

# OmniVista 3600 Air Manager 8.2.14.0



Getting Started Guide

**Copyright**

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit: <https://www.al-enterprise.com/en/legal/trademarks-copyright>. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (April 2020)

**Open Source Code**

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

---

|  |            |
|--|------------|
| <b>Contents</b> .....  | <b>iii</b> |
| <b>Overview of Initial Setup and Common Configurations</b> .....                   | <b>5</b>   |
| <b>Initial Setup</b> .....   | <b>5</b>   |
| <b>How Do I Add Devices?</b> .....   | <b>5</b>   |
| Adding Devices with the Device Setup > Add Page .....                              | 5          |
| <b>How are Folders and Groups Organized?</b> .....                                 | <b>13</b>  |
| Groups .....   | 13         |
| Folders .....  | 14         |
| <b>How Do I Define New Users and Roles?</b> .....                                  | <b>14</b>  |
| <b>How Do I Define Credentials for Devices that Communicate with OV3600?</b> ..... | <b>15</b>  |
| <b>I Have a Mismatch. What Do I Do?</b> .....                                      | <b>17</b>  |
| Auditing to Resolve Mismatches .....   | 17         |
| Importing Group Settings to Resolve Mismatches .....                               | 18         |
| Importing Device Specific Settings .....   | 19         |
| <b>Common Configuration Options</b> .....  | <b>21</b>  |
| <b>How Do I Acknowledge Alerts?</b> .....  | <b>21</b>  |
| Workflow .....   | 21         |
| Auto-Acknowledgement of Device Down Alerts .....                                   | 21         |
| Alert Suppression .....  | 22         |
| <b>Trigger Conditions</b> .....  | <b>22</b>  |
| <b>Notification Options</b> .....  | <b>22</b>  |
| <b>Alert Visibility</b> .....  | <b>22</b>  |
| <b>Which Triggers Are Most Important?</b> .....                                    | <b>22</b>  |
| <b>All Triggers</b> .....  | <b>23</b>  |
| <b>Which Reports Should I Use?</b> .....   | <b>23</b>  |
| Creating Report Definitions .....  | 24         |
| Report Types .....   | 24         |
| Recommended Reports .....  | 30         |
| <b>Monitoring Practices</b> .....  | <b>33</b>  |
| <b>Viewing Device Monitoring Statistics</b> .....                                  | <b>33</b>  |
| <b>Monitoring Data for Wired Devices (Routers and Switches)</b> .....              | <b>34</b>  |

---

|  |           |
|--|-----------|
| <b>Understanding the Devices &gt; Monitor Pages for all Device Types</b> ..... | <b>35</b> |
| <b>Understanding the Devices &gt; Interfaces Page</b> .....                    | <b>36</b> |
| <b>Monitoring with the RF Performance Page</b> .....                           | <b>37</b> |
| <b>Viewing Syslog Messages</b> .....   | <b>38</b> |

This document is designed to help you with your initial setup and provides information on common configuration options and daily monitoring practices.

Refer to the following sections:

- [Initial Setup](#)
- [Common Configuration Options](#)
- [Monitoring Practices](#)

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 help with the tasks:

- [How Do I Add Devices?](#)
- [Discovering New Devices](#)
- [How are Folders and Groups Organized?](#)
- [How Do I Define New Users and Roles?](#)
- [How Do I Define Credentials for Devices that Communicate with OV3600?](#)
- [I Have a Mismatch. What Do I Do?](#)

In many cases, you will add devices after the devices have been discovered. Refer to [Discovering New Devices](#) 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 8.2.14.0 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.

To manually add devices to OV3600:

1. Navigate to **Device Setup > Add**, then select the vendor and model of the device from the drop-down menu.
2. Click **Add**. The Device Setup > Add page displays Device Communications and Location configuration options.

3. Enter the **Device Communications** settings for the new device.

**Figure 1** *Device Communications Settings*

The screenshot shows a form titled "Device Communications" with the following fields and values:

| Field   | Value         |
|---|---------------|
| Name:<br><small>Leave name blank to read it from device</small> | Enter a Value |
| IP Address:   | Enter a Value |
| SNMP Port:  | 161           |
| SSH Port:   | 22            |
| Community String:   | *****         |
| Confirm Community String:                                       | *****         |
| SNMPv3 Username:  | Enter a Value |
| Auth Password:  |               |
| Confirm Auth Password:  |               |
| SNMPv3 Auth Protocol:   | SHA-1         |
| 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:                                      | *****         |

4. In the Location section, select the group and folder for the device from the drop-down menus.
5. At the bottom of the page, select **Monitor Only + Firmware Upgrades** or **Manage read/write**, depending 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. Click **Add** at the bottom of the page.

## 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 8.2.14.0 User Guide*.

- **SNMP/HTTP Discovery Scanning** – This is the primary method for discovering devices. Refer to [Configuring and Running a Scan Set](#) 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 in OV3600 8.2.14.0 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 1 a - 1 d 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 user name 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.




---

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?](#) 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 **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 **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 2](#).

**Figure 2** *Devices > New* page



To discover more devices, visit the [Discover](#) page.

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

Default View: New Devices:Configuration ▾

| DEVI  | TYPE            | LAN MAC ADDRESS   | IP ADDRESS  | DISCOVERED       |
|---|-----------------|-------------------|-------------|------------------|
| <input type="checkbox"/> corvina-dev-1            | Aruba S3500-24P | 00:00:00:00:00:00 | 10.51.3.205 | 7/23/14, 9:32 AM |
| <input type="checkbox"/> Aruba-S3500-25SP-1stFlr3 | Aruba S3500-24T | 00:0B:86:6A:62:00 | 10.51.3.55  | 7/23/14, 9:32 AM |
| <input type="checkbox"/> ArubaS3500-48P           | Aruba S3500-48P | 00:0B:86:6C:1E:00 | 10.51.3.57  | 7/23/14, 9:32 AM |

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 **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 **Monitor 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 **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/SSH to read a device's configuration. SNMP is used for Cisco controllers. OV3600 uses Telnet or SSH to read device configurations from Alcatel-Lucent devices, and wired routers and switches.

Perform these steps to verify the device configuration status:

1. Browse to the **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 **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
- Authentication password
- SNMPv3 auth protocol
- Privacy password
- SNMPv3 privacy protocol
- SNMPv3 user name
- Telnet user name
- 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 3](#).

**Figure 3** *Device Setup > Add > Import Devices via CSV Page Illustration*

Upload a list of devices

| Location |                    |
|----------|--------------------|
| Group:   | IGC <span>▼</span> |
| Folder:  | Top <span>▼</span> |

No file selected.

The list must be in comma-separated values (CSV) format, containing 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  
IP Address is required, the others are optional.  
Type is a case-insensitive string; you can view a list of device types.

Download a sample file or see the example below:

```
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
10.34.64.163,private,switch1.example.com,Router/Switch,nonradiance,md5,privacy123,aes,sv3user,telnetuser,telnetpwd,enable,161
10.172.97.172,private,switch2.example.com,Router/Switch,nonradiance,sha,privacy123,des,user
10.70.36.172,public,Cisco-WLC-4012-3,Cisco 4000 WLC
10.46.111.48,,
```

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](#).

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 **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 **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 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](#); however, additional steps are described to ensure that the controller or switch is configured properly for monitoring.

1. Select the Alcatel-Lucent OmniSwitch Device 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 user name
  - Telnet/SSH password
  - Enable password
5. Assign the device to the correct Group and to a Folder.
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 **Devices > New** page.
10. Select the Alcatel-Lucent switch you just added from the list of new devices.
11. Ensure **Monitor Only** option is selected.
12. Select **Add**.

## Adding as a Management Server

Use the following commands in AOS-W 6.3.1 and later releases. To get the commands for earlier versions of Alcatel-Lucent AOS-W, refer to the *AOS-W Command-Line Interface Reference Guide* for that version.



---

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 or later (to obtain RF utilization metrics) or 6.1 or later (to obtain RF utilization *and* classified interferer information) before you enter this command.

---

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

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

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

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



---

You can add up to four <OV3600-IP> addresses.

---

In order to send UCC, Clarity, Traffic Analysis, and APs/Device data to OV3600, you must enable the following flags in the management server profile (OV3600-profile) on the switch:

- uccmonitoring-enable
- inline-ap-stats
- inline-auth-stats
- inline-dhcp-stats
- inline-dns-stats

- location-enable
- misc-enable
- monitored-info-enable
- sessions-enable
- stats-enable
- tag-enable

## Adding as a Trap Host

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

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

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

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




---

OV3600 supports SNMP v2 traps. For SNMPv3, Airwave support SNMPv3 informs only; SNMPv3 traps are not supported.

---

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 **Devices > Manage** or **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 8.2.14.0 User Guide* for more information.

---

## Folders

The devices on the **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 user 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 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.

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.



---

User name 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 8.2.14.0 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.

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 4](#).

Figure 4 Device Setup > Communication Page (Partial View)

The screenshot displays the 'Default Credentials' section, which includes a list of device models with 'Edit' and 'View' links for each. Below this, the 'SNMP Settings' section contains input fields for 'SNMP Timeout (3-60 sec):' (set to 3) and 'SNMP Retries (1-40):' (set to 3). The 'SNMPv3 Informs' section has an 'Add' button and a 'New SNMPv3 User' link. The 'Telnet/SSH Settings' section has a 'Telnet/SSH Timeout (3-120 sec):' field (set to 10). The 'HTTP Discovery Settings' section has an 'HTTP Timeout (3-120 sec):' field (set to 5). The 'ICMP Settings' section has a radio button selection for 'Attempt to ping devices that were unreachable via SNMP:' with 'Yes' selected. At the bottom, there is a section for 'Symbol 4131 and Cisco Aironet IOS SNMP Initialization' with radio buttons for 'Do not modify SNMP settings' (selected) and 'Enable read-write SNMP'. 'Save' and 'Revert' buttons are at the bottom right.

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

1. Configure default credentials.

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.

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.

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 Conductor switch. In this case, OV3600 recognizes policies defined on a global level (on the conductor switch).

## Auditing to Resolve Mismatches

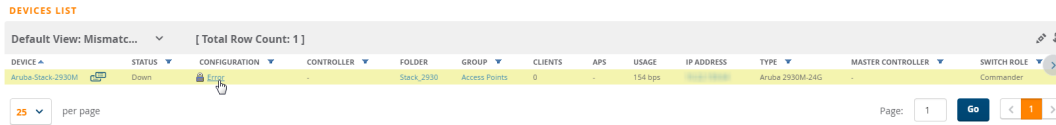
Updating your configuration and then performing an audit on a device can resolve most mismatches.

Follow these steps to audit the device configuration:

1. Make a configuration change on the device.
2. Navigate to **Devices > List** page, then select the device that shows a configuration mismatch. You will go to the view of mismatched devices.

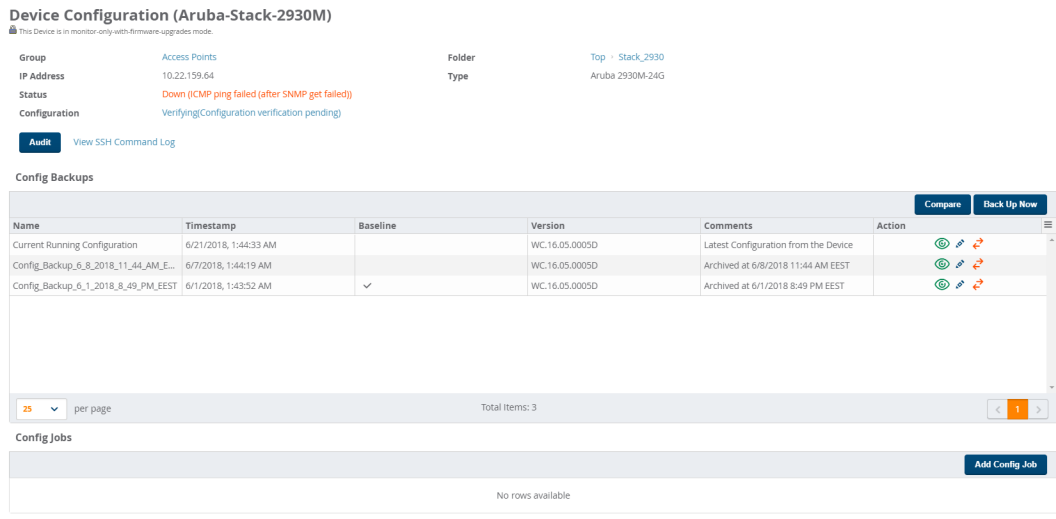
3. Locate the device in the Device List table, then click the configuration link.

**Figure 5** Accessing the Device Configuration Page



4. From the Device Configuration page, click **Audit** to view the current and desired configuration settings. While running the audit, OV3600 will display "pending" for configuration status.

**Figure 6** Pending Audit



5. Review the audit:
  - 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 can be ignored, click **Customize** to select the items that can be ignored during the upcoming audit.
6. 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** 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?](#)
- [Trigger Conditions](#)
- [Notification Options](#)
- [Alert Visibility](#)
- [Which Triggers Are Most Important?](#)
- [All Triggers](#)
- [Which Reports Should I Use?](#)

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 7** Alerts List

1-5 of 6 Alerts Page 1 of 2 > | Choose columns Export CSV

| Alerts                   |                |   |                  |
|--------------------------|----------------|---|------------------|
|                          | TRIGGER TYPE ▲ | TRIGGER SUMMARY   | TRIGGERING AGENT |
| <input type="checkbox"/> | Device Down    | Device has rebooted: Device uptime value changed (current: <a href="#">more...</a> )  | SH-4F-004        |
| <input type="checkbox"/> | Device Down    | Device has rebooted: Device uptime value changed (current: <a href="#">more...</a> )  | SH-4F-005        |
| <input type="checkbox"/> | Device Down    | Device has rebooted: Device uptime value changed (current: <a href="#">more...</a> )  | SH-4F-005        |
| <input type="checkbox"/> | Device Down    | Device has rebooted: Device uptime value changed (current: <a href="#">more...</a> )  | SH-4F-005        |
| <input type="checkbox"/> | Device Down    | Device Type is Access Point, Device Type is Access Point, ( <a href="#">more...</a> ) | rap3             |
| <input type="checkbox"/> | Device Down    | Device Type is Access Point   | rap3             |

1-5 of 6 Alerts Page 1 of 2 > |  
[Select All](#) - [Unselect All](#)  
[Acknowledge](#) [Delete](#)  
[View Acknowledged Alerts](#)

## 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, its 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.

You can fine-tune when OV3600 sends alerts by setting trigger conditions. For many types of triggers, you can use multiple conditions. When you configure multiple trigger conditions, you decide whether all trigger conditions must match, or just a few.

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.

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.

Enable the following triggers every time you install a new OV3600 server:

- **Device Down.** Configure a separate trigger for controllers, access points, and routers or switches because they have different severity levels. Use the trigger condition to specify the device type.
- **Device Up.** Configure this trigger by setting the **Auto Acknowledge Up/Down Alerts** option to **Up and Down**, thereby acknowledging Device Down alerts when the device returns online.

- **Channel Utilization.** Configure this trigger to receive notifications of high utilization or high interference. An interference percentage of 30-40% makes a good starting point. For example, add a trigger condition by setting the **Time Busy (%)** option to **>= 80** and the **Interference (%)** option to **>= 30**.
- **Rogue Device Classified.** Configure this trigger to alert you when OV3600 detects devices classified as rogue or greater.
- **Connected Clients.** Configure this trigger with the device MAC address, so that, when the device is missing, OV3600 sends an alert whenever the device is seen on the network. For some customers, disabling alert suppression makes sense when enabling this trigger.
- **Client RADIUS Authentication Issues.** Configure this trigger to identify devices that fail continuously to authenticate and avoid performance issues with the authentication server. For example, add a trigger condition to receive an alert after 10 counts.

You can configure all triggers from the **System > Triggers** page. OV3600 8.2.14.0 includes the following triggers:

- |  |  |   |
|--|--|---|
| <ul style="list-style-type: none"> <li>■ <b>Devices</b></li> <li>○ Device Down</li> <li>○ Device Up</li> <li>○ Configuration Mismatch</li> <li>○ AP Usage</li> <li>○ Device Resources</li> <li>○ Device Event</li> <li>○ Device Uplink Status</li> <li>○ AP Uplink Speed</li> <li>○ Controller Cluster Trigger</li> <li>○ Device Crash</li> <li>■ <b>Interfaces/Radios</b></li> <li>○ Radio Down</li> <li>○ Radio Up</li> <li>○ 802.11 Frame Counters</li> <li>○ 802.11 QoS Counters</li> <li>○ Interface Usage</li> <li>○ Interface Errors</li> <li>○ Channel Utilization</li> <li>○ Radio Noise Floor</li> <li>○ Channel Change</li> </ul> | <ul style="list-style-type: none"> <li>■ <b>Discovery</b></li> <li>○ New Devices Discovered</li> <li>■ <b>Clients</b></li> <li>○ New Clients</li> <li>○ Connected Clients</li> <li>○ Client Count</li> <li>○ Client Usage</li> <li>○ New VPN User</li> <li>○ Connected VPN Users</li> <li>○ VPN Session Usage</li> <li>○ Inactive Tag</li> <li>○ IPv4 Link-Local Addresses</li> <li>○ Client Goodput</li> <li>○ Client Speed</li> <li>○ Disconnected VPN Users</li> <li>○ Disconnected Clients</li> <li>■ <b>RADIUS Authentication Issues</b></li> <li>○ Client RADIUS Authentication Issues</li> <li>○ Device RADIUS Authentication Issues</li> <li>○ Total RADIUS Authentication Issues</li> </ul> | <ul style="list-style-type: none"> <li>■ <b>RADIUS Accounting Issues</b></li> <li>○ Client RADIUS Accounting Issues</li> <li>○ Device RADIUS Accounting Issues</li> <li>○ Total RADIUS Accounting Issues</li> <li>■ <b>IDS Events</b></li> <li>○ Device IDS Events</li> <li>○ Rogue Device Classified</li> <li>○ Client on Rogue AP</li> <li>○ OV3600 Health</li> <li>○ Disk Usage</li> <li>○ System Resources</li> <li>○ VisualRF Down</li> <li>■ <b>Clarity</b></li> <li>○ Authentication Time</li> <li>○ DHCP Response Time</li> <li>■ <b>GRE Tunnels</b></li> <li>○ Tunnel Up</li> <li>○ Tunnel Down</li> <li>○ Tunnel Group</li> <li>○ Tunnel Duplicate Id</li> <li>○ Tunnel Duplicate Ip</li> </ul> |
|--|--|---|

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](#)
- [Report Types](#)
- [Recommended Reports](#)

## 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: 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 the modify icon () on right side of the table title bar, choose the devices on which you want to report, then click **Run Report**.

**Figure 8** *Modify Devices*

| CONTROLLER   | FOLDER | GROUP | CLIENTS | USAGE | IP ADDRESS    | TYPE          |
|--------------|--------|-------|---------|-------|---------------|---------------|
| 7210-alpha-1 | Top    | APs   | 0       | 0 bps | 10.20.101.229 | Aruba AP 205H |
| 7210-alpha-1 | Top    | APs   | 0       | 0 bps | 10.20.101.240 | Aruba AP 205H |
| 7210-alpha-1 | Top    | APs   | 0       | 0 bps | 10.20.101.227 | Aruba AP 205H |
| 7210-alpha-1 | Top    | APs   | 0       | 0 bps | 10.20.101.228 | Aruba AP 205H |

## Report Types



OV3600 has multiple predefined reports that contain one or more sections of data, (also called widgets). The most commonly used reports are the Alcatel-Lucent 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.

## Traffic Analysis Report Widgets

- Top Applications Summary
- Top Destinations Summary
- Top 10 Applications By Device Types
- Top 10 Applications By User Roles
- Top 10 Applications By SSIDs
- Top 3 Applications For Top 10 Users
- User Detail

## Alcatel-Lucent License Report Widgets

- License Info

## Capacity Planning Report Widgets

- Summary
- Interface Usage
- Interfaces Vs. Percent of Time Above Threshold
- Raw Capacity Data

## Client Inventory Report Widgets

- AOS Device Type Summary
- Device Type Summary
- Device Manufacturer and Model Summary
- Device Manufacturer Summary
- Device Model Summary
- OS Summary
- Device OS Detail Summary
- Network Vendor Summary
- Network Chipset Summary
- Network Driver Summary
- EAP Supplicant Summary
- Asset Group Summary
- Asset Category Summary
- Last SSID Summary
- Last Alcatel-Lucent Role Summary
- Last Connection Mode Summary
- Last Auth. Type Summary
- Clients

## Client Session Report Widgets

- Session Data by OS (List)
- Session Data by OS (Charts)
- Session Data by OS Detail (List)
- Session Data by OS Detail (Charts)
- Session Data by Model (List)
- Session Data by Model (Charts)
- Session Data by Manufacturer (List)
- Session Data by Manufacturer (Charts)
- Session Data by Device Type (List)
- Session Data by Device Type (Charts)
- Session Data by AOS Device Type (List)
- Session Data by AOS Device Type (Charts)
- Session Data by Network Interface Vendor (List)
- Session Data by Network Interface Vendor (Charts)
- Session Data by Network Chipset (List)
- Session Data by Network Chipset (Charts)
- Session Data by Network Driver (List)
- Session Data by Network Driver (Charts)
- Session Data by EAP Supplicant (List)
- Session Data by EAP Supplicant (Charts)
- Session Data by Asset Group (List)
- Session Data by Asset Group (Charts)
- Session Data by Asset Category (List)
- Session Data by Asset Category (Charts)
- Session Data by Connection Mode (List)
- Session Data by Connection Mode (Charts)
- Session Data by SSID (List)
- Session Data by SSID (Charts)
- Session Data by Role (List)
- Session Data by Role (Charts)
- Session Data by VLAN (List)
- Session Data by VLAN (Charts)
- Session Data by Cipher (List)
- Session Data by Cipher (Charts)
- Top Clients by Total MB Used
- Top Clients by Total MB Used by Folder
- Summary
- Sessions
- Session Data by Client

## Configuration Audit Report Widgets

- Detail

## Device Summary Report Widgets

- Most Utilized Folders by Maximum Concurrent Clients
- Most Utilized Folders by Usage
- Most Utilized by Maximum Concurrent Clients
- Most Utilized by Usage
- Least Utilized by Maximum Concurrent Clients
- Least Utilized by Usage
- Devices

## Device Uptime Report Widgets

- Avg Uptime by Device
- Avg Uptime by Any AP
- Avg Uptime by Any Controller
- Avg Uptime by Any Switch
- Avg Uptime by Group
- Avg Uptime by Folder
- Device Downtime Detail
- Uptime by Device

## IDS Events Report Widgets

- Top IDS Events by Device
- Top IDS Events by Controller
- Raw IDS Data

## Inventory Report Widgets

- Vendor Summary
- Firmware Version Summary
- Model/Firmware Version Summary
- Bootloader Version Summary
- Model/Bootloader Version Summary
- Type Summary
- Model Summary
- Alcatel-Lucent AP Interfaces Summary
- Devices

## Match Event Report Widgets

- By Folder
- By AP
- By Client
- Details

- Device Type Summary
- Reasons for Match Summary
- Connection Mode Summary

## Memory and CPU Utilization Report Widgets

- Top CPU Utilization by Device
- Top Memory Usage by Device
- CPU Utilization Details
- Memory Usage Details

## Network Usage Report Widgets

- Usage
- Client Count
- Usage and Client Count by Folder
- Usage by SSID
- Total Usage

## New Clients Report Widgets

- Detail

## New Rogue Devices Report Widgets

- Devices by RAPIDS Classification
- Devices by Controller Classification
- Top Rogue Devices by Discovering APs
- Top Rogue Devices by Signal Strength
- Devices by LAN MAC Address Vendor
- Devices by Radio MAC Address Vendor
- Summary
- Devices Discovered Wirelessly and on the LAN
- Devices Discovered Only Wirelessly
- Devices Discovered on the LAN Only
- All Rogue Devices
- Discovery Events

## Port Usage Report Widgets

- Summary
- Folder Summary
- Histogram
- Most Utilized Switches
- Most Utilized Ports
- Switches
- Ports

## RADIUS Issues Report Widgets

- Top 10 RADIUS Issues by Device
- Top 10 RADIUS Issues by Controller
- Top 10 RADIUS Issues by RADIUS Server
- Top 10 RADIUS Issues by Client
- RADIUS Issues

## RF Health Report Widgets

- Thresholds
- Top Folders By Worst Client and Radio Statistics Combined 2.4 GHz and 5 GHz
- Radio Statistics by Folder - Combined 2.4 GHz and 5 GHz
- Top Folders By Worst Client and Radio Statistics 2.4 GHz
- Radio Statistics by Folder - 2.4 GHz
- Top Folders By Worst Client and Radio Statistics 5 GHz
- Radio Statistics by Folder - 5 GHz
- Problem 5 GHz Radios
- Problem 2.4 GHz Radios
- Most Noise (5 GHz)
- Most Noise (2.4 GHz)
- Most Interfering Devices (5 GHz)
- Most Interfering Devices (2.4 GHz)
- Most Utilized by Channel Usage (5 GHz)
- Most Utilized by Channel Usage (2.4 GHz)
- Least Utilized by Channel Usage (5 GHz)
- Least Utilized by Channel Usage (2.4 GHz)
- Most MAC/Phy Errors (5 GHz)
- Most MAC/Phy Errors (2.4 GHz)
- Most Channel Changes (5 GHz)
- Most Channel Changes (2.4 GHz)
- Most Mode Changes (5 GHz)
- Most Mode Changes (2.4 GHz)
- Most Transmit Power Changes (5 GHz)
- Most Transmit Power Changes (2.4 GHz)
- Clients with Least Goodput
- Clients with Least Speed
- Radios with Least Goodput

## Rogue Clients Report Widgets

- Clients Per Classification
- Misassociations by Rogue APs

- Misassociations by Rogue Clients
- Details

## Rogue Containment Audit Report Widgets

- Rogue Containment by Controller

## UCC Report Widgets

- Thresholds and Filters
- UCC Data by Call Quality (List)
- UCC Data by Call Quality (Charts)
- UCC Data by Connectivity Type (List)
- UCC Data by Connectivity Type (Charts)
- UCC Data by Call Type (List)
- UCC Data by Call Type (Charts)
- UCC Data by Application Type (List)
- UCC Data by Application Type (Charts)
- UCC Data by Device Type (List)
- UCC Data by Device Type (Charts)
- Folders by Poor Call Quality
- APs by Poor Call Quality
- Clients by Poor Call Quality

## VPN Session Report Widgets

- Session Data by VLAN (List)
- Session Data by VLAN (Charts)
- Session Data by VPN Type (List)
- Session Data by VPN Type (Charts)
- Session Data by Controller (List)
- Session Data by Controller (Charts)
- Session Data by HTTP Fingerprint (List)
- Session Data by HTTP Fingerprint (Charts)
- Session Data by AOS Device Type (List)
- Session Data by AOS Device Type (Charts)
- Summary
- Session Data by Users
- Sessions

## Recommended Reports

Although OV3600 includes a large number of report types, Alcatel-Lucent recommends running the following reports on a regular basis, as these reports supply helpful information for monitoring, managing and troubleshooting your network.

1. [Client Session Reports](#)
2. [RF Health Reports](#)
3. [Network Usage Reports](#)
4. [Device Summary Reports](#)
5. [Traffic Analysis Reports](#)





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](#)
- [Monitoring Data for Wired Devices \(Routers and Switches\)](#)
- [Understanding the Devices > Monitor Pages for all Device Types](#)
- [Understanding the Devices > Interfaces Page](#)
- [Monitoring with the RF Performance Page](#)
- [Viewing Syslog Messages](#)

You can view device monitoring statistics in the **Devices > List** page. The **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**. It displays the **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** drop-down list at the top of the page to filter the list by folder, or click **Expand folders to show all 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 9** *Devices > List (partial view)*

Go to folder: Top (41/77 Devices)

|                      |                   |                |              |                     |
|----------------------|-------------------|----------------|--------------|---------------------|
| <b>TOTAL DEVICES</b> | <b>MISMATCHED</b> | <b>CLIENTS</b> | <b>USAGE</b> | <b>VPN SESSIONS</b> |
| 41 ↑ 39 ↓ 2          | 1                 | 0              | -            | 0                   |



Default View: Devices [ Total Row Count: 41 ]

| DEVICE     | STATUS | CONFIGURATION | CONTROLLER | FOLDER | GROUP         | CLIENTS | USAGE   | IP ADDRESS   | TYPE         |
|------------|--------|---------------|------------|--------|---------------|---------|---------|--------------|--------------|
| Chuckwagon | Up     | Mismatched    | -          | Top    | Access Points | 0       | 544 bps | 10.11.0.11   | Aruba 7220   |
| (id: 62)   | Down   | Unknown       | -          | Top    | Access Points | 0       | 0 bps   | 192.168.0.10 | Aruba Device |
| 1341-AP122 | Up     | Good          | Chuckwagon | Top    | Access Points | 0       | 0 bps   | 10.6.130.157 | Aruba AP 325 |
| 1341-AP126 | Up     | Good          | Chuckwagon | Top    | Access Points | 0       | 0 bps   | 10.6.130.177 | Aruba AP 325 |
| 1341-AP107 | Up     | Good          | Chuckwagon | Top    | Access Points | 0       | 0 bps   | 10.6.130.158 | Aruba AP 325 |
| 1341-AP105 | Up     | Good          | Chuckwagon | Top    | Access Points | 0       | 0 bps   | 10.6.130.163 | Aruba AP 325 |
| 1341-AP109 | Up     | Good          | Chuckwagon | Top    | Access Points | 0       | 0 bps   | 10.6.130.170 | Aruba AP 325 |
| 1341-AP104 | Up     | Good          | Chuckwagon | Top    | Access Points | 0       | 0 bps   | 10.6.130.161 | Aruba AP 325 |
| 1341-AP110 | Up     | Good          | Chuckwagon | Top    | Access Points | 0       | 0 bps   | 10.6.130.141 | Aruba AP 325 |
| 1341-AP127 | Up     | Good          | Chuckwagon | Top    | Access Points | 0       | 0 bps   | 10.6.130.175 | Aruba AP 325 |

10 per page Page: 1 Go

Alert Summary updated at 1/21/2016 4:41 PM PST

| TYPE          | LAST 2 HOURS | LAST DAY | TOTAL | LAST EVENT |
|---------------|--------------|----------|-------|------------|
| AMP Alerts    | 0            | 0        | 0     | -          |
| IDS Events    | 0            | 0        | 0     | -          |
| RADIUS Issues | 0            | 0        | 0     | -          |

| FOLDER   | APS/DEVICES |
|----------|-------------|
| iap_test | 2           |
| ...      | ...         |

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.

All managed wired devices include an **Interfaces** subtab, as shown in [Figure 10](#).

**Figure 10** *Devices > Interfaces Page for Wired Devices (partial view)*

Interface Summary for :

7210-alpha-1 in group Controllers in folder Top > Bangalore > Bangalore 4

| SWITCH ▲     | TOTAL | UP | DOWN | ACCESS | UP | DOWN | DISTRIBUTION | UP | DOWN |
|--------------|-------|----|------|--------|----|------|--------------|----|------|
| 7210-alpha-1 | 15    | 10 | 5    | 15     | 10 | 5    | 0            | 0  | 0    |

1-6 of 6 Interfaces Page 1 of 1 Reset filters Choose columns Export CSV

| Physical Interfaces |        |         |                |             |                  |                   |                |                      |  |
|---------------------|--------|---------|----------------|-------------|------------------|-------------------|----------------|----------------------|--|
| INTERFACE ▲         | MODE   | NAME    | TYPE ▼         | DESCRIPTION | INTERFACE LABELS | MAC ADDRESS       | ADMIN STATUS ▼ | OPERATIONAL STATUS ▼ |  |
| GE0/0/0             | Access | GE0/0/0 | ethernetCsmacd | GE0/0/0     | -                | 00:1A:1E:01:5C:81 | Up             | Up                   |  |
| GE0/0/1             | Access | GE0/0/1 | ethernetCsmacd | GE0/0/1     | -                | 00:1A:1E:01:5C:82 | Up             | Down                 |  |
| GE0/0/2             | Access | GE0/0/2 | ethernetCsmacd | GE0/0/2     | -                | 00:1A:1E:01:5C:83 | Up             | Down                 |  |
| GE0/0/3             | Access | GE0/0/3 | ethernetCsmacd | GE0/0/3     | -                | 00:1A:1E:01:5C:84 | Up             | Down                 |  |
| GE0/0/4             | Access | GE0/0/4 | ethernetCsmacd | GE0/0/4     | -                | 00:1A:1E:01:5C:85 | Up             | Down                 |  |
| GE0/0/5             | Access | GE0/0/5 | ethernetCsmacd | GE0/0/5     | -                | 00:1A:1E:01:5C:86 | Up             | Down                 |  |

1-6 of 6 Interfaces Page 1 of 1 Reset filters

1-9 of 9 Interfaces Page 1 of 1 Reset filters Choose columns Export CSV

| Virtual Interfaces |                     |                  |                     |                  |            |                   |                |  |
|--------------------|---------------------|------------------|---------------------|------------------|------------|-------------------|----------------|--|
| INTERFACE ▲        | NAME                | TYPE ▼           | DESCRIPTION         | INTERFACE LABELS | IP ADDRESS | MAC ADDRESS       | ADMIN STATUS ▼ |  |
| loop               | SWITCH IP INTERFACE | softwareLoopback | SWITCH IP INTERFACE | -                | -          | 00:1A:1E:01:5C:80 | Up             |  |
| vlan 1             | 802.1Q VLAN         | I3ipvlan         | 802.1Q VLAN         | -                | -          | 00:1A:1E:01:5C:80 | Up             |  |
| vlan 101           | 802.1Q VLAN         | I3ipvlan         | 802.1Q VLAN         | -                | -          | 00:1A:1E:01:5C:80 | Up             |  |
| vlan 102           | 802.1Q VLAN         | I3ipvlan         | 802.1Q VLAN         | -                | -          | 00:1A:1E:01:5C:80 | Up             |  |
| vlan 103           | 802.1Q VLAN         | I3ipvlan         | 802.1Q VLAN         | -                | -          | 00:1A:1E:01:5C:80 | Up             |  |
| vlan 104           | 802.1Q VLAN         | I3ipvlan         | 802.1Q VLAN         | -                | -          | 00:1A:1E:01:5C:80 | Up             |  |
| vlan 105           | 802.1Q VLAN         | I3ipvlan         | 802.1Q VLAN         | -                | -          | 00:1A:1E:01:5C:80 | Up             |  |
| vlan 2000          | 802.1Q VLAN         | I3ipvlan         | 802.1Q VLAN         | -                | -          | 00:1A:1E:01:5C:80 | Up             |  |

The top of the **Interfaces** page includes a summary of all interfaces. In the case of stacked switches, the conductor 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.



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.

You can quickly go to any device's monitoring page after you go to its specific folder or group on the **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 11](#).

**Figure 11** Monitoring Page Top-level Data Common to all Device Types

| Device Info         |   |                          |                                |          |                        |
|---------------------|---|--------------------------|--------------------------------|----------|------------------------|
| Status: Up (OK)     |   |                          |                                |          |                        |
| Configuration: Good |   |                          |                                |          |                        |
| Firmware:           | 6.4.4.3                                   | <a href="#">Licenses</a> |                                |          |                        |
| Upstream Device:    | -   | Upstream Port:           | -                              |          |                        |
| Controller Role:    | Master                                    |                          |                                |          |                        |
| Type:               | Aruba 7220                                | Last Contacted:          | 1/21/2016 3:32 PM PST          | Uptime:  | 32 days 15 hrs 29 mins |
| LAN MAC Address:    | 00:1A:1E:00:0E:28                         | Serial:                  | BB0000118                      |          |                        |
| Location:           | 1344-1 Rack 28                            | Contact:                 | -                              |          |                        |
| IP Address:         | 10.11.0.11                                | APs:                     | 38                             | Clients: | 22                     |
| VPN Sessions:       | 0   | VPN Usage:               | -                              |          |                        |
| Quick Links:        | <a href="#">Open controller web UI...</a> |                          | <a href="#">Run command...</a> |          |                        |
| Notes:              |   |                          |                                |          |                        |

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 12](#).

**Figure 12** Monitoring Page Bottom Level Data Common to all Device Types (Partial View)

| Alert Summary updated at 1/21/2016 3:43 PM PST |              |          |       |            |
|--|--------------|----------|-------|------------|
| TYPE ▲   | LAST 2 HOURS | LAST DAY | TOTAL | LAST EVENT |
| AMP Alerts                                     | 0            | 0        | 0     | -          |
| IDS Events                                     | 0            | 0        | 0     | -          |
| RADIUS Issues                                  | 0            | 0        | 0     | -          |

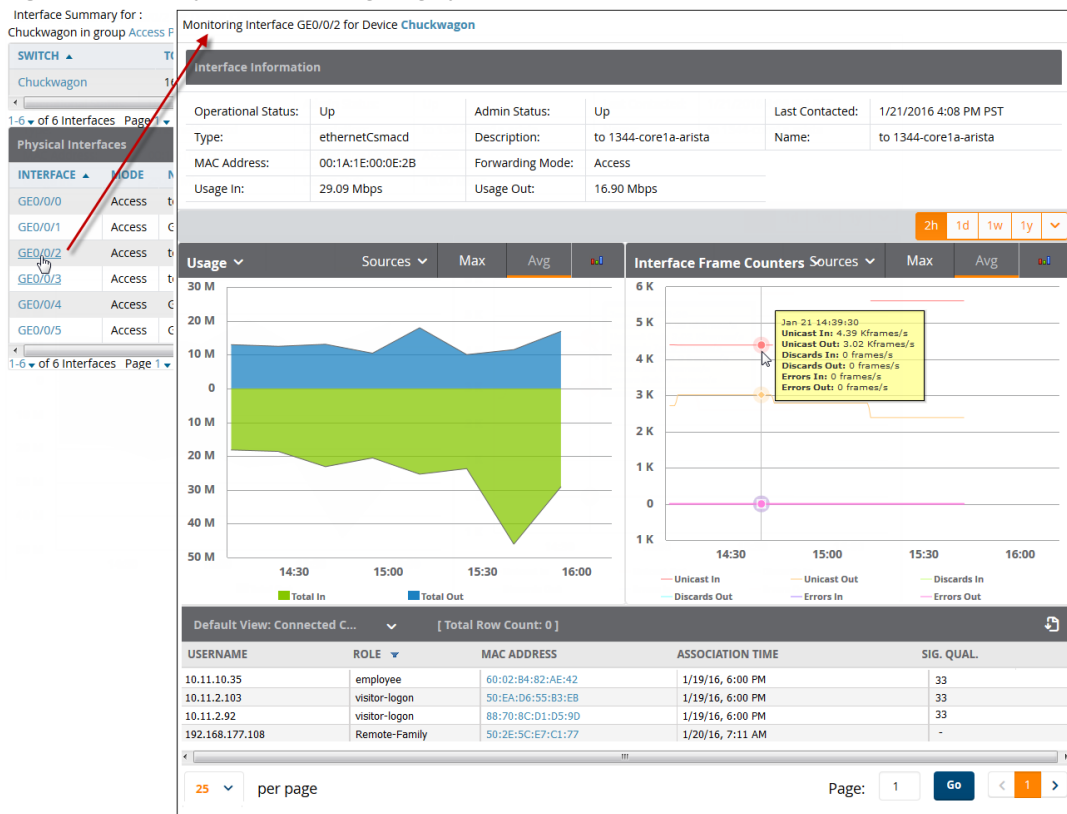
**DEVICE EVENTS**  
No records available.

| Recent AMP Device Events (view system event log) |        |   |
|--|--------|---|
| TIME   | USER   | EVENT   |
| Thu Jan 21 04:23:57 2016                         | System | Configuration verification succeeded; configuration is good |
|  |        | ...omitted 28 duplicate messages...                         |
| Fri Dec 25 04:23:55 2015                         | System | Configuration verification succeeded; configuration is good |

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.

The [Monitoring Data for Wired Devices \(Routers and Switches\)](#) on page 34 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 13](#).

**Figure 13** Interface Monitoring Page for a Wired Device



An **Interface Monitoring** page has three sections. The **Interface Information** table at the top of the page displays specific details about the interface, the **Usage** and **Interface Frame Counters** graphs appear in the middle of the page, and the **Connected Clients** table at the bottom of the page lists the user name, role, MAC address, association time and signal quality for any connected clients.

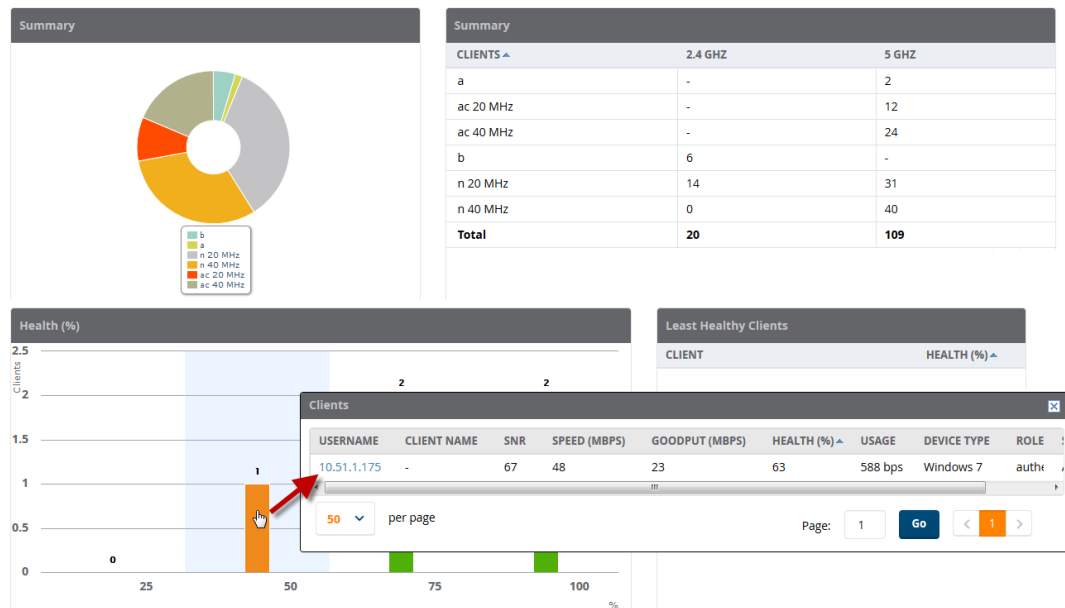
The **Home > RF Performance** page provides graphs that enable you to identify clients with poor health, Signal-to-noise (SNR) ratios, and speed rates. In the upper-right corner of this page, you can limit the information that displays by selecting a specific folder.



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

Click any graph to view information for a specific client, device, or location. As shown in [Figure 14](#), clicking on a bar in the **Health** graph opens a popup window that displays information for those clients.

**Figure 14** Drill Down to View Client Data



Click any user name in the **Clients** popup window to open the **Clients > Diagnostics** page and view additional detailed information about the selected client.

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.



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

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 local.



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**.