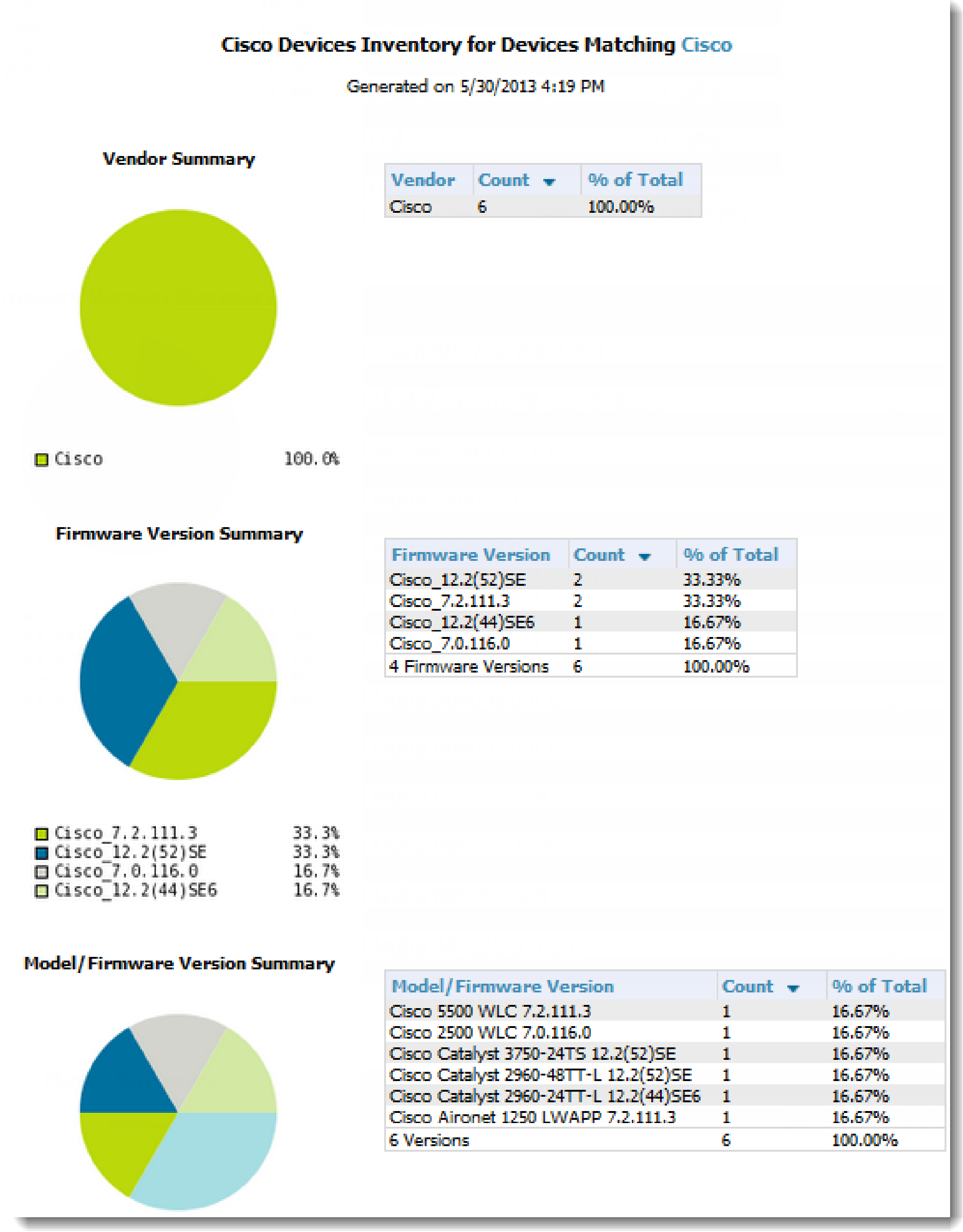
Example Custom Report

The following example creates a report of all Cisco devices on your network. Any field omitted from this example remains the default value.

1. Navigate to **Reports > Definitions**, then click **Add New Report Definition**.

2. Enter the title "Cisco Devices Inventory."
3. Select **Inventory** from the **Type** drop-down menu.
4. Type "Cisco" in the **Device Search Filter** field.
5. In the Summarize report by section, select **Type Summary**. This option will categorize the Cisco devices found in your network by device type.
6. Click **Save and Run**. The report displays on the Generated Reports page when it is available, as shown in Figure 219.

Figure 219: *Inventory Report*



Cisco Devices Inventory for Devices Matching Cisco

Generated on 5/30/2013 4:19 PM

Vendor Summary

Vendor	Count ▼	% of Total
Cisco	6	100.00%

🟩 Cisco 100.0%

Firmware Version Summary

Firmware Version	Count ▼	% of Total
Cisco_12.2(52)SE	2	33.33%
Cisco_7.2.111.3	2	33.33%
Cisco_12.2(44)SE6	1	16.67%
Cisco_7.0.116.0	1	16.67%
4 Firmware Versions	6	100.00%

🟩 Cisco_7.2.111.3 33.3%
🟦 Cisco_12.2(52)SE 33.3%
⬜ Cisco_7.0.116.0 16.7%
🟩 Cisco_12.2(44)SE6 16.7%

Model/Firmware Version Summary

Model/Firmware Version	Count ▼	% of Total
Cisco 5500 WLC 7.2.111.3	1	16.67%
Cisco 2500 WLC 7.0.116.0	1	16.67%
Cisco Catalyst 3750-24TS 12.2(52)SE	1	16.67%
Cisco Catalyst 2960-48TT-L 12.2(52)SE	1	16.67%
Cisco Catalyst 2960-24TT-L 12.2(44)SE6	1	16.67%
Cisco Aironet 1250 LWAPP 7.2.111.3	1	16.67%
6 Versions	6	100.00%

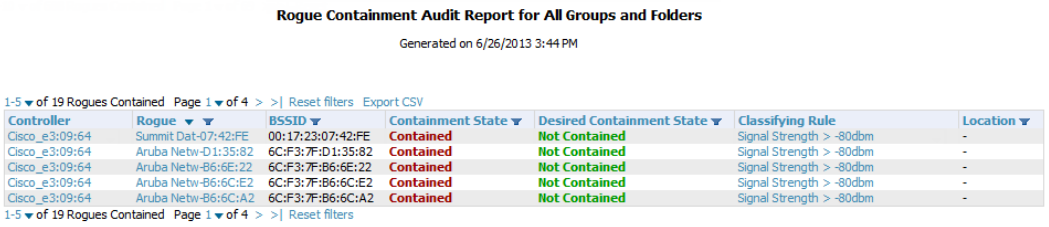
Table 150: *Inventory Report Fields and Descriptions*

Field	Description
Vendor	Displays the device type or name. In the example above, the only vendor specified in the report definition was Cisco.
Count	Shows the total number of each device current included in the client inventory.
% of Total	Shows the percentage of each of those devices that are included in the client inventory.
Firmware Version	The firmware version on each device. This includes the total number of devices and the percentage of each of those devices compared to other devices. In the example above, 33% (or 2 total) of the Cisco devices are on firmware Cisco_7.2.111.3.
Model/Firmware Version	This field further breaks down the firmware version into specific device models and specific versions. This includes the total number of devices and the percentage of each of those devices compared to other devices. As indicated previously, the example above shows that 2 of the Cisco devices are on firmware Cisco_7.2.111.3. Each is a separate model, though.

Using the Rogue Containment Audit Report

The Rogue Containment Audit report that lets you know if any containment is failing. Figure 220 illustrates the output of this report, and Table 151 describes the fields available in the report.

Figure 220: *Rogue Containment Audit Report Page Illustration*



Rogue Containment Audit Report for All Groups and Folders

Generated on 6/26/2013 3:44 PM

1-5 ▾ of 19 Rogues Contained Page 1 ▾ of 4 > >| Reset filters Export CSV

Controller	Rogue ▾ ▼	BSSID ▼	Containment State ▼	Desired Containment State ▼	Classifying Rule	Location ▼
Cisco_e3:09:64	Summit Dat-07:42:FE	00:17:23:07:42:FE	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-D1:35:82	6C:F3:7F:D1:35:82	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-B6:6E:22	6C:F3:7F:B6:6E:22	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-B6:6C:E2	6C:F3:7F:B6:6C:E2	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-B6:6C:A2	6C:F3:7F:B6:6C:A2	Contained	Not Contained	Signal Strength > -80dbm	-

1-5 ▾ of 19 Rogues Contained Page 1 ▾ of 4 > >| Reset filters

Table 151: *Rogue Containment Report fields and descriptions*

Field	Description
Controller	The controller attempted to contain the Rogue
Rogue	The name of the rogue device
BSSID	The BSSID of the rogue device
Containment State	Shows the current containment state

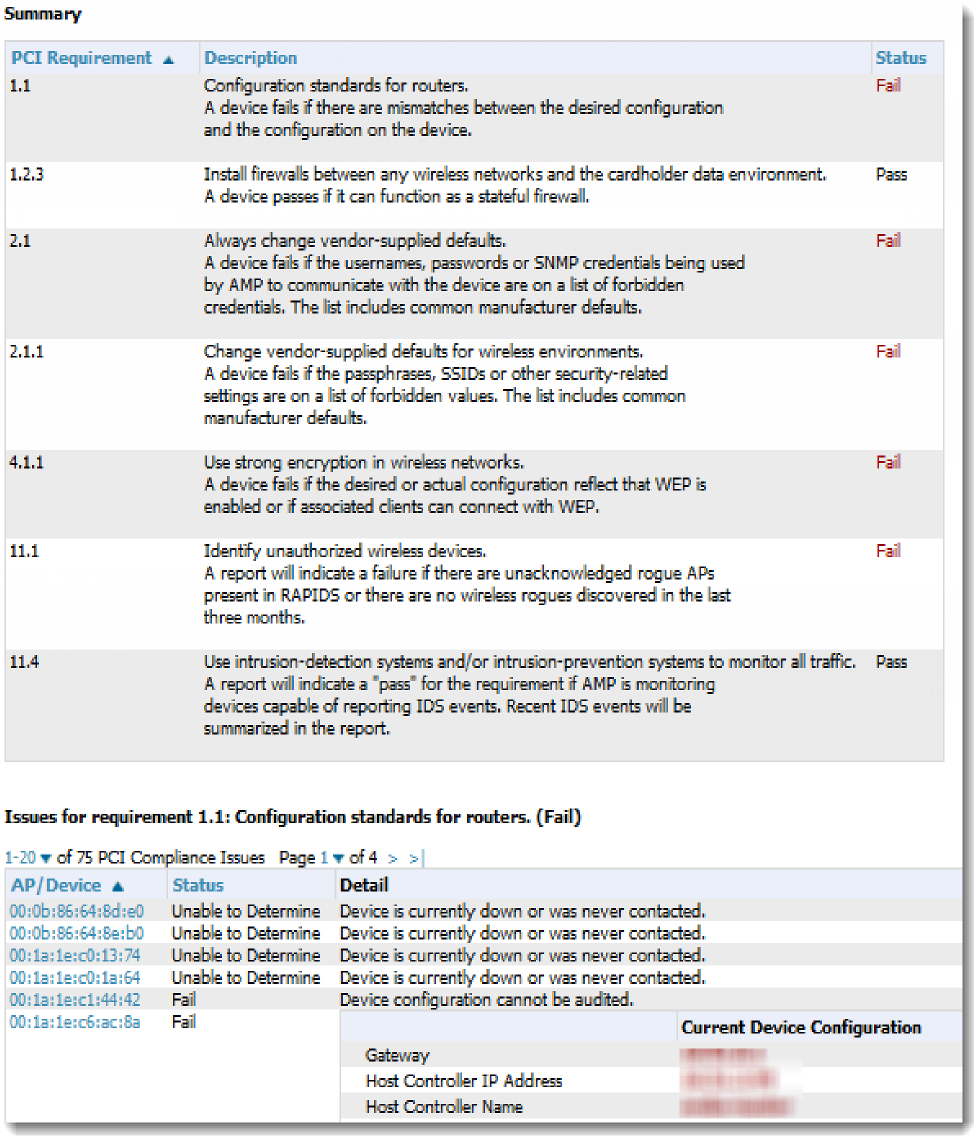
Table 151: *Rogue Containment Report fields and descriptions (Continued)*

Field	Description
Desired Containment State	Shows the desired containment state
Classifying Rule	Shows the rule that the controller followed when determining the status of the rogue
Location	The location of the rogue device, if available

Using the PCI Compliance Report

OV3600 supports PCI requirements in accordance with the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI compliance report, shown in Figure 1, displays current PCI configurations and status. This report provides recommendations to resolve issues when possible.

Figure 221: *PCI Compliance Report*



Summary

PCI Requirement ▲	Description	Status
1.1	Configuration standards for routers. A device fails if there are mismatches between the desired configuration and the configuration on the device.	Fail
1.2.3	Install firewalls between any wireless networks and the cardholder data environment. A device passes if it can function as a stateful firewall.	Pass
2.1	Always change vendor-supplied defaults. A device fails if the usernames, passwords or SNMP credentials being used by AMP to communicate with the device are on a list of forbidden credentials. The list includes common manufacturer defaults.	Fail
2.1.1	Change vendor-supplied defaults for wireless environments. A device fails if the passphrases, SSIDs or other security-related settings are on a list of forbidden values. The list includes common manufacturer defaults.	Fail
4.1.1	Use strong encryption in wireless networks. A device fails if the desired or actual configuration reflect that WEP is enabled or if associated clients can connect with WEP.	Fail
11.1	Identify unauthorized wireless devices. A report will indicate a failure if there are unacknowledged rogue APs present in RAPIDS or there are no wireless rogues discovered in the last three months.	Fail
11.4	Use intrusion-detection systems and/or intrusion-prevention systems to monitor all traffic. A report will indicate a "pass" for the requirement if AMP is monitoring devices capable of reporting IDS events. Recent IDS events will be summarized in the report.	Pass

Issues for requirement 1.1: Configuration standards for routers. (Fail)

1-20 ▼ of 75 PCI Compliance Issues Page 1 ▼ of 4 > >|

AP/Device ▲	Status	Detail
00:0b:86:64:8d:e0	Unable to Determine	Device is currently down or was never contacted.
00:0b:86:64:8e:b0	Unable to Determine	Device is currently down or was never contacted.
00:1a:1e:c0:13:74	Unable to Determine	Device is currently down or was never contacted.
00:1a:1e:c0:1a:64	Unable to Determine	Device is currently down or was never contacted.
00:1a:1e:c1:44:42	Fail	Device configuration cannot be audited.
00:1a:1e:c6:ac:8a	Fail	

	Current Device Configuration
Gateway	[redacted]
Host Controller IP Address	[redacted]
Host Controller Name	[redacted]

For information about turning on this feature, see "Enabling PCI Compliance Monitoring" on page 68.

Using the IDS Events Report

The IDS Events Report lists and tracks IDS events on the network involving APs or controller devices. This report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours, and provides links to support additional analysis or configuration in response. You can filter this report to show IDS events for specific devices (Controllers, APs, etc.) By default, this report will show up to 10 IDS for each specified device type. You can change this value to anything other than 0.

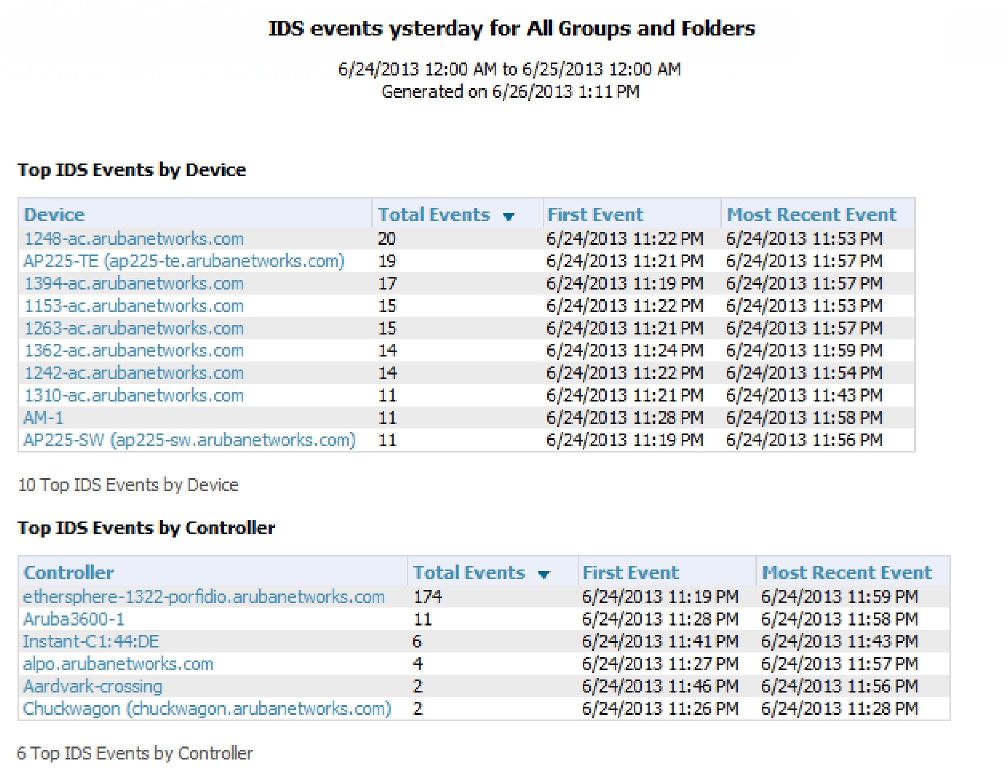
NOTE

Your role must be enabled to view RAPIDS in order to see this report. In addition, this report requires that you enter a start and stop time range.

The **Home > Overview** page also cites IDS events. Triggers can be configured for IDS events. Refer to "Creating New Triggers" on page 267 for additional information.

Figure 222 and Table 152 illustrate and describe the IDS Events Detail report. Selecting the AP device or controller name takes you to the **Devices > List** page.

Figure 222: *IDS Events Report Illustration*



IDS events ysterday for All Groups and Folders

6/24/2013 12:00 AM to 6/25/2013 12:00 AM
Generated on 6/26/2013 1:11 PM

Top IDS Events by Device

Device	Total Events ▼	First Event	Most Recent Event
1248-ac.arubanetworks.com	20	6/24/2013 11:22 PM	6/24/2013 11:53 PM
AP225-TE (ap225-te.arubanetworks.com)	19	6/24/2013 11:21 PM	6/24/2013 11:57 PM
1394-ac.arubanetworks.com	17	6/24/2013 11:19 PM	6/24/2013 11:57 PM
1153-ac.arubanetworks.com	15	6/24/2013 11:22 PM	6/24/2013 11:53 PM
1263-ac.arubanetworks.com	15	6/24/2013 11:21 PM	6/24/2013 11:57 PM
1362-ac.arubanetworks.com	14	6/24/2013 11:24 PM	6/24/2013 11:59 PM
1242-ac.arubanetworks.com	14	6/24/2013 11:22 PM	6/24/2013 11:54 PM
1310-ac.arubanetworks.com	11	6/24/2013 11:21 PM	6/24/2013 11:43 PM
AM-1	11	6/24/2013 11:28 PM	6/24/2013 11:58 PM
AP225-SW (ap225-sw.arubanetworks.com)	11	6/24/2013 11:19 PM	6/24/2013 11:56 PM

10 Top IDS Events by Device

Top IDS Events by Controller

Controller	Total Events ▼	First Event	Most Recent Event
ethersphere-1322-porfidio.arubanetworks.com	174	6/24/2013 11:19 PM	6/24/2013 11:59 PM
Aruba3600-1	11	6/24/2013 11:28 PM	6/24/2013 11:58 PM
Instant-C1:44:DE	6	6/24/2013 11:41 PM	6/24/2013 11:43 PM
alpo.arubanetworks.com	4	6/24/2013 11:27 PM	6/24/2013 11:57 PM
Aardvark-crossing	2	6/24/2013 11:46 PM	6/24/2013 11:56 PM
Chuckwagon (chuckwagon.arubanetworks.com)	2	6/24/2013 11:26 PM	6/24/2013 11:28 PM

6 Top IDS Events by Controller

Table 152: *IDS Events Detail Unique Fields and Descriptions*

Field	Description
Device/Controller	These columns list the controllers and other devices for which IDS events have occurred in the specified time range, and provides a link to the **Devices > Monitor** page for each.
Total Events	Shows the number of events for each AP and/or Controller.
First Event	Shows the date and time of the first event.

Table 152: *IDS Events Detail Unique Fields and Descriptions (Continued)*

Field	Description
Most Recent Event	Shows the date and time of the last/most recent event.
Attack	Displays the name or label for the IDS event.
Attacker	Displays the MAC address of the device that generated the IDS event.
Radio	Displays the 802.11 radio type associated with the IDS event.
Channel	Displays the 802.11 radio channel associated with the IDS event, when known.
SNR	Displays the signal-to-noise (SNR) radio associated with the IDS event.
Precedence	Displays precedence information associated with the IDS event, when known.
Time	Displays the time of the IDS event.

Using the Match Event Report

Use the Match Events report to track matching events that occurred on devices. For example, you could use the report to find sticky client problems and break down the information by folder, AP, and/or client, as shown in Figure 223.

Figure 223: *Example of a Match Event Report*

Table 153: *Match Event Report output details*

Field	Description
Folder/AP/Client	The total number of matches that occurred in each folder, each AP, and each Client. The tables also include a reason for the match event. This information is obtained directly from the controller. Data will only display for a Folder, AP, and Client if each has experienced at least one match event.
Device Type Summary	This shows the total number and percentage of match events that occurred on all device types (for example, iPhone, Kindle, etc.). The graph shows the top 5 devices.
Reasons for Match Summary	This graph and table break down the number and percentage of matches based on the match reason.
Connection Mode Summary	This graph and table show the number and percentage of matches based on the device's connection mode.

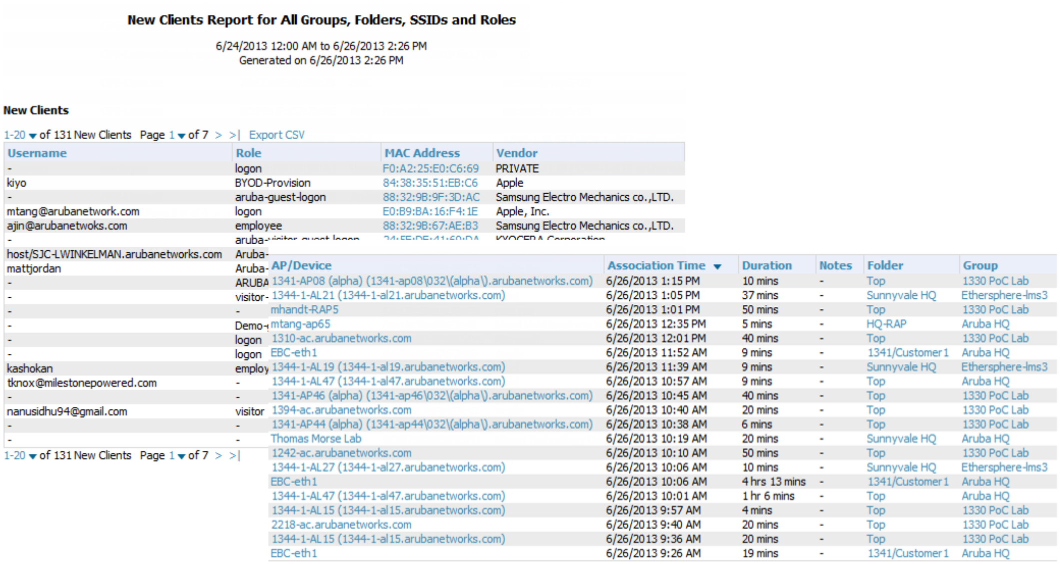
Using the New Clients Report

The New Clients Report lists all new users that have appeared on the network during the time duration defined for the report. This report covers the user identifier, the associated role when known, device information and more. This report gives you the option to filter instead on specific devices and/or users. Whether viewing information for devices or clients, the report can configured to display additional options. For many of these options, you can choose to view all information or a specific set of information (Matching option). If Matching is selected, a text entry field displays. When you put your cursor in the text entry field, an additional side menu displays providing you with a list of available options that you can select.

- SSID - All or Selected
- Alcatel-Lucent Role - All or Selected
- Classification (for possible Rogue devices) - All or Selected
- Device Type - All or Matching
- AOS Device Type - All or Matching
- Manufacturer - All or Matching
- Model - All or Matching
- OS - All or Matching
- OS Detail - All or Matching
- Network Chipset - All or Matching
- Network Driver - All or Matching
- EAP Supplicant - All or Matching
- Asset Group - All or Matching
- Asset Category - All or Matching

Figure 224 illustrates the fields and information in the New Clients Report. The fields that display on this output are described in Table 154.

Figure 224: *New Clients Report Illustration (split view)*



New Clients Report for All Groups, Folders, SSIDs and Roles

6/24/2013 12:00 AM to 6/26/2013 2:26 PM
Generated on 6/26/2013 2:26 PM

New Clients

1-20 ▾ of 131 New Clients Page 1 ▾ of 7 > >| Export CSV

Username	Role	MAC Address	Vendor
-	logon	F0:A2:25:E0:C6:69	PRIVATE
kiyo	BYOD-Provision	84:38:35:51:EB:C6	Apple
-	aruba-guest-logon	88:32:9B:9F:3D:AC	Samsung Electro Mechanics co.,LTD.
mtang@arubanetwork.com	logon	E0:B9:BA:16:F4:1E	Apple, Inc.
ajin@arubanetwoks.com	employee	88:32:9B:67:AE:B3	Samsung Electro Mechanics co.,LTD.
-	aruba-visitor-guest-logon	24:FF:DE:41:60:DA	KYOCERA Corporation
host/SJC-LWINKELMAN.arubanetworks.com	Aruba-		
mattjordan	Aruba-		
-	ARUBA		
-	visitor-		
-	-		
-	Demo-		
-	logon		
-	logon		
kashokan	employ		
tknox@milestonepowered.com	-		
-	-		
nanusidhu94@gmail.com	visitor		
-	-		
-	-		

1-20 ▾ of 131 New Clients Page 1 ▾ of 7 > >|

AP/Device	Association Time ▾	Duration	Notes	Folder	Group
1341-AP08 (alpha) (1341-ap08\032\(alpha\).arubanetworks.com)	6/26/2013 1:15 PM	10 mins	-	Top	1330 PoC Lab
1344-1-AL21 (1344-1-al21.arubanetworks.com)	6/26/2013 1:05 PM	37 mins	-	Sunnyvale HQ	Ethersphere-lms3
mhandt-RAP5	6/26/2013 1:01 PM	50 mins	-	Top	1330 PoC Lab
mtang-ap65	6/26/2013 12:35 PM	5 mins	-	HQ-RAP	Aruba HQ
1310-ac.arubanetworks.com	6/26/2013 12:01 PM	40 mins	-	Top	1330 PoC Lab
EBC-eth1	6/26/2013 11:52 AM	9 mins	-	1341/Customer1	Aruba HQ
1344-1-AL19 (1344-1-al19.arubanetworks.com)	6/26/2013 11:39 AM	9 mins	-	Sunnyvale HQ	Ethersphere-lms3
1344-1-AL47 (1344-1-al47.arubanetworks.com)	6/26/2013 10:57 AM	9 mins	-	Top	Aruba HQ
1341-AP46 (alpha) (1341-ap46\032\(alpha\).arubanetworks.com)	6/26/2013 10:45 AM	40 mins	-	Top	1330 PoC Lab
1394-ac.arubanetworks.com	6/26/2013 10:40 AM	20 mins	-	Top	1330 PoC Lab
1341-AP44 (alpha) (1341-ap44\032\(alpha\).arubanetworks.com)	6/26/2013 10:38 AM	6 mins	-	Top	1330 PoC Lab
Thomas Morse Lab	6/26/2013 10:19 AM	20 mins	-	Sunnyvale HQ	Aruba HQ
1242-ac.arubanetworks.com	6/26/2013 10:10 AM	50 mins	-	Top	1330 PoC Lab
1344-1-AL27 (1344-1-al27.arubanetworks.com)	6/26/2013 10:06 AM	10 mins	-	Sunnyvale HQ	Ethersphere-lms3
EBC-eth1	6/26/2013 10:06 AM	4 hrs 13 mins	-	1341/Customer1	Aruba HQ
1344-1-AL47 (1344-1-al47.arubanetworks.com)	6/26/2013 10:01 AM	1 hr 6 mins	-	Top	Aruba HQ
1344-1-AL15 (1344-1-al15.arubanetworks.com)	6/26/2013 9:57 AM	4 mins	-	Top	1330 PoC Lab
2218-ac.arubanetworks.com	6/26/2013 9:40 AM	20 mins	-	Top	1330 PoC Lab
1344-1-AL15 (1344-1-al15.arubanetworks.com)	6/26/2013 9:36 AM	20 mins	-	Top	1330 PoC Lab
EBC-eth1	6/26/2013 9:26 AM	19 mins	-	1341/Customer1	Aruba HQ

Table 154: *New Clients Report output details*

Field	Description
Username	The client name, if available.
Role	The client's role, if available
MAC Address	The new client's MAC address

Table 154: *New Clients Report output details (Continued)*

Field	Description
Vendor	The vendor for the client device.
AP/Device	The AP/Device that the client is currently connected to.
Association Time	The time when the client last associated with the device.
Duration	How long the client has been connected to the device.
Folder/Group	Shows the folder and group of the device that the client is currently connected to.

Using the New Rogue Devices Report

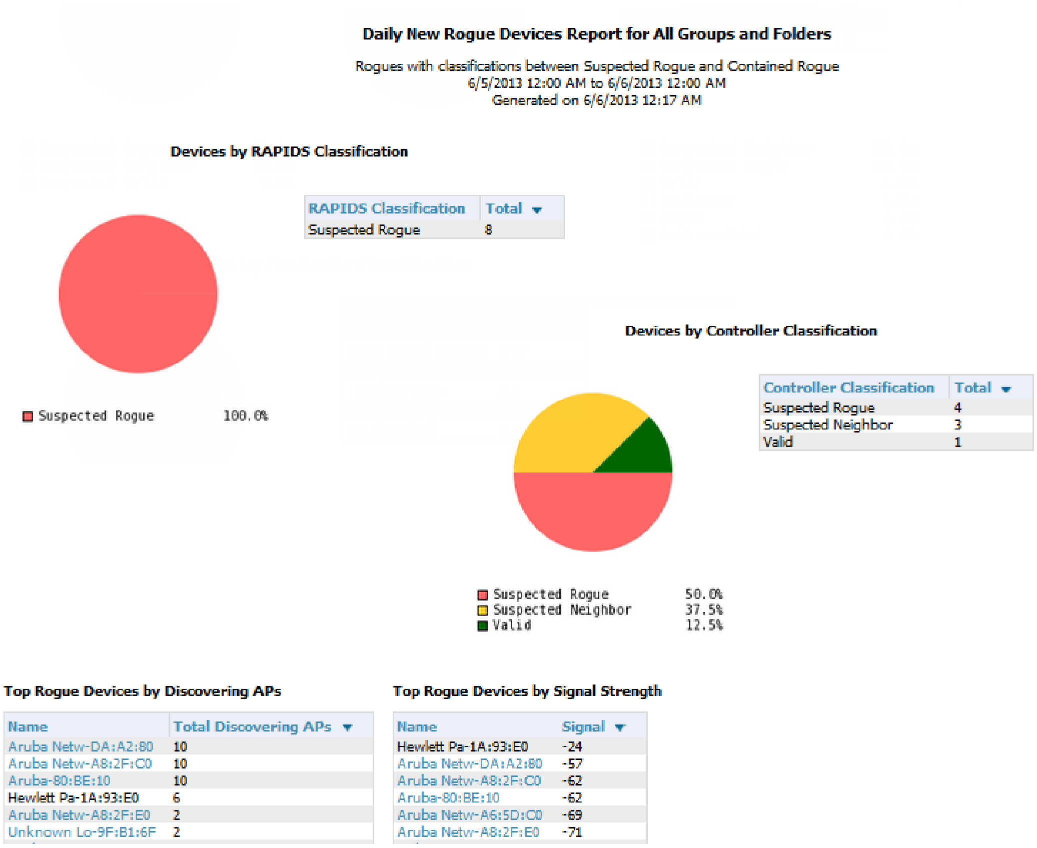
The New Rogue Devices Report summarizes rogue device information including the following categories of information:

- Rogue devices by RAPIDS classification—described in "Using RAPIDS" on page 243
- Top rogue devices by number of discovering APs
- Top rogue devices by signal strength
- Graphical summary of rogue devices by LAN MAC address vendor
- Graphical summary of rogue devices by radio MAC address vendor
- Text-based table summary of rogue device counts
- Detailed and text-based table of rogue devices discovered wirelessly, with extensive device parameters and hyperlink interoperability to additional OV3600 pages
- Detailed and text-based table of all rogue devices supporting all discovery methods with extensive device parameters and hyperlink interoperability to additional OV3600 pages
- Detailed and text-based table of discovery events pertaining to the discovery of rogue devices with extensive parameters and hyperlink interoperability to additional OV3600 pages

This report is not run by default, but is available after you define it.

Refer to Figure 225 for a sample illustration of this report.

Figure 225: *New Rogue Devices Report Illustration (partial view)*



Daily New Rogue Devices Report for All Groups and Folders

Rogues with classifications between Suspected Rogue and Contained Rogue
6/5/2013 12:00 AM to 6/6/2013 12:00 AM
Generated on 6/6/2013 12:17 AM

Devices by RAPIDS Classification

RAPIDS Classification	Total ▼
Suspected Rogue	8

Devices by Controller Classification

Controller Classification	Total ▼
Suspected Rogue	4
Suspected Neighbor	3
Valid	1

Top Rogue Devices by Discovering APs

Name	Total Discovering APs ▼
Aruba Netw-DA:A2:80	10
Aruba Netw-A8:2F:C0	10
Aruba-80:BE:10	10
Hewlett Pa-1A:93:E0	6
Aruba Netw-A8:2F:E0	2
Unknown Lo-9F:B1:6F	2

Top Rogue Devices by Signal Strength

Name	Signal ▼
Hewlett Pa-1A:93:E0	-24
Aruba Netw-DA:A2:80	-57
Aruba Netw-A8:2F:C0	-62
Aruba-80:BE:10	-62
Aruba Netw-A6:5D:C0	-69
Aruba Netw-A8:2F:E0	-71

The rogue device inventories that comprise this report contain many fields, described in Table 155.

Table 155: *New Rogue Devices Report Fields*

Field	Description
Name	Displays the device name, if it can be determined.
RAPIDS Classification	Displays the RAPIDS classification for the rogue device, as classified by rules defined on the **RAPIDS > Rules** page. Refer to "Using RAPIDS" on page 243 for additional information.
Threat Level	Displays the numeric threat level by which the device has been classified, according to rules defined on the **RAPIDS > Rules** page. Refer to "Using RAPIDS" on page 243 for additional information.
Ack	Indicates whether the device has been acknowledged with the network.
First Discovered	Displays the date and time that the rogue device was first discovered on the network.
First Discovery Method	Displays the method by which the rogue device was discovered.
First Discovery Agent	Displays the network device that first discovered the rogue device.
Last Discovering AP	Displays the network device that most recently discovered the rogue device.

Table 155: *New Rogue Devices Report Fields (Continued)*

Field	Description
Model	Displays the rogue device type when known.
Operating System	Displays the operating system for the device type, when known.
IP Address	Displays the IP address of the rogue device when known.
SSID	Displays the SSID for the rogue device when known.
Network Type	Displays the network type on which the rogue was detected, when known.
Channel	Displays the wireless RF channel on which the rogue device was detected.
WEP	Displays WEP encryption usage when known.
RSSI	Displays Received Signal Strength (RSSI) information for radio signal strength when known.
Signal	Displays signal strength when known.
LAN MAC Address	Displays the MAC address for the associated LAN when known.
LAN Vendor	Displays LAN vendor information associated with the rogue device, when known.
Radio MAC Address	Displays the MAC address for the radio device, when known.
Radio Vendor	Displays the vendor information for the radio device when known.
Port	Displays the router or switch port associated with the rogue device when known.
Last Seen	Displays the last time in which the rogue device was seen on the network.
Total Discovering APs	Displays the total number of APs that detected the rogue device.
Total Discovery Events	Displays the total number of instances in which the rogue device was discovered.

Using the RADIUS Reports

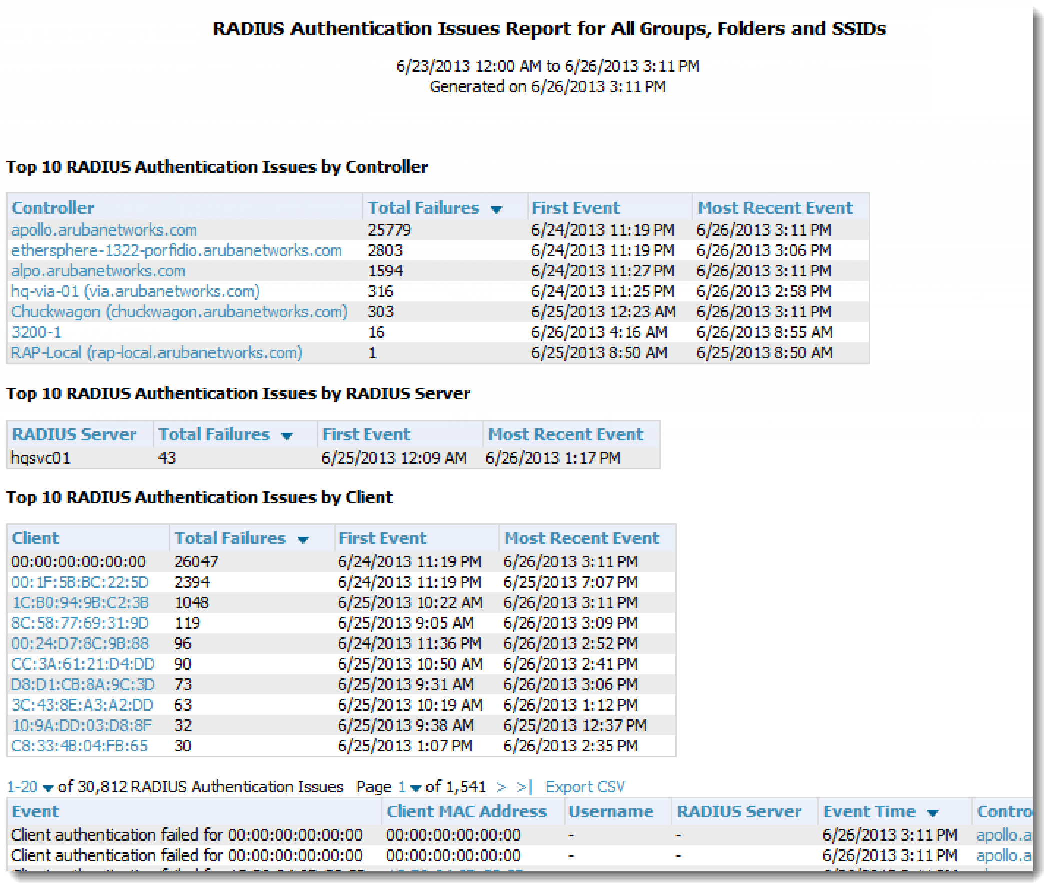
These reports display issues that may appear with controllers, RADIUS servers, and users, or about RADIUS accounting issues.

RADIUS Authentication Issues

This report include the number of total failures and the first and most recent event times. This report shows the top 10 RADIUS authentication items in each table. You can change this value to anything other than 0.

You can filter this report by BSSID, or view detailed information about RADIUS failures. By selecting RADIUS failures, OV3600 summarizes authentication issues for each event.

Figure 226: *RADIUS Authentication Issues Report*



RADIUS Authentication Issues Report for All Groups, Folders and SSIDs

6/23/2013 12:00 AM to 6/26/2013 3:11 PM
Generated on 6/26/2013 3:11 PM

Top 10 RADIUS Authentication Issues by Controller

Controller	Total Failures ▼	First Event	Most Recent Event
apollo.arubanetworks.com	25779	6/24/2013 11:19 PM	6/26/2013 3:11 PM
ethersphere-1322-porfidio.arubanetworks.com	2803	6/24/2013 11:19 PM	6/26/2013 3:06 PM
alpo.arubanetworks.com	1594	6/24/2013 11:27 PM	6/26/2013 3:11 PM
hq-via-01 (via.arubanetworks.com)	316	6/24/2013 11:25 PM	6/26/2013 2:58 PM
Chuckwagon (chuckwagon.arubanetworks.com)	303	6/25/2013 12:23 AM	6/26/2013 3:11 PM
3200-1	16	6/26/2013 4:16 AM	6/26/2013 8:55 AM
RAP-Local (rap-local.arubanetworks.com)	1	6/25/2013 8:50 AM	6/25/2013 8:50 AM

Top 10 RADIUS Authentication Issues by RADIUS Server

RADIUS Server	Total Failures ▼	First Event	Most Recent Event
hqsvc01	43	6/25/2013 12:09 AM	6/26/2013 1:17 PM

Top 10 RADIUS Authentication Issues by Client

Client	Total Failures ▼	First Event	Most Recent Event
00:00:00:00:00:00	26047	6/24/2013 11:19 PM	6/26/2013 3:11 PM
00:1F:5B:BC:22:5D	2394	6/24/2013 11:19 PM	6/25/2013 7:07 PM
1C:B0:94:9B:C2:3B	1048	6/25/2013 10:22 AM	6/26/2013 3:11 PM
8C:58:77:69:31:9D	119	6/25/2013 9:05 AM	6/26/2013 3:09 PM
00:24:D7:8C:9B:88	96	6/24/2013 11:36 PM	6/26/2013 2:52 PM
CC:3A:61:21:D4:DD	90	6/25/2013 10:50 AM	6/26/2013 2:41 PM
D8:D1:CB:8A:9C:3D	73	6/25/2013 9:31 AM	6/26/2013 3:06 PM
3C:43:8E:A3:A2:DD	63	6/25/2013 10:19 AM	6/26/2013 1:12 PM
10:9A:DD:03:D8:8F	32	6/25/2013 9:38 AM	6/25/2013 12:37 PM
C8:33:4B:04:FB:65	30	6/25/2013 1:07 PM	6/26/2013 2:35 PM

1-20 ▼ of 30,812 RADIUS Authentication Issues Page 1 ▼ of 1,541 > >| Export CSV

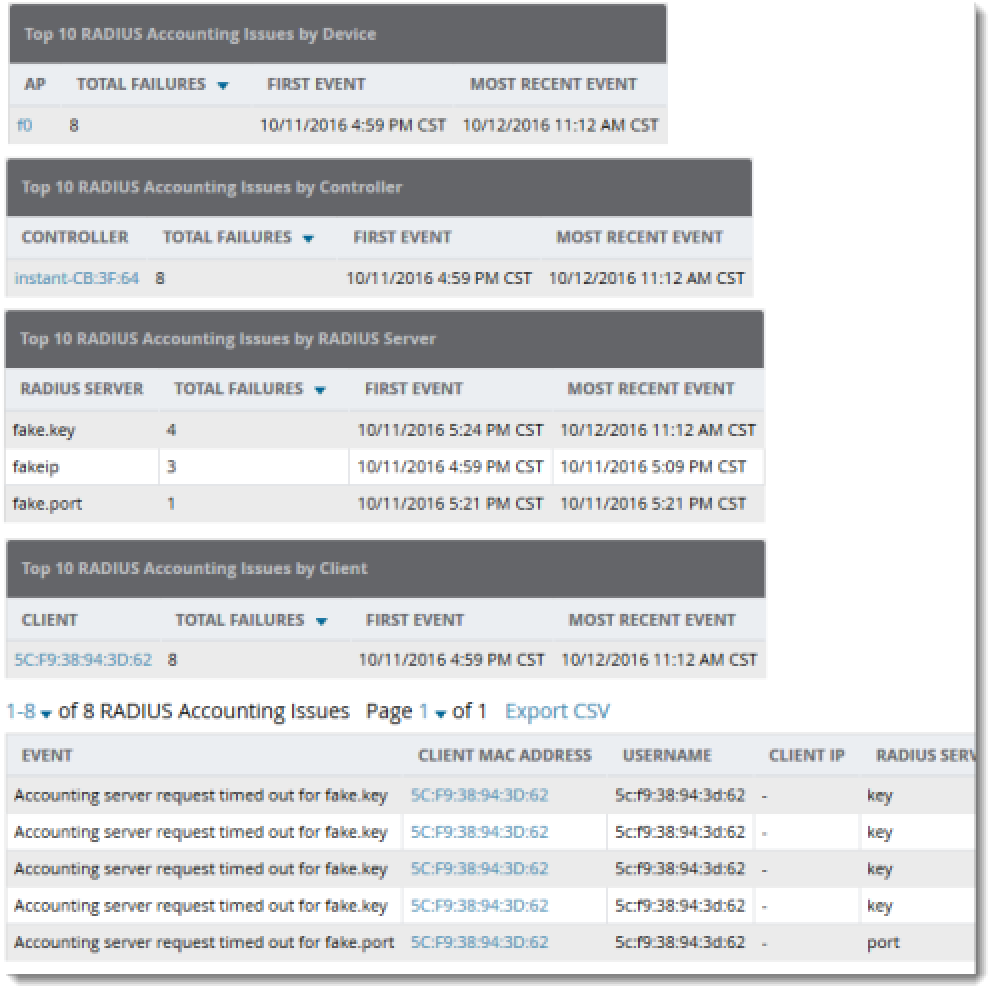
Event	Client MAC Address	Username	RADIUS Server	Event Time ▼	Contro
Client authentication failed for 00:00:00:00:00:00	00:00:00:00:00:00	-	-	6/26/2013 3:11 PM	apollo.a
Client authentication failed for 00:00:00:00:00:00	00:00:00:00:00:00	-	-	6/26/2013 3:11 PM	apollo.a

RADIUS Accounting Issues

In order to run this report, you need to create a custom report that includes RADIUS accounting information. From the **Reports>Definitions**page, click **Add** to open the new report template. The **Custom Options** list will include options for RADIUS Accounting, as well as RADIUS Authentication.

To view a generated RADIUS accounting report, navigate to **Reports > Generated** and select the name of a report that includes RADIUS accounting details.

Figure 227: *RADIUS Accounting Issues Report*



Top 10 RADIUS Accounting Issues by Device

AP	TOTAL FAILURES ▾	FIRST EVENT	MOST RECENT EVENT
f0	8	10/11/2016 4:59 PM CST	10/12/2016 11:12 AM CST

Top 10 RADIUS Accounting Issues by Controller

CONTROLLER	TOTAL FAILURES ▾	FIRST EVENT	MOST RECENT EVENT
instant-CB:3F:64	8	10/11/2016 4:59 PM CST	10/12/2016 11:12 AM CST

Top 10 RADIUS Accounting Issues by RADIUS Server

RADIUS SERVER	TOTAL FAILURES ▾	FIRST EVENT	MOST RECENT EVENT
fake.key	4	10/11/2016 5:24 PM CST	10/12/2016 11:12 AM CST
fakeip	3	10/11/2016 4:59 PM CST	10/11/2016 5:09 PM CST
fake.port	1	10/11/2016 5:21 PM CST	10/11/2016 5:21 PM CST

Top 10 RADIUS Accounting Issues by Client

CLIENT	TOTAL FAILURES ▾	FIRST EVENT	MOST RECENT EVENT
5C:F9:38:94:3D:62	8	10/11/2016 4:59 PM CST	10/12/2016 11:12 AM CST

1-8 ▾ of 8 RADIUS Accounting Issues Page 1 ▾ of 1 Export CSV

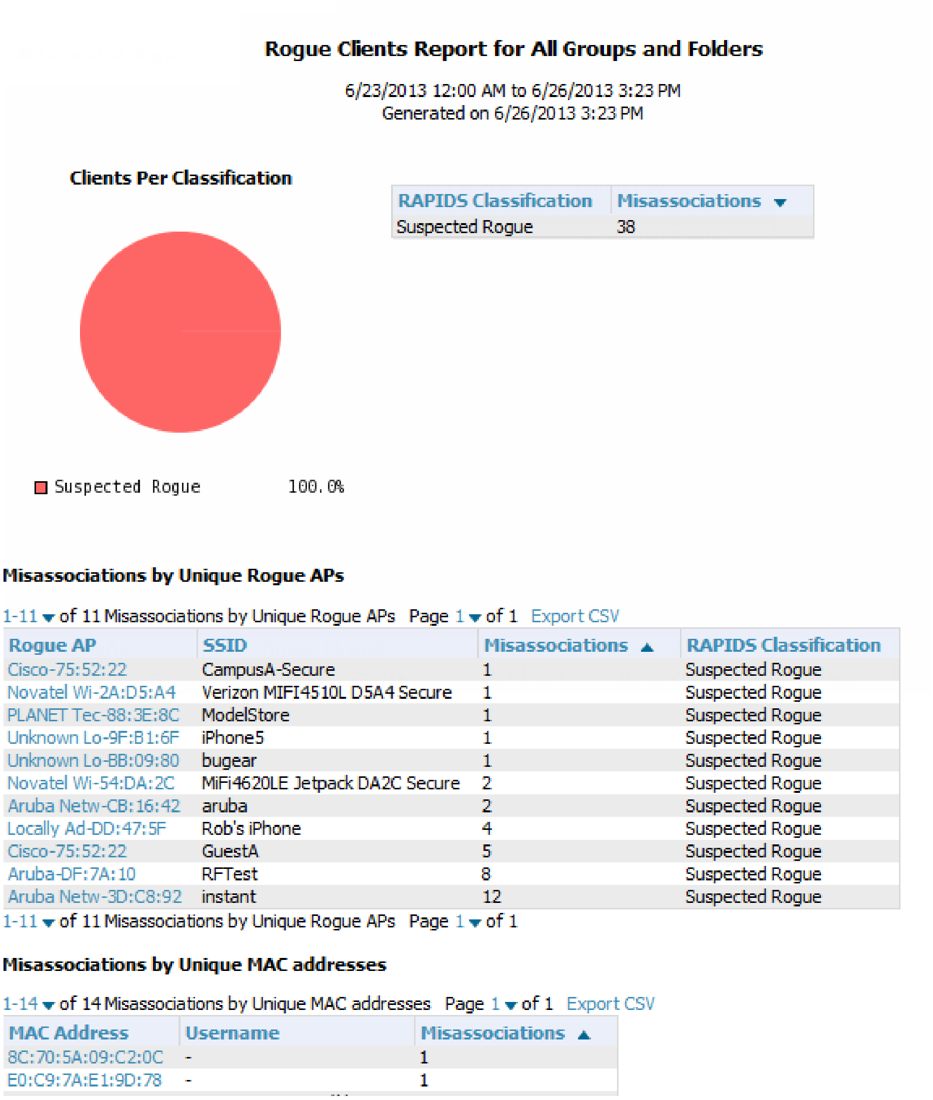
EVENT	CLIENT MAC ADDRESS	USERNAME	CLIENT IP	RADIUS SERV
Accounting server request timed out for fake.key	5C:F9:38:94:3D:62	5c:f9:38:94:3d:62	-	key
Accounting server request timed out for fake.key	5C:F9:38:94:3D:62	5c:f9:38:94:3d:62	-	key
Accounting server request timed out for fake.key	5C:F9:38:94:3D:62	5c:f9:38:94:3d:62	-	key
Accounting server request timed out for fake.key	5C:F9:38:94:3D:62	5c:f9:38:94:3d:62	-	key
Accounting server request timed out for fake.port	5C:F9:38:94:3D:62	5c:f9:38:94:3d:62	-	port

Using the Rogue Clients Report

The Rogue Clients report tracks the number of valid users that connected to rogues in the specified time frame, and can be filtered by rogue classification. You can specify to include ad-hoc devices can be included and detailed information about the clients.

By default, the minimum RAPIDS classification is Suspected Rogue, and the maximum is Contained Rogue.

Figure 228: *Rogue Clients Report Page Illustration*



Rogue Clients Report for All Groups and Folders

6/23/2013 12:00 AM to 6/26/2013 3:23 PM
Generated on 6/26/2013 3:23 PM

Clients Per Classification

🟥 Suspected Rogue 100.0%

RAPIDS Classification	Misassociations ▼
Suspected Rogue	38

Misassociations by Unique Rogue APs

1-11 ▼ of 11 Misassociations by Unique Rogue APs Page 1 ▼ of 1 Export CSV

Rogue AP	SSID	Misassociations ▲	RAPIDS Classification
Cisco-75:52:22	CampusA-Secure	1	Suspected Rogue
Novatel Wi-2A:D5:A4	Verizon MIFI4510L D5A4 Secure	1	Suspected Rogue
PLANET Tec-88:3E:8C	ModelStore	1	Suspected Rogue
Unknown Lo-9F:B1:6F	iPhone5	1	Suspected Rogue
Unknown Lo-BB:09:80	bugear	1	Suspected Rogue
Novatel Wi-54:DA:2C	MiFi4620LE Jetpack DA2C Secure	2	Suspected Rogue
Aruba Netw-CB:16:42	aruba	2	Suspected Rogue
Locally Ad-DD:47:5F	Rob's iPhone	4	Suspected Rogue
Cisco-75:52:22	GuestA	5	Suspected Rogue
Aruba-DF:7A:10	RFTest	8	Suspected Rogue
Aruba Netw-3D:C8:92	instant	12	Suspected Rogue

1-11 ▼ of 11 Misassociations by Unique Rogue APs Page 1 ▼ of 1

Misassociations by Unique MAC addresses

1-14 ▼ of 14 Misassociations by Unique MAC addresses Page 1 ▼ of 1 Export CSV

MAC Address	Username	Misassociations ▲
8C:70:5A:09:C2:0C	-	1
E0:C9:7A:E1:9D:78	-	1

Table 156: *Rogue Clients fields and descriptions*

Field	Description
Misassociations by Unique Rogue APs	For each Rogue AP, this table includes the SSID of the device, the number of misassociations, and the RAPIDS Classification.
Misassociations by Unique MAC addresses	This table shows details about MAC address that are being registered as rogue clients, including the user name (if available) and the number of misassociations.
Rogue Clients	
MAC Address	The MAC address of the rogue client
Username	The user name of the rogue client, if available
SSID	The SSID of the rogue client

Table 156: *Rogue Clients fields and descriptions (Continued)*

Field	Description
First Heard	The date/time when the rogue client was first detected on the network
Ch BW	The channel bandwidth of the client, if available
Radio Mode	The radio mode that the rogue client is using
SNR	The signal-to-noise ratio, if available
Channel	The channel of the rogue device, if available
Location	The location of the rogue client, if available
RAPIDS Classification	The current classification of the rogue client

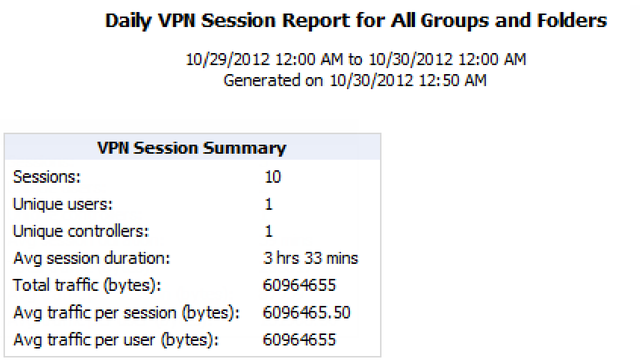
Using the VPN Session Report

The **VPN Session Report** extensively itemizes VPN activity by session. This report can be filtered to show devices or clients/users, including those that match a certain search criteria. You can also specify device types to include in the report. Finally, you can specify to include summary or detailed information about VPN sessions and users.

The output can display in chart and table form.

In list and chart form, this report tracks and display session information that can include any or all of the following:

Figure 229: *VPN Session Report Summary View*



Daily VPN Session Report for All Groups and Folders

10/29/2012 12:00 AM to 10/30/2012 12:00 AM
Generated on 10/30/2012 12:50 AM

VPN Session Summary	
Sessions:	10
Unique users:	1
Unique controllers:	1
Avg session duration:	3 hrs 33 mins
Total traffic (bytes):	60964655
Avg traffic per session (bytes):	6096465.50
Avg traffic per user (bytes):	60964655

Table 157 describes the fields that display when "Summarize Report By" list information is selected for the following tables:

- VPN Session Data by VPN Type
- VPN Session Data by Controller
- VPN Session Data by AOS Device Type
- VPN Session Data by HTTP Fingerprint
- VPN Session Data by VLAN

Table 157: *VPN Session Data tables for each session type*

Field	Description
Name	The VPN Type, Controller, AOS Device Type, HTTP Fingerprint, or VLAN
Users	The number of users that logged a VPN session over the specified time range for each VPN Type, Controller, AOS Device Type, HTTP Fingerprint, and VLAN
Total Duration	The amount of time that each type was connected during the specified time range.
Total Data	The amount of data in MB each type was collected during the specified time range.

Creating Custom Reports

You can customize reports to meet your needs. In order to do so, you need admin privilege to create reports and view all report information. OV3600 reports and information displayed in the WebUI varies depending on configurations, user roles, and folders.

Follow these steps to create a report:

1. Navigate to **Reports > Definition**, then click **Add**. Or click ✎ to edit a report.
2. Enter the name of the report in the **Title** field.
3. Add report widgets:
   - For a default report, select the report widget from the available options, then press and hold the mouse while you drag it to the selected options. Or, you can double-click the widget.
   - For a custom report, click the down arrow next to select a report from the drop-down list.

   Change the order in which the report displays data by dragging the widget to reorder it.
4. Complete the **Report Restrictions** section. All reports allow you to restrict based on a group, folder, and type of device. When you select custom options to include in a report, additional restrictions will become available.
5. Click **Yes** to schedule a report, then enter how often the report should run and when the report starts and ends. If these fields are not available, the report provides a snapshot of current status rather than spanning a period of time.
6. If you want non-admin users to see a generated reports, choose **By Subject**. By default, any report can be seen by an OV3600 admin.
7. Click **Yes** if you want to email the report. They can be sent in HTML, PDF, and CSV formats.
8. Click **Yes** to you want to share the report by FTP or SCP to an external server.
9. Click **Add** to save your report. The report displays on the **Report Definition** page.

Tips for Restricting Time Ranges

Custom reports require extra consideration. Some reports, like client session data, are always restricted by a time range. Other reports, like client inventory, defaults to show all data. As a result, you might see conflicting device counts in these reports. To configure the time range, you must select **Limit to active devices** from the drop-down menu, and then select **Active during report timeframe** option.

Cloning Reports

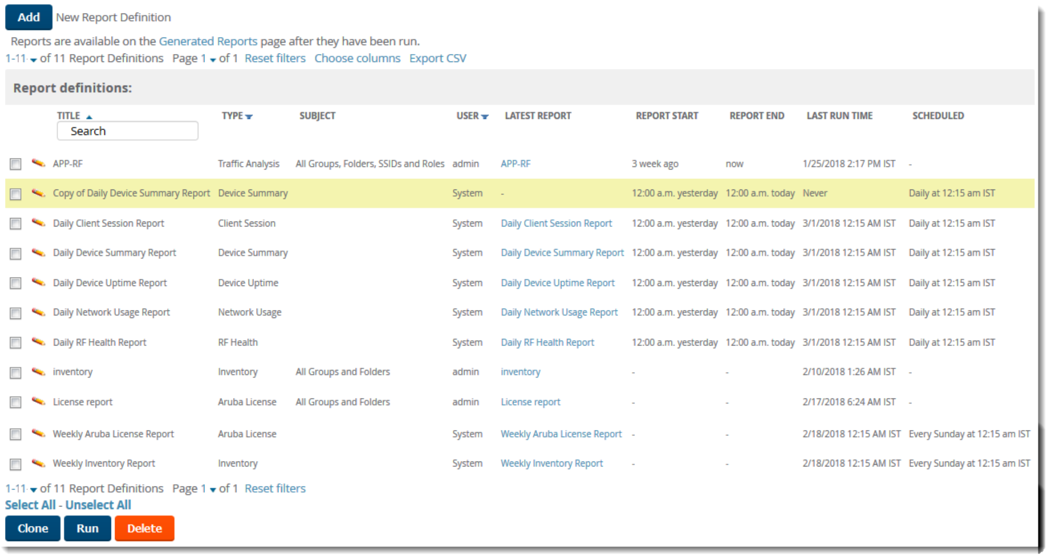
There are two places where you can clone and run a report. One is where you select a report definition from the Report Definition list. The other is where you use the Modify Devices option from a device list view, which you can access from **Groups** or **Devices**.

Selecting the Report Definition

To clone a report using a report definition:

1. Navigate to **Reports > Definitions** then select a report definition.
2. Click **Clone**. The copied report will be added to the report definition list with "copy of" appended in front of the report name.

Figure 230: *Cloning a Report*



Reports are available on the Generated Reports page after they have been run.

1-11 ▾ of 11 Report Definitions Page 1 ▾ of 1 Reset filters Choose columns Export CSV

Report definitions:

		TITLE ▲ Search	TYPE ▾	SUBJECT	USER ▾	LATEST REPORT	REPORT START	REPORT END	LAST RUN TIME	SCHEDULED
□	✎	APP-RF	Traffic Analysis	All Groups, Folders, SSIDs and Roles	admin	APP-RF	3 week ago	now	1/25/2018 2:17 PM IST	-
□	✎	Copy of Daily Device Summary Report	Device Summary		System	-	12:00 a.m. yesterday	12:00 a.m. today	Never	Daily at 12:15 am IST
□	✎	Daily Client Session Report	Client Session		System	Daily Client Session Report	12:00 a.m. yesterday	12:00 a.m. today	3/1/2018 12:15 AM IST	Daily at 12:15 am IST
□	✎	Daily Device Summary Report	Device Summary		System	Daily Device Summary Report	12:00 a.m. yesterday	12:00 a.m. today	3/1/2018 12:15 AM IST	Daily at 12:15 am IST
□	✎	Daily Device Uptime Report	Device Uptime		System	Daily Device Uptime Report	12:00 a.m. yesterday	12:00 a.m. today	3/1/2018 12:15 AM IST	Daily at 12:15 am IST
□	✎	Daily Network Usage Report	Network Usage		System	Daily Network Usage Report	12:00 a.m. yesterday	12:00 a.m. today	3/1/2018 12:15 AM IST	Daily at 12:15 am IST
□	✎	Daily RF Health Report	RF Health		System	Daily RF Health Report	12:00 a.m. yesterday	12:00 a.m. today	3/1/2018 12:15 AM IST	Daily at 12:15 am IST
□	✎	inventory	Inventory	All Groups and Folders	admin	inventory	-	-	2/10/2018 1:26 AM IST	-
□	✎	License report	Aruba License	All Groups and Folders	admin	License report	-	-	2/17/2018 6:24 AM IST	-
□	✎	Weekly Aruba License Report	Aruba License		System	Weekly Aruba License Report	-	-	2/18/2018 12:15 AM IST	Every Sunday at 12:15 am IST
□	✎	Weekly Inventory Report	Inventory		System	Weekly Inventory Report	-	-	2/18/2018 12:15 AM IST	Every Sunday at 12:15 am IST

1-11 ▾ of 11 Report Definitions Page 1 ▾ of 1 Reset filters

Select All - Unselect All

3. Click ✎ to modify the report settings.
4. Change the title of the report.
5. Click **Save**.

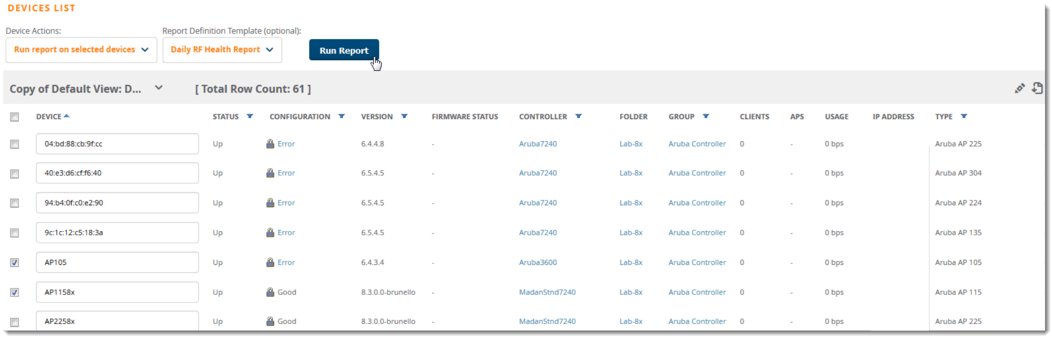
Selecting the Devices and a Report Template

You can select devices from the device list and modify the clone using a report template or by choosing report widgets. If you want to customize the report with widgets, see "Selecting the Devices Without Using a Report Template" on page 350.

To clone a report from the Modify Devices list using a report template:

1. Navigate to **Groups** and select a group, or **Devices > List**, then click ✎ to select the devices from the Modify Devices list.
2. From the Device Actions drop down menu, select **Run report on selected devices**.
3. Choose a report definition template.

Figure 231: *Running a Report Using a Definition Template*



DEVICES LIST

Device Actions: Run report on selected devices

Report Definition Template (optional): Daily RF Health Report

Run Report

Copy of Default View: D... [Total Row Count: 61]

	DEVICE	STATUS	CONFIGURATION	VERSION	FIRMWARE STATUS	CONTROLLER	FOLDER	GROUP	CLIENTS	APS	USAGE	IP ADDRESS	TYPE
□	04:bd:88:cb:9f:cc	Up	Error	6.4.4.8	-	Aruba7240	Lab-8x	Aruba Controller	0	-	0 bps		Aruba AP 225
□	40:e3:d6:cf:f6:40	Up	Error	6.5.4.5	-	Aruba7240	Lab-8x	Aruba Controller	0	-	0 bps		Aruba AP 304
□	94:b4:0f:c0:e2:90	Up	Error	6.5.4.5	-	Aruba7240	Lab-8x	Aruba Controller	0	-	0 bps		Aruba AP 224
□	9c:1c:12:c5:18:3a	Up	Error	6.5.4.5	-	Aruba7240	Lab-8x	Aruba Controller	0	-	0 bps		Aruba AP 135
☑	AP105	Up	Error	6.4.3.4	-	Aruba3600	Lab-8x	Aruba Controller	0	-	0 bps		Aruba AP 105
☑	AP1158x	Up	Good	8.3.0.0-brunello	-	MadanStnd7240	Lab-8x	Aruba Controller	0	-	0 bps		Aruba AP 115
□	AP2258x	Up	Good	8.3.0.0-brunello	-	MadanStnd7240	Lab-8x	Aruba Controller	0	-	0 bps		Aruba AP 225

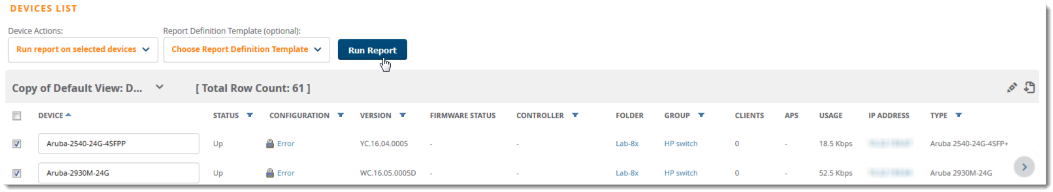
4. Click **Run Report**. OV3600 opens the Reports Definitions page. The copied report will be added to the report template with "copy of" appended in front of the report name.
5. Choose additional restrictions for the copy of the report.
6. Cick **Save and Run**. The newly created report is added in the Report Definitions page. You can make further report modifications at any time from the Report Definitions page.

Selecting the Devices Without Using a Report Template

To clone a report from the Modify Devices list without using a report template:

1. Navigate to **Devices**, then click ✎ to select the devices from the Modify Devices list.
2. From the Device Actions drop down menu, select **Run report on selected devices**.

Figure 232: *Running a Report Without a Template*



DEVICES LIST

Device Actions: Run report on selected devices

Report Definition Template (optional): Choose Report Definition Template

Run Report

Copy of Default View: D... [Total Row Count: 61]

	DEVICE	STATUS	CONFIGURATION	VERSION	FIRMWARE STATUS	CONTROLLER	FOLDER	GROUP	CLIENTS	APS	USAGE	IP ADDRESS	TYPE
☑	Aruba-2540-24G-4SFPP	Up	Error	YC.16.04.0005	-	-	Lab-8x	HP switch	0	-	18.5 Kbps	[redacted]	Aruba 2540-24G-4SFP+
☑	Aruba-2930M-24G	Up	Error	WC.16.05.0005D	-	-	Lab-8x	HP switch	0	-	52.5 Kbps	[redacted]	Aruba 2930M-24G

3. Click **Run Report**. OV3600opens the Custom Options page with the selected devices listed in the Report Restrictions area.
4. Choose report widgets and other report options.
5. Click **Add and Run**. The newly created report is added in the Report Definitions page. You can make further report modifications at any time from the Report Definitions page.

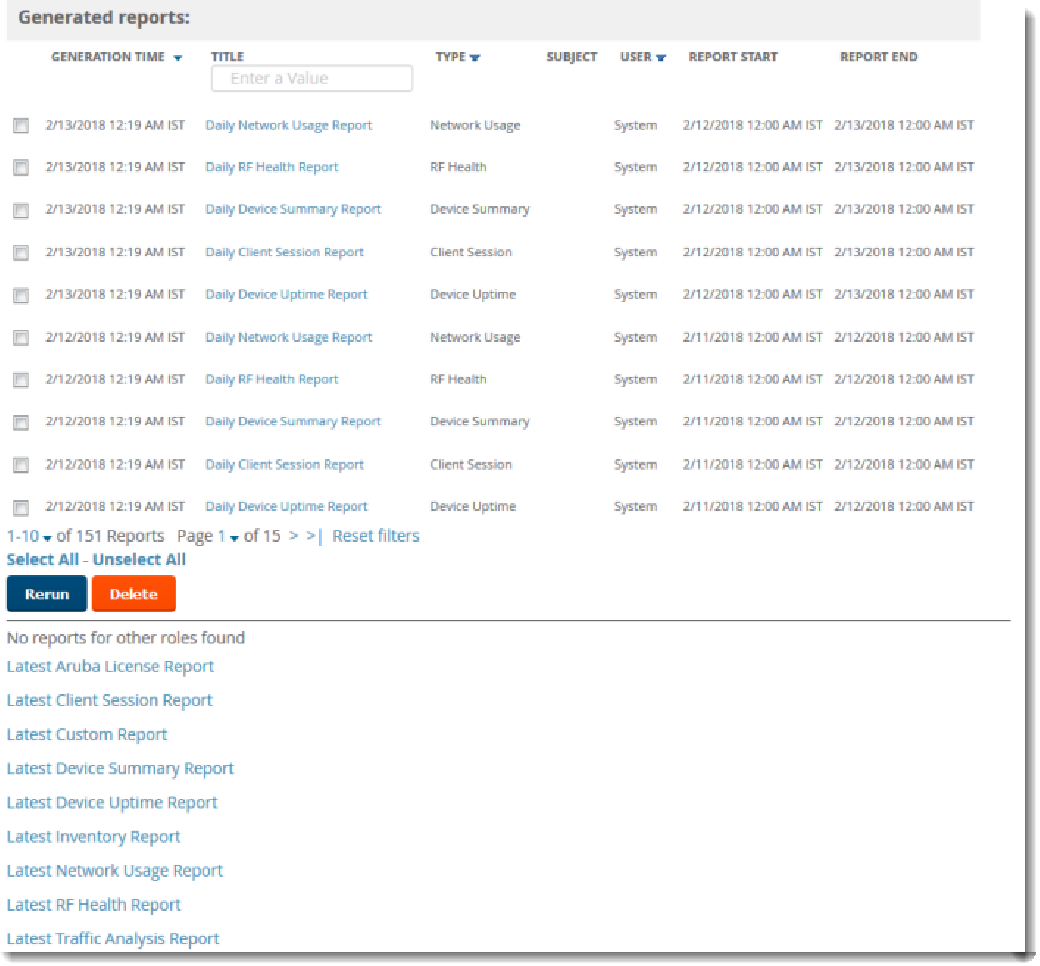
Viewing Generated Reports

The **Reports > Generated** page lists reports that have been run and the latest version of all daily reports. From the Generated reports list, you can click the title hyperlink to view the report details. By default, OV3600 orders reports by generation time. You can sort reports by any other column header in sequential or reverse sequential order. You can also choose columns, export the list in CSV format, and modify the pagination.

NOTE

An Admin user can see and edit all report definitions. Users with "Monitor Only" roles can see reports and definitions only if they have access to all devices in the reports. OV3600 displays reports for the current role and for additional roles.

Figure 233: *Generated Reports Page*



Generated reports:

	GENERATION TIME ▾	TITLE Enter a Value	TYPE ▾	SUBJECT	USER ▾	REPORT START	REPORT END
□	2/13/2018 12:19 AM IST	Daily Network Usage Report	Network Usage		System	2/12/2018 12:00 AM IST	2/13/2018 12:00 AM IST
□	2/13/2018 12:19 AM IST	Daily RF Health Report	RF Health		System	2/12/2018 12:00 AM IST	2/13/2018 12:00 AM IST
□	2/13/2018 12:19 AM IST	Daily Device Summary Report	Device Summary		System	2/12/2018 12:00 AM IST	2/13/2018 12:00 AM IST
□	2/13/2018 12:19 AM IST	Daily Client Session Report	Client Session		System	2/12/2018 12:00 AM IST	2/13/2018 12:00 AM IST
□	2/13/2018 12:19 AM IST	Daily Device Uptime Report	Device Uptime		System	2/12/2018 12:00 AM IST	2/13/2018 12:00 AM IST
□	2/12/2018 12:19 AM IST	Daily Network Usage Report	Network Usage		System	2/11/2018 12:00 AM IST	2/12/2018 12:00 AM IST
□	2/12/2018 12:19 AM IST	Daily RF Health Report	RF Health		System	2/11/2018 12:00 AM IST	2/12/2018 12:00 AM IST
□	2/12/2018 12:19 AM IST	Daily Device Summary Report	Device Summary		System	2/11/2018 12:00 AM IST	2/12/2018 12:00 AM IST
□	2/12/2018 12:19 AM IST	Daily Client Session Report	Client Session		System	2/11/2018 12:00 AM IST	2/12/2018 12:00 AM IST
□	2/12/2018 12:19 AM IST	Daily Device Uptime Report	Device Uptime		System	2/11/2018 12:00 AM IST	2/12/2018 12:00 AM IST

1-10 ▾ of 151 Reports Page 1 ▾ of 15 > >| Reset filters

Select All - **Unselect All**

No reports for other roles found

Latest Aruba License Report

Latest Client Session Report

Latest Custom Report

Latest Device Summary Report

Latest Device Uptime Report

Latest Inventory Report

Latest Network Usage Report

Latest RF Health Report

Latest Traffic Analysis Report

Here are some of the details you can view about a generated report:

- Generated Time. The date and time of the last time the report was run, or when the latest report is available. Selecting the link in this field displays the latest version of a given report. When the latest version of a given report is not available, this field is blank. In this case, a report can be run by selecting the report title and selecting **Run**.
- Title. The user-configured title of the report.
- Type. The type of the report.
- User. The user who created the customized report.
- Subject. The scope of the report, including groups, folders, SSIDs, or a combination of these included in the report.
- Report Start. The designated start of the time period to be covered by the report. You can enter a start date of 6 months 3 weeks 5 days 9 hours ago, or 5/5/2018 13:00. This field is supported by most report types. When this field isn't available, the report provides a snapshot of current status.
- Report End. The designated end of the time period covered by the report. You can enter an end date of 4 months 2 weeks 1 day ago, or 6/6/2018 9:00. This field is supported by most report types. When this field isn't available, the report provides a snapshot of current status.

Get an Updated Report

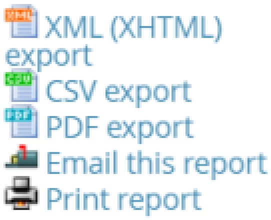
There are several ways to get an updated report:

- From the generated reports list, select a check box beside a report and click **Rerun**. When you run or rerun a report, the Generation Time column changes to pending until the report is completed.
- From the latest reports list at the bottom of the page, click the report hyperlink.

Sending Reports

All reports contain links to export, email, and print reports at the top right of the page (see Figure 234). Graphics and links are included with exported reports. When sending reports to multiple email addresses, separate them with commas.

Figure 234: *Send Report Options*



Exporting Reports in CSV Format

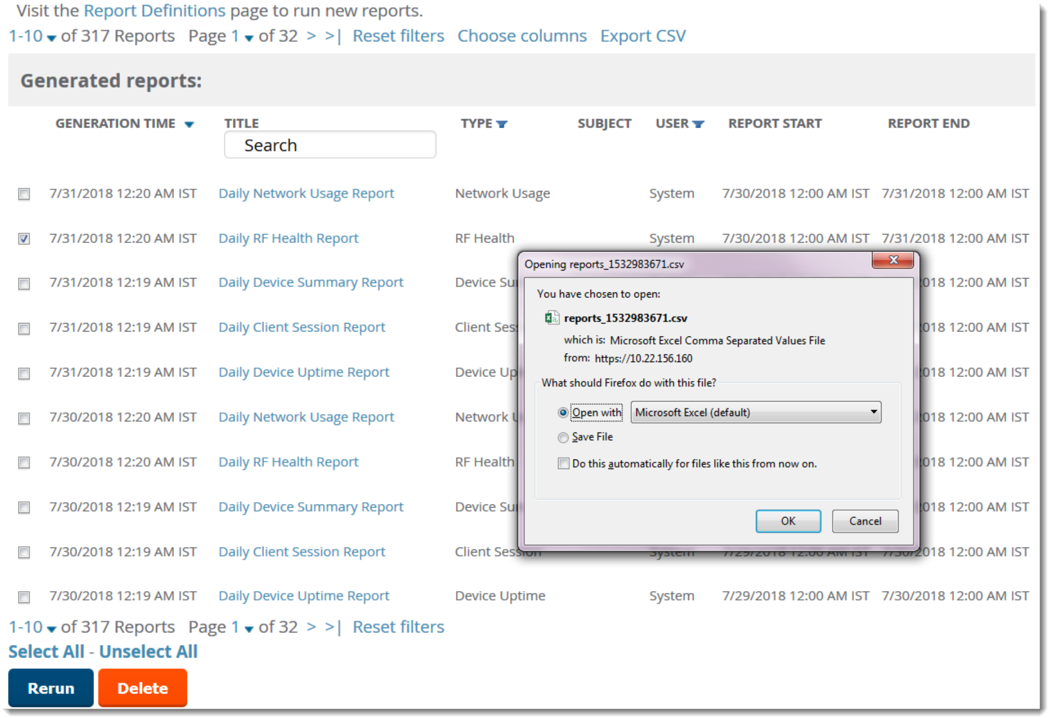
You can export reports (and some tables) from the WebUI. OV3600 will append a number to the file name like **1532986103**. This number changes every time you generate the report.

Exporting a Report

If you want to export an individual report, follow these steps:

1. Go to **Reports > Generated** and select a report from the report table.
2. Click the blue **Export CSV** link above the report table. If a message asks you what to do with the file, click **Open**. Or you can click **Save file** and view the file later.
3. Click **OK**.

Figure 235: *Exporting a Report in CSV Format*



Visit the Report Definitions page to run new reports.

1-10 ▾ of 317 Reports Page 1 ▾ of 32 > >| Reset filters Choose columns Export CSV

Generated reports:

	GENERATION TIME ▾	TITLE Search	TYPE ▾	SUBJECT	USER ▾	REPORT START	REPORT END
□	7/31/2018 12:20 AM IST	Daily Network Usage Report	Network Usage		System	7/30/2018 12:00 AM IST	7/31/2018 12:00 AM IST
☑	7/31/2018 12:20 AM IST	Daily RF Health Report	RF Health		System	7/30/2018 12:00 AM IST	7/31/2018 12:00 AM IST
□	7/31/2018 12:19 AM IST	Daily Device Summary Report	Device Su				018 12:00 AM IST
□	7/31/2018 12:19 AM IST	Daily Client Session Report	Client Ses				018 12:00 AM IST
□	7/31/2018 12:19 AM IST	Daily Device Uptime Report	Device Up				018 12:00 AM IST
□	7/30/2018 12:20 AM IST	Daily Network Usage Report	Network U				018 12:00 AM IST
□	7/30/2018 12:20 AM IST	Daily RF Health Report	RF Health				018 12:00 AM IST
□	7/30/2018 12:19 AM IST	Daily Device Summary Report	Device Su				018 12:00 AM IST
□	7/30/2018 12:19 AM IST	Daily Client Session Report	Client Session		System	7/29/2018 12:00 AM IST	7/30/2018 12:00 AM IST
□	7/30/2018 12:19 AM IST	Daily Device Uptime Report	Device Uptime		System	7/29/2018 12:00 AM IST	7/30/2018 12:00 AM IST

1-10 ▾ of 317 Reports Page 1 ▾ of 32 > >| Reset filters

Select All - Unselect All

Rerun Delete

Opening reports_1532983671.csv

You have chosen to open:

reports_1532983671.csv

which is: Microsoft Excel Comma Separated Values File

from: https://10.22.156.160

What should Firefox do with this file?

● Open with Microsoft Excel (default) ▾

○ Save File

□ Do this automatically for files like this from now on.

OK Cancel

Exporting Multiple Reports

When you export all files at once, OV3600 creates a zip file of all the CSV files and saves it to a temporary or download directory on your local OV3600 server.

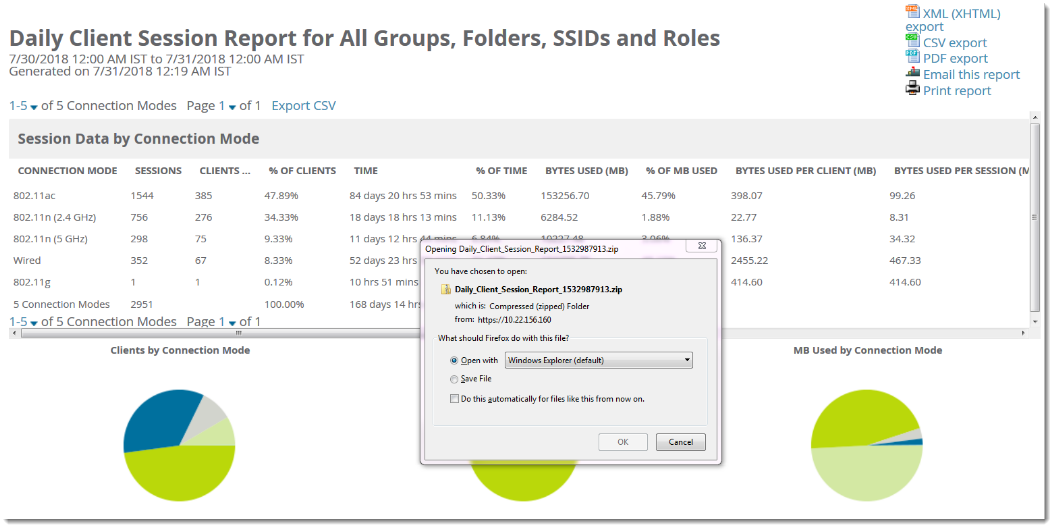
NOTE

If you are exporting reports to a remote server and name the report when you enter the file path, OV3600 will append a report ID to the CSV files and put it in a folder in a zip file on the remote server.

To export multiple reports:

1. Go to **Reports > Generated** and select a report from the list. Or you can scroll down to the bottom of the page, then click the blue link for the latest version of the report.
2. From the detailed report, click the **CSV Export** link at the top right of page.
3. Follow the onscreen instructions to open the CSV files, or save the zip file.
4. Click **OK**. Figure 236 shows an example of exporting client session reports in CSV format.

Figure 236: *Exporting Multiple CSV Files*



Daily Client Session Report for All Groups, Folders, SSIDs and Roles

7/30/2018 12:00 AM IST to 7/31/2018 12:00 AM IST
Generated on 7/31/2018 12:19 AM IST

1-5 of 5 Connection Modes Page 1 of 1 Export CSV

Session Data by Connection Mode

CONNECTION MODE	SESSIONS	CLIENTS ...	% OF CLIENTS	TIME	% OF TIME	BYTES USED (MB)	% OF MB USED	BYTES USED PER CLIENT (MB)	BYTES USED PER SESSION (M
802.11ac	1544	385	47.89%	84 days 20 hrs 53 mins	50.33%	153256.70	45.79%	398.07	99.26
802.11n (2.4 GHz)	756	276	34.33%	18 days 18 hrs 13 mins	11.13%	6284.52	1.88%	22.77	8.31
802.11n (5 GHz)	298	75	9.33%	11 days 12 hrs 44 mins	6.84%	10227.48	3.06%	136.37	34.32
Wired	352	67	8.33%	52 days 23 hrs				2455.22	467.33
802.11g	1	1	0.12%	10 hrs 51 mins				414.60	414.60
5 Connection Modes	2951		100.00%	168 days 14 hrs					

1-5 of 5 Connection Modes Page 1 of 1

Opening Daily_Client_Session_Report_1532987913.zip

You have chosen to open:

Daily_Client_Session_Report_1532987913.zip

which is: Compressed (zipped) Folder
from: https://10.22.156.160

What should Firefox do with this file?

● Open with Windows Explorer (default)
○ Save File
☐ Do this automatically for files like this from now on.

Sending Reports to a Smart Host

OV3600 uses Postfix to deliver alerts and reports via email, because it provides a high level of security and locally queues email until delivery. If OV3600 sits behind a firewall, which prevents it from sending email directly to the specified recipient, use the following procedure to forward email to a smart host.

To add a forwarding email address:

1. Add the following line to `/etc/postfix/main.cf`:

   ```
   relayhost = [mail.example.com]
   ```

   Where: `mail.example.com` is the IP address or hostname of your smart host.
2. Run **`service postfix restart`**
3. Send a test message to an email address.

   ```
   Mail -v xxx@xxx.com
   Subject: test mail
   .
   CC:
   ```
4. Press **Enter**.
5. Check the mail log to ensure mail was sent by running this command:

   ```
   tail -f /var/log/maillog
   ```

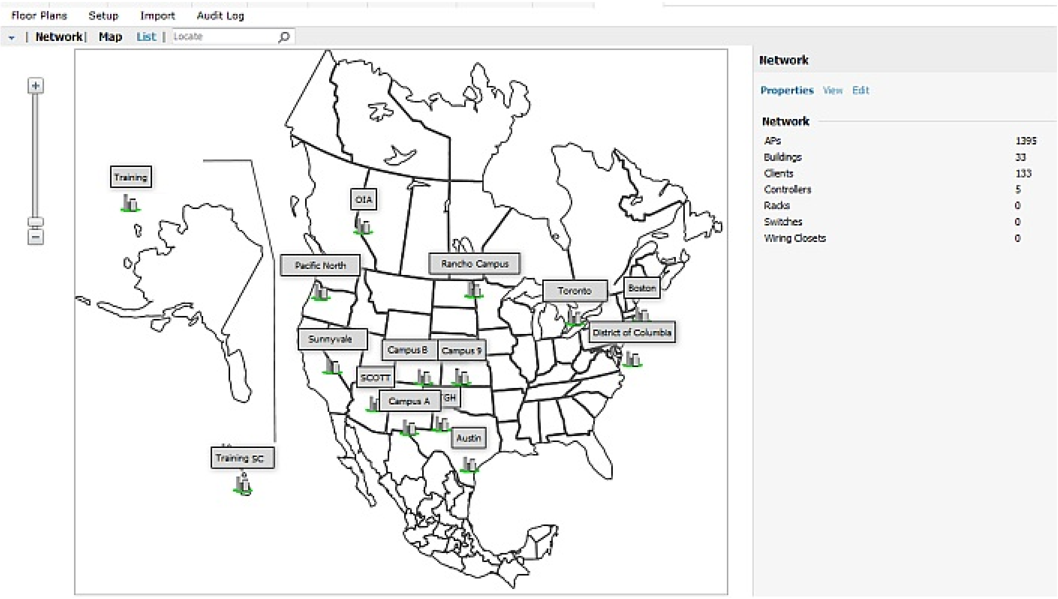
Using VisualRF

This chapter contains information about VisualRF and includes the following topics:

The VisualRF module provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. To understand what is happening on your wireless network, you need to know where your users and devices are located, and you need to monitor the RF environment in those areas. VisualRF puts this information at your fingertips through integrated mapping and location data.

VisualRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every wireless device in range. Moreover, VisualRF does not require dedicated RF sensors or a costly additional location appliance - all the necessary information is gathered from your existing wireless access points and controllers.

Figure 237: *Example VisualRF Page Showing all networks*



Network

Network	
APs	1395
Buildings	33
Clients	133
Controllers	5
Racks	0
Switches	0
Wiring Closets	0

Features

- Mesh monitoring page specially for viewing Alcatel-Lucent AirMesh devices. VisualRF automatically renders Mesh APs based on GPS coordinates.
- Floor plan upload wizard enables direct importation of JPG/JPEG, GIF, PNG, PDF (single page only) and CAD files for floor plans. **NOTE**: PDF floor plans must be generated from a source file. Other PDFs, such as those scanned from a printer, will not import properly. Similarly, CAD files must be generated by AutoCAD.
- Batch upload wizard enables batch uploads of multiple CAD files with corresponding walls, and access points.
- Accurate calculation of the location of all client devices (laptops, RFID Tags, PDAs, Phones) using RF data from your existing APs and controllers. Increased accuracy of device placement can be achieved with periodic site surveys.
- Graphical navigation allows your Help Desk to view floor plans simply by clicking on the appropriate campus, building, or floor.
- Tree view allows you to navigate to a specific campus, building, or floor via a tree navigation.
- Heatmaps depict the strength of RF coverage in each location.
- Speed (data rate) view which depicts the highest data speed at every location on a floor plan.
- Display of alerts and error conditions. For instance, an AP icon will display in red when a critical alert is active or when usage conditions exceed predefined thresholds.
- Location playback viewer which allows visual tracking of up to 24 hours of location history.
- Dynamically recalculated path loss and device locations based on real-time data from your wireless LAN, for increased location accuracy.
- Calibrated RF data from multiple vendors' APs (and across different product lines from the same vendor) for accurate display even in multi-vendor and multi-architecture environments. Refer to the *Supported Infrastructure Devices* document for a list of vendors and supported devices.
- Full planning capabilities based on speed or signal requirements.

Useful Terms

- **AP-to-AP Signal (Neighbor)** - Some APs/Controllers have the ability to report the signal strength of APs that they hear. OV3600 uses these signal strength readings to dynamically attenuate floor plans to increase the accuracy of client locations and heat maps.
- **Clients** - Clients are end-user devices that access the network through other devices monitored or managed by OV3600.
- **Client Health** - The client health metric compares the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means the AP is taking four times longer than the ideal transmission time, or sending 3 extra transmissions to that client for every packet.
- **dB (Decibels)** - difference/ratio between two signal levels.
- **dBm** - dB as compared to 1 mW. It is a logarithmic measurement (integer) which is typically used in place of mW to represent receive-power level. OV3600 normalizes all signals to dBm, so it is easy to evaluate performance between various vendors.
- **mW** - 1/1000 of a Watt. It is a linear measurement (always positive) generally used to represent transmission.
- **Rogue Surveys** - Rogue surveys are facilitated by VisualRF and the client's radio to understand which access points they hear and what signal strength.

- **RSSI (Received Signal Strength Indicator)** - IEEE defines RSSI is a mechanism by which RF energy is to be measured by the circuitry on a wireless NIC (0-255). RSSI is not standard across vendors. Each vendor determines their own RSSI scale/values.
- **Session** - A session is an instance when a client connects to the network. The period of time in which the client remains connected to the network is typically calculated as a single session. However, if a client roams between APs, the periods of time the client connected to the different APs may be calculated as separate sessions.
- **Unassociated Client Information** - Some APs/Controllers have the ability to report the signal strength of visible clients that are associated to a radio on a neighboring AP. OV3600 also uses these signal strength readings to more accurately place these unassociated clients.
- **VisualRF** - The OV3600 service that calculates location, calculates path loss, and provides floor plan editing capabilities.
- **VisualRF Plan** - Makes the planning portions of VisualRF available in an offline software package that does not require a server. For more information about VisualRF Plan, see "About VisualRF Plan" on page 393.

Starting VisualRF

In order to launch VisualRF, **OV3600 Setup > General** settings must be configured to display the VisualRF tab, and the VisualRF engine must be enabled using the **VisualRF > Setup** menu. Both of these pages are only visible to users logged-in with administrators credentials. By default:

- **Display VisualRF** is enabled in **OV3600 Setup > General**.
- **Enable VisualRF Engine** is disabled in **VisualRF > Setup**.

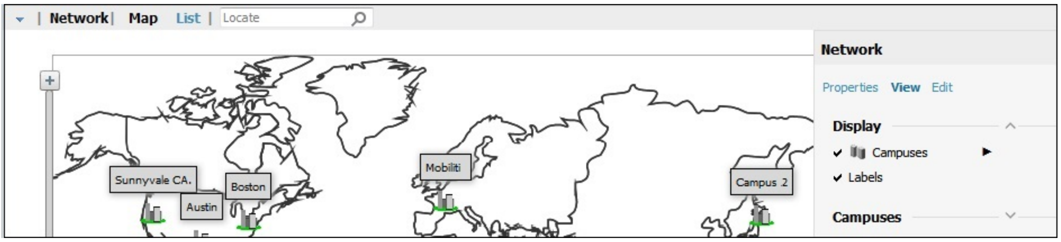
To enable VisualRF, follow these instructions while logged in as an administrator:

1. Navigate to **VisualRF > Setup**.
2. In the **Server Settings** section, select **Yes** in the **Enable VisualRF Engine** field, and then select **Save**.

Basic VisualRF Navigation

The top-level VisualRF menu shows only the **Network** view, as shown in Figure 238.

Figure 238: *Default VisualRF Top Level Menu - Network View*



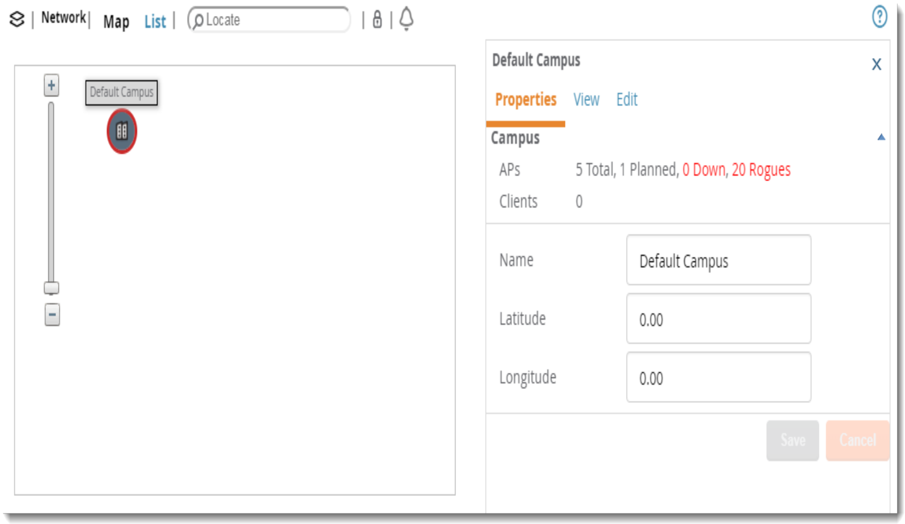
The top-level Network view can display network campuses on a map, or in a list. You can toggle between these two displays by clicking the **Map** or **List** links at the top of the Network view.

Network View Navigation

The Network view provides page specially for viewing campuses, buildings and floors within your network.

You can select any campus or building to view the numbers of APs and clients at that location. Figure 239 displays an example of a campus view with a building icon selected:

Figure 239: *Viewing a Campus Network*



Default Campus

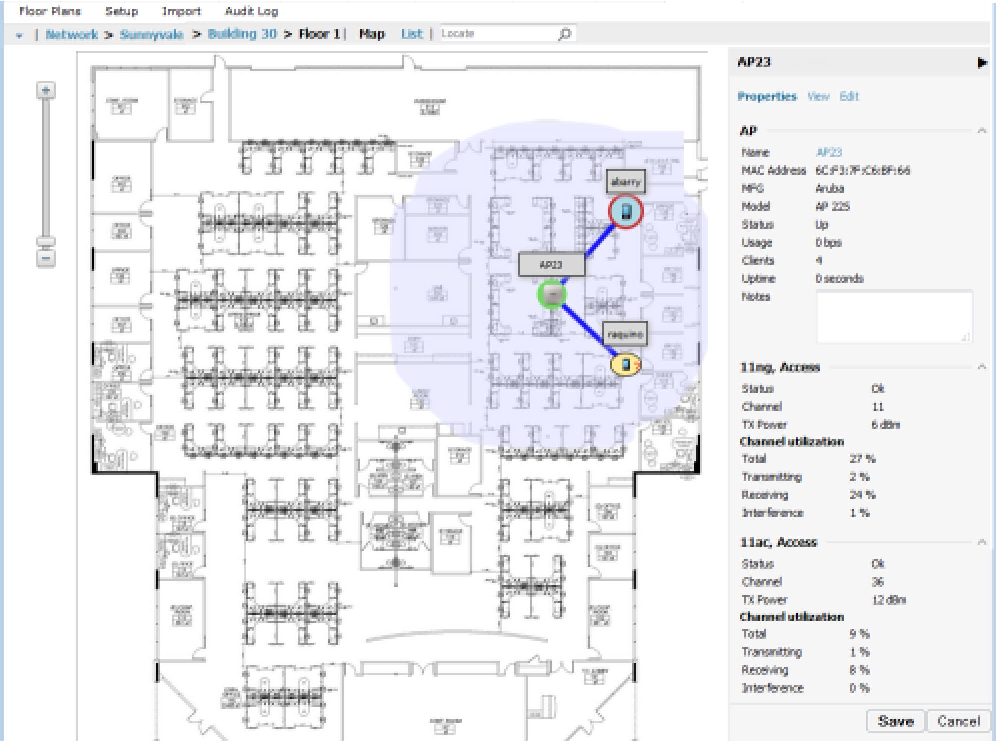
Campus

APs	5 Total, 1 Planned, 0 Down, 20 Rogues
Clients	0

Name	Default Campus
Latitude	0.00
Longitude	0.00

Click on an building within the selected campus, then select a floor to display the APs and clients on that floor. Select an AP or client to view detailed information about that device, as shown in Figure 240

Figure 240: *Viewing a Floor Plan in VisualRF*



AP23

AP

Name	AP23
MAC Address	6C:F3:7F:C6:BF:66
MFG	Aruba
Model	AP 225
Status	Up
Usage	0 bps
Clients	4
Uptime	0 seconds
Notes	

11ng, Access

Status	Ok
Channel	11
TX Power	6 dBm
Channel utilization	
Total	27 %
Transmitting	2 %
Receiving	24 %
Interference	1 %

11ac, Access

Status	Ok
Channel	36
TX Power	12 dBm
Channel utilization	
Total	9 %
Transmitting	1 %
Receiving	8 %
Interference	0 %

Customize Your Floor Plan View

You can customize your floor plan view by selecting the devices, client and AP overlays, display lines, and floor plan features from the **View** tab.

Devices

Click the following device options:

- **APs**, then click ▶ to select an option, such as planned or deployed, air monitors, channel, and transmit power.
- **Clients**, then click ▶ to select the size of the icon displayed for wireless users.
- **Interferers**, then click ▶ to select the size of the icon displayed for sources of Wi-Fi interference. This option works for Alcatel-Lucent AOS-W devices running 6.1 or greater that have run the **mgmt-server type** OV3600 command and have APs performing spectrum analysis through hybrid scanning or dedicated spectrum monitors.
- **Rogues**, then click ▶ to select the size of the icon displayed for rogue devices.
- **Tags**, then click ▶ to select the size of the icon to display Wi-Fi tags.

Client Overlays

Click the following client overlay options:

- **Traffic Anaylsis**, then click ▶ to customize thresholds based on your network and view the top 10 apps used in the last 2 hours. In the floorplan, hover your mouse over a client icon to see user and device details.

  You can edit the following color presets:
  - Green indicates that a client used between 0 and 20 MB in the past two hours.
  - Yellow indicates that a client used between 20 MB and 1GB in the past two hours.
  - Red indicates that a client has used more than 1 GB in the past two hours.
- **Client Health** to view metrics for controllers running Alcatel-Lucent AOS-W 6.3 or greater. For more information on how this value is calculated, see "Useful Terms" on page 356.
- **UCC**, then click ▶ to select an option, such as Protocol, Type, or Quality.

AP Overlays

The channel utilization, channel, heatmap and speed overlays display information for adjacent floors to determine how the bleed through from adjacent floors affects the viewed floor. Besides the current floor, you can view all floors, or data from APs located on the floor above or below.

Click the following device overlay options:

- **Ch. Utilization**, then click ▶ to select an option, such as Current, Dataset, Frequency, Floors, or whether to show the overlay as a grid. Airtime usage is a good indication of how busy an area is.
- **Channel**, then click ▶ to select an option, such as Signal Cutoff, Band, Channel, or Floors. This overlay identifies regions covered by specific channels, or regions with overlapping coverage on one selected channel or all channels in the 2.4 Ghz or 5 Ghz radio band. Hover your mouse over coverage areas for details about the APs.
- **Heatmap**, then click ▶ to select an option, such as Signal Cutoff, Frequencies, Floors, or whether to show the overlay as a grid.
- **Speed**, then click ▶ to select an option, such as Client TX, Rate, Frequencies, Floors, or whether to show the overlay as a grid. This overlay provides the highest data rate a user will receive for all areas of a floor plan. transmit power value for the overlay.
- **Voice**, then click ▶ to select an option, such as Signal Cutoff, Frequencies, Floors, or whether to show the overlay as a grid. This overlay uses color-codes to indicate the number of radios covering each grid cell based on the selected signal cutoff.

Relation Lines

Click the following relation line options:

- **APs** to view AP neighbor lines, which show the APs that hear each other.
- **Client Association** to view client to AP lines. The thicker lines designate AP of association, and the thinner lines show the APs that hear the client. This overlay uses color-codes to represent the radio band.
- **Client Neighbors** to view lines between a client and radios that hear the client , excluding the radio of association.
- **Interferers** to view lines between sources of Wi-Fi interference and the radios that have discovered them. For interferers, there is no radio of association.
- **Rogues** to view rogue AP to radio lines.
- **Surveys** to view lines between an AP and a client heard during a client survey. The ability to define a client survey was deprecated in OV3600 8.2, but surveys created in previous 7.x and 8.x releases can still be displayed on a VisualRF floor plan.
- **Tags** to view lines between Wi-Fi tags and radios which hear the tags. For tags, there is no radio of association.

Floor Plan Features

You can display floor plan features, such as Grid Lines, Labels, Origin, Regions, Walls, or Wiring Closets. If you created a client survey in OV3600 8.0.x and earlier, they also display on the floor plan when you select Surveys from the options.

To customize your grid lines, click ▶ to select Gridsize or Color.

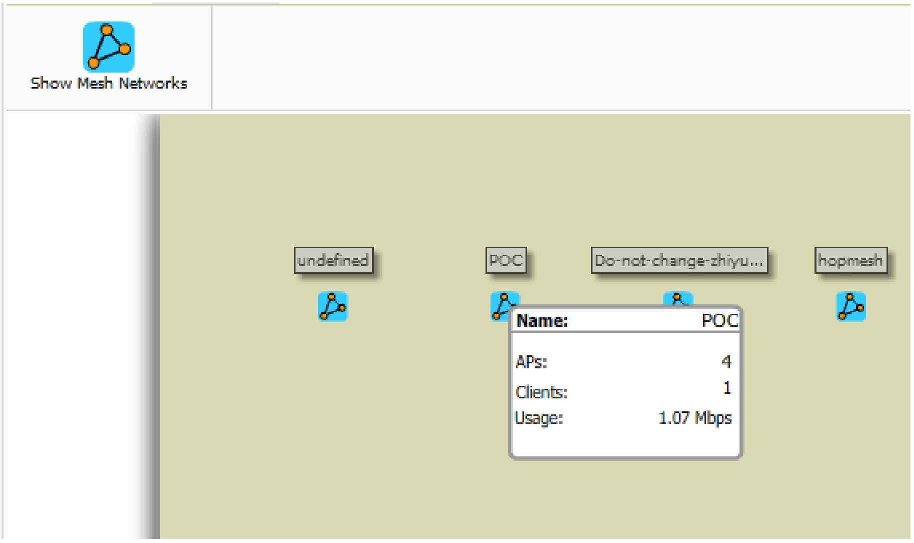
To ensure that multi-floor heatmaps display properly, ensure that your floor plans are vertically aligned. VisualRF uses the origination point for this alignment. By default, the origin appears in the upper left corner of the floor plan. You can drag and drop the origin point to the correct position.

Mesh View Navigation

Mesh view provides a visual Mesh monitoring page specially for viewing Alcatel-Lucent AirMesh devices. It automatically renders Mesh APs based on GPS coordinates.

You can mouse over each mesh network icon to view the numbers of APs and clients, and network usage in Mbps. Figure 241 displays an example of a Mesh Network view with a mouseover above a network icon:

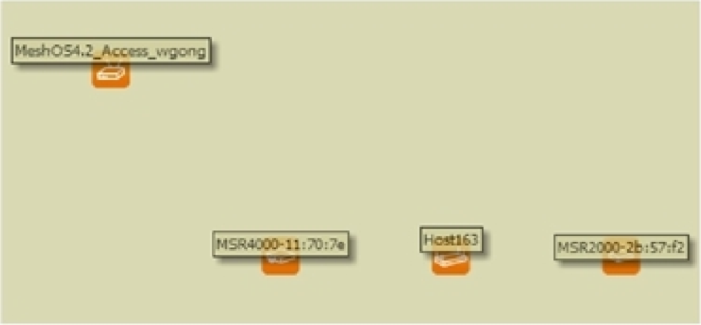
Figure 241: *Viewing Mesh Networks in VisualRF*



Name: POC
APs: 4
Clients: 1
Usage: 1.07 Mbps

Click on an AirMesh network to display the APs with labels, as shown in Figure 242

Figure 242: *APs in a mesh network*



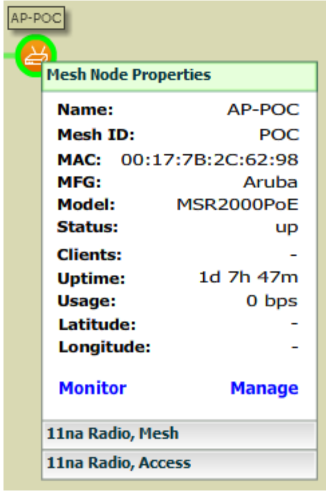
Select an AirMesh AP icon to bring up the pop up menu showing the Mesh Node Properties by default. This window shows the node's name, MeshID, MAC, Manufacturer, and other information. Clicking the blue **Monitor** link inside this window opens the **Devices > Monitor** page in a new tab. Clicking the blue **Manage** link inside this window opens the **Devices > Manage** page for this AP in a new tab.

The top-level Mesh view includes the Refresh, Site Tree, Preferences and Help icons. Table 158 describes these icons and their functions in the VisualRF Mesh view.

Table 158: *Top Level Icons and Descriptions*

Operation	Icon	Description
Refresh	🔄	Refresh the floor plan to see changes.
Open Site Tree	☰	Display the Network Tree View Window on top of the floor plan.
Preferences	⚙	Configure personal viewing preferences. The Preferences menu allows you to configure user preferences
Help	?	Launch the online help. **NOTE:** This User Guide currently contains the most up-to-date help information for the VisualRF interface.

Figure 243: *Properties for a Mesh Gateway Illustration*



AP-POC

Mesh Node Properties

Name:	AP-POC
Mesh ID:	POC
MAC:	00:17:7B:2C:62:98
MFG:	Aruba
Model:	MSR2000PoE
Status:	up
Clients:	-
Uptime:	1d 7h 47m
Usage:	0 bps
Latitude:	-
Longitude:	-

Monitor Manage

11na Radio, Mesh

11na Radio, Access

For radio-level status information on an AirMesh device in your network, select the menus in the AP’s pop up window for each radio (**11na Radio, Access**; **11na Radio, Mesh**; and so forth).

Advanced VisualRF Settings

You can configure advanced settings for VisualRF on the **Setup** page (see). These settings can impact your server's performance and location accuracy.

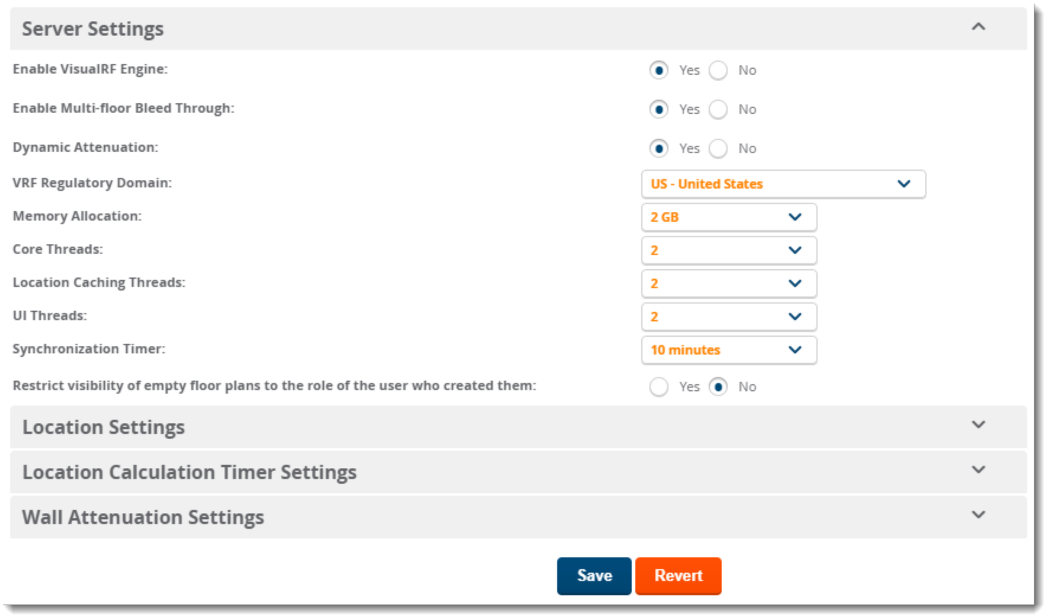
When you click **Save**, VisualRF will restart, causing a delay that might take a minute to 30 minutes, depending on the size of your VisualRF database.

Server Settings

To enable VisualRF and tune memory and performance, navigate to the **Server Settings** section on the **VisualRF > Setup** page.

In previous versions of OV3600, you set measurement preferences on the **VisualRF > Setup** page. In OV3600 8.2.5.1 and later versions, this preference is set by choosing the "Meters" or "Feet " option on the **VisualRF > Floor Plans > Network >Edit** page. For more information about setting your preferences, see "Change Settings in VisualRF Floor Plans" on page 372.

Figure 244: *Server Settings*



Server Settings

Enable VisualRF Engine: ● Yes ○ No

Enable Multi-floor Bleed Through: ● Yes ○ No

Dynamic Attenuation: ● Yes ○ No

VRF Regulatory Domain: US - United States

Memory Allocation: 2 GB

Core Threads: 2

Location Caching Threads: 2

UI Threads: 2

Synchronization Timer: 10 minutes

Restrict visibility of empty floor plans to the role of the user who created them: ○ Yes ● No

Location Settings
Location Calculation Timer Settings
Wall Attenuation Settings
Save
Revert

The server settings are detailed in Table 159.

Table 159: *Server Settings*

Setting	Default	Description
Enable VisualRF Engine	No	Enables or disables the VisualRF engine. This setting must be enabled to use VisualRF. If you do not have a license for VisualRF, this page will not appear.

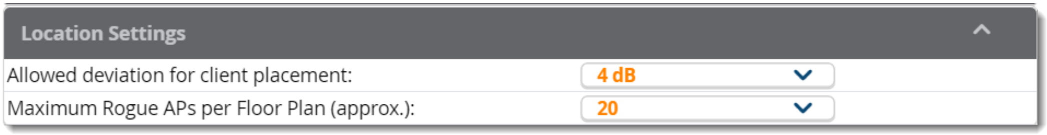
Table 159: *Server Settings (Continued)*

Setting	Default	Description
Enable Multi-floor Bleed Through	Yes	Enables or disables calculating the impact APs on floors above and below the currently viewed floor in the Quick View.
Dynamic Attenuation	Yes	Incorporate AP to AP readings as well as site survey information and dynamically recalculate the path loss of each radio to every grid cell on the floor plan, increasing coverage and location accuracy.
VRF Regulatory Domain	United States	Sets the regulatory domain in OV3600.
Memory Allocation	512 MB	The amount of memory dedicate to VisualRF. It is not dynamically allocated and all the memory is consumed upon starting the service. Be sure to check the memory and swap utilization in the **Systems > Performance** page before making any changes. The exact amount of memory used per floor plan will vary heavily based on the size, number of devices and number of grid cells on the floor plan. ● 25 floors or less 512 MB ● 25 to 50 floors 768 MB ● 50 to 75 floors 1 GB ● 75 to 100 floors 1.5 GB ● 100 to 200 floors 3 GB ● 200 to 300 floors 5 GB (64-bit only) ● Above 300 8 GB (64-bit only) **NOTE:** If you see Out of Memory errors in the httpd/error_log on the **System > Status** page, you should increase memory allocation.
Core Threads	1x number of cores	Number of threads that calculate path loss for each floor. These threads also regenerate a floor's RF properties when new APs, walls, or regions are added to a floor plan.
Location Caching Threads	1x number of cores	Number of threads that calculate the location of all clients associated with access points on this floor plan.
UI Threads	1x number of cores	Number of threads that service the users accessing VisualRF, as well as OV3600-to-VisualRF communication. **NOTE**: If users experience timeout errors while using VisualRF, allocate additional WebUI Threads.
Synchronization Timer	15 minutes	This timer indicates how often VisualRF will synchronize with the APs within OV3600. This synchronization includes checking the Up/Down status and parsing the XML.
Restrict visibility of empty floor plans to the role of the user who created them	No	When enabled, only the creator can view an empty floor plan.

Location Settings

To tune location accuracy, click ⌄ to access the location settings on the **VisualRF > Setup** page.

Figure 245: *Location Settings*



Location Settings

Allowed deviation for client placement: 4 dB

Maximum Rogue APs per Floor Plan (approx.): 20

The location settings are detailed in Table 160

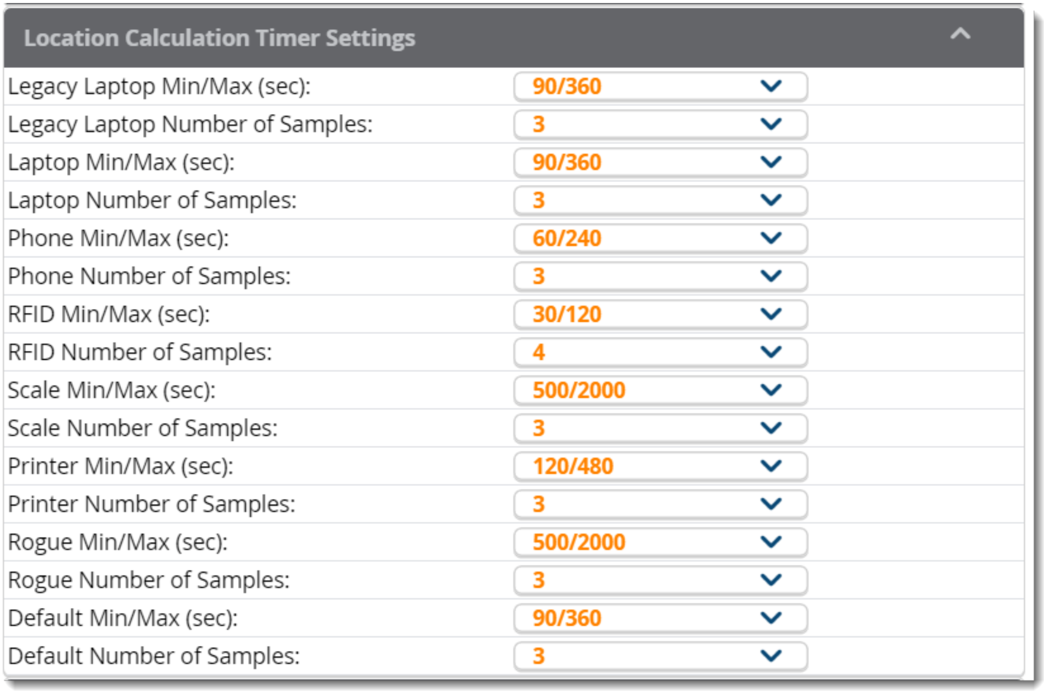
Table 160: *Location Settings*

Setting	Default	Description
Allowed deviation for client placement	4 dB	When VisualRF locates a client or rogue it utilizes signal metrics from all the APs that hear the client or rogue device. VisualRF builds a fingerprint location for all clients with similar transmit-power capability. All subsequent clients that fall within the deviation is placed on the same location fingerprint or *x, y* coordinates. **Example:** AP1 hears Client1 at -72, and AP2 hears Client 1 at -64. VisualRF calculates the client's location to be at coordinates 100, 200. Client2 is heard by AP1 at -71 and AP2 at -65. VisualRF will use the average of the difference in signals (AP1 -72 and -71) to see if the client matches a pre-calculated location fingerprint. 1 + 1 (differences in signals) / 2 (# of APs) = 1 which falls within the deviation of 2, hence the client would be located at 100,200.
Maximum Rogue APs per Floor Plan	20	Sets the maximum number of rogues OV3600 will place on a Floor. Use this filter in combination with the **RAPIDS Export Threshold** configured on the **RAPIDS > Setup** page to intelligently control the number of rogue devices displayed per floor. **NOTE:** Increasing this value can increase the load on the server and the clutter on the screen.

Location Calculation Timer Settings

You can configure VisualRF to calculate client locations by setting timers on the **VisualRF > Setup** page.

Figure 246: *Location Calculation Timer Settings*



Location Calculation Timer Settings

Legacy Laptop Min/Max (sec):	90/360
Legacy Laptop Number of Samples:	3
Laptop Min/Max (sec):	90/360
Laptop Number of Samples:	3
Phone Min/Max (sec):	60/240
Phone Number of Samples:	3
RFID Min/Max (sec):	30/120
RFID Number of Samples:	4
Scale Min/Max (sec):	500/2000
Scale Number of Samples:	3
Printer Min/Max (sec):	120/480
Printer Number of Samples:	3
Rogue Min/Max (sec):	500/2000
Rogue Number of Samples:	3
Default Min/Max (sec):	90/360
Default Number of Samples:	3

The location calculation timer settings are described in Table 161

Table 161: *Location Calculation Timer Settings*

Setting	Default	Description
Legacy Laptop Min/Max (sec)	90/360	This timer determines how often to calculate the location for legacy laptop devices. Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 90 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 3 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 360 seconds) and then recalculate.
Legacy Laptop Number of Samples	3	See definition above.

Table 161: *Location Calculation Timer Settings (Continued)*

Setting	Default	Description
Laptop Min/Max (sec)	90/360	This timer determines how often to calculate the location for laptop (non-legacy) devices. Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 90 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 3 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 360 seconds) and then recalculate.
Laptop Number of Samples	3	See definition above.
Phone Min/Max (sec)	60/240	This timer determines how often to calculate the location of phones. Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 60 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 3 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 240 seconds) and then recalculate.
Phone Number of Samples	3	See definition above.
RFID Min/Max (sec)	30/120	This timer determines how often to calculate the location of RFIDs (such as devices with tag readers for tracking). Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 30 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 4 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 120 seconds) and then recalculate.
RFID Number of Samples	4	See definition above.
Scale Min/Max (sec)	500/2000	

Table 161: *Location Calculation Timer Settings (Continued)*

Setting	Default	Description
Scale Number of Samples	3	
Printer Min/Max (sec)	120/480	This timer determines how often to calculate the location of printers. Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 120 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 3 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 480 seconds) and then recalculate.
Printer Number of Samples	3	See definition above.
Rogue Min/Max (sec)	500/2000	This timer determines how often to calculate the location of rogues. Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 500 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 3 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 2000 seconds) and then recalculate.
Rogue Number of Samples	3	See definition above.
Default Min/Max (sec)	90/360	This timer determines how often to calculate the locations of clients
Default Number of Samples	3	This quantity indicates how many samples are taken to calculate the location and place the client on the floor plan. The default is 3 samples.

Wall Attenuation Settings

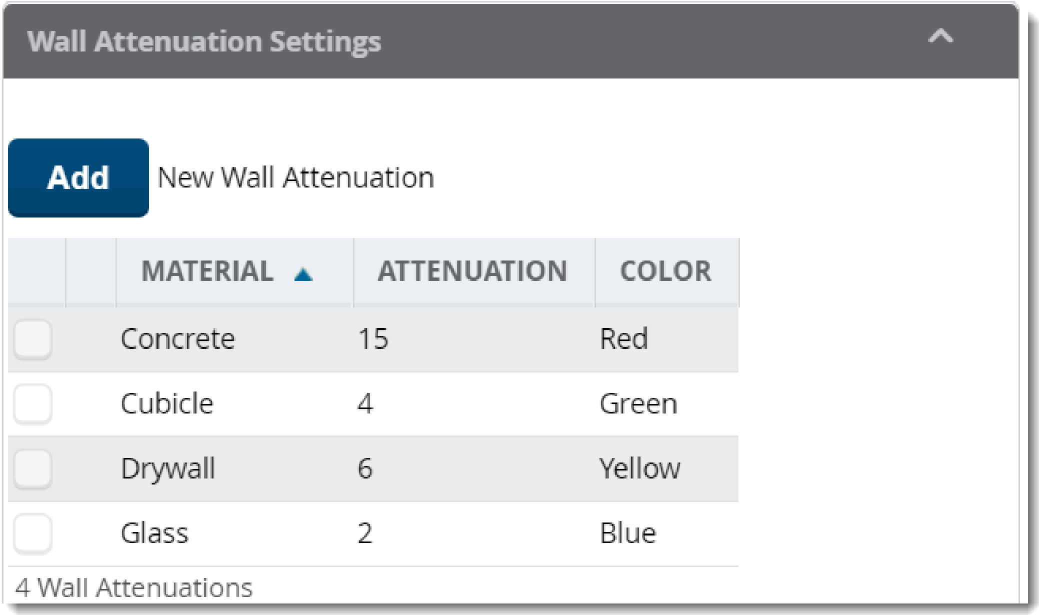
Signal attenuation is the loss of signal strength during transmission. You can indicate the causes of attenuation using attenuation settings on the **VisualRF > Setup** page.

NOTE

VisualRF uses these values to calculate path loss and client locations. Walls within VisualRF are interpreted as pure dB loss without adjusting for wall thickness.

VisualRF provides default attenuation settings for individual floor plans that you cannot change.

Figure 247: *Wall Attenuation Settings*



	MATERIAL ▲	ATTENUATION	COLOR
□	Concrete	15	Red
□	Cubicle	4	Green
□	Drywall	6	Yellow
□	Glass	2	Blue

4 Wall Attenuations

The default wall attenuation settings are described in Table 162.

Table 162: *Default Wall Attenuations*

Item	Description
Material	Type of material that reduces the signal strength, including concrete, cubicle, dry wall, and glass.
Attenuation	Signal loss represented in decibels (dB).
Color	Color representation in the floor plan.

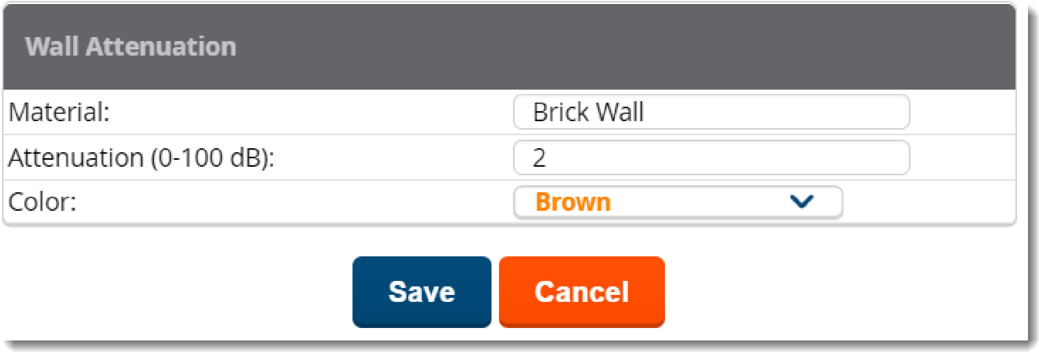
Adding a Wall Attenuation

Follow these steps to create a wall attenuation:

1. Navigate to **VisualRF > Setup**, then click **Add**.
2. Enter the wall material.
3. Enter the attenuation in decibels.
4. Select the color used to represent the attenuation on the floor plan.

   Figure 248 shows an example of RF signal power decreasing by 3 db of attenuation for brick walls.

Figure 248: *Adding a Wall Attenuation*

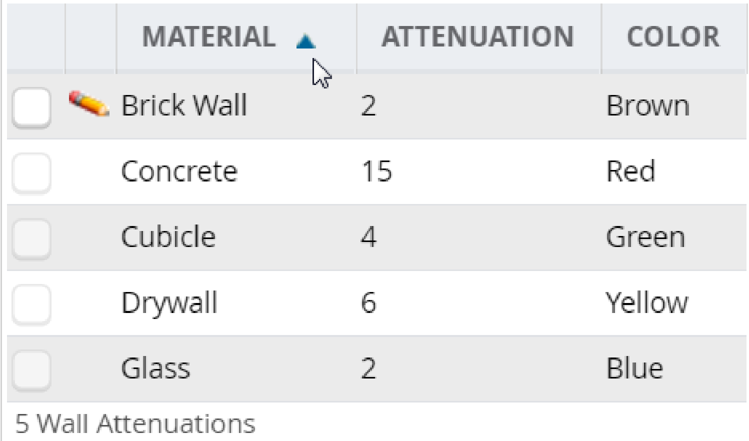


Wall Attenuation

Material:	Brick Wall
Attenuation (0-100 dB):	2
Color:	Brown

5. Click **Save**. The brick wall attenuation you added in Step 4 displays in the Wall Attenuation table.

Figure 249: *Wall Attenuation*



	MATERIAL ▲	ATTENUATION	COLOR
□ ✎	Brick Wall	2	Brown
□	Concrete	15	Red
□	Cubicle	4	Green
□	Drywall	6	Yellow
□	Glass	2	Blue

5 Wall Attenuations

You can later change the attenuation by clicking ✎ next to the material in the Wall Attenuation table.

VisualRF Resource Utilization

When tuning the VisualRF server, use the default settings as recommended. If you do change any of these settings, change one at a time and see how the system performs. Each time you restart VisualRF, you will notice a delay before returning to normal processing. This delay can last anywhere from a minute to upwards of 30 minutes, depending on the size of the VisualRF database.

If you use the 'top' command to check on VisualRF resource utilization, ensure you use the '1' and 'H' flags to show cores and threads. Remember 'top' also takes 1-2 minutes to normalize and provide accurate data.

NOTE

It is normal for VisualRF to consume 20% of each core with a combination of threads. It will utilize excess CPU cycles on all cores when required.

Planning and Provisioning

VisualRF provides the capability to plan campuses, buildings, floors, and access points prior to the actual access point deployment. The following procedure describes the workflow:

- "Creating a New Campus" on page 370
- "Creating a New Building" on page 370
- "Adding a Floor Plan" on page 371
- "Editing a Floor Plan Image" on page 372

- "Defining Floor Plan Boundaries" on page 374
- "Defining Floor Plan Regions" on page 375
- "Editing a Planning Region" on page 376
- "Adding Deployed Access Points onto the Floor Plan" on page 377
- "Adding Planned APs onto the Floor Plan" on page 378
- "Editing a Planning Region" on page 376
- "Auto-Matching Planned Devices" on page 379
- "Printing a Bill of Materials Report" on page 379

Creating a New Campus

Floors are associated with a building, and buildings are associated with a campus. In order to create a new floor, you must first create a campus with at least one building.

To create and place your campus:

1. Navigate to **VisualRF > Floor Plans**.
2. Navigate to the **Add Campus** menu.
3. Select **Edit** from the toolbar on the right window pane of the Network view, then click **New Campus**.
4. Enter the name of the campus, then click **Save**. A new campus icon appears on the campus background.
5. Select an appropriate network geographical background or upload a personalized image by right-clicking on the background, and selecting one of the following options:
   - **World Map**: browse and select any of the included maps.
   - **Custom Image**: upload your own image as the map background.
6. Drag the new campus icon to the appropriate location on the map background, or right-click the background and select **Auto Arrange Campuses** to arrange the campus in alphabetical order across the background.

Creating a New Building

1. Select the icon for the campus created in the previous procedure.
2. When the campus area opens, add the new building. Select **Edit** from the toolbar on the right window pane of the Network view, then click **New Building**.
3. When the **New Building** window appears, enter the following information:

Table 163: *New Building Fields and Descriptions*

Field	Description
Name	Name of the building located in an existing campus.
Address	Building or Campus address
Longitude & Latitude	These fields are used to represent a building on Google Earth.
Ceiling Height	The normal distance between floors in the building. This value can be overridden as each floor is created, but this is the default value for every new floor added to the system. This data element can be imported or exported to external planning tools like Ekahau. It is not currently used by OV3600.

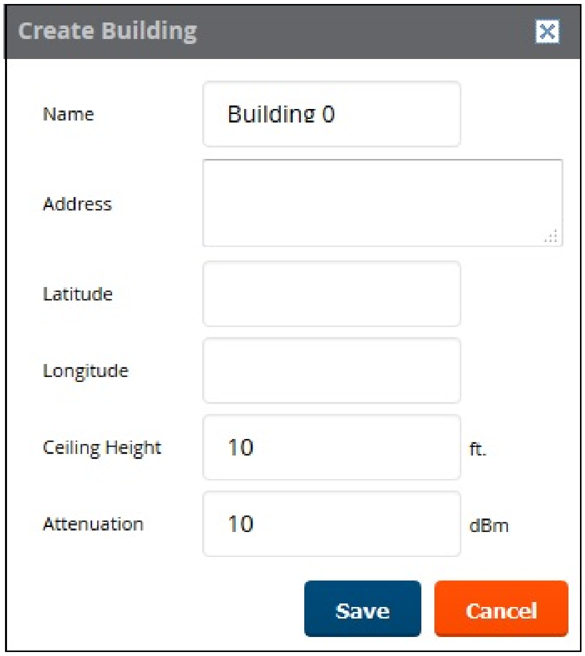
Table 163: *New Building Fields and Descriptions (Continued)*

Field	Description
Attenuation	Enter the attenuation loss in decibels between floors. This value can be overridden as each floor is created, but this is the default value for every new floor added to the system. This data element can be imported or exported to external planning tools like Ekahau. It is not currently used by OV3600.

NOTE

The WebUI also includes fields to configure client transmit power and desired speed values used for automatic placement of APs into floors within this campus. These fields are located in the **Advanced** section of the floor **Properties** menu.

Figure 250: *Create New Building Window*



Create Building

Name	Building 0	
Address		
Latitude		
Longitude		
Ceiling Height	10	ft.
Attenuation	10	dBm

4. Select **Save**. A new building icon will appear in the upper-left corner of the background canvas.
5. Drag the Building icon to the appropriate location on the map background.

You are now ready to import your floor plan.

Adding a Floor Plan

Floor plans can be added (imported), edited, and deleted. If you want to import a newer floor plan to replace a current one, you must first delete the original plan and then add the new floor plan.

VisualRF supports floor plans in CAD, DWG , GIF, SVG, JPEG, PNG, and PDF format. Consider the following guidelines:

- CAD files must be generated from Autodesk's AutoCAD® software.
- The floor size is restricted to 800 X 800 meters.
- If the files include cross-referencing bindings, they might not display properly.
- PDF files must be generated from an original source file. Altered PDF files, such a scanned file, will not import properly.

When importing a floor plan, ensure that the devices to be included are also available in the device catalog.

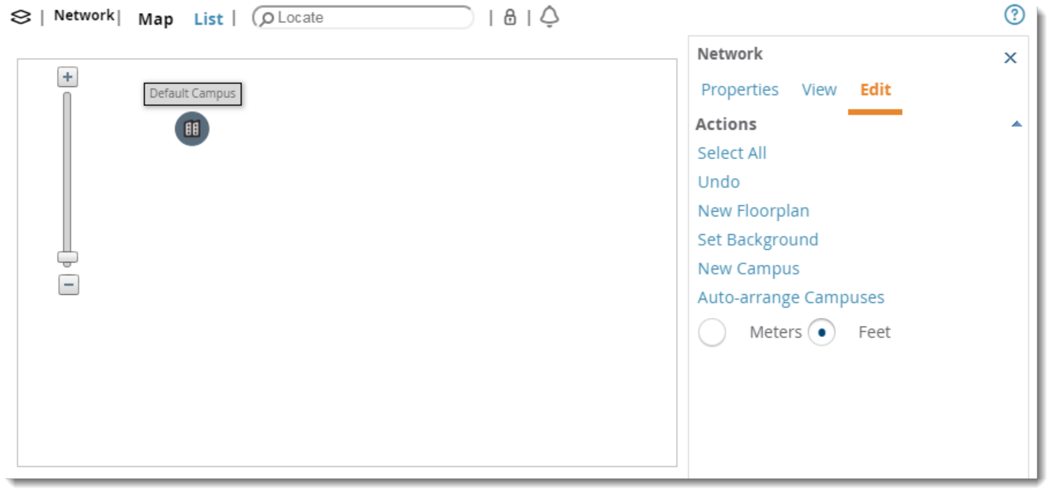
To add a floor plan:

1. Navigate to **VisualRF > Floor Plans** and drill down into the network and campus maps to select the building for which you want to import a new floor plan.
2. Right-click anywhere on the floor plan, then select **New Floorplan**. Or, you can select **Edit** from the toolbar on the right window pane of the Network view, then click **New Floorplan**. If an incomplete floor plan is in floor wizard mode, it will appear as a windowless floor in the building icon. Double-click that floor to open the floor in the **New Floorplan** window.
3. Click **Browse** and find the floor plan file in your hard drive.
4. If your network has multiple campuses or buildings, select the campus and building. You can also rename the floor and floor number.
5. Click **Save**. The floor plan opens in VisualRF, with planning tools on the side navigation bar.

Change Settings in VisualRF Floor Plans

You can customize your floor plans in VisualRf by changing the settings on the **VisualRF > Floor Plans > Network >Edit** page. For example, options that determine whether floor plan measurements are in meters or feet are located at the bottom of the Edit task pane. Options to change backgrounds and replace floor plans are also available from the Edit taskpane.

Figure 251: *Setting the Unit of Measurement*



○ Meters ● Feet

Editing a Floor Plan Image

There are several ways to edit a floor plan that you have uploaded, as explained in the following topics:

- "Replacing the Background" on page 372
- "Cropping the Floor Plan Image" on page 373
- "Sizing a Non-CAD Floor Plan " on page 374

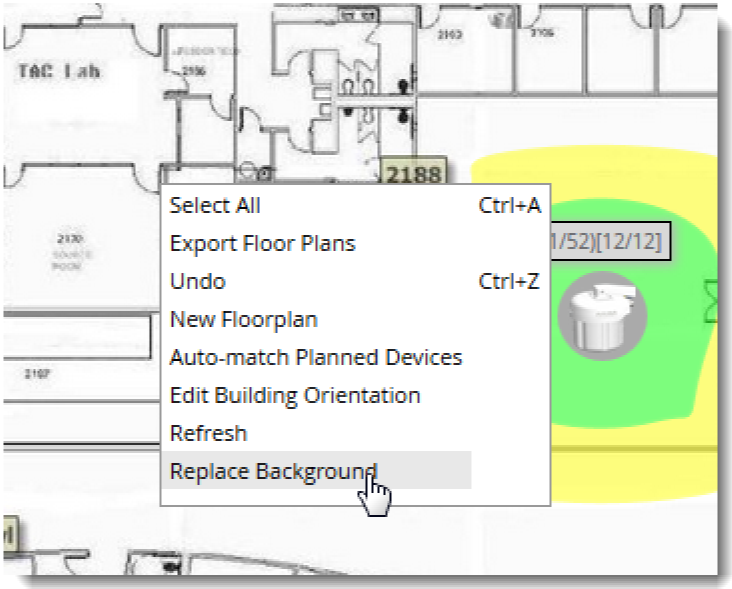
Replacing the Background

You can change your background when you update your floor plan and prefer not to delete the original floor plan and upload a new one.

To replace the background:

1. Navigate to **VisualRF > Floor Plans** and drill down into the network and campus maps to select the building floor plan you want to change.
2. Right-click anywhere on the floor plan, then select **Replace Background**.

Figure 252: *Replacing the Background*



3. Click **Browse** to find the image file in your hard drive, then click **Next**. OV3600 applies the background to the floor plan.
4. Rescale and set the dimensions for the background.
5. Click **Finish**.

Cropping the Floor Plan Image

Cropping is available from within the VisualRF Floor Upload Wizard.

1. Launch the Floor Upload wizard, as described in "Adding a Floor Plan" on page 371.
2. Use the cropping handles (circles at the corners of the image) to remove extra white space around the floor plan. VisualRF will calculate an attenuation grid for the entire map including white space. Reducing the white space on a floor plan will increase location accuracy and decrease the load an on the server. A good rule of thumb would be not more than ½ inch white space, if possible, on all sides.

VisualRF dissects each floor plan into a grid consisting of cells specified in this setting. The Core Thread service calculates the path loss for every radio to every cell on the floor plan.

By default the importation wizard allocates 2,500 grid cells to each site based on dimensions. If you have a site that is 250 ft. by 100 ft, the Floor Plan importation wizard would calculate the grid cell size at 10 feet. 250 ft. x 100 ft. = 25,000 ft. 25,000 ft. / 2,500 ft. = 10 ft.

NOTE

Decreasing the grid cell size will increase accuracy, but it also increase CPU consumption by the floor caching threads and the location caching threads. Check the **System > Performance** page to ensure your server is functioning properly when you make a change to this setting.

Other items worth noting:

- If this is a CAD file, then the Floor Plan creation wizard will automatically inherit height and width from the drawing.
- If this is a non-CAD file, then the height and width is zero.

- CAD files are converted to a JPG with a resolution of 4096 horizontal pixels at 100% quality prior to cropping. If you crop, then you will lose clarity.
- CAD files must be generated from AutoCAD and may not exceed 10 MB.
- Metric CAD files are supported.
- Importing GIF files for floor plans can result in blank VisualRF thumbnails.

Copying a Floor Plan in the Same Building

When you want to create a duplicate floor plan , simply copy an existing floor plan in the same building. To do this, use the Floor plan **Duplicate** option.

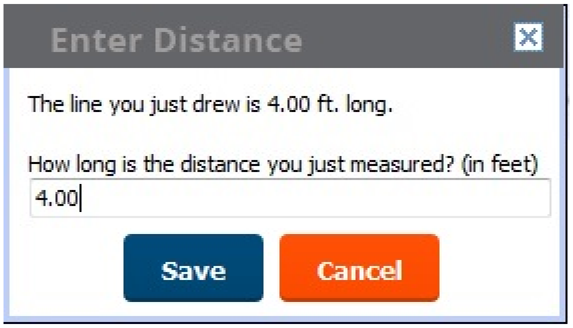
Sizing a Non-CAD Floor Plan

You should not have to resize a CAD drawing unless you see nonsensical dimensions. To resize a non-CAD image if you already know the dimensions, follow the procedures below.

To resize a Non-CAD floor plan:

1. In the **Scale** section of the floor upload wizard, click the **Measure** button. The pointer changes to a cross-hair icon.
2. Locate two points within the floor plan that you know the distance. Most door jams (door openings) are 3 feet. Use the slider bar at the upper left corner of the upload wizard to zoom in to a section of the floor plan, if necessary.
3. Select and hold to establish the first point and drag your mouse to the second point and release.
4. An **Enter Distance** dialogue box appears. Enter the proper length in feet, as shown in Figure 253.
5. Click **OK**.

Figure 253: *Manually Measuring a Floor Plan*



Enter Distance

The line you just drew is 4.00 ft. long.

How long is the distance you just measured? (in feet)

4.00

Defining Floor Plan Boundaries

Use the **Floorplan Boundary** section of the Floor Upload Wizard to refine the floor plan to remove whitespace, or to create a floorplan based on a portion of the interior of the graphic, such as an atrium.

To define a floorplan boundary:

1. Click the **Define Floorplan Boundary** button. The pointer changes to a cross-hair icon.
2. Click on the floor plan graphic to define the boundaries of the floor plan. Use the slider bar at the upper left corner of the upload wizard to zoom in to a section of the floor plan, if necessary.
3. If your floor plan has regions with different requirements than the rest of the floorplan, continue to Defining Floor Plan Regions below. Otherwise, click **Next**.

Defining Floor Plan Regions

Define regions within a floor plan that have different wireless networking requirements than the rest of the floor. For example, you can use the planning regions tool to define two small regions of high density clients within a larger floor plan with lower client density. You can define regions on a new floor plan using the Floor Upload wizard, or edit a an existing floor plan to add a new region.

Adding Region to a New Floor using the Floor Upload Wizard

You can define a floor plan region when you create a new floor plan using the Floor Upload Wizard.

1. Launch the Floor Upload wizard as described in "Adding a Floor Plan" on page 371.
1. Click the **Define Planning Regions** button. The pointer changes to a cross-hair icon.
2. (Optional) Enter a name for the region in the **Name** field.
3. Click on the floor plan graphic to define the boundaries of the region. Use the slider bar at the upper left corner of the wizard to zoom in to a section of the floor plan, if necessary.
4. Repeat steps 1-2 to create an additional regions, as required.
5. Once you have defined all necessary regions on your floor plan, click **Next** to continue to the Access Points section of the Floor Upload Wizard, as described in "Adding Planned APs onto the Floor Plan" on page 378 and "Adding Deployed Access Points onto the Floor Plan" on page 377.

Adding a Region to an Existing Floor Plan

To add a region to an existing floor:

1. Select the floor to which you want to add a region.
2. Click **Edit** in the navigation bar to open the Edit menu.
3. Click **Draw Region**. The pointer changes to a cross-hair icon.
4. Click on the floor plan graphic to define the edge of the new region. Use the slider bar at the upper left corner of the wizard to zoom in to a section of the floor plan, if necessary.
5. Once the floor plan region is defined, select the region and click the **Properties** menu. The **Name** field shows the current name for that region. You can rename a region by entering a new name into this field.
6. Click **Type** to specify a region type .
   - **Boundary**: This option creates a region that defines the boundaries of an area.
   - **Planning**: This option creates a region to plan for new access points, and define transmit power and PHY types for AP radios.
   - **Probability**: Define the location probability for the region. Location probability regions are optional regions that can be used to increase the accuracy of device location. VisualRF can calculate device locations based on probability, and use this information to place the device into regions where they are more likely to be located, like conference rooms and cubical farms, or pull users out of regions where they are less likely to be, like parking lots and courtyards.
   - **AirPlay/AirPrint**: Reserved for future use.
7. Click **Save** to save your region.

Table 164: *Fields in the Region Properties Window*

Planning Region Type	
AP Type	The type of AP used in this planning region.
Count	Number of APs of the selected type to provision onto the selected region.

Table 164: *Fields in the Region Properties Window (Continued)*

Phy	Whether they PHY is set to 11n or no radio.
Tx Power	Transmit power of the AP radio, in dBm.
Gain	This read-only parameter displays the AP antenna gain in dBi.
Planned Air Monitors	Enter the number of Air Monitors to be deployed in this region
Environment	A range from 1-4 that best describes whether the environment is related to an office space, cubicles, offices, or concrete.
Probability / Location Probability Region Type	
Probability	Click and drag this slider to specify if users are likely to be in this region. A location probability of **Very Low** will decrease the probability of a device being placed in that region by 20%. **Very High** will increase the probability of a device being placed in that region by 20%.

Editing a Planning Region

You can edit a region by right-clicking within the region to see the following options:

- **Select All** - Selects all regions on the floorplan.
- **Draw Walls Around Region** - This action surrounds the region with walls of the last used wall type (concrete, cubicle, drywall or glass). For information on defining different wall types, see Adding Exterior Walls.
- **Bring to Back**, **Send to Front** - If one region is within the boundaries of another region, or two regions overlap, you may not be able to select the desired region until that region is brought to the front, or the overlapping region is sent to the back.
- **Delete Planned Devices** - Deletes all planned APs within the region.
- **Remove** - Delete the region. Any planned devices within the region will stay on the floor plan.

Floor Plan Properties

You can edit an existing floor plan by changing the floor plan properties described in Table 165. To access the **Properties** menu:

1. Navigate to **VisualRF> Floor Plans**.
2. Open the floor plan in Network view.
3. Click the **Properties** link to open the **Properties** menu.

Table 165: *Floor Plan Properties*

Setting	Default	Description
Floor Name	Floor [Number]	A descriptive name for the floor. It inherits the floor number as a name if nothing is entered.
Floor Number	0.0	The floor number. You can enter negative numbers for basements. **NOTE:** Each floor plan within a building must have a unique floor number.

Table 165: *Floor Plan Properties (Continued)*

Setting	Default	Description
Width Height	N/A	These fields display the current width and height of the floor plan. To change these settings, click the **Measure** icon and measure a portion of the floor. For details, see Sizing a Non-CAD Floor Plan .
Gridsize	5 x 5 feet	Decreasing the grid size will enable the location to place clients in a small grid which will increase accuracy.
Advanced		
Client TX	30mW	Client transmit power, used in auto placement of access points onto floors within this campus. The range is 30mW to 100mW.
Speed	200 Mbps	The data transmission speed used in auto placement of access points onto floors within this campus. The range is 6 Mbps to 1.3 Gbps.
Ceiling Height	10	Specifies the height from the floor to the ceiling. This will default to the ceiling height for the building, but you can override here if needed for atria or basements.
Ceiling Attenuation	20	Specifies the attenuation characteristics in dB of the ceiling or the floor above. For details on defining attenuation values, see Wall Attenuation Settings.

Adding Deployed Access Points onto the Floor Plan

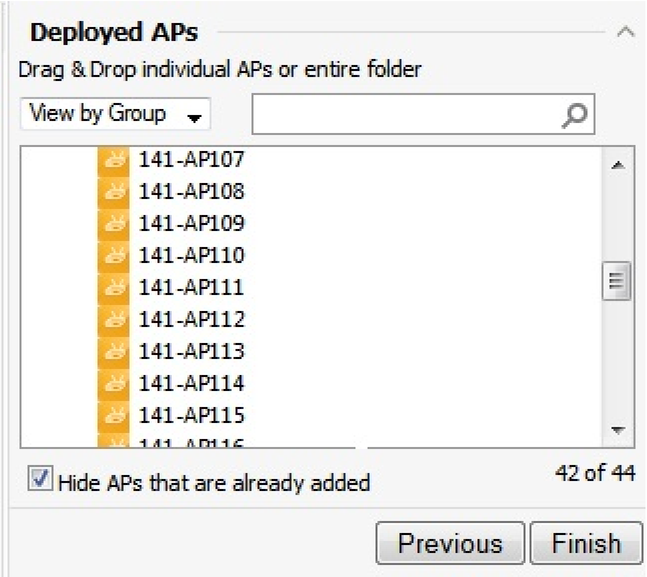
You can provision existing APs in your network onto a new floor plan using the Floor Upload wizard, or edit an existing floor plan to add new APs using the **Properties** menu for that floor.

NOTE

OV3600 recalculates path loss and client locations after adding a deployed AP. All changes may not be visible on a refresh until this process complete.

1. Determine if you want to add APs to a new floor plan, or an existing floor plan.
   - To add APs to a new floor plan using the Floor Upload wizard, click **Access Points** in the wizard navigation bar, then select **Add deployed APs**.
   - To add APs an existing floor plan, select that floor plan, click the **Edit** menu in the navigation bar, then click the **Add Deployed AP** icon
2. A list of devices in your OV3600 appears, as shown in Figure 254.
3. Select whether to view APs by **Group** or by **Folder**. You can also use the **Search** field to identify APs to add to the floor.
4. Expand the Group or Folder containing the access points which need to be provisioned on this floor plan. Note that by default, devices that have already been added to VisualRF are hidden. To show them, clear the **Hide Devices already added to VisualRF** check box at the bottom of the list.
5. Click and drag an AP (or a Group or Folder of APs) to its proper location on the floor.
6. If you are adding APs to a floor using the Floor Upload wizard, click the **Finish** button. Otherwise:
   - Remove a device from the floor plan by right-clicking that device then clicking **Remove.**
   - Return to an earlier section of the Floor Upload wizard by clicking **Previous**.
   - Add existing devices to the floor plan. See "Adding Deployed Access Points onto the Floor Plan" on page 377.

Figure 254: *List of Deployed APs*



Deployed APs

Drag & Drop individual APs or entire folder

View by Group

141-AP107
141-AP108
141-AP109
141-AP110
141-AP111
141-AP112
141-AP113
141-AP114
141-AP115

☑ Hide APs that are already added

42 of 44

Adding Planned APs onto the Floor Plan

You can plan for and provision new APs onto a new floor plan using the Floor Upload wizard, or add new APs to an existing floor plan using the **Properties** menu for that floor.

1. Determine if you want to plan for APs on a new floor using the Floor Upload wizard, or plan for APs on an existing floor plan.
   - To add APs to a new floor plan using the Floor Upload Wizard, click **Access Points** in the wizard navigation bar, then select **Plan APs**.
   - To add APs to an existing floor plan, open the selected floor plan, then click **Edit** menu in the navigation bar.
2. Click the **Type** drop-down list and select a device type from the list of available devices.
3. In the **Count** field, enter the number of devices of that type to add to the new floor.
4. (Optional) Click and drag the **Deployment Type** slider bar to adjust data rates for a high-density or low-density environment.
5. (Optional) Click the **Advanced** link and configure the advanced deployment options
   - **Service level**: Select **Speed** or **Signal** to plan coverage by adjusting data rate requirements (Speed) or AP signal strength settings. Click **Calculate AP** count to recalculate the suggested number of APs based on these advanced settings.
   - **Client Density**: In the **Max Clients** field, set the anticipated number of clients that will be stationed in the floor. in the **Clients per AP** field, enter the maximum number of clients supported by each radio. Click **Calculate AP** count to recalculate the suggested number of APs based on these advanced settings.
6. Click **Add APs to Floorplan**.
7. Click and drag the device, to the desired location.
8. If you are done creating the floor plan, click the **Finish** button. Otherwise:
   - Remove a planned device from the floor plan by right-click that device then clicking **Remove.**
   - Return to an earlier section of the Floor Upload wizard by clicking **Previous**.
   - Add existing devices to the floor plan. See "Adding Deployed Access Points onto the Floor Plan" on page 377

Auto-Matching Planned Devices

You can right-click a floor plan or campus, building, or network icon and select the **Auto-Match Planned Devices** option to efficiently match planned APs to managed APs. If you select this option for a campus, then all planned APs in that campus are checked. If used on a building, then all the APs in that building are checked. If used on a floor, then all APs on that floor are checked.

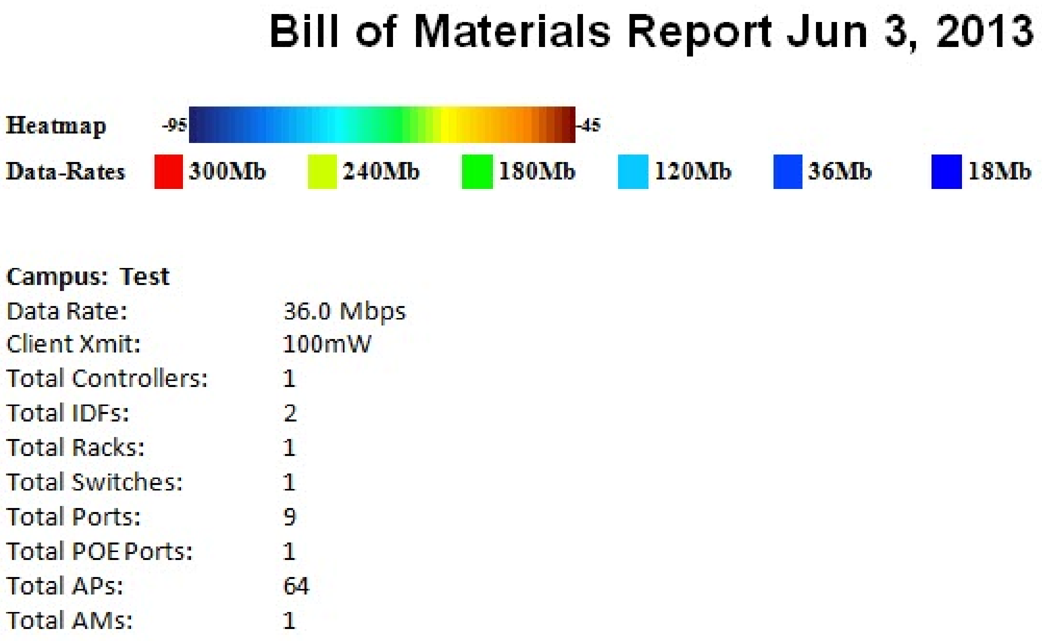
Planned devices first attempt to auto-match on MAC address, and then by name. The VisualRF MAC address checks against all of the LAN MAC addresses of a deployed AP.

Printing a Bill of Materials Report

You can generate a Bill of Materials (BOM) Report from within VisualRF in Word format. Follow these steps:

1. Navigate back to the Network view.
2. Right-click a campus icon, a building icon, or a builiding floor and select **Show Bill of Materials**. A generating report pop up appears.
3. Select options such as heatmap, speed, sensor coverage, wired range, and summary.
4. Select **OK**. A BOM report appears in Microsoft Word as illustrated in Figure 255:

Figure 255: *Bill of Materials Report Illustration*



Bill of Materials Report Jun 3, 2013

Campus: Test	
Data Rate:	36.0 Mbps
Client Xmit:	100mW
Total Controllers:	1
Total IDFs:	2
Total Racks:	1
Total Switches:	1
Total Ports:	9
Total POE Ports:	1
Total APs:	64
Total AMs:	1

Increasing Location Accuracy

The Location Service will use all RF information available to increase location accuracy of clients, tags, and rogue devices. Understanding your infrastructure's inherent capabilities helps you learn the extra effort required to ensure location accuracy.

There are three key elements read from controllers or access points that increase location accuracy:

- Signal strength of a client as heard by the AP of association
- Signal strength of a client as heard by APs other than the AP of association
- Signal strength at which an AP hears other APs.

These factors are detailed further in Table 166:

Table 166: *Elements Read From Controllers to Increase Location Accuracy*

MFG/Model	Client Signal Associated AP	AP-to-AP Signals (Dynamic Attenuation)	Unassociated Client Signal	Rogue AP Signal
Alcatel-Lucent	Yes	Yes	Yes	Yes
Cisco LWAPP	Yes	Yes	Yes	Yes
Cisco IOS	Yes	No	No	With WLSE
Cisco VxWorks	Yes	No	No	No
Trapeze	Yes	No	No	Yes
Meru	No	No	No	Yes
Proxim	Yes	Yes	Yes	Yes
Symbol Auton. AP	Yes	No	No	Yes
Symbol Thin AP	Yes	No	Yes	Yes
Proxim AP-2000	Yes	No	Yes	Yes
Proxim AP-4000	Yes	Yes	Yes	Yes
ProCurve WeSM	Yes	Yes	No	Yes
ProCurve 530	Yes	Yes	Yes	Yes
ProCurve 420	Yes	Yes	No	Yes

OV3600 provides four main methods to increase accuracy once your access points are deployed:

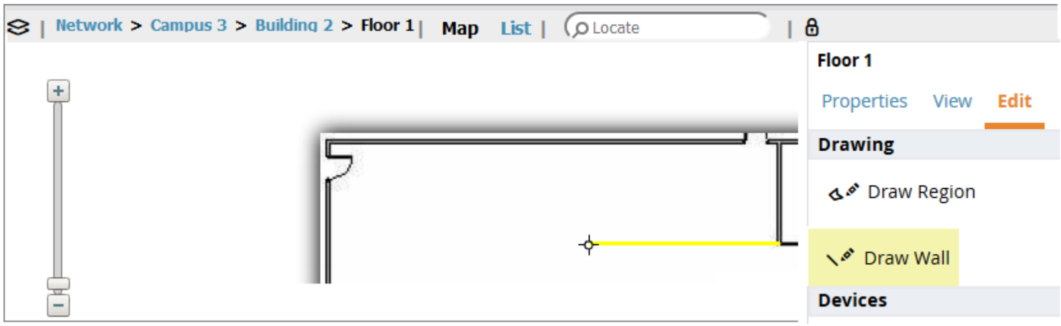
- Adding Exterior Walls - increases location accuracy by reducing the statistical probability of placements outside the office confines. See "Adding Exterior Walls" on page 380.
- Remote Client Surveys - provides additional attenuation inputs for corners and low-coverage areas without the burden of actually carrying a laptop to the physical location. See "" on page 1.
- Location Probability Regions - Probability regions will increase or decrease the chances of a device being located within the region. See Defining Floor Plan Regions.

Adding Exterior Walls

Because VisualRF utilizes much existing RF information, generally only external walls are required for accurate client locations. The VisualRF Dynamic Attenuation feature uses AP-to-AP information to calculate attenuation for interior areas, negating the need to enter interior walls. If your devices support AP-to-AP information in the table above, you should only draw exterior walls.

1. Navigate to **VisualRF>Floor Plans** and select a floor plan.
2. Select the **Draw Wall** button in the **Edit** menu.
3. The cursor changes to a crosshair icon, indicating that the view is in wall editing mode. Use this cursor to draw the wall directly over the floor plan, as shown in Figure 256.

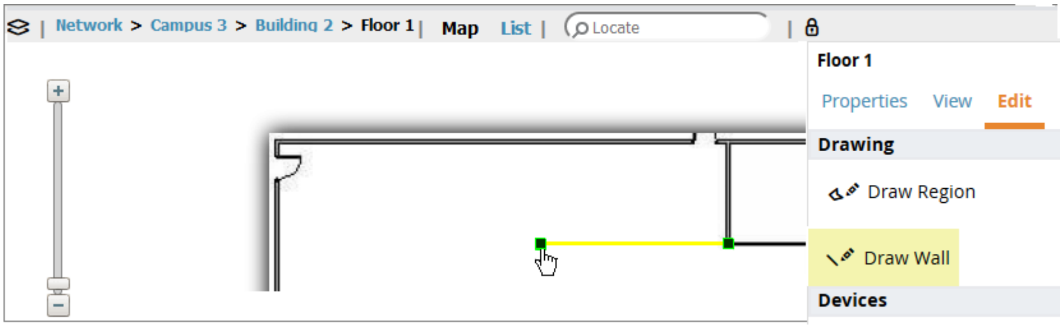
Figure 256: *Drawing a wall*



4. (Optional) Change the attenuation of a wall by selecting the appropriate building material for that wall.To define the wall material , select the wall, click the **Properties** tab, then select the building material type from the **Material** drop-down list.
5. When you are done creating walls, click the **Draw Wall** button again to exit the wall editing mode.

You can edit or remove a wall at any time. To move or resize the wall, select the **Draw Walls** button in the Edit menu again. The cursor changes to a hand, and the ends of the wall is highlighted. Click and drag the end point handles to change the wall, as shown in Figure 257.

Figure 257: *Moving and resizing an existing wall*



To delete a wall, select the wall and press the **Delete** key. You can also right-click on a wall and select **Delete** from the pop up menu.

NOTE

Best practices is to draw only outside walls. If you are seeing inaccurate client locations or heat maps after entering exterior walls, proceed to Client Surveys. If you still experience problems, then consider adding interior walls.

Fine-Tuning Location Service in VisualRF > Setup

There are several options on the **VisualRF > Setup** page which increase client location accuracy. All of these items will increase the processing requirements for the location service and could negatively impact the overall performance of OV3600.

Decreasing Grid Size

Decreasing the grid size will enable the location to place clients in a small grid, which will increase accuracy. Select the floor plan, click the Properties menu, then click the **Gridsize** drop-down list.

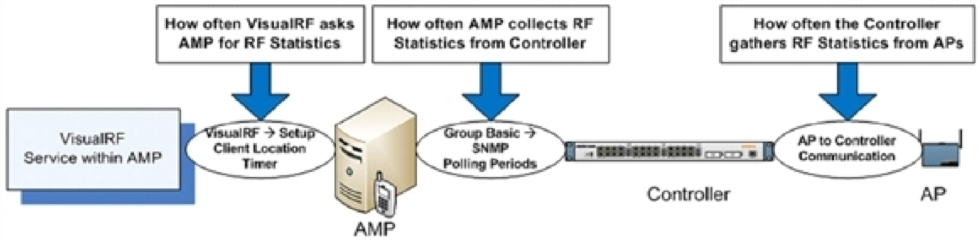
Enabling Dynamic Attenuation

The dynamic attenuation feature (which is enabled by default) instructs the location service to sample the current RF environment and to dynamically adjust Path Loss. This feature can be enabled or disable in the **VisualRF>Setup** page.

Configuring Infrastructure

Fine-tune location services to ensure that the hardware is configured to retrieve the RF information, and that it provides this information on a timely basis. There are three unique timing mechanisms which impact location accuracy: how often the infrastructure collects and correlates RF statistics in their MIB, how often OV3600 queries those MIB entries, and how often VisualRF service queries OV3600 for this RF information.

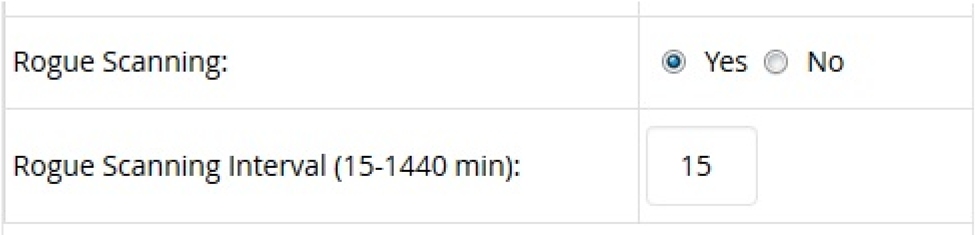
Figure 258: *Timing Factors Impacting Location Accuracy*


How often VisualRF asks AMP for RF Statistics
How often AMP collects RF Statistics from Controller
How often the Controller gathers RF Statistics from APs
VisualRF Service within AMP
VisualRF → Setup Client Location Timer
Group Basic → SNMP Polling Periods
AP to Controller Communication
AMP
Controller
AP

These best practices are recommended when configuring hardware infrastructure:

- For legacy autonomous APs, ensure on the **Group > Radio** page that **Rogue Scanning** is enabled and the interval is accurate, as shown in Figure 259:

Figure 259: *Group Rogue Scanning Configuration*



Rogue Scanning:	● Yes ○ No
Rogue Scanning Interval (15-1440 min):	15

- For thin APs, ensure that the controllers are configured to gather RF information from the thin APs frequently.
- For Cisco LWAPP, navigate to **Groups > Cisco WLC Config** page in OV3600. Navigate the tree control to the **Wireless** section, and for each PHY navigate to **RRM > General** section. Review the values in the **Monitor Intervals** section. These should be configured to a recommended setting of **180** for better accuracy.

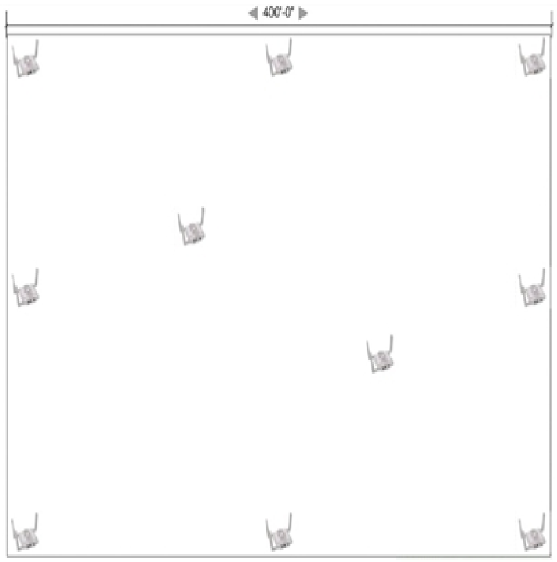
Deploying APs for Client Location Accuracy

Deploying access points for client location accuracy can be different than deploying access points for capacity. Follow these guidelines for best results:

- Ensure that at least 3 radios can hear each client devices at -85 dBm or below
- Ensure that you deploy an access point approximately every 3,500 square feet.
- For square or rectangular floor plans ensure access points are deployed on the exterior walls of each floor with access points in the middle as well.

Refer to Figure 260 for an example.

Figure 260: *Rectangular Floor Plan AP Deployment*



Using VisualRF to Assess RF Environments

VisualRF has four distinct views or entry points: client view, access point view, floor plan view, and network, campus, and building view.

This section contains the following corresponding topics:

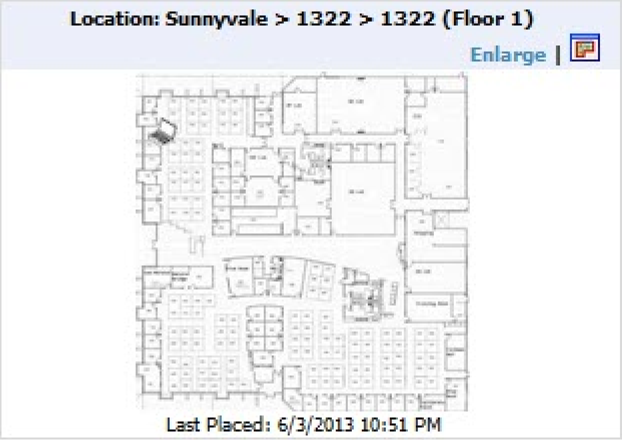
- "Viewing a Wireless User's RF Environment" on page 383
- "Viewing an AP's Wireless RF Environment" on page 385
- "Viewing a Floor Plan's RF Environment" on page 386
- "Viewing a Network, Campus, Building's RF Environment " on page 387
- "Viewing Campuses, Buildings, or Floors from a List View" on page 387

Viewing a Wireless User's RF Environment

You can use Visual RF to view information about a user's RF environment.

1. from the **Clients > Client Detail** page for the client whose RF environment you want to view, select the VisualRF thumbnail, located next to the **Current Association** section at the bottom of the of this page (as shown in Figure 261):

Figure 261: *VisualRF thumbnail in Clients > Client Detail*



Location: Sunnyvale > 1322 > 1322 (Floor 1)

Last Placed: 6/3/2013 10:51 PM

This view is focused on the wireless user enabling you quick resolution of a user's issues and therefore disables most RF objects by default.

- Users - only the user in focus is displayed
- APs - only the access point in which the focus client is associated with is displayed
- Radios - the heatmap represents only the radio to which the client in focus is associated
- Rogues - all rogues are off
- Client/Rogue Surveys - all surveys are off
- Walls - all walls are displayed
- Lines - client to AP of association
- Labels - all labels are disabled

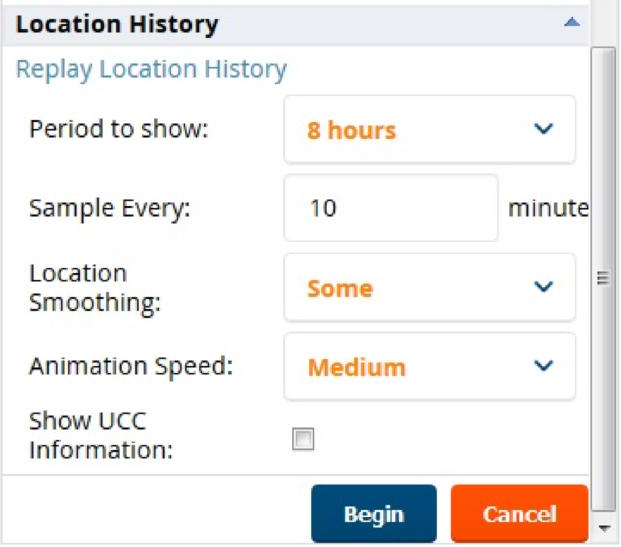
Tracking Location History

The VisualRF Location History tracker can display the location history for the selected user by indicating on the floor plan the locations to which that user traveled over the selected time period.

1. To view location tracking, select a client icon in the floor plan, click the **View** link in the right navigation pane, then select **Replay Location History**.
2. Select the period of time over which you want to track that client's movements, and the optionally, the frequency of sample times. Longer sample times will impact animation speeds, and location smoothing. When the animation smoothing feature is turned off or set to a lower value, the tracking history displays smaller client movements. When the smoothing value is set to higher values, these small movements are not displayed, and only larger location movements are animated.

The location history settings, illustrated in Figure 262, appears at the bottom of the VisualRF window.

Figure 262: *Location History Player*



Location History

Replay Location History

Period to show: 8 hours

Sample Every: 10 minute

Location Smoothing: Some

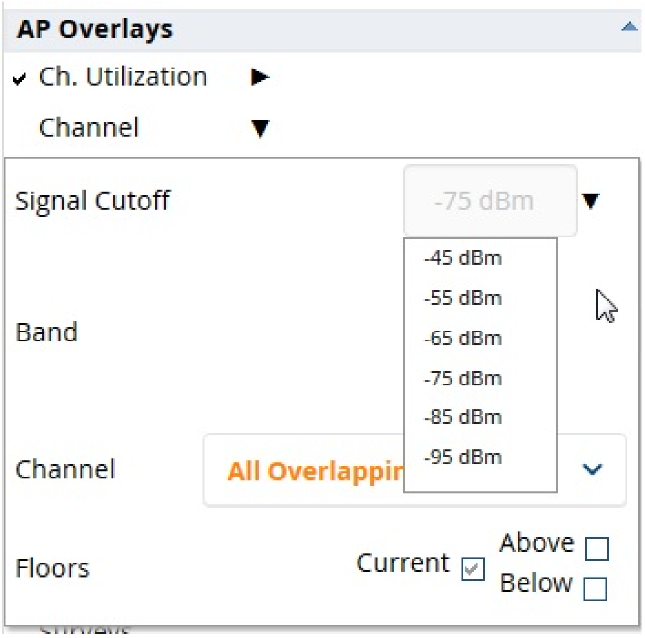
Animation Speed: Medium

Show UCC Information: □

Checking Signal Strength to Client Location

1. Open a floor plan in the **VisualRF > Floor Plans** page.
2. Click the **View** tab.
3. In the **AP Overlays** section of this tab, select the **Channel** option.
4. Click the **Signal Cutoff** drop-down list.
5. Select the desired signal level to display, as shown in Figure 263. The heatmap updates immediately.

Figure 263: *Signal Cutoff dBm Dropdown Menu*



AP Overlays

✓ Ch. Utilization ▶

Channel ▼

Signal Cutoff -75 dBm ▼

-45 dBm
-55 dBm
-65 dBm
-75 dBm
-85 dBm
-95 dBm

Band

Channel All Overlappir

Floors Current ☑ Above □ Below □

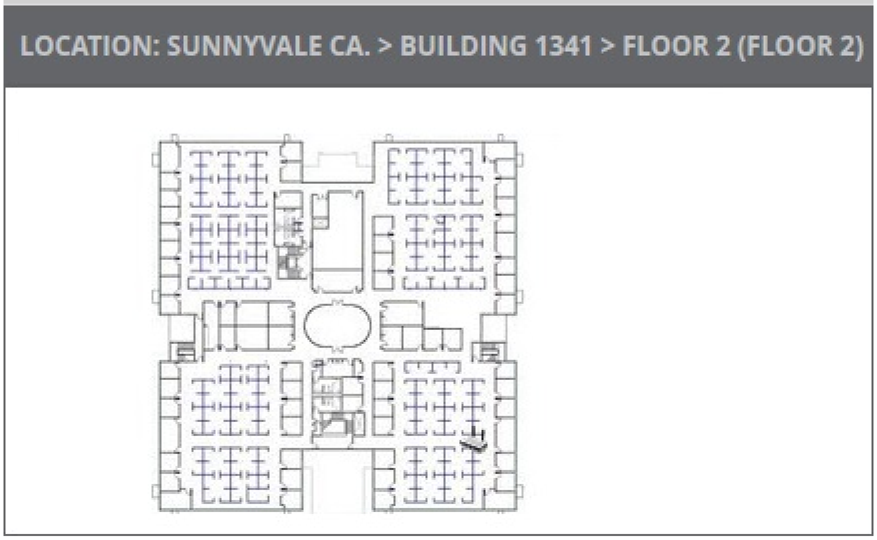
Viewing an AP's Wireless RF Environment

To view an access point's RF environment from **Devices > Monitor** page:

1. Select a device of interest from **Devices > List**, or any other OV3600 page that lists your APs. The **Devices > Monitor** page opens.

2. If the AP is associated with a floor plan, the page displays a VisualRF thumbnail showing the location of the AP. Click this thumbnail to open the floor plan in VisualRF.

Figure 264: *VisualRF Thumbnail on the* ***Devices > Monitor*** *page*

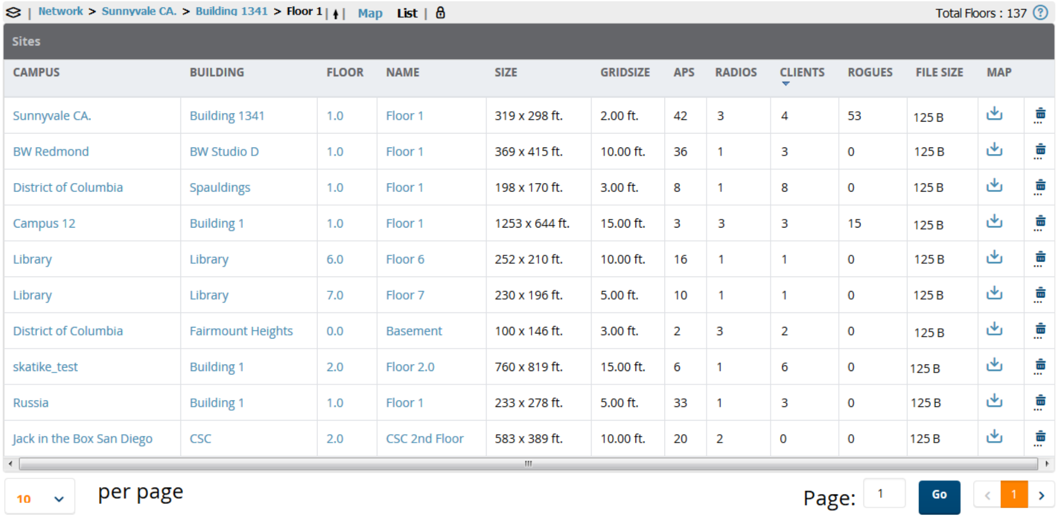


LOCATION: SUNNYVALE CA. > BUILDING 1341 > FLOOR 2 (FLOOR 2)

Viewing a Floor Plan’s RF Environment

To view a floor plan's RF environment, navigate to the **VisualRF > Floor Plans** page. Click the **List** link at the top right of the **Floor Plans** page to view a sortable, clickable list that allows you to select and instantly view any campus, building or floor in the network.

Figure 265: *Floor Plans List View*



| Network > Sunnyvale CA. > Building 1341 > Floor 1 | ⬆ | Map List | 🔒 Total Floors : 137 ?

Sites

CAMPUS	BUILDING	FLOOR	NAME	SIZE	GRIDSIZE	APS	RADIOS	CLIENTS	ROGUES	FILE SIZE	MAP	
Sunnyvale CA.	Building 1341	1.0	Floor 1	319 x 298 ft.	2.00 ft.	42	3	4	53	125 B	⤓	🗑
BW Redmond	BW Studio D	1.0	Floor 1	369 x 415 ft.	10.00 ft.	36	1	3	0	125 B	⤓	🗑
District of Columbia	Spauldings	1.0	Floor 1	198 x 170 ft.	3.00 ft.	8	1	8	0	125 B	⤓	🗑
Campus 12	Building 1	1.0	Floor 1	1253 x 644 ft.	15.00 ft.	3	3	3	15	125 B	⤓	🗑
Library	Library	6.0	Floor 6	252 x 210 ft.	10.00 ft.	16	1	1	0	125 B	⤓	🗑
Library	Library	7.0	Floor 7	230 x 196 ft.	5.00 ft.	10	1	1	0	125 B	⤓	🗑
District of Columbia	Fairmount Heights	0.0	Basement	100 x 146 ft.	3.00 ft.	2	3	2	0	125 B	⤓	🗑
skatike_test	Building 1	2.0	Floor 2.0	760 x 819 ft.	15.00 ft.	6	1	6	0	125 B	⤓	🗑
Russia	Building 1	1.0	Floor 1	233 x 278 ft.	5.00 ft.	33	1	3	0	125 B	⤓	🗑
Jack in the Box San Diego	CSC	2.0	CSC 2nd Floor	583 x 389 ft.	10.00 ft.	20	2	0	0	125 B	⤓	🗑

10 per page Page: 1 Go ‹ 1 ›

The **VisualRF > Floor Plans** page provides a snapshot of how VisualRF is performing, as described in Table 167:

Table 167: *Floor Plans list columns*

Field	Description
Campus	Campus associated to the floor.

Table 167: *Floor Plans list columns (Continued)*

Field	Description
Building	Building associated to the floor.
Floor	Floor number. The decimal place can be used for mezzanine levels.
Name	Optional name of a floor. (If the name is not changed, it displays the name as Floor [Number] by default.)
Size	The height and width in feet of the floor plan, including white space.
Grid Cell Size	The size of the grid cells, in feet.
APs	The number of access points on the floor.
Radios	The number of radios associated with access points on the floor.
Clients	The number of wireless clients associated with access points on the floor. **NOTE:** Locating clients consumes significant VisualRF resources. A floor with hundreds or thousands of clients can take a long time to process.
Rogues	The number of rogue devices heard by access points on the floor. This number reflects the filters configured on the **VisualRF > Setup**. This means that while APs on the floor might hear more rogue devices, they are being filtered because of weak signal, they haven't been heard recently, or they are ad-hoc.
File Size	The floor plan background or image reported, in kilobytes. The larger the file, the longer it will take to render in the canvas.
Original Floor Plan	A link to download the original image background file.

Viewing a Network, Campus, Building's RF Environment

To view floors from a geographical perspective:

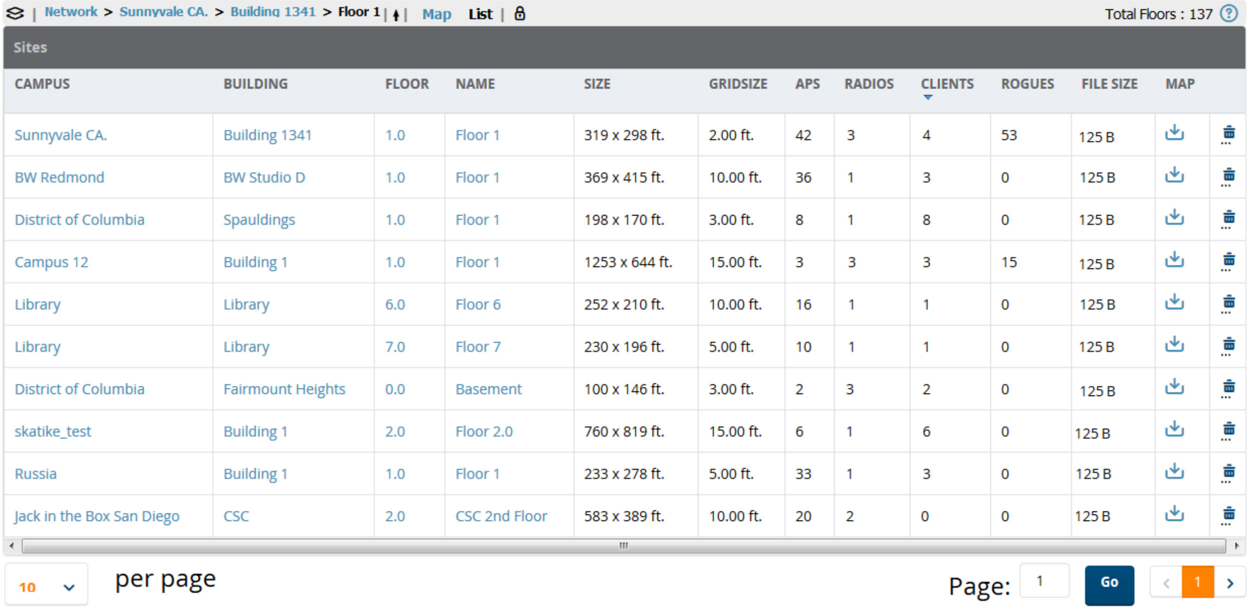
1. Navigate to the **VisualRF > Floor Plans** page.
2. Click on each network, campus, or building successively to drill down further until you reach the floor plan. This navigation provides information in each view as follows:
   - Network View - Contains all campuses within your WLAN
   - Campus View - All buildings within a campus
   - Building View - All floors within a building
   - Floor Plan View - All regions, wiring closets, Wi-Fi tags within the floor

Viewing Campuses, Buildings, or Floors from a List View

The WebUI supports a List View that displays a sortable, clickable list that allows you to select and instantly view any campus, building or floor in the network:

1. Navigate to the **VisualRF > Floor Plans** page.
2. Click the **List** link at the top right of any view. The **Network List View** window, shown in Figure 266, appears on the screen. If a floor is in floor upload wizard mode, it appears in the list with an asterisk (*) by the floor name.

Figure 266: *Network List View*



| Network > Sunnyvale CA. > Building 1341 > Floor 1 | Map List | Total Floors : 137

Sites

CAMPUS	BUILDING	FLOOR	NAME	SIZE	GRIDSIZE	APS	RADIOS	CLIENTS	ROGUES	FILE SIZE	MAP	
Sunnyvale CA.	Building 1341	1.0	Floor 1	319 x 298 ft.	2.00 ft.	42	3	4	53	125 B	⤓	🗑
BW Redmond	BW Studio D	1.0	Floor 1	369 x 415 ft.	10.00 ft.	36	1	3	0	125 B	⤓	🗑
District of Columbia	Spauldings	1.0	Floor 1	198 x 170 ft.	3.00 ft.	8	1	8	0	125 B	⤓	🗑
Campus 12	Building 1	1.0	Floor 1	1253 x 644 ft.	15.00 ft.	3	3	3	15	125 B	⤓	🗑
Library	Library	6.0	Floor 6	252 x 210 ft.	10.00 ft.	16	1	1	0	125 B	⤓	🗑
Library	Library	7.0	Floor 7	230 x 196 ft.	5.00 ft.	10	1	1	0	125 B	⤓	🗑
District of Columbia	Fairmount Heights	0.0	Basement	100 x 146 ft.	3.00 ft.	2	3	2	0	125 B	⤓	🗑
skatike_test	Building 1	2.0	Floor 2.0	760 x 819 ft.	15.00 ft.	6	1	6	0	125 B	⤓	🗑
Russia	Building 1	1.0	Floor 1	233 x 278 ft.	5.00 ft.	33	1	3	0	125 B	⤓	🗑
Jack in the Box San Diego	CSC	2.0	CSC 2nd Floor	583 x 389 ft.	10.00 ft.	20	2	0	0	125 B	⤓	🗑

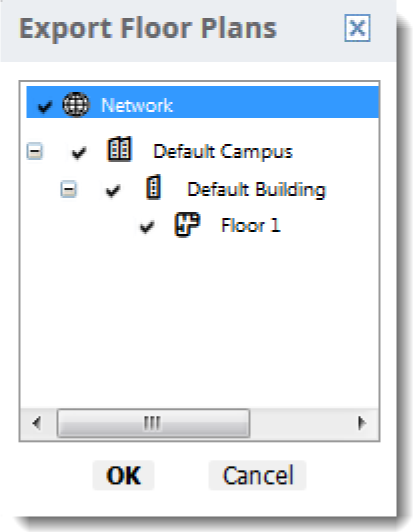
3. Click any of the links to view that location, or click a column heading to sort the list by that column criteria. The **Original Floor Plan** column contains links to download the floor plan graphic for the selected floor.
4. To return to the Map view, click the **Map** link at the top right of the page.

Importing and Exporting in VisualRF

You can export a floor plan from a building view, or an individual floor plan view, and import the file later into another OV3600 server.

To export a floor plan:

1. Navigate through the Network view and select the campus, building or floor that you want to view. Or you can work from the List view and click the blue **Building**, **Floor**, or **Name** links to make your selections.
2. Right-click to choose **Export Floor Plans** from the shortcut menu.
3. Select a campus, building, or floor to export, then click **OK**.



4. Select **Save File** to save the **backup.zip** file to your local hard drive.

5. Click **OK**.

At this point, you can deploy a production OV3600 and manage devices by importing your exported floor plan. For more information, see "Adding a Floor Plan" on page 371.

Importing from CAD

The Floor Plan Upload Wizard (FUW) should inherit all pertinent information from your CAD file if you follow this procedure:

1. Determine UNITS - all modern CAD versions (2001 and newer) support UNITS
2. Determine MEASURE - Legacy CAD versions (2000 and older) used a Imperial or Metric system.
   - If UNITS are 0 or undefined, then the standard dictates defaulting to MEASURE value
   - If MEASURE is 0 or undefined, then the standard dictates defaulting to English and inches
3. Find MODEL VIEW - If the drawing contains multiple views the FUW will default to the Model view
4. Determine Bounding Box - FUW will encompass all lines and symbols on the drawing and create a bounding box which is generally smaller than entire drawing. It is based on the UNITS or MEASUREMENT above.
5. Convert to JPG - FUW will convert the bounding box area to a JPG file with a resolution of 4096 horizontal pixels at 100% quality.
6. Start WebUI of FUW Step #1 - This is the cropping step.

This and all subsequent steps use the converted JPG file. The greater the floor plan dimensions, the less clarity the background image provides.

Batch Importing CAD Files

This process provides the ability to automatically upload many CAD files and auto provision existing walls and access points, and contains the following topics:

- "Requirements" on page 389
- "Pre Processing Steps" on page 389
- "Upload Processing Steps" on page 390
- "Post Processing Steps" on page 390
- "Sample Upload Instruction XML File" on page 390
- "Common Importation Problems" on page 391

Requirements

- Operating System: Client machine must be Windows XP, Windows Vista, or Windows 7
- Flash: Version 9 or later

Pre Processing Steps

1. Increase Memory Allocation in **VisualRF > Setup** as follows:
   - 25 floors or less - 512 MB
   - 25 to 75 floors - 1 GB
   - More than 75 floors - 1.5 GB
2. Massage the output data.
3. Increase the **Location Caching Timer** to 1 hour so that VisualRF does not overload the server calculating client locations while calculating path loss and process floor plan images.

Upload Processing Steps

1. Create CAD XML files which contain drawing filename, dimensions and optional information like device manufacture and model, device coordinates, wall coordinates and building material. This step is usually performed by your facilities or CAD department. The output of AutoCAD will not be properly formed XML, so you may need to massage the output data.
2. Copy all CAD drawings and corresponding XML files into a single directory on Windows machine. All files must be in a single directory.
3. Compress all files into a single *.zip file.
4. Open your browser and navigate to your OV3600 : https://<OV3600_NAME>/visualrf/site_batch.
5. Select **Browse** to launch the File Explorer Window.
6. Select the zip file containing the upload instructions and click the **Open** button. The **File Explorer** Window will disappear you will return to the **Batch Floor Upload Wizard**.
7. Select **Next**.
8. The application validates the following information
   - Well-formed XML
   - All drawing files are accessible
   - All APs are present
   - All Building and Campuses are present
9. If there are any errors, none of the floor plans are created.

Post Processing Steps

1. Decrease the Location Caching Timer to previous value.
2. Review the **VisualRF > Floor Plans** page to ensure server is keeping up.

Sample Upload Instruction XML File

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<visualrf:site_batch xmlns:visualrf="http://www.ov3600.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1" origin="lower-left">
        <floor name="1st Floor" number="43" building-name="Library" campus-name="University">
                <image filename="blueprint1.dwg"/>
                <access-points>
                        <access-point name="ART.1.1" x="190.26" y="222.31"/>
                        <access-point name="ART.1.2" x="136.12" y="208.60"/>
                        <access-point name="ART.1.3" x="75.02" y="221.47"/>
                        <access-point name="ART.1.4" x="73.41" y="132.48"/>
                        <access-point name="ART.1.9" x="196.67" y="98.34"/>
                        <access-point name="ART.1.8" x="179.07" y="55.97"/>
                        <access-point name="ART.1.7" x="119.64" y="56.12"/>
                        <access-point name="ART.1.6" x="74.53" y="56.36"/>
                        <access-point name="ART.1.5" x="59.18" y="38.01"/>
                </access-points>
        </floor>
        <floor name="2nd Floor" number="44" building-name="Library" campus-name="University">
                <image filename="blueprint2.dwg"/>
                <access-points>
                        <access-point name="ART.2.12" x="196.31" y="92.19"/>
                        <access-point name="ART.2.11" x="204.82" y="55.78"/>
                        <access-point name="ART.2.10" x="133.08" y="55.81"/>
                        <access-point name="ART.2.9" x="73.79" y="55.78"/>
                        <access-point name="ART.2.8" x="73.72" y="104.26"/>
                        <access-point name="ART.2.7" x="73.91" y="134.88"/>
                        <access-point name="ART.2.6" x="73.83" y="162.72"/>
                        <access-point name="ART.2.5" x="73.82" y="183.61"/>
                        <access-point name="ART.2.4" x="63.74" y="125.48"/>
                </access-points>
        </floor>
</visualrf:site_batch>
```

Common Importation Problems

- Improper or undefined UNITS or MEASURE
- Text embedded into the Model view which causes an inconsistent bounding box
- Large dimensions which cause grainy resolution upon zoom
- Legacy CAD versions prior to Release 15 or AutoCAD 2000.

Importing from an Alcatel-Lucent Controller

The instructions below will enable you to seamlessly migrate all building, campus, and floor plan information previously entered into an Alcatel-Lucent controller.

Pre-Conversion Checklist

Prior to importing floor plans, ensure that the VisualRF memory allocation is sufficient for the anticipated number of floor 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 OV3600 server. VisualRF 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.

Process on Controller

1. On the controller's WebUI , navigate to the **Plan > Building List** page.
2. Select the buildings to be exported and select **Export**.
3. When the dialog box appears, make sure that you have included all images and select **Save to a file**.

Process on OV3600

1. Navigate to **VisualRF > Import**.
2. Select the **Import floor plans from an Aruba/Alcatel-Lucent Controller** link.
3. Select the **Begin Importing Floor Plans** link.
4. When prompted for input file, use the file saved from the controller process.

VisualRF Location APIs

VisualRF provides the following location APIs:

Site Inventory: **`https://[ov3600_host]/visualrf/site.xml?site_id=...`**

- You can find the site_id from the Floor Plan List query defined on the XML API page
- This interface provides floor details including access points, walls, regions, surveys, etc.
- The corresponding example XML and schema are attached in visualrf_site_inventory.*

Device Location: **`https://[ov3600_host]/visualrf/location.xml?mac=...`**

- Provide the radio MAC of the client to locate.

- The corresponding site where the user was placed is provided along with the dimensions
- If a client is heard on multiple floors, it will only be placed on the floor that contains the AP it is associated with.'

NOTE

When interacting with the OV3600 API, the system requires that clients send the 'X-BISCOTTI' header along with posts. The value of the header is provided as a part of the response when a client authenticates against /LOGIN. A X-BISCOTTI token lasts as long as authentication session.

Sample Device Location Response

```
<visualrf:device_location version="1" xmlns:visualrf="www.example.com">
 <device mac="00:13:02:C2:39:28" name="Peter"
    site_id="4f674301-4b47-4ac6-8417-4eba3f7df3a6"
    site_name="NewYork">
    <site-width>124.51</site-width>
    <site-height>161.14</site-height>
    <x>82.50</x>
    <y>37.50</y>
 </device>
</visualrf:device_location>
```

Sample Site Inventory Response

```
<ov3600:ov3600_site_inventory version="1"
    xmlns:ov3600=http://www.example.com
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <site id="b45e7a49-23b5-4db0-891a-2e60bff90d2c" version="677">
    <name>Remax</name>
    <uom>ft</uom>
    <width>314.45</width> <height>425.88</height>
    <property name="site_owner" value="" format="" />
    <property name="name" value="Remax" format="" />
    <property name="installer" value="" format="" />
    <property name="planner" value="" format="" />
    <image type="background">
      <filename>/var/example/snapshot/b45e7a49-23-2e6d2c.677/background.jpg</filename>
      <relative-url>/snapshot/b423b5-4db0-891a2e0d2c.677/background.jpg</relative-url>
      <pixel-width>1151</pixel-width>
      <pixel-height>1557</pixel-height>
    </image>
    <image type="thumbnail">
      <filename>/var/example/snapshot/b45e7a49891af90d2c.677/thumb.jpg</filename>
      <relative-url>/snapshot/b45e7a49-23b5-4db0-891a2c.677/thumb.jpg</relative-url>
      <pixel-width>230</pixel-width>
      <pixel-height>311</pixel-height>
    </image>
    <ap id="12615" name="AP-4000M-1">
      <x>118.97</x> <y>130.38</y>
      <total-bandwidth>0</total-bandwidth>
      <total-clients>0</total-clients>
      <status>down</status>
      <uptime>0.0</uptime>
      <radio index="1" phy="g" mac="00:20:A6:5A:63:66" beamwidth="0.0"
          gain="1.5" antenna="" orientation="0.0" mount="Ceiling" valid="false">
        <discovering-radio id="11276" index="1" dBm="-85" />
        <discovering-radio id="11828" index="1" dBm="-93" />
      </radio>
    </ap>
  </site>
</ov3600:ov3600_site_inventory>
```

About VisualRF Plan

Overview

VisualRF Plan is a standalone Windows client that can be used for planning sites that do not yet use the OV3600 service on the Web. You can use VisualRF Plan to do basic planning procedures like adding a floor plan, provisioning APs, and generating a Bill of Materials (BOM) report. VisualRF Plan is free to use for anyone with an Alcatel-Lucent support account. No license is required.

The client can be downloaded from the Alcatel-Lucent Support Center.

Minimum requirements

VisualRF Plan must be installed on a Windows machine with the following minimum specifications:

- 250 MB Hard drive storage space
- 2 GB RAM
- 2.0 GHz dual-core CPU

NOTE

If installing VisualRF Plan on a VMware virtual machine hosted by a Mac computer, you must disable **Folder Sharing.**

VisualRF Plan Installation

After you have downloaded VisualRF Plan from the Alcatel-Lucent support site, the installer will prompt you for the location of the data directory. You must have access to the directory you choose for the installation. Also choose a directory for auto-backup. (The default is the user directory.) Follow the rest of the instructions on your installation screen.

Differences between VisualRF and VisualRF Plan

Table 168: *VisualRF vs. VisualRF Plan*

Feature	VisualRF	VisualRF Plan
Hardware sizing		X
Installation required		X
How to plan a site	X	X
Navigation	X	X
Track users	X	
Track interferers	X	
VisualRF APIs	X	
Location accuracy	X	
VisualRF preferences	X	
Resource utilization	X	

Table 168: *VisualRF vs. VisualRF Plan (Continued)*

Feature	VisualRF	VisualRF Plan
Add external walls	X	X
Client surveys	X	
Wiring Closet	X	X
View deployed switches	X	
View signal strength	X	
Planning and provisioning	X	X
Import and Export	X	X

Appendix A
Using FIPS Encryption

Enabling FIPS 140-2 Approved Mode

Users who are subject to government or industry regulations must enable FIPS 140-2 approved mode when using OV3600. When FIPS 140-2 approved mode is on, users can connect to the OV3600 server using FIPS 140-2 approved functions (ciphers).

To enable FIPS 140-2 approved mode:

1. Open a console window, then log into the system.
2. In the window, enter 9-5 to enable FIPS.

   The OV3600 server reboots automatically after it turns on FIPS mode.

About the Command Line Interface

OV3600 provides a modular command line interface (CLI) that allows you to run a finite set of management tools and configuration tasks. Some of these tasks include transferring files, enabling support connections, enabling FIPS security, upgrading software, and configuring network interfaces.

CLI Access

A change introduced in OV3600 8.2.4 prevents the root user from being able to connect to the CLI. You can access the CLI through an SSH connection by logging in to the OV3600 server with the admin user created when you install or upgrade your software to OV3600 8.2.4 or later. For information about the admin user, see the *OmniVista 3600 Air Manager 8.2.7.1 Installation Guide*.

When the database is down and you access the CLI through an SSH connection, OV3600 will skip the click through agreement and advance to the AMP CLI menu.

Custom Modules

OV3600 provides a selection of custom modules that is available by customer support request.

To get the module key:

1. Log in to the CLI as the admin user.
2. Select **9** to open the Security menu.
3. Select **7** to get the module key. A message asks you to show or save the module key for later. If you choose to save the module key, go to the next step.
4. Go back to the main menu and select **2** to download the module key to an SCP reachable destination.
5. Send module key to technical support.
6. After you receive the module, select **1** to upload the module.
7. Select **10** to add the module to your CLI custom modules menu.

How to Reset Your Password

If you forgot your CLI password, you can generate a recovery key and contact Technical Support to decode the key and provide recovery password to you.

To reset your password:

1. From a local terminal, or the VM host console, log in using the amprecovery credentials:

   ```
   <AMP server> login: amprecovery
   Password: recovery
   ```

2. Select **1** to generate the recovery key.
3. Select **2** to upload the recovery key to another server using an SCP file transfer application.
4. At the prompt, enter the destination location for the file (for example, user@host:path. User is the name of the account on the destination computer, host is the hostname or IP address of the computer on which the file will be transferred, and path is the path of the destination folder).
5. At the prompt, enter the password on the destination computer.
6. Send the **recovery.gpg** file to Technical Support for key translation.
7. Select **3** to activate the recovery password, then press **y** to continue.

8. Enter the password you received from Technical Support. If you enter the password incorrectly, the password remains unchanged.
9. Log out from the recovery user.
10.Log back in to the CLI as ampadmin using the recovery password:

```
<AMP server> login: <ampadmin>
Password: recovery password
```

11.Select **9** to open the Security menu, then select **2** to reset the OS user password.
12.At the prompt, select **2** to change the amprecovery password.
13.Type a new password and press **Enter**.

CLI Options

Table 169 lists the CLI commands that are available in OmniVista 3600 Air Manager 8.2.7.1. If there are other important tasks that you can't do from the CLI, contact technical support for help.

Table 169: *CLI Options*

Option	Description
1 Upload File	Uploads a file to the OV3600 server you're currently logged in to using SCP for Unix.
2 Download File	Downloads a file from the local AMP to another server using SCP for Unix.
3 Delete File	Deletes a file from the OV3600 server. Files shown for deletion might include downloaded files, temporary files, and backup files.
4 Backup	Displays AMP Backup options.
4-1 Backup Now	Runs the back up now.
4-2 Configure Automatic Transfer	Sets the destination for the nightly backup files.
4-3 Local Backup Retention	Changes how many backups OV3600 retains (maximum of 4).
5 Restore	Displays restore options.
5-1 AMP Restore	Restores the AMP server from an on-demand, nightly, or imported backup that you select.
5-2 VisualRF Restore	Restores the VisualRF database from the **visualrf_backup.pl** file that you select. Files shown for backup might include downloaded files, temporary files, and backup files. **NOTE:** If the STIG module is enabled on your system, this command option is unavailable.
6 Support	Displays support options.
6-1 Show Tech Support	Displays information about the AMP server to show technical support.
6-2 Generate Diagnostic Tarball	Displays the compressed log collection for sending to customer support.
6-3 Initialize Support Connection	Loads the **support_connection.tar** file provided by customer support and creates the support user (by default, awsupport) and password.

Option	Description
6-4 Start Support Connection	Toggles on and off the support connection.
6-5 Delete Support User	Deletes the **awsupport.gpg** file.
6-6 Show contents of awsupport.gpg	Displays the encrypted support credentials.
6-7 Paste Encoded Text	Provides the option to paste the encoded format of the support_connection.tar file instead of upload the package.
7 Upgrade	Displays upgrade options.
7-1 Upgrade OV3600 Management Platform	Runs the OV3600 software upgrade.
7-2 Upgrade OS Kernel	Runs the kernel upgrade (requires rebooting the OV3600 server).
8 Advanced	Displays system options.
8-1 Restart Application	Restarts the OV3600 services.
8-2 Reboot System	Reboots the OV3600 server.
8-3 Configure Network Settings	Configures network settings.
8-4 Set Hostname	Sets the hostname of the OV3600 server.
8-5 Set Timezone	Sets the timezone of the AMP server.
8-6 Shutdown System (halt)	Shuts down the OV3600 server gracefully.
8-7 Add File Transfer User	Creates a new file transer user account that works to transfer files between the OV3600 server and an SSHD client.
9 Security	Displays security options.
9-1 Reset Web admin Password	Resets the Web UI log in password for admin.
9-2 Change OS User Password	Changes the CLI log in password.
9-3 Add SSL Certificate	Installs the SSL certificate, used to establish secure web sessions, on your OV3600 server.
9-4 Add DTLS Certificates	Installs the DTLS certificates, used to encrypt secure AMON traffic, on your OV3600 server.
9-5 Enable FIPS	Toggles on or off FIPS 140-2 Approved Mode (requires a reboot).

Option	Description
9-6 Show EngineID	Displays the SNMPv3 engine ID.
9-7 Module Key	Displays module key options.
9-8 Apply STIGs	Applies and enforces the STIG modules according to the Defense Information Systems Agency (DISA) for STIG compliance. If you enable this setting, it can't be changed.
9-9 Set MaxAuthTries value for sshd	Sets a limit on how many authentication attempts are allowed per user session.
9-10 Make OCSP Optional	Toggles on or off OCSP certificate validation when certificate authentication is required from the UI.
9-11 Generate Certificate Signing Request	Creates a CSR that identifies which server will use the certificate.
9-12 Install Signed Certificate	Installs a signed certificate. OV3600 supports signed certificates in PEM format with *.crt file extensions.
9-13 Remove amprecovery Account	Removes the amprecovery account. **NOTE:** When you remove the amprecovery account, OV3600 removes this command option from the menu.
10 Custom Commands	Displays custom command option.
10-1 Add New Menu Module	Adds a new CLI menu module that you select (requires requesting module encrypted with a module key from customer support).
b >> Back (or Ctrl+c)	Returns to the previous menu.
c >> Cancel	Cancels the key request.
11 Enter Commands	Some read-only commands are available from this menu. To see a list of commands, type a question mark (?) at the prompt. For more information, see Table 170. **NOTE:** If the STIG module is enabled on your system, this command option is unavailable.
q	Exits the CLI session.

Table 170 lists the running enter commands that are available when you select **11** from the CLI.

Table 170: *Running Enter Commands*

Command	Description
?	Displays the list of commands.
help <topic>	Displays the help for the <topic>.
man <topic>	Invokes the linux `man` command for the <topic>.
quit	Returns to CLI menu.

Table 170: *Running Enter Commands (Continued)*

Command	Description
q	Returns to CLI menu.
exit	Returns to CLI menu.
history	Displays the history of commands you have typed.
h	Displays the history of commands you have typed.
h <pattern>	Displays history of all commands, matching the specified <pattern> input.
ch	Clears the history of commands displayed on the screen.
r	Repeats the previous command.
r <number>	Repeats the command, specified by the <number> from the history list.
r /x/y	Repeats the previous command, replacing x with y.
clear	Clears the terminal screen.
date	Displays the current date and time.
date MMDDhhmm	Changes the date and time on the OV3600 server.
top	Displays the status of running processes.
daemons	Displays the running daemons.
wd	Displays the monitoring of running daemons, refreshing after 1-second intervals.
wd <n>	Displays the monitoring of running daemons, refreshing after the <n> interval.
ls	Lists the files in the AMP CLI directory. **NOTE:** You can use shell patterns with *, ?, and [ ].
rm	Removes files from the AMP CLI directory. **NOTE:** You can use shell patterns with *, ?, and [ ].
cleanup	Deletes files that are no longer needed, including log files, old source files, and pre-upgrade backups.
rd	Restarts the daemons.
psg <pattern>	Displays the running processes, matching the <pattern> you typed.
pss <pattern>	Displays the running processes like grep but shows more detailed information, matching the <pattern> you typed.
show_tech_support	Displays information about the AMP server to show technical support.

Table 170: *Running Enter Commands (Continued)*

Command	Description
dbsize	Displays the 30 largest database tables.
dbsize <n>	Displays the <n> largest database tables.
dbsize -l	Displays details of disk space consumed, tuple spaces, and the actual size of the 30 largest tables.
dbsize -l <n>	Displays details of disk space consumed, tuple spaces, and the actual size of the <n> largest tables.
osrel	Displays the release version of the operating system.
license	Displays the license for the OV3600 server.
amp_version	Displays the OV3600 version on your OV3600 server.
df -h	Shows disk space usage.
git diff	Checks for patches.
hostname	Displays the DNS name of the OV3600 server.
amp_backup	Runs a backup and puts the file in the AMP CLI directory.
amp_restore <filename>	Restores the OV3600 server from the backup.
remove_visualrf_cache	Clears the **visualrf_bootstrap** file.
iptables -L	Displays the IP tables.
dmidecode	Displays the serial number of the OV3600 server along with BIOS information.
network	Runs the network setup wizard.
dci	Displays the device communication interface, which configures the ethernet interface used for communication with devices.
ifconfig <interface>	Displays the status of the network interfaces.
ip route	Displays the IP routing tables.
disable_whitelist	Resets the AMP whitelist to allow access (and restarts the AMP web server).
sw <ap id> args	Uses SNMP v1GETBULK to send a request to the database and walks back a list of all items up to a specified limit.
sw2 <ap id> args	Uses SNMP v2c GETBULK to send a request to the database and walks back a list of all items up to a specified limit.

Table 170: *Running Enter Commands (Continued)*

Command	Description
sw3 <ap id> args	Uses SNMP v3 GETBULK to send a request to the database and walks back a list of all items up to a specified limit.
tcpdump args	Sends TCP packet data to an output file that you can use for later troubleshooting.
ping args	Sends ICMP echo request to confirm whether your network is reachable.
nslookup args	Queries the Internet name server, or the host name of the name server.
traceroute args	Tracks the route packets from an IP network to a host, using the IP protocol's time to live (TTL) value and getting an ICMP time exceeded response from each gateway along the path to the host.
free args	Displays the amount of free and used memory in the system.
service iptables	Displays the full status for IP tables.
service	Lists all services and allows you to manage them.
service <service> status|start|stop|restart	Manages the <service> you typed.
service <service>	Displays the status of the service.
qlog	Lists the status of available qlog topics.
qlog enable <topic>	Enables debugging. As files are created, they appear in the AMP CLI directory. **NOTE:** If there is more than 1 qlog topic matching the substring, a numbered picklist will be displayed. Enter the desired qlog topic number or multiple numbers separate by spaces. You can give a unique prefix or a unique substring.
qlog disable <topic>	Disables debugging for an individual topic. **NOTE:** You can give a unique prefix or a unique substring.
qlog disable all	Disables debugging for all qlog topics. **NOTE:** If there is more than 1 qlog topic matching the substring, a numbered picklist will be displayed. Enter the desired qlog topic number or multiple numbers separate by spaces. You can give a unique prefix or a unique substring.
snoop	Displays the list of work queue snoop debug topics. **NOTE:** If there is more than 1 qlog topic matching the substring, a numbered picklist will be displayed. Enter the desired qlog topic number or multiple numbers separate by spaces. You can give a unique prefix or a unique substring.
snoop <topic>	Enables work queue snoop debug for the desired topics. **NOTE:** You can give a unique prefix or a unique substring.
snoop active	Displays the active work queue snoop topics.

Table 170: *Running Enter Commands (Continued)*

Command	Description
snoop stop <topic>	Stops work queue snoop on the selected topic. **NOTE:** You can give a unique prefix or a unique substring.
snoop stop all	Stops all active work queue snoop debugging.
ethernet_bonding <ip><netmask><gateway>	Enables ethernet bonding of two network interfaces. **NOTE:** If you enter ethernet_bonding without variables, you will be prompted for 3 input variables.
docker <bridge_ip_ address/cidr_bits>	Configures the OV3600 Glass feeder service. **NOTE:** If you enter docker without variables, you will be prompted for 2 input variables.