OmniVista 3600
Air Manager 8.0

Getting Started Guide

Chapter 1 Overview 5
Initial Setup 5
How Do I Add Devices? 5
Adding Devices with the Device Setup > Add Page 5
Discovering New Devices 7
Configuring and Running a Scan Set 7
Add Newly Discovered Devices to a Group 8
Auditing Device Configuration 9
Adding Multiple Devices from a File 9
Adding Universal Devices 11
Adding an Alcatel-Lucent Device 11
Adding as a Management Server 11
Adding as a Trap Host 12
How are Folders and Groups Organized? 12
Groups 12
Folders 13
How Do I Define New Users and Roles? 13
How Do I Define Credentials for Devices that Communicate with OV3600? 14
I Have a Mismatch. What Do I Do? 15
Auditing to Resolve Mismatches 15
Importing Group Settings to Resolve Mismatches 15
Importing Device Specific Settings 15
Chapter 2 Common Configuration Options 17
How Do I Acknowledge Alerts? 17
Workflow 17
Auto-Acknowledgement of Device Down Alerts 17
Alert Suppression 17
Trigger Conditions 18
Notification Options 18
Alert Visibility 18
Which Triggers Are Most Important? 18
Device Down Trigger 18
Device Up Trigger 19
Channel Utilization Trigger 19
Rogue Reclassified Trigger 20
Connected Clients Trigger 20
Client RADIUS Authentication Issues Trigger 20
All Triggers 21
Which Reports Should I Utilize? 21
Creating Report Definitions 21
Scheduling 21
Sharing 21
Access to Generated Reports 22
Creating a Report Using the Modify Devices Feature 22
Report Types 22

Device Reports 22
Client Reports 22
Network Reports 22
Security Reports 23
Custom Reports 23
Chapter 3 Monitoring Practices 25
Viewing Device Monitoring Statistics 25
Monitoring Data for Wired Devices (Routers and Switches) 26
Understanding the APs/Devices > Monitor Pages for all Device Types 27
Understanding the APs/Devices > Interfaces Page 27
Monitoring with the RF Performance Page 28
Viewing Syslog Messages 29

Congratulations on successfully installing OmniVista 3600 Air Manager 8.0! So where do you go from here? This document is designed to help you with your initial setup. It also provides information on common configuration options and daily monitoring practices.

Refer to the following sections:

- "Initial Setup" on page 5
- "Common Configuration Options" on page 17
- "Monitoring Practices" on page 25

Initial Setup

OmniVista 3600 Air Manager 8.0 initial setup consists of creating folders and groups, discovering and adding devices, and defining credentials for devices that communicate with OV3600. Refer to the following sections for additional information.

- "How Do I Add Devices?" on page 5
- "Discovering New Devices" on page 7
- "How are Folders and Groups Organized?" on page 12
- "How Do I Define New Users and Roles?" on page 13
- "How Do I Define Credentials for Devices that Communicate with OV3600?" on page 14
- "I Have a Mismatch. What Do I Do?" on page 15

How Do I Add Devices?

In many cases, you will add devices after the devices have been discovered. Refer to "Discovering New Devices" on page 7 for more information. In other cases, your deployment may require that you manually add devices to OV3600. You can add devices manually by uploading a CSV file or from the **Device Setup > Add** page.

Alcatel-Lucent Instant devices are automatically discovered. Refer to the *Alcatel-Lucent Instant in OV3600 8.0 Deployment Guide* for more information on Instant devices in OV3600.

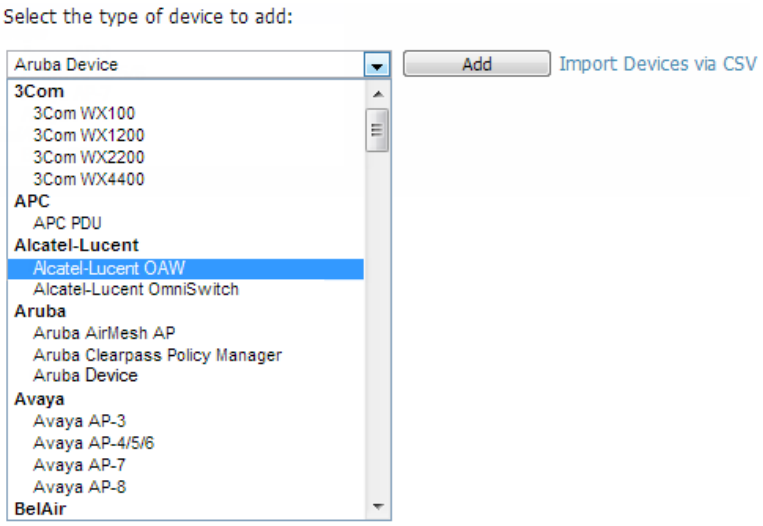
Adding Devices with the Device Setup > Add Page

Manually adding devices from the **Device Setup > Add** page to OV3600 is an option for adding all device types. You only need to select device vendor information from the drop-down list, and OV3600 automatically finds and adds specific make and model information into its database.

Perform these steps to manually add devices to OV3600:

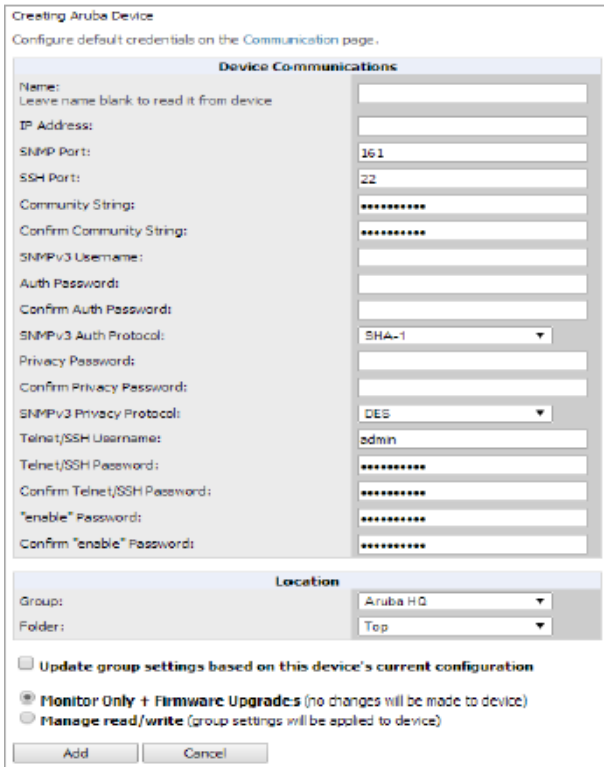
1. Add a device manually by selecting the vendor and model. Browse to the **Device Setup > Add** page and select the vendor and model of the device to add (see Figure 1).

Figure 1: ***Device Setup > Add*** *Page Illustration*



2. Select **Add**. The **Device Communications** and **Location** sections appear (see Figure 2).

Figure 2: *Device Setup > Add >* ***Device Communications*** *and* ***Location*** *Sections*



3. Complete the **Device Communications** and **Location** settings for the new device. Settings can differ from device to device based on the type of device and the features that the device supports. In several cases, the default values in the Device Communication page from any given device are derived from the **Device Setup > Communication** page.
4. In the **Location** field, select the appropriate group and folder for the device.
5. At the bottom of the page, select either the **Monitor Only** or **Management read/write** button. The choice depends on whether you want to overwrite the **Group** settings for the device being added.

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.

6. Select **Add** to finish manually adding devices to the network.

Discovering New Devices

In addition to manually adding devices, devices connected to your network can automatically be discovered and added. OV3600 performs device discovery using the following methods. These methods are described in greater detail in the *OmniVista 3600 Air Manager 8.0 User Guide*.

- **SNMP/HTTP Discovery Scanning** – This is the primary method for discovering devices. Refer to "Configuring and Running a Scan Set" on page 7 for information about how to utilize this feature.
- **Cisco Discovery Protocol (CDP)** - CDP uses the polling interval configured for each individual Cisco switch or router on the **Groups > List** page. For device discovery, OV3600 requires read-only access to a router or switch for all subnets that contain wired or wireless devices in order to discover a Cisco device's CDP neighbors. The CDP Neighbor Data Polling Period is specified on the **Groups > Basic** page for a specific group.

Alcatel-Lucent Instant devices are automatically discovered. Refer to the *Alcatel-Lucent Instant Deployment Guide* for more information on Alcatel-Lucent Instant devices in OV3600.

Configuring and Running a Scan Set

Configuring a scan set consists of defining the network segments that will be scanned along with the credentials used for governing the scanning of a given network. Perform the following tasks to configure a scan set.

1. Add networks for SNMP/HTTP scanning.
   a. Navigate to the **Device Setup > Discover** page and locate the Networks section.
   b. Click **Add**. A New Networks form opens.
   c. Enter a name for the network, the IP network range or first IP address on the network to be scanned, and the subnet mask for the network to be scanned. Note that the largest subnet that OV3600 supports is 255.255.0.0.
   d. Click **Add** . Repeat steps 1a - 1d to add all the networks on which to enable device scanning.
2. Add credentials for scanning.
   a. Navigate to the **Device Setup > Discover** page and scroll down to the Credentials section.
   b. Click **Add**. The New Scan Credentials form opens.
   c. Enter a name for the credential in the field (for example, Default). This field supports alphanumeric characters (both upper and lower case), blank spaces, hyphens, and underscore characters.
   d. Select the type of scan to be completed.
      - SNMPv1 and SNMPv2 differ between their supported traps, supported MIBs, and network query elements used in device scanning.
      - HTTP is not as robust as SNMP in processing network events, but HTTP might be sufficient, simpler, or preferable in certain scenarios.
   e. If you selected SNMP, then define the community string to be used during scanning. If you selected HTTP, then enter a username and password for the scan credentials.
   f. Click **Add**. Repeat steps 2a - 2f to add credentials on which to enable device scanning.
3. Define a scan set.
   a. Navigate to the **Device Setup > Discover** page and select the **Add New Scan Set** button.
   b. Select the Network(s) to be scanned and the Credential(s) to use. OV3600 defines a unique scan for each Network/Credential combination.

c. 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, or a specified auto-authorization group and folder. Be sure to note this location.

d. Select **Add** when you are finished, and repeat these steps for each scan set that you want to create.

NOTE

Discovered devices use the default credentials configured on the **Device Setup > Communication** page for each vendor-specific device. Refer to "How Do I Define Credentials for Devices that Communicate with OV3600?" on page 14 for more information.

4. Running a scan set.

   a. Navigate to the **Device Setup > Discover** page and select the check boxes for each scan to run.

   b. Click **Scan**.

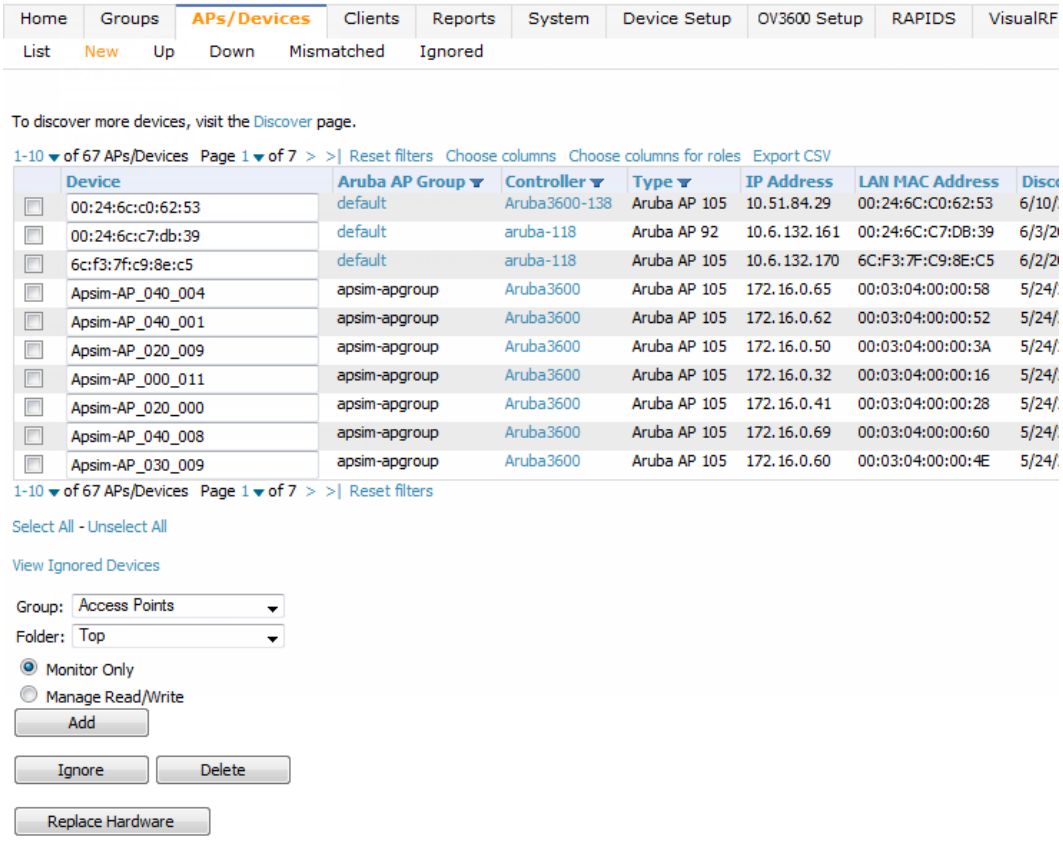
   c. View the **Start** and **Stop** columns to see the status of the scan. Refresh the browser until both the Start and Stop columns display date and time information. Newly discovered devices will be displayed on the **APs/Devices > New** page. These devices can now be added to your network.

Add Newly Discovered Devices to a Group

1. Select the **New Devices** link in the header. This opens the location where all newly-discovered devices are displayed. This location is normally **APs/Devices > New**, though you might have specified a different location while defining a scan set.

   The information on the page includes the related switch (when known/applicable), the device type (including vendor and model), the LAN MAC Address, the IP address, and the date/time of discovery. See Figure 3.

Figure 3: *APs/Devices > New page*



2. Select the check box beside the device(s) you want to add.
3. Use the drop-down lists to select the **Group**, **Folder**, and **Alcatel-Lucent AP Group** to which the devices will be added. The default group appears at the top of the Group list.

Devices cannot be added to a Global Group because groups designated as "Global Groups" cannot contain access points.

4. Select either **Monitor Only** or **Manage Read/Write** as the mode in which the new device(s) will operate.
   - In Monitor Only + Firmware Upgrades mode, OV3600 updates the firmware, compares the current configuration with the policy, and displays any discrepancies on the **APs/Devices > Audit** page. OV3600 does not change the configuration of the device.
   - In Manage Read/Write mode, OV3600 compares the device's current configuration settings with the Group configuration settings and automatically updates the new device's configuration to match the Group policy.

Put devices in Monitory Only + Firmware Upgrades mode when they are added to a newly established device group. This avoids overwriting any important existing configuration settings.

5. Click **Add**. You can go to the **APs/Devices > List** page and select the folder that contains the newly added devices. This enables you to verify that the devices have been properly assigned.

Auditing Device Configuration

When you have added a newly discovered device successfully to a Group in **Monitor** mode, the next step is to verify device configuration status. Determine whether any changes will be applied to that device when you convert it to **Managed read/write** mode.

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.

Perform these steps to verify the device configuration status:

1. Browse to the **APs/Devices > List** page.
2. Locate the device in the list and check the information in the **Configuration** column.
3. If the device is in **Monitor** mode, the **lock** symbol appears in the **Configuration** column, indicating that the device is locked and will not be configured by OV3600.
4. Verify the additional information in the **Configuration** column for that device.
   - A status of **Good** indicates that all of the device's current settings match the group policy settings and that no changes will be applied when the device is shifted to **Manage** mode.
   - A status of **Mismatched** indicates that at least one of the device's current configuration settings does not match the group policy and will be changed when the device is shifted to **Manage** mode.
5. If the device configuration is **Mismatched**, select the **Mismatched** link to go to the **APs/Devices > Audit** page. This page lists detailed information for all existing configuration parameters and settings for an individual device.

   The group configuration settings are displayed on the right side of the page. If the device is moved from **Monitor** to **Manage** mode, the settings on the right side of the page overwrite the settings on the left.
6. 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 reassign the device to another Group.

Adding Multiple Devices from a File

You can add devices in bulk from a file to OV3600. Here you also have the option of specifying vendor name only, and OV3600 will automatically determine the correct type while bringing up the device. If the .csv file includes make and

model information, OV3600 will add the information provided in the file. It will not override what you have specified in this file in any way.

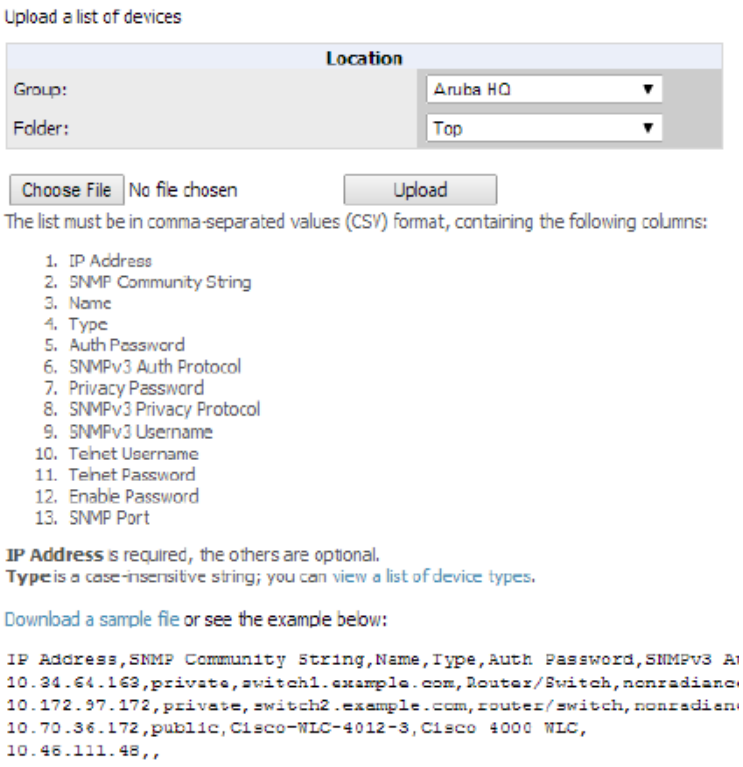
The CSV list must contain the following columns:

- IP Address
- SNMP Community String
- Name
- Type
- Auth Password
- SNMPv3 Auth Protocol
- Privacy Password
- SNMPv3 Privacy Protocol
- SNMPv3 Username
- Telnet Username
- Telnet Password
- Enable Password
- SNMP Port

You can download and customize a file.

1. To import a CSV file, go to the **Device Setup > Add** page.
2. Click the **Import Devices via CSV** link. The **Upload a list of devices** page displays. See Figure 4.

Figure 4: *Device Setup > Add > Import Devices via CSV Page Illustration*



3. Select a group and folder into which to import the list of devices.
4. Click **Choose File** and select the CSV list file on your computer.
5. Click **Upload** to add the list of devices to OV3600.

Adding Universal Devices

OV3600 gets basic monitoring information from every device including switches, routers and APs whether or not the devices are supported. 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. See "Adding Devices with the Device Setup > Add Page" on page 5.

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

Select the **pencil** icon next to an interface, to select to be non-monitored or monitored as an interface. OV3600 collects this information and displays it on the **APs/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.

Adding an Alcatel-Lucent Device

Alcatel-Lucent controllers and switches can be discovered during a scan or can be added manually. The steps are similar to those described in "Adding Devices with the Device Setup > Add Page" on page 5; however, additional steps are described to ensure that the controller or switch is configured properly for monitoring.

1. Select the Alcatel-Lucent OmniSwitchDevice type and select **Add**.
2. Enter the **Name** and the **IP Address** for the device.
3. Enter the **SNMP Community String**, which is required field for device discovery.

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

4. Enter the required fields for configuration and basic monitoring:
   - Telnet/SSH Username
   - Telnet/SSH password
   - Enable password
5. Assign the device to the correct Group and to a Folder. Beginning in OV3600 7.7, new switches cannot be added to groups that contain controllers.
6. Ensure that the **Monitor Only** option is selected.
7. Select **Add**. The Confirmation page displays.
8. Select **Apply Changes Now**.
9. Navigate to the **APs/Devices > New** page.
10. Select the Alcatel-Lucent device you just added from the list of new devices.
11. Ensure **Monitor Only** option is selected.
12. Select **Add**.

Adding as a Management Server

This section describes how to set up OV3600 as a management server.

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

The following commands are for AOS-W 6.4. To get the commands for other versions, refer to the AOS-W *Command-Line Interface Reference Guide* for that version.

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

```
(switch-Name) # configure terminal


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

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

You can add up to four <AMP-IP> addresses.

Adding as a Trap Host

To ensure the OV3600 server is defined as a trap host, access the command line interface of each switch (master and local), enter enable mode, and issue the following commands:

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

(switch-Name) (config) # snmp-server host <OV3600 IP ADDR> version 2c <SNMP Community String of switch>

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

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

How are Folders and Groups Organized?

Folders and Groups are useful ways of organizing your devices. Folders are used for monitoring; groups are used for configuration. Group configuration applies to controllers and switches. Configuration for APs is done through the **APs/Devices > Manage** or **APs/Devices List** pages.

Groups should be comprised of similar devices that will utilize a consistent configuration. Controllers and switches though, must reside in separate groups.

Folders are used to filter devices by location. For example, you are monitoring a campus with several dormitories that use Alcatel-Lucent controllers and thin AP devices. The controllers might be part of one collection, and the thin APs might be part of another. Both of those collections can reside in a folders named Dorm1, Dorm2, and so on. In addition, folders can be nested, so that both Dorm1 and Dorm2 can reside under a top folder named Campus.

Groups

Enterprise APs, controllers, routers, and switches have hundreds of variable settings that must be configured precisely to achieve optimal performance and network security. Configuring all settings on each device individually is time consuming and error prone. OV3600 addresses this challenge by automating the processes of device configuration and compliance auditing. At the core of this approach is the concept of Device Groups, with the following functions and benefits:

- OV3600 allows certain settings to be managed at the Group level, while others are managed at an individual device level.

- OV3600 defines a Group as a subset of the devices on the wireless LAN, ranging in size from one device to hundreds of devices that share certain common configuration settings.
- Groups can be defined based on geography (such as 5th Floor APs), usage or security policies (such as Guest Access APs), function (such as Manufacturing APs), or any other appropriate variable.
- Devices within a group can originate from the same vendor or hardware model and might share certain basic configuration settings.
- Controllers and switches cannot reside in the same group.

Typical group configuration variables include:

- Basic settings - SSID, SNMP polling interval, and so forth
- Security settings - VLANs, WEP, 802.1x, ACLs, and so forth
- Radio settings - data rates, fragmentation threshold, RTS threshold, DTIM, preamble, and so forth.

When configuration changes are applied at a group level, they are assigned automatically to every device within that group. These changes must be applied to every device while in **Managed** mode.

When you first configure OV3600, only a group named Access Points is available. You can add groups by navigating to the **Groups > List** page and selecting the **Add New Group** button. You can also select the **Duplicate** button for a current group (normally the very last column in the **Groups > List** page). Selecting this button creates a copy of the specified group and opens immediately to the **Groups > Basic** page. Refer to the *OmniVista 3600 Air Manager 8.0 User Guide* for more information.

Folders

The devices on the **APs/Devices > List** page are arranged in collections called folders. Folders provide a logical organization of devices unrelated to the configuration groups of the devices. Using folders, you can quickly view basic statistics about devices. You must use folders if you want to limit the APs and devices that OV3600 users can see.

The amount and type of information that a user can see is based on his/her role.

Folder views are persistent in OV3600. For example, if you created a folder named "Store1", you can select that folder and then select the **Down** link in the header section of the page (top), to view only the down devices in the Store1 folder.

If you want to see every down device, select the **Expand folders to show all APs/Devices** link. When the folders are expanded, you see all of the devices on OV3600 that satisfy the criteria of the page. You also see a column that lists the folder containing the APs.

How Do I Define New Users and Roles?

OV3600 installs with only one OV3600 user: admin. Admin users are authorized to perform the following functions:

- Define additional users with varying levels of privilege, including managing 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.

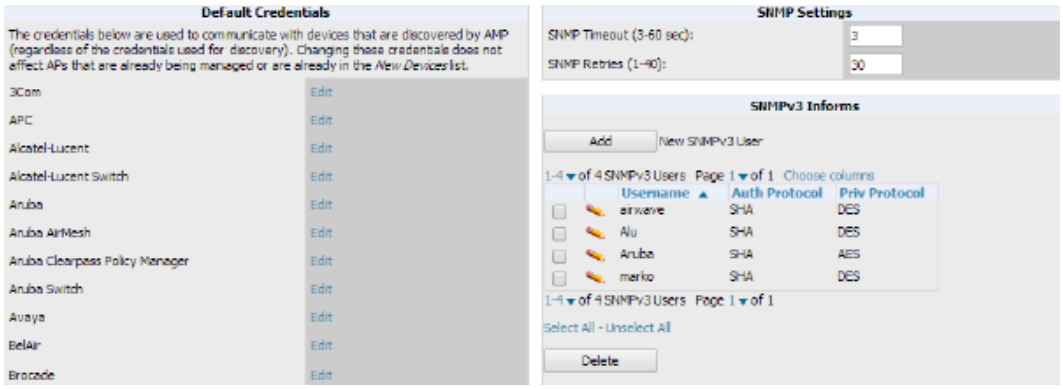
Username and password are not required if you configure OV3600 to use RADIUS, TACACS, or LDAP authentication. In addition, you do not need to add individual users to the OV3600 server if you use RADIUS, TACACS, or LDAP authentication. Refer to the following sections in the *OmniVista 3600 Air Manager User Guide*: Configuring RADIUS Authentication and Authorization, Configuring TACACS+ Authentication, and Configuring LDAP Authentication and Authorization.

User roles determine the level of access that a user has to folders. For example, you can create non-administrative users, such as help desk or IT staff, who support a subset of accounts or sites within a single OV3600 deployment. These non-admin users can be set up to monitor data and users for devices within their assigned folders. Roles also determine a user's access to VisualRF and RAPIDS.

How Do I Define Credentials for Devices that Communicate with OV3600?

On the **Device Setup > Communication** page, you can configure OV3600 to communicate with your vendor-specific devices, and you can set SNMP polling information. The configuration defines the default credentials for future devices; it does not impact existing devices. See Figure 5.

Figure 5: *Device Setup > Communication Page (Partial View)*



Perform the following steps to define the default credentials and SNMP settings for your wireless network.

1. Configure default credentials.
   a. Navigate to the **Device Setup > Communication** page and enter the credentials for each device model on your network. These credentials represent the default credentials that are assigned to all newly discovered APs.

Community strings and shared secrets must have read-write access in order for OV3600 to configure the devices. Without read-write access, OV3600 can monitor the devices only; it cannot apply any configuration changes.

2. Specify SNMP Settings.
   a. Specify an **SNMP Timeout** value. This is the number of seconds that OV3600 will wait for a response from a device after sending an SNMP request, so a smaller number is more ideal.
   b. Enter a value for **SNMP Retries**. This value represents the number of times OV3600 attempts 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. As a best practice, we recommend a value of 10.
3. Configure SNMPv3 Informs.
   a. Locate the SNMPv3 Informs section and select the **Add** button to configure all SNMPv3 users that are configured on the switch. The SNMP Inform receiver in OV3600 will restart when users are changed or added to the switch.
4. Specify Telnet/SSH, HTTP Discovery, and ICMP settings.
   a. Specify the Telnet/SSH Timeout value. This value represents the number of seconds when performing Telnet and SSH commands.
   b. Specify the HTTP Timeout value. This value represents the number of seconds used when running an HTTP discovery scan.
   c. In the ICMP Settings section, specify whether to ping devices that were unreachable via SNMP.

This value should be set to "**No**" if ICMP is disabled on your network.

5. Specify read/write settings for Symbol 4131 and Cisco Aironet SNMP Initialization.
   - If you select **Do Not Modify SNMP Settings**, then 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.
   - If you select **Enable read-write SNMP**, then OV3600 can manage networks with Symbol, Nomadix, Cisco IOS AP that do not have SNMP initialized.

I Have a Mismatch. What Do I Do?

OV3600 has a configuration policy and a mismatch is a device that does not match the configuration that OV3600 wants. Mismatches can occur for a variety of reasons. For example, you might have some policies that are defined on a Local switch that override policies on the Master switch. In this case, OV3600 recognizes policies defined on a global level (on the Master switch).

Auditing to Resolve Mismatches

Updating your configuration and then performing an audit on a device can resolve most mismatches.

1. Go to the device and change the configuration.
2. From the **APs/Devices > List** page, select the device that shows a configuration mismatch.
3. Click the **Audit** tab to view the current and desired configuration settings.
   a. If you determine that certain configuration options require change, make those changes within OV3600 so that they match the desired configuration setting, and then click **Save and Apply** before Auditing again.
   b. If you determine that some mismatch configurations on the **Audit** page can be ignored, click **Customize** to select the items that can be ignored during the upcoming audit.
4. Click **Audit**. The configuration state changes from Mismatched to Verifying. Note that this process can take several minutes to complete.

After the audit is complete, the configuration state should change from Verifying to Good.

Importing Group Settings to Resolve Mismatches

Some mismatches can occur because the switch's group settings do not match the desired configuration. In this case, importing group settings can resolve the mismatch.

1. Click the **Audit** tab to view the current and desired configuration settings.
2. Click **Import**.

After the import is completed, the device settings on OV3600 will match the desired configuration on the switch.

Importing Device Specific Settings

You can import device specific settings to resolve a mismatch.

1. Navigate to the device's **Manage** page.
2. Click **Import Settings**.

This section describes common configuration options for triggers, reports, and alerts that you might use on a daily basis. Refer to the following sections for additional information:

- "How Do I Acknowledge Alerts?" on page 17
- "Trigger Conditions" on page 18
- "Notification Options" on page 18
- "Alert Visibility" on page 18
- "Which Triggers Are Most Important?" on page 18
- "All Triggers" on page 21
- "Which Reports Should I Utilize?" on page 21

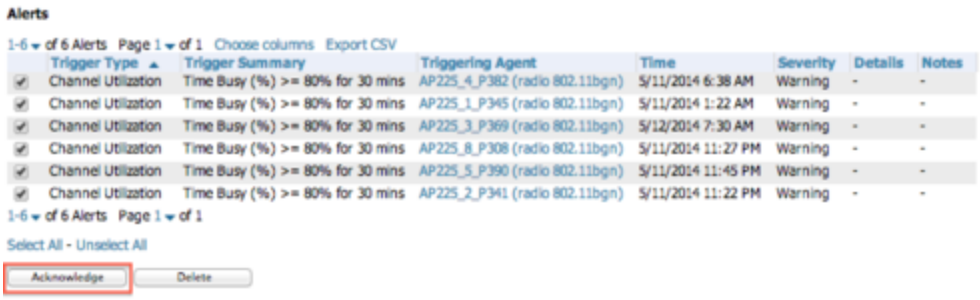
How Do I Acknowledge Alerts?

OV3600 can send out customizable alerts on over 35 types of events. You can control the alerting behavior by creating triggers on the **System >Triggers** page.

Workflow

Normally OV3600 will not alert on an event if there is an existing, unacknowledged alert for the same event (for example, a radio with > 80% utilization). To tell OV3600 that you are ready for it to start alerting on that event again, the alert needs to be either acknowledged or deleted on the **System >Alerts** page.

Figure 6: *Alerts List*



Auto-Acknowledgement of Device Down Alerts

Device Down alerts can be automatically acknowledged when the device comes back up. To enable auto-acknowledgement of Device Down alerts, create a Device Up alert with the Auto Acknowledge setting enabled in one of these ways:

- Up - When a device comes up, its Device Down alerts are acknowledged.
- Up and Down - Like above, and in addition if the device goes down, it's Device Up alerts are acknowledged.

Alert Suppression

It's important to understand the "Suppress Until Acknowledged" setting for triggers.

- If suppression is set to No, then OV3600 will send out an alert every time it detects the symptom. For example, if an AP were down, we would send an alert every time we poll for Thin AP Status, typically every 5 minutes.
- If suppression is set to Yes, then OV3600 will not send another alert until one of these things happens:

- A user acknowledges or deletes the alert.
- The alert is automatically acknowledged or purged by nightly maintenance. The thresholds for automatically acknowledging and purging are configurable on the OV3600 Setup page.

Trigger Conditions

Conditions can be used to fine-tune when alerts are sent. For many types of triggers, multiple conditions can be used. When there are multiple conditions you can control whether all conditions must be met (Matching Conditions = All) for the trigger to fire, or it will fire if any one condition is met (Any). The Channel Utilization trigger below is a good example of a trigger that will fire if either of the two conditions is met.

Notification Options

OV3600 includes the following notification options:

- Alerts are always logged on the **System > Alerts** page.
- Email - Alerts can be sent to multiple email addresses.
- SNMP Traps to External NMS - Traps can be sent to external systems. Add external NMS servers on the **OV3600 Setup > NMS** page.

Alert Visibility

There are two options for alert visibility:

- By Role - only users with the same role as the trigger creator will see the alerts.
- By Triggering Agent - If an OV3600 user is allowed to see the AP/rogue/client that the alert is about, then he can see the alert. If he is not allowed to see the AP/rogue/client, then he also cannot see the alert.

Which Triggers Are Most Important?

There are over 35 types of triggers available. This section shows which are the most valuable ones, the ones that should be enabled every time you install a new OV3600 server.

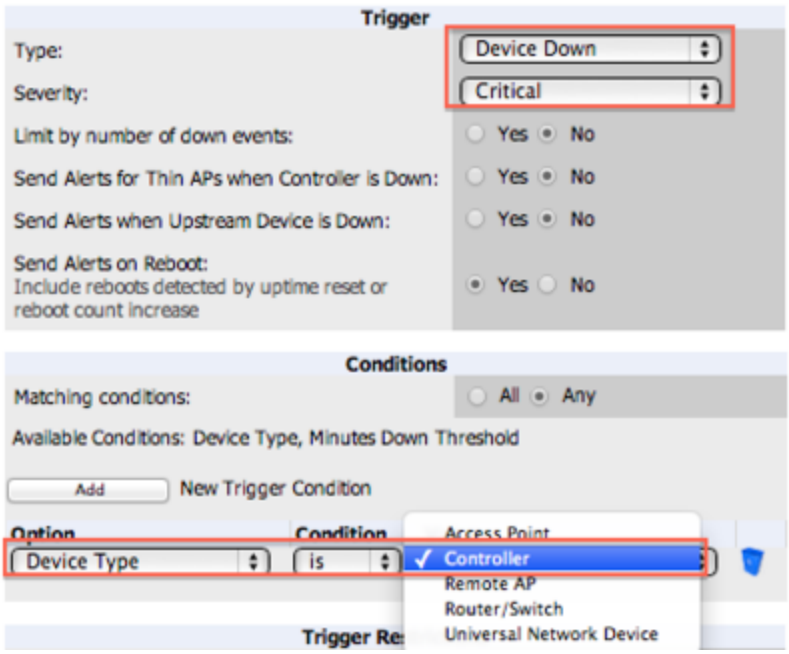
- "Device Down Trigger" on page 18
- "Device Up Trigger" on page 19
- "Channel Utilization Trigger" on page 19
- "Rogue Reclassified Trigger" on page 20
- "Connected Clients Trigger" on page 20
- "Client RADIUS Authentication Issues Trigger" on page 20

Device Down Trigger

Since there is a different severity when a controller goes down versus when an AP goes down versus a switch, we recommend to set up three separate device down triggers, one for each class of device.

Figure 7 shows an example of a Controller Down Trigger.

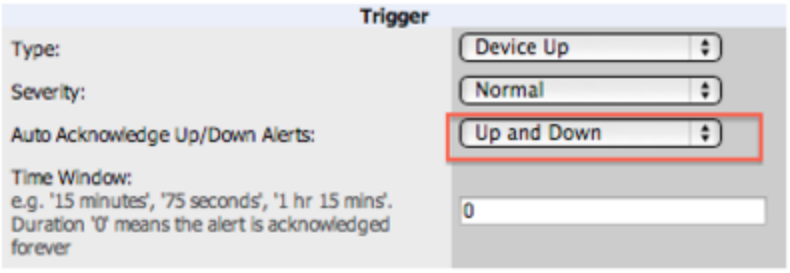
Figure 7: *Controller Down Trigger*



Device Up Trigger

Adding a Device Up trigger with the Auto Acknowledge feature enabled helps with the workflow by acknowledging Device Down alerts when devices come back up.

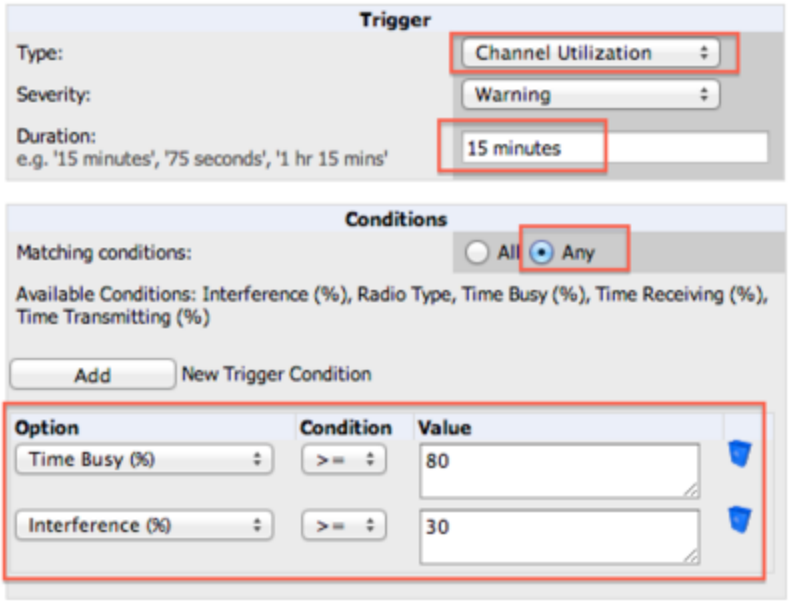
Figure 8: *Device Up Trigger*



Channel Utilization Trigger

Alert on high utilization or high interference. For interference percentage, a value of 30-40% makes a good starting point. Figure 9 below uses 40%, which would result in fewer alerts than a 30% threshold.

Figure 9: *Channel Utilization Trigger*



Rogue Reclassified Trigger

Use this trigger for things that are classified as rogue or greater.

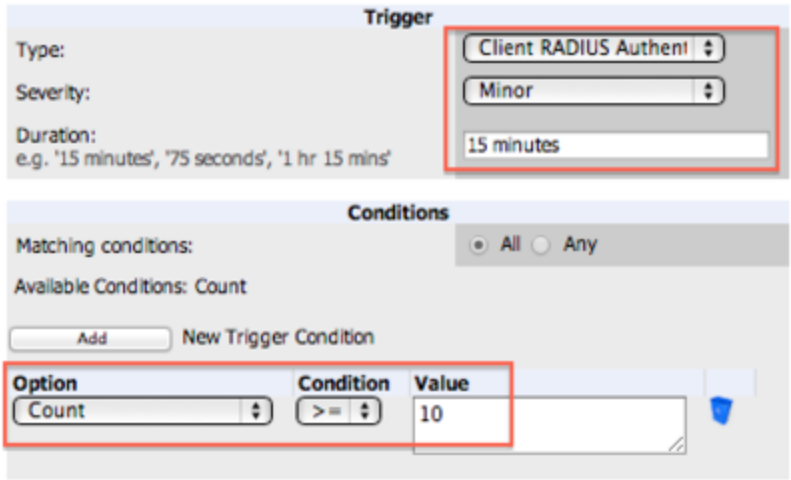
Connected Clients Trigger

This is sometimes called the "stolen iPad" trigger. If a device is missing, set up a trigger with its MAC address, and this will send an alert whenever the device is seen on the network. For some customers, disabling alert suppression makes sense for this trigger.

Client RADIUS Authentication Issues Trigger

A Client RADIUS Authentication Issues Trigger can help identify devices that are failing authentication over and over, possibly impacting the performance of the authentication server.

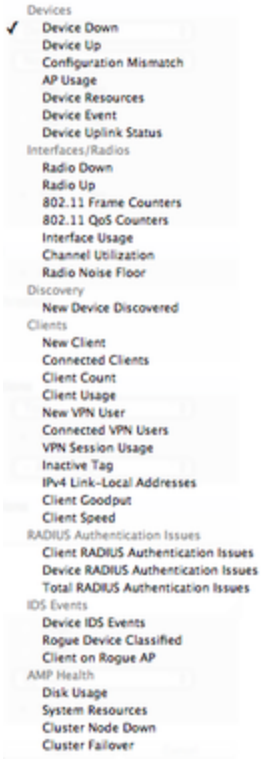
Figure 10: *Client RADIUS Authentication Issues Trigger*



All Triggers

Figure 11 shows a list of all the triggers available in OmniVista 3600 Air Manager 8.0.

Figure 11: *All Triggers*



Which Reports Should I Utilize?

OV3600 includes a powerful, industry leading reporting feature, with customizable reports on devices, clients, the wireless and wired network, and security. This section describes some of the best practices in using reports.

This section includes the following topics:

- "Creating Report Definitions" on page 21
- "Report Types" on page 22

Creating Report Definitions

You can use the following features when defining reports.

Scheduling

When OV3600 is first installed, every type of report is pre-configured to run every night, reporting on the previous day. This is great for giving new customers a look into many of the reporting features, but over time it becomes a lot of data. It's a good idea to figure out what types of reports are most important for each customer and run those as often as it makes sense. Weekly and monthly reports are good for minimizing inbox clutter.

Sharing

- Email: Reports can be emailed in html, pdf, or csv format. Multiple addresses can be separated by spaces, commas, or semicolons.
- External server: Starting with 8.0, reports can be sent via ftp or scp to an external server.

Access to Generated Reports

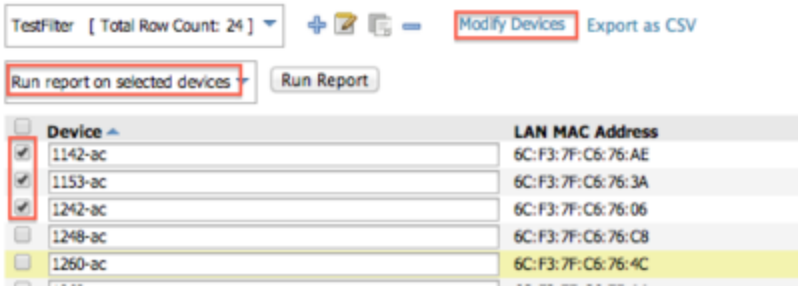
When a report is defined you can choose between two visibility options:

- By Role: Only OV3600 users who have the same user role will be able to see the report. Users from other roles have no access.
- By Subject: If a user's role allows her to view all of the devices/users/rogues in the report, she will be able to access to the report. If the report contains information about any devices/users/rogues that she is not allowed to see, she will not be able to see the report at all.

Creating a Report Using the Modify Devices Feature

Usually, an OV3600 user will create a new report definition by going to the **Reports > Definitions** page and clicking the **Add** button. It's also possible to create a report starting from any device list. Just click **Modify Devices**, choose the devices you want to report on, and click **Run Report**.

Figure 12: *Modify Devices*



Report Types

There are over 20 types of reports in OV3600. Here's a breakdown of them. The most commonly used reports are: Alcatel-Lucent License, Device Summary, Inventory, Client Details, AppRF, and RF Health.

Device Reports

- Alcatel-Lucent License
- Configuration Audit
- Device Summary - shows most- and least-utilized devices based on user count and bandwidth. Also includes an option to show most- and least-utilized folders, which is useful for things like seeing which stores have extreme usage.
- Device Uptime
- Inventory
- Memory and CPU Utilization

Client Reports

- Client Inventory
- Client Details - usage of the wireless network summarized by user device type, OS, user role, SSID and so on.
- New Clients
- VPN Session

Network Reports

- AppRF- Added in 8.0. Shows top destinations and applications, broken down by SSID, user role, and so on.
- Capacity Planning
- Match Event

- Network Usage
- Port Usage
- RF Health - reports on radio data. Which radios have highest utilization, interference MAC/Phy errors etc.

Security Reports

- IDS Events
- New Rogue Devices
- RADIUS Authentication Issues
- Rogue Clients
- Rogue Containment Audit

Custom Reports

A Custom report lets a user choose any widgets from within the other report types, and combine them in any way they like.

With OV3600, you can monitor devices on your network with the click of a button and see real-time statistics as well as historical information. Diagnostic summaries highlight anomalies and situations that can affect end-user network performance. OV3600 includes monitoring views designed to aggregate critical information for the help desk, as well as the high-end monitoring functions network engineers need.

OV3600 monitoring features include:

- The ability to automatically track every user and device – wireless and remote – on the network.
- Visibility into the wired infrastructure that connects wireless controllers and APs.
- Logging and displaying of radio and RADIUS errors, a frequent cause of connectivity problems.
- Rapid drill-downs from network-wide to device-level monitoring view.
- Logging audit and system events to an external syslog server.

Refer to the following sections for information on common monitoring practices that you will utilize on a daily basis.

- "Viewing Device Monitoring Statistics" on page 25
- "Monitoring Data for Wired Devices (Routers and Switches)" on page 26
- "Understanding the APs/Devices > Monitor Pages for all Device Types" on page 27
- "Understanding the APs/Devices > Interfaces Page" on page 27
- "Monitoring with the RF Performance Page" on page 28
- "Viewing Syslog Messages" on page 29

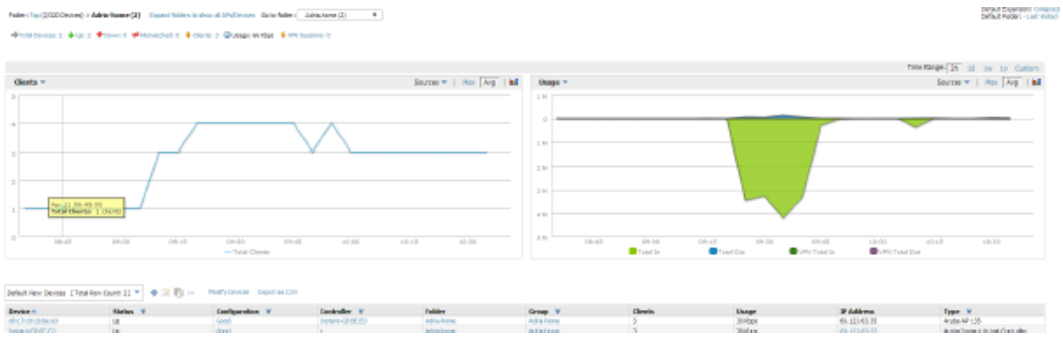
Viewing Device Monitoring Statistics

You can view device monitoring statistics in the **APs/Devices > List** page. The **APs/Devices > List** page displays interactive graphs of Clients and Usage and lists all devices that are managed or monitored by OV3600.

To see only the Up devices, click the **Up** link in the Top Header Stats bar (next to the green arrow). It displays the **APs/Devices > Up** page with the same information, but only containing active devices. You can do the same with the **Down** and **Mismatched** top header stats links.

Use the **Go to folder** field to filter the list by folder, or click **Expand folders to show all APs/Devices** if you are looking at a filtered device list. A lock icon in the **Configuration** column indicates that the device in that row is in **Monitor only** mode.

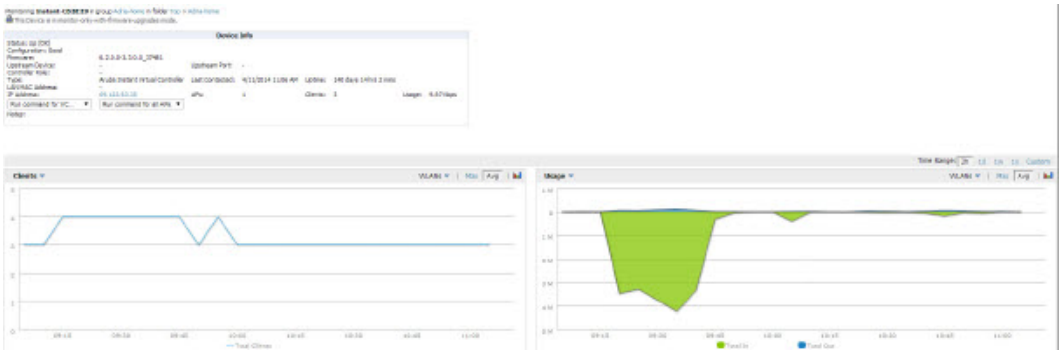
Figure 13: *APs/Devices > List (partial view)*



Monitoring Data for Wired Devices (Routers and Switches)

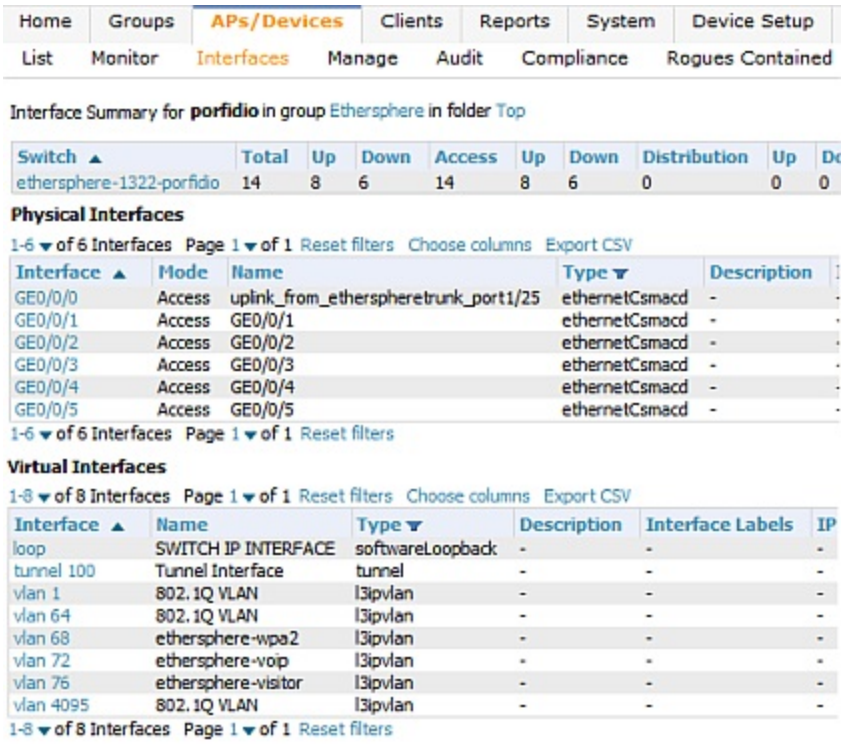
The monitoring page for routers and switches includes basic device information at the top. Beneath that are graphs that display the number of clients and their usage. A menu in each graph allows you to change the graph to view CPU and Memory utilization data.

Figure 14: *APs/Devices > Monitor Page for a Mobility Access Switch*



All managed wired devices include an **Interfaces** subtab, as shown in Figure 15.

Figure 15: *APs/Devices > Interfaces Page for Wired Devices (partial view)*



The top of the **Interfaces** page includes a summary of all interfaces. In the case of stacked switches, the master includes the interfaces of all the members, including its own. The physical and virtual interfaces are displayed in separate tables, labeled **Physical Interfaces** and **Virtual Interfaces**. VLANs are listed below the interface.

NOTE

The Interfaces page for AirMesh APs includes VLANs as part of the Virtual Interfaces. When no management interface is specified, VLAN1 will be treated as management interface. If VLAN1 does not exist, then ethernet 0 will be treated as the management interface.

OV3600 monitors **Up/Down** status and bandwidth information on all interfaces. You can edit multiple interfaces concurrently by selecting one of the two **Edit Interfaces** links. Interface labels are used to group one or more interfaces for the purpose of defining interface bandwidth triggers.

Understanding the APs/Devices > Monitor Pages for all Device Types

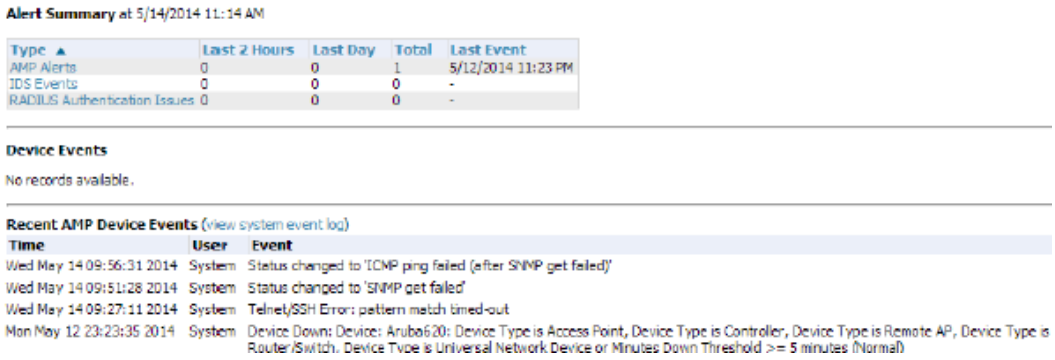
You can quickly go to any device's monitoring page after you go to its specific folder or group on the **APs/Devices > List** page by selecting its hyperlinked name in the **Device** column.

All **Monitor** pages include a section at the top displaying information such as monitoring/configuration status, serial number, total users, firmware version, and so on, as shown in Figure 16.

Figure 16: *Monitoring Page Top-level Data Common to all Device Types*

The alert summary and recent events sections are the same regardless of the device type, and these sections appear toward the bottom of these pages. A link to the Audit Log is available on the bottom of this page. A portion of this page is shown in Figure 17.

Figure 17: *Monitoring Page Bottom Level Data Common to all Device Types (Partial View)*

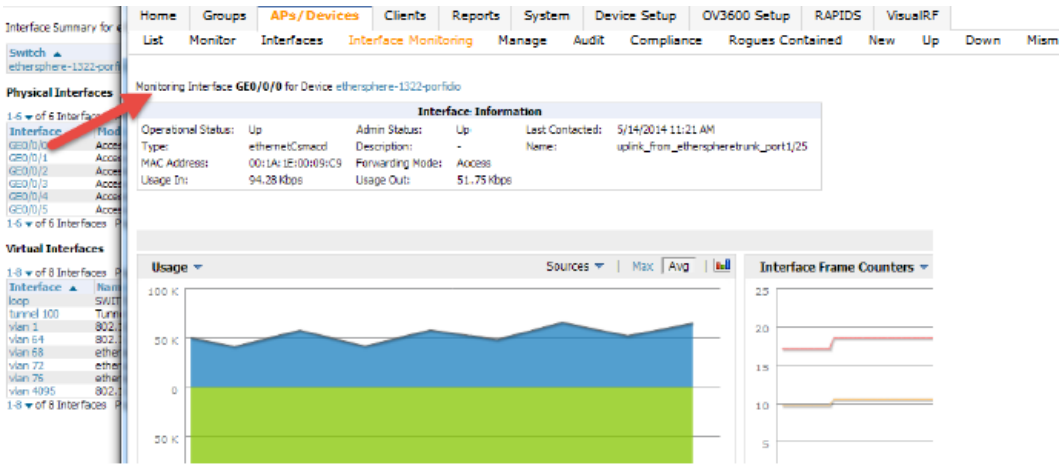


Monitoring pages vary according to whether the devices being monitored are wired routers/switches, controllers/WLAN switches, or thin or fat APs; whether the device is a Mesh device; and whether Spectrum is enabled. These differences are discussed in the sections that follow.

Understanding the APs/Devices > Interfaces Page

The "Monitoring Data for Wired Devices (Routers and Switches)" on page 26 section described how to view high-level interface information for all physical and virtual interfaces on an entire router or switch. Select an interface link in the **Interface** column of the Physical or Virtual Interfaces tables on the stacked switches to go to an **Interface Monitoring** page to display data relevant to that specific interface, as shown Figure 18.

Figure 18: *Interface Monitoring Page for a Wired Device*



An **Interface Monitoring** page has three sections: Interface Information, Usage and Interface Frame Counters graphs, and Connected Clients.

Specifics of the interface are in the Interface Information section, as depicted in Figure 19.

Figure 19: *Individual Interface Information Section*

Monitoring Interface **gigabitethernet0/0/2** for Device S3500-TS-SW

Interface Information					
Operational Status:	Up	Admin Status:	Up	Last Contacted:	6/24/2013 11:19 AM
Type:	etherretCsmacd	Description:	GE0/0/2	Name:	GE0/0/2
MAC Address:	00:0B:86:6A:E0:84	Forwarding Mode:	Access		
Usage In:	0.525 Kbps	Usage Out:	2.48 Kbps		

Bandwidth and other frame-counter information are displayed in the lower section in a tabbed graph, which is shown in Figure 18.

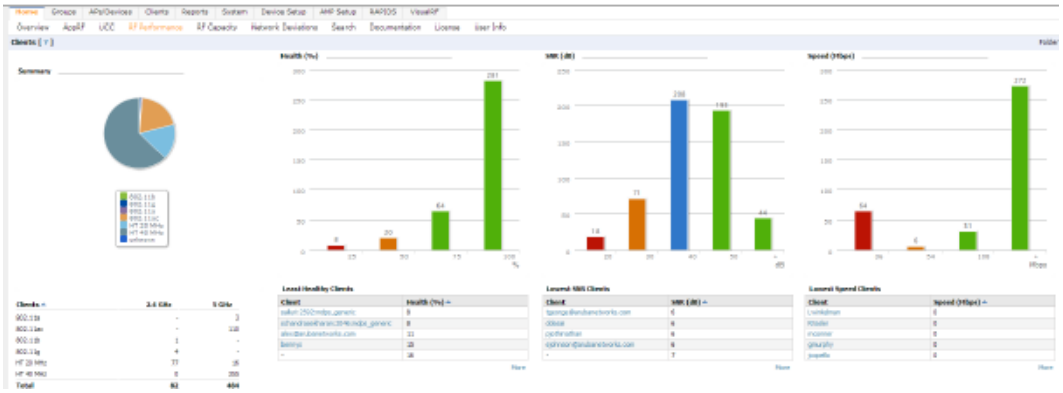
Connected Clients, if any, are listed in a table below the interactive graphs.

Monitoring with the RF Performance Page

The **Home > RF Performance** page provides graphs that enable you to identify clients with low Health, SNR, and Speed rates. In the upper-right corner of this page, you can limit the information that displays by selecting a specific folder.

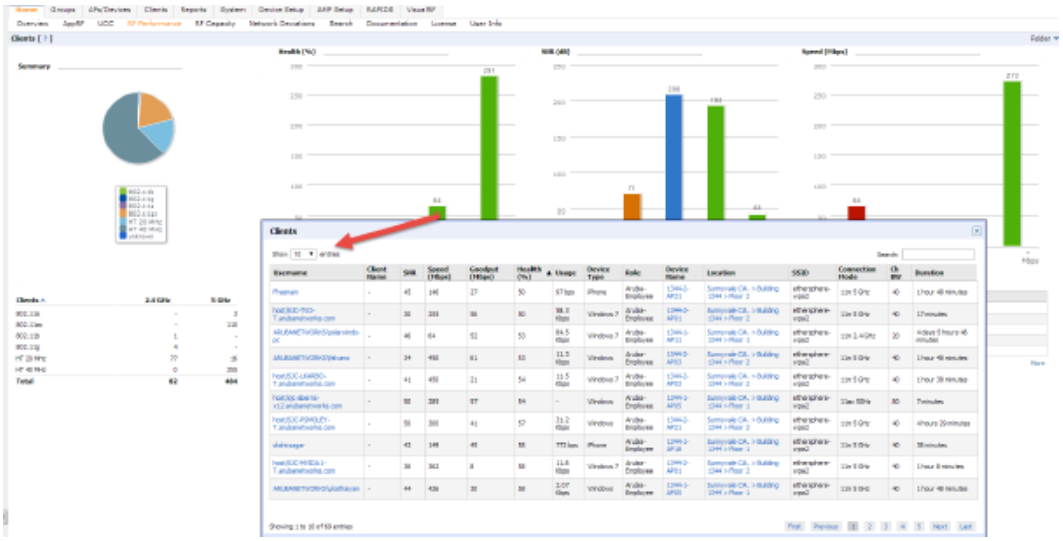
The Health, SNR, and Speed graphs will only be populated with information from Alcatel-Lucent devices that support AMON.

Figure 20: *Home > RF Performance*



Click a value in any graph to view the associated list of clients.

Figure 21: *Drill Down to View all Clients*



When the client information is displayed, click a point on a bar to view information for a specific client, device, or location.

NOTE

After you click a Username in the Client page, the drill down takes you to the **Clients > Diagnostics** page. Navigate to the **Clients > Client Details** page for additional detailed information about the selected client.

Viewing Syslog Messages

OV3600 allows you to specify an external syslog server for storing audit and system events. After the external server is set up, everything written to the OV3600 Event Log and audit logs will be sent to a specified syslog server.

NOTE

You can find the OV3600 event log on the System > Event Log page and at /var/log/ov3600_events from the OV3600 command line.

Perform the following steps to set up an external server

1. Navigate to the **OV3600 Setup > General** page and scroll down to the External Logging section.
2. Enter the IP address and port value of the syslog server.

3. Specify **Yes** for the "Include Event Log Messages" option.
4. Select an Event Log facility from the drop-down list. Typically, facility identifiers local0-local7 are available to the administrator to use as "custom" identifiers. (An exception is local5. On some systems, ftpd defaults to local5.)

Messages "tagged" with these identifiers can be sorted by the syslog server into separate log files. You set this up on the syslog server in the /etc/syslog.conf file.

5. Specify **Yes** for the "Include Audit Log Messages" option.
6. Select an Audit Log facility from the menu.
7. Send a test message to the syslog server.
8. Click **Save**.