OmniVista 3600 Air Manager

Version 7.2

Alcatel·Lucent

User Guide

Copyright

Specifications in this manual are subject to change without notice.

Originated in the USA.

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 are trademarks of Alcatel-Lucent in the United States and certain other countries.

Any other trademarks appearing in this manual are the property of their respective companies.

Legal Notice

The use of Alcatel-Lucent switching platforms and software, by all individuals or corporations, to terminate Cisco or Nortel VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Alcatel-Lucent from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of Cisco Systems or Nortel Networks.

Alcatel·Lucent

www.alcatel-lucent.com

26801 West Agoura Road
Calabasas, CA 91301

Contents

Preface

This preface provides an overview of this guide, a list of all documentation available for OV3600 7.2, including contact information for Alcatel-Lucent, and includes the following sections:

- "Document Organization" on page 11
- "Notice Icons" on page 12
- "Contacting Support" on page 12

Document Organization

This user guide includes instructions and examples of the graphical user interface (GUI) for installation, configuration, and daily operation of OmniVista 3600 Air Manager™. This includes wide deployment of wireless access points (APs), device administration, rogue detection and classification, wireless controller devices, security, reports, and additional features of OV3600.

Table 1 *Document Organization and Purposes*

Chapter	Description
Chapter 1, "Introduction"	Introduces and presents the OmniVista 3600 Air Manager, components, and general network functions.
Chapter 2, "Installing OV3600"	Describes system and network requirements, Linux OS installation, and OV3600 installation.
Chapter 3, "Configuring OV3600"	Describes the primary and required configurations for startup and launch of OV3600, with frequently used optional configurations.
Chapter 4, "Configuring and Using Device Groups in OV3600"	Describes configuration and deployment for group device profiles.
Chapter 5, "Discovering, Adding, and Managing Devices"	Describes how to discover and manage devices on the network.
Chapter 6, "Creating and Using Templates"	Describes and illustrates the use of templates in group and global device configuration.
Chapter 7, "Using RAPIDS and Rogue Classification"	Describes the RAPIDS module of OV3600, and enhanced rogue classification supported in OV3600.
Chapter 8, "Performing Daily Administration in OV3600"	Describes common daily operations and tools in OV3600, to include general user administration, the use of triggers and alerts, network monitoring, and backups.
Chapter 9, "Creating, Running, and Emailing Reports"	Describes OV3600 reports, scheduling and generation options, and distribution of reports from OV3600.
Chapter 10, "Using the OV3600 Helpdesk"	Describes how to use the OV3600 Helpdesk GUI and related functions.
Appendix A, "Package Management for OV3600"	Describes the Yum packaging management system, and provides advisories on alternative methods that may cause issues with OV3600.
Appendix B, "Third-Party Security Integration for OV3600"	Describes additional and optional security configurations in OV3600.
Appendix C, "Access Point Notes"	Provides guidelines and suggestions for APs in OV3600.

Table 1 *Document Organization and Purposes*

Chapter	Description
Appendix D, “Initiating a Support Connection”	Provides instructions about how to create and use a support connection between OV3600 and Alcatel-Lucent Support.
Appendix E, “Cisco Clean Access Integration (Perfigo)”	Provides instructions for integrating Cisco Clean Access within OV3600.
Appendix F, “HP Insight Install Instructions for OV3600 Servers”	Provides instructions for installing HP Insight on OV3600 servers.
Appendix G, “Installing OV3600 on VMware ESX (3i v. 3.5)”	Provides instructions for an alternative installation option on VMware ESX for OV3600.
Appendix H, “Third-Party Copyright Information”	Presents multiple copyright statements from multiple equipment vendors that interoperate with OV3600.
Index	Provides extensive citation of and links to document topics, with emphasis on the OV3600 GUI and tasks relating to OV3600 installation and operation.

Notice Icons

This document uses the following notice icons to emphasize advisories for certain actions, configurations, or concepts:

NOTE

Indicates helpful suggestions, pertinent information, and important things to remember.

CAUTION

Indicates a risk of damage to your hardware or loss of data.

WARNING

Indicates a risk of personal injury or death.

Contacting Support

Table 2 *Alcatel-Lucent Contact Information*

Online Contact and Support	
Main Website	http://www.alcatel-lucent.com/enterprise
Support Website	http://service.esd.alcatel-lucent.com
Alcatel-Lucent Enterprise Service and OmniVista 3600 Email Support	Esd.support@alcatel-lucent.com

Chapter 1

Introduction

Thank you for choosing OmniVista3600 Air Manager (OV3600), or OV3600. OV3600 makes it easy and efficient to manage your wireless network by combining industry-leading functionality with an intuitive user interface, enabling network administrators and helpdesk staff to support and control even the largest wireless networks in the world.

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

- "OV3600—A Unified Wireless Network Command Center" on page 13
- "Integrating OV3600 into the Network and Organizational Hierarchy" on page 15

If you have any questions or comments, please contact Alcatel support.

OV3600—A Unified Wireless Network Command Center

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

The OmniVista 3600 Air Manager supports hardware from leading wireless vendors including Aruba Networks, Avaya, Cisco (Aironet and WLC), Enterasys, Juniper Networks, LANCOM Systems, Meru, Nomadix, Nortel, ProCurve by HP, Proxim, Symbol, Trapeze, Tropos, and many others.

The components of the OmniVista 3600 Air Manager are listed here, and detailed below:

- The OV3600 wireless network management software, including the AOS-W Configuration feature that supports global and group configuration of Alcatel-Lucent devices
- *VisualRF* location and RF mapping software module
- *RAPIDS* rogue access point detection software module
- **Master Console** and **Failover** tabs

OV3600 Management Platform

OV3600 is the centerpiece of the Alcatel-Lucent Wireless Management Solution, offering the following functions and benefits:

- Core network management functionality:
  - Network discovery
  - Configuration of APs & controllers
  - Automated compliance audits
  - Firmware distribution
  - Monitoring of every device and user connected to the network
  - Real-time and historical trend reports
- Granular administrative access
  - Role-based (for example, Administrator contrasted with Help Desk)
  - Network segment (for example, "Retail Store" network contrasted with "Corporate HQ" network)
- Flexible device support
  - Thin, thick, mesh network architecture

  - Multi-vendor support
  - Current and legacy hardware support

Alcatel-Lucent Configuration

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

OV3600 consolidates AOS-W configuration and pushes global Alcatel-Lucent configurations from within OV3600.

Two pages in OV3600 support Alcatel-Lucent Configuration:

- **Device Setup > Alcatel-Lucent Configuration** for global Alcatel-Lucent Configuration
- **Groups > Alcatel-Lucent Config** for group-level Alcatel-Lucent Configuration

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

VisualRF™

VisualRF is a powerful tool for monitoring and managing radio frequency (RF) dynamics within your wireless network, to include the following functions and benefits:

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

RAPIDS™

RAPIDS is a powerful and easy-to-use tool for monitoring and managing security on your wireless network, to include the following features and benefits:

- Automatic detection of unauthorized wireless devices
- Rogue device classification that supports multiple methods of rogue detection
- Wireless detection:
  - Uses authorized wireless APs to report other devices within range.
  - Calculates and displays rogue location on VisualRF map.
- Wired network detection:
  - Discovers rogue APs located beyond the range of authorized APs/sensors.
  - Queries routers and switches.
  - Ranks devices according to the likelihood they are rogues.
  - Multiple tests to eliminate false positive results.
  - Provides rogue discovery that identifies the switch and port to which a rogue device is connected.

Master Console and Failover

The OV3600 **Master Console** and **Failover** tools enable network-wide information in easy-to-understand presentation, to entail operational information and high-availability for failover scenarios. The benefits of these tools include the following:

- Provides network-wide visibility, even when the WLAN grows to 50,000+ devices
- Executive Portal allows executives to view high-level usage and performance data
- Aggregated alerts
- Failover
  - Many-to-one failover
  - One-to-one failover

The Master Console and Failover servers can be configured with a Device Down trigger that generates an alert if communication is lost. In addition to generating an alert, the Master Console or Failover server can also send email or NMS notifications about the event. See "Using Triggers and Alerts" on page 232.

Integrating OV3600 into the Network and Organizational Hierarchy

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

The power, performance, and usability of the OV3600 solution become more apparent when considering the diverse components within a WLAN. Table 4 itemizes such network components, as an example.

Table 4 *Components of a WLAN*

Component	Description
Autonomous AP	Standalone device which performs radio and authentication functions
Thin AP	Radio-only device coupled with WLAN controller to perform authentication
WLAN switch	Used in conjunction with thin APs to coordinate authentication and roaming
NMS	Network Management Systems and Event Correlation (OpenView, Tivoli, and so forth)
RADIUS Authentication	RADIUS authentication servers (Funk, FreeRADIUS, ACS, or IAS)
RADIUS Accounting	OV3600 itself serves as a RADIUS accounting client
Wireless Gateways	Provide HTML redirect and/or wireless VPNs
TACACS+	Used to authenticate OV3600 administrative users
Routers/Switches	Provide OV3600 with data for user information and AP and Rogue discovery
Help Desk Systems	Remedy EPICOR
Rogue APs	Unauthorized APs not registered in the OV3600 database of managed APs

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

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

Chapter 2

Installing OV3600

This chapter contains information and procedures for installing and launching the OmniVista 3600 Air Manager (OV3600), and includes the following topics:

- “OV3600 Hardware Requirements and Installation Media” on page 17
- “Installing Linux CentOS 5 (Phase 1)” on page 17
- “Installing OV3600 Software (Phase 2)” on page 18
- “Configuring and Mapping Port Usage for OV3600” on page 21
- “OV3600 Navigation Basics” on page 22
- “Getting Started with OV3600” on page 28

NOTE

OV3600 does not support downgrading to older versions. Significant data could be lost or compromised in such a downgrade. In unusual circumstances requiring that you return to an earlier version of OV3600, we recommend you perform a fresh installation of the earlier OV3600 version, and then restore data from a pre-upgrade backup.

OV3600 Hardware Requirements and Installation Media

The OV3600 installation CD includes all software (including the Linux OS) required to complete the installation of the OmniVista 3600 Air Manager. OV3600 supports any hardware that is Red Hat Enterprise Linux 5 certified. By default, all installs are based on a 64-bit operating system.

OV3600 hardware requirements vary by version. As additional features are added to OV3600, increased hardware resources become necessary. For the most recent hardware requirements, refer to the *Hardware Sizing Guide*.

OV3600 is intended to operate as a soft appliance. Other applications should not run on the same installation. Additionally, local shell users can access data on OV3600, so it is important to restrict access to the shell only to authorized users.

You can create sudo users in place of root for companies that don't allow root logins.

Installing Linux CentOS 5 (Phase 1)

Perform the following steps to install the Linux CentOS 5 operating system. The Linux installation is a prerequisite to installing OV3600 on the network management system.

CAUTION

This procedure erases the hard drive(s) on the server.

1. Insert the OV3600 installation CD-ROM into the drive and boot the server.
2. If this is a new installation of the OV3600 software, type **install** and press **Enter**.

   To configure the partitions manually, type **expert** and press **Enter**.

   The following message appears on the screen.

   ```
   Welcome to OV3600 Installer Phase I
   - To install a new OV3600, type install <ENTER>.
     WARNING: This will ERASE all data on your hard drive.
   ```

```
- To install OV3600 and manually configure hard drive settings, type expert <ENTER>.

boot:
```

3. Allow the installation process to continue. Installing the CentOS software (Phase I) takes 10 to 20 minutes to complete. This process formats the hard drive and launches Anaconda to install all necessary packages. Anaconda gauges the progress of the installation.

   Upon completion, the system will prompt you to eject the installation CD and reboot the system.

4. Remove the CD from the drive and store in a safe location.

Installing OV3600 Software (Phase 2)

Getting Started

After the reboot, the GRUB screen appears.

1. Press **Enter** or wait six seconds, and the system automatically loads the kernel.
2. When the kernel is loaded, log into the server using the following credentials:
   - login = **root**
   - password = **admin**
3. Start the OV3600 software installation script by executing the **./amp-install** command.

   Type **`./amp-install`** at the command prompt and press **Enter** to execute the script.

Step 1: Configuring Date and Time, Checking for Prior Installations

Date and Time

The following message appears, and this step ensures the proper date and time are set on the server.

```
------------------------ Date and Time Configuration ------------------
Current Time: Fri Nov 21 09:18:12 PST 2008
1)  Change Date and Time
2)  Change Time Zone

0)  Finish
```

Ensure that you enter the accurate date and time during this process. *Errors will arise later in the installation if the specified date varies significantly from the actual date,* ***especially*** *if the specified date is in the future and it is fixed later.* It is recommended to configure ntpd to gradually adjust your clock to the correct time.

1. Select **1** to set the date and select **2** to set the time zone. Press **Enter** after each configuration to return to the message menu above.

CAUTION

Changing these settings after the installation can cause data loss, especially for time-series data such as bandwidth and client count graphs. Avoid delayed configuration.

2. Press **0** to complete the configuration of date and time information, and to continue to the next step.

Previous OV3600 Installations

The following message appears after date and time are set.

```
Welcome to OV3600 Installer Phase 2
STEP 1:  Checking for previous OV3600 installations
```

If a previous version of OV3600 software is not discovered, the installation program automatically proceeds to "Step 2: Installing OV3600 Software, Including OV3600" on page 19. If a previous version of the software is discovered, the following message appears on the screen.

```
The installation program discovered a previous version of the software. Would you like to
reinstall OV3600? This will erase OV3600's database. Reinstall (y/n)?
```

Type **y** and press **Enter** to proceed.

CAUTION

This action erases the current database, including all historical information. To ensure that the OV3600 database is backed up prior to reinstallation, answer `n` at the prompt above and contact your Value Added Reseller or directly contact Alcatel-Lucent support.

Step 2: Installing OV3600 Software, Including OV3600

The following message appears while OV3600 software is transferred and compiled.

```
STEP 2:  Installing OV3600 software
  This will take a few minutes.
  Press Alt-F9 to see detailed messages.
  Press Alt-F1 return to this screen.
```

This step requires no user input, but you can follow the instructions to monitor its progress and switch back to the installation screen.

Step 3: Checking the OV3600 Installation

After the OV3600 software installation is complete, the following message appears:

```
STEP 3:  Checking OV3600 installation
  Database is up.
  OV3600 is running version: (version number)
```

This step requires no user input. Proceed to the next step as prompted to do so.

Step 4: Assigning an IP Address to the OV3600 System

While the OV3600 primary network interface accepts a DHCP address initially during installation, *OV3600 does not function when launched unless a static IP is assigned.* Complete these tasks to assign the static IP address. The following message appears:

```
STEP 4: Assigning OV3600's address
     OV3600 must be configured with a static IP.

--------------- Primary Network Interface Configuration -------------

         1)  IP Address   : xxx.xxx.xxx.xxx
         2)  Netmask      : xxx.xxx.xxx.xxx
         3)  Gateway      : xxx.xxx.xxx.xxx
         4)  Primary DNS  : xxx.xxx.xxx.xxx
         5)  Secondary DNS: xxx.xxx.xxx.xxx

         9)  Commit Changes
         0)  Exit (discard changes)

If you want to configure a second network interface, please
use OV3600's web interface, AMP Setup --> Network Tab
```

1. Enter the network information.

NOTE

The Secondary DNS setting is an optional field.

2. Commit the changes by typing **9** and pressing **Enter**.
   To discard the changes, type **0** and press **Enter**.

Step 5: Naming the OV3600 Network Administration System

Upon completion of the previous step, the following message appears.

```
STEP 5:  Naming OV3600
OV3600 name is currently set to: New OV3600
Please enter a name for your OV3600:
```

At the prompt, enter a name for your OV3600 server and press **Enter**.

Step 6: Assigning a Host Name to the OV3600

Upon completion of the previous step, the following message appears on the screen.

```
STEP 6:  Assigning OV3600's hostname
 Does OV3600 have a valid DNS name on your network (y/n)?
```

1. If OV3600 does not have a valid host name on the network, enter **n** at the prompt. The following appears:

   ```
   Generating SSL certificate for < IP Address >
   ```

2. If OV3600 does have a valid host name on the network, enter **y** at the prompt. The following appears:

   ```
   Enter OV3600's DNS name:
   ```

3. Type the OV3600 DNS name and press **Enter**. The following message appears:

   ```
   Generating SSL certificate for < IP Address >
   ```

Proceed to the next step as the system prompts you.

Step 7: Changing the Default Root Password

Upon completion of the prior step, the following message appears.

```
STEP 7:  Changing default root password.
You will now change the password for the 'root' shell user.

Changing password for user root.
New Password:
```

Enter the new root password and press **Enter**. The Linux root password is similar to a Windows administrator password. The root user is a super user who has full access to all commands and directories on the computer.

This password should be kept as secure as possible because it allows full access to the machine. This password is not often needed on a day-to-day basis, but is required to perform OV3600 upgrades and advanced troubleshooting. If you lose this password, contact Alcatel support for resetting instructions.

Completing the Installation

Upon completion of all previous steps, the following message appears.

```
CONGRATULATIONS!  OV3600 is configured properly.
 To access OV3600 web console, browse to https://<IP Address>
 Login with the following credentials:
 Username: admin
 Password: admin
```

- To view the Phase 1 installation log file, type **cat /root/install.log**.
- To view the Phase 2 installation log file, type **cat /tmp/amp-install.log**.
- To access the OV3600 GUI, enter the OV3600 IP address in the address bar of any browser. The OV3600 GUI then prompts for your license key. If you are entering a dedicated **Master Console** or OV3600 **Failover** license, refer to "Supporting OV3600 Servers with the Master Console" on page 210 for additional information.

Configuring and Mapping Port Usage for OV3600

The following diagram itemizes the communication protocols and ports necessary for OV3600 to communicate with wireless LAN infrastructure devices, including access points (APs), controllers, routers, switches, and RADIUS servers. Assign or adjust port usage on the network administration system as required to support these components.

Table 5 *OV3600 Protocol and Port Chart*

Port	Type	Protocol	Description	Direction	Device Type
21	TCP	FTP	Firmware distribution	>	APs or controllers
22	TCP	SSH	Configure devices	>	APs or controllers
22	TCP	SSH	Configure OV3600 from CLI	<	Laptop or workstation
22	TCP	VTUN	Support connection (optional)	>	Alcatel-Lucent support home office
22	TCP	SCP	Transfer configuration files or FW	<	APs or controllers
23	TCP	Telnet	Configure devices	>	APs or controllers
23	TCP	VTUN	Support connection (optional)	>	Alcatel-Lucent support home office
25	TCP	SMTP	Support email (optional)	>	Alcatel-Lucent support email server
49	UDP	TACACS	OV3600 Administrative Authentication	>	Cisco TACACS+
53	UDP	DNS	DNS lookup from OV3600	>	DNS Server
69	UDP	TFTP	Transfer configuration files or FW	<	APs or controllers
80	TCP	HTTP	Configure devices	>	Legacy APs
80	TCP	VTUN	Support connection (optional)	>	Alcatel-Lucent support home office
161	UDP	SNMP	Get and Set operations	>	APs or controllers
162	UDP	SNMP	Traps from devices	<	APs or controllers
162	UDP	SNMP	Traps from OV3600	>	NMS
443	TCP	HTTPS	Web management	<	Laptop or workstation
443	TCP	HTTPS	WLSE polling	>	WLSE
443	TCP	VTUN	Support connection (optional)	>	Alcatel-Lucent support home office
1701	TCP	HTTPS	AP and rogue discovery	>	WLSE
1741	TCP	HTTP	WLSE polling	>	WLSE
1813	UDP	RADIUS	Retrieve client authentication info	<	Accounting Server
1813	UDP	RADIUS	Retrieve client authentication info	<	APs or controllers
1813	UDP	RADIUS	Outbound from OV3600 to a RADIUS server for OV3600 administrator authentication	>	RADIUS server
2002	TCP	HTTPS	Retrieve client authentication info	>	ACS
5050	UDP	RTLS	Real Time Location Feed	<	Alcatel-Lucent thin APs
8211	UDP	PAPI	Real Time Feed	< >	WLAN switches
		ICMP	Ping Probe	>	APs or controllers

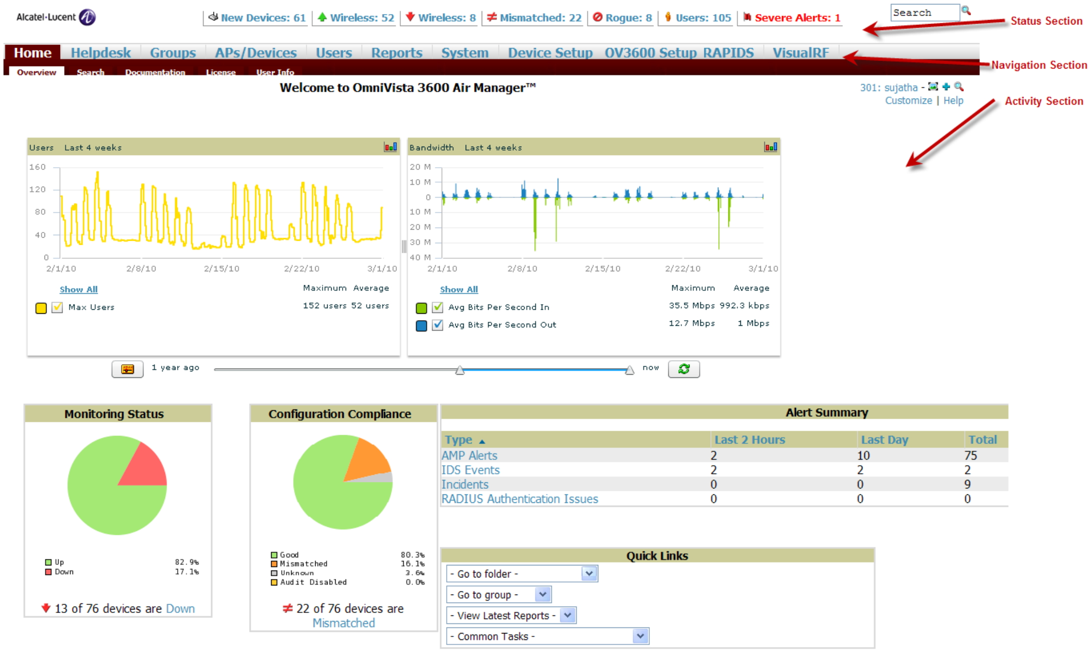
OV3600 Navigation Basics

Every OV3600 page contains three basic sections as illustrated in Figure 1:

- Status Section
- Navigation Section
- Activity Section

The OV3600 pages also contain **Help** links with GUI-specific help information and certain standard action buttons.

Figure 1 ***Home* > *Overview*** *Page Illustration*



Alert Summary

Type ▲	Last 2 Hours	Last Day	Total
AMP Alerts	2	10	75
IDS Events	2	2	2
Incidents	0	0	9
RADIUS Authentication Issues	0	0	0

Status Section

The Status section is a snapshot view of overall WLAN performance and provides direct links for immediate access to key system components. The Status section remains at the top of all pages in the OV3600 and RAPIDS modules. OV3600 includes the ability to customize the contents of the Status section from the **Home > User Info** page, to include support for both wireless and wired network components. Refer to "Configuring Your Own User Information with the Home > User Info Page" on page 202.

The table below describes these elements in further detail.

Table 6 *Status Section Components of the OV3600 GUI*

Field	Description
New Devices	The number of wireless APs or wireless LAN controllers that have been discovered by OV3600 but not yet managed by network administrators. When selected, OV3600 directs you to a page that displays a detailed list of devices awaiting authorization.
Up	The number of managed authorized devices that are currently responding to OV3600 requests. When selected, OV3600 shows a detailed list of all **Up** devices.
Down	The number of managed, authorized devices that are not currently responding to OV3600 SNMP requests. When selected, OV3600 shows a detailed list of all "Down" devices.
Mismatched	The total number of Mismatched devices. A device is considered mismatched when the desired configuration in OV3600 does not match the actual device configuration read from the device.
Rogue	The number of devices that have been classified by the RAPIDS rules engine above the threshold defined on the **Home > User** Info page.

Table 6 *Status Section Components of the OV3600 GUI*

Field	Description
Users	The number of wireless users currently associated to the wireless network via all the APs managed by OV3600. When selected, OV3600 shows a list of users that are associated.
Alerts	Displays the number of non-acknowledged OV3600 alerts generated by user-configured triggers. When selected, OV3600 shows a detailed list of active alerts.
Severe Alerts (conditional)	When triggers are given a severity of **Critical**, they generate **Severe Alerts**. When a Severe Alert exists, a new component appears at the right of the **Status** field in bold red font. Only users configured on the **Home > User Info** page to be enabled to view critical alerts can see Severe Alerts. The functionality of Severe Alerts is the same as that described above for Alerts. Unlike Alerts, the Severe Alerts section is hidden if there are no Severe Alerts.
Device Types to Include in Header Stats	You can support statistics for any combination of the following device types: ● Autonomous APs ● Controllers ● Routers/Switches ● Thin APs ● Universal Devices Refer to "Configuring Your Own User Information with the Home > User Info Page" on page 202.
Search	Search performs partial string searches on a large number of fields including the notes, version, secondary version, radio serial number, device serial number, LAN MAC, radio MAC and apparent IP of all the APs as well as the client MAC, VPN user, LAN IP, VPN IP fields.

Navigation Section

The Navigation section displays tabs for all main GUI pages within OV3600. The top navigation bar contains tabs for the main components of OV3600, while the lower bar is context-sensitive and displays the subtabs for the highlighted tab.

Table 7 *Components and Subtabs of the OV3600 Navigation Screen*

Main Tab	Description	Subtabs
Home	The **Home** tab provides basic OV3600 information including system name, host name, IP address, current time, running time, and software version. The **Home** page also provides a central point for network status information and monitoring tools, giving graphical display of network activity, and links to many of the most frequent tools in OV3600. For additional information, refer to "Monitoring and Supporting OV3600 with the Home Pages" on page 197.	● Overview ● Search ● Documentation ● License ● User Info
Helpdesk	The **Helpdesk** pages provide an interface for support and diagnostic tools. For additional information refer to Chapter 10, "Using the OV3600 Helpdesk" on page 247.	● Incidents ● Setup

Table 7 *Components and Subtabs of the OV3600 Navigation Screen (Continued)*

Main Tab	Description	Subtabs
Groups	The **Groups** pages provide information on the logical "groups" of devices that have been established for efficient monitoring and configuration. For additional information, see Chapter 4, “Configuring and Using Device Groups in OV3600” on page 69. **NOTE:** Some of the focused subtabs will not appear for all groups. Focused subtabs are visible based on the device type field on the **Groups > Basic** page. This subtab is the first page to appear when adding or editing groups. **NOTE:** When individual device configurations are specified, device-level settings override the Group-level settings to which a device belongs.	● List ● Focused Subtabs ■Monitor ■Basic ■Templates ■Security ■SSIDs ■AAA Servers ■Radio ■Alcatel-Lucent Config ■Cisco WLC Config ■PTMP ■Proxim Mesh ■MAC ACL ■Firmware ■Compare
APs/Devices	The **APs/Devices** pages provide detailed information about all authorized APs and wireless LAN switches or controllers on the network, including all configuration and current monitoring data. These pages interact with several additional pages in OV3600. One chapter to emphasize the **APs/Devices** pages is Chapter 5, “Discovering, Adding, and Managing Devices” on page 107. **NOTE:** When specified, device-level settings override the default Group-level settings.	● List ● New ● Up ● Down ● Mismatched ● Ignored ● Focused Subtabs ■Manage ■Interfaces ■Audit ■Compliance ■Containment Status
Users	The **Users** pages provide detailed information about all client devices and users currently associated to the WLAN. For additional information, refer to “Monitoring and Supporting WLAN Users” on page 187.	● Connected ● All ● Guest Users ■User Detail ■Diagnostics ● Tags
Reports	The **Reports** pages list all the standard and custom reports generated by OV3600. OV3600 supports 13 reports in the OV3600 module. For additional information, refer to Chapter 9, “Creating, Running, and Emailing Reports” on page 219.	● Generated ● Definition ■Detail
System	The **System** page provides information about OV3600 operation and administration, including overall system status, the job scheduler, trigger/alert administration, and so forth. For additional information, refer to “Monitoring and Supporting OV3600 with the System Pages” on page 204.	● Status ● Event Log ● Triggers ● Alerts ● Backups ● Configuration Change Jobs ● Firmware Upgrade Jobs ● Performance

Table 7 *Components and Subtabs of the OV3600 Navigation Screen (Continued)*

Main Tab	Description	Subtabs
Device Setup	The **Device Setup** pages provide the ability to add, configure, and monitor devices, to include setting AP discovery parameters, performing firmware management, defining VLANs, and so forth. For additional information, refer to "Enabling OV3600 to Manage Your Devices" on page 47.	● Discover ● Add ● Communication ● Alcatel-Lucent Configuration *(if global Alcatel-Lucent Configuration is enabled)* ● Upload Files
OV3600 Setup	The **OV3600 Setup** pages provide all information relating to the configuration of OV3600 itself and its connection to your network. This page entails several processes, configurations, or tools in OV3600. For additional information, start with Chapter 3, "Configuring OV3600" on page 29. **NOTE:** The **OV3600 Setup** pages may not be visible, depending on the role of the logged-in user and license set in OV3600.	● General ● Network ● Users ● Roles ● Guest Users ● Authentication ● MDM Server ● WLSE ● ACS ● NMS ● RADIUS Accounting ● PCI Compliance
RAPIDS	The **RAPIDS** pages provide all information relating to rogue access points, including methods of discovery and lists of discovered and possible rogues. For additional information, refer to Chapter 7, "Using RAPIDS and Rogue Classification" on page 163. The RAPIDS pages may not be visible depending on the role and license set in OV3600.	● Overview ● List ● IDS Events ● Setup ● Rules ● Score Override ● Audit Log
VisualRF	**VisualRF** pages provide graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network. For additional information, refer to the *VisualRF User Guide*. VisualRF may not be visible depending on the role and license set in OV3600.	● Floor Plans ● Setup ● Import ● Audit Log

NOTE

The **OV3600 Setup** tab varies with user role. The RAPIDS and VisualRF tabs appear based on the license entered on the **Home > License** page, and might not be visible on your OV3600 view.

Activity Section

The **Activity** section displays all detailed configuration and monitoring information, and is where changes are implemented.

Help Links in the GUI

The **Help** link is available on every page within OV3600. When selected, this launches a PDF document with information describing the OV3600 page that is currently displayed.

NOTE

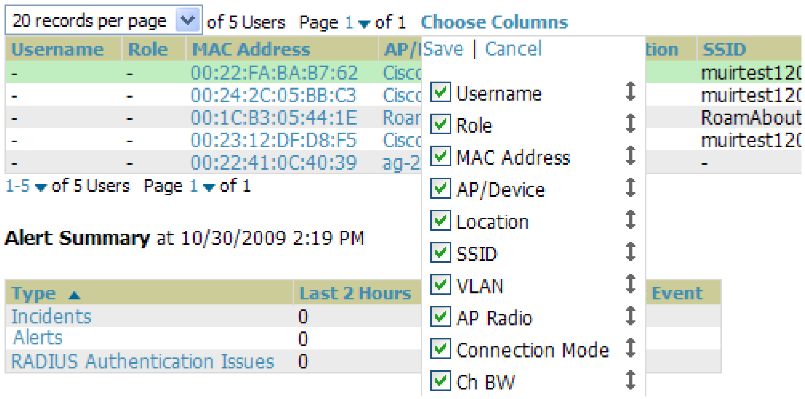
Adobe Reader must be installed to view the settings and default values in the PDF help file.

Common List Settings

All of the lists in OV3600 have some common options such as pagination with a configurable number of items per page, as shown at the top left of Figure 2. Selecting the **Records Per Page** dropdown menu enables you select or enter the number of rows that appear at a time in the list. The next down arrow displays a dropdown menu that allows you to select the exact page you would like to view.

The **Choose Columns** option, illustrated on Figure 2, allows you to configure the columns that are presented in the list and the order in which they are presented. To disable a column, clear its checkbox. To reorder the columns, drag a row to the appropriate new position. When you are satisfied with the enabled columns and their order, select **Save** at the top of the columns list.

Figure 2 *Common List Settings and **Choose Columns** Illustration*



20 records per page ▾ of 5 Users Page 1 ▾ of 1 Choose Columns

Username	Role	MAC Address	AP/I	tion	SSID
-	-	00:22:FA:BA:B7:62	Cisc		muirtest12(
-	-	00:24:2C:05:BB:C3	Cisc		muirtest12(
-	-	00:1C:B3:05:44:1E	Roar		RoamAbout
-	-	00:23:12:DF:D8:F5	Cisc		muirtest12(
-	-	00:22:41:0C:40:39	ag-2		-

1-5 ▾ of 5 Users Page 1 ▾ of 1

Save | Cancel

- ☑ Username ↕
- ☑ Role ↕
- ☑ MAC Address ↕
- ☑ AP/Device ↕
- ☑ Location ↕
- ☑ SSID ↕
- ☑ VLAN ↕
- ☑ AP Radio ↕
- ☑ Connection Mode ↕
- ☑ Ch BW ↕

Alert Summary at 10/30/2009 2:19 PM

Type ▲	Last 2 Hours	Event
Incidents	0	
Alerts	0	
RADIUS Authentication Issues	0	

These settings are user specific. To reset them, select **Reset List Preferences** on **Home > User Info**.

Buttons and Icons

Standard buttons and icons are used throughout the OV3600 as follows:

Table 8 *Standard Buttons and Icons of the OV3600 User Page*

Function	Image[a]	Description
Acknowledge		Acknowledges and clears an OV3600 alert.
Add		Adds the object to both OV3600' database and the onscreen display list.
Add Folder	📁	Adds a new folder to hierarchically organize APs.
Alert	🚩	Indicates an alert.
Apply		Applies all "saved" configuration changes to devices on the WLAN.
Attach	🖼	Attaches a snapshot of an OV3600 screen to a Helpdesk incident.
Audit		Reads device configuration, compare to desired, and update status.
Bandwidth	◔	Displays current bandwidth for group.
Choose	🔍	Chooses a new Helpdesk incident to be the Current Incident.
Create	✚	Creates a new Helpdesk incident.
Customize		Ignores selected settings when calculating the configuration status.
Delete	🗑	Deletes an object from OV3600' database.
Down	⬇	Indicates down devices and radios.
Drag and Drop	✥	Dragging and dropping objects with this icon changes the sequence of items in relation to each other. Refer to "Using RAPIDS and Rogue Classification" on page 163 as one example of drag-and-drop.

Table 8 *Standard Buttons and Icons of the OV3600 User Page (Continued)*

Function	Image[a]	Description
Duplicate	📄	Duplicates or makes a copy of the configuration of an OV3600 object.
Edit	✏	Edits the object properties.
Email	📫	Links to email reports.
Filter		Filters rogue list by score and/or ad hoc status.
Google Earth	🌐	Views device's location in Google Earth (requires plug-in).
Manage	🔧	Manages the object properties.
Mismatched	≠	Indicates mismatched device configuration, in which the most recent configuration in OV3600 and the current configuration on a device are mismatched.
Monitor	🔒	Indicates an access point is in “monitor only" mode.
Ignore		Ignores specific device(s) - devices selected with check boxes.
Import		Updates a Group's desired settings to match current settings.
New Devices		Indicates new access points and devices.
Poll Now		Polls device (or controller) immediately, override group polling settings.
Preview		Displays a preview of changes applicable to multiple groups.
Print	🖨	Prints the report.
Reboot		Reboots devices or OV3600.
Refresh	🔄	Refreshes the display of interactive graphs when settings have changed.
Relate	↷	Relates an AP, Group or Client to a Helpdesk incident.
Replace Hardware		Confers configuration and history of one AP to a replacement device.
Revert		Returns all configurable data on the screen to its original status.
Rogue	⊘	Indicates a rogue access point and links to RAPIDS.
Run		Runs a new user-defined report.
Save		Saves the information on the page in the OV3600 database.
Save & Apply		Saves changes to OV3600' database and apply all changes to devices.
Scan		Scans for devices and rogues using selected networks.
Schedule		Schedules a window for reports, device changes, or maintenance.
Search	🔍	Searches OV3600 for the specified name, MAC or IP address.
Set Time Range	📅	Sets the time range for interactive graphs to the range specified.
Up	⬆	Indicates access points which are in the up status.
Update Firmware		Applies a new firmware image to an AP/device.
User	👤	Indicates a user.
View Historical Graph in New Window	📊	Displays all data series for the selected graph over the last two hours, last day, last week, last month, and last year in one page.
VisualRF		Links to VisualRF - real time visualization.
XML	⬇	Links to export XHTML versions of reports.

[a] Not all OV3600 GUI components are itemized in graphic format in this table.

Getting Started with OV3600

This topic describes how to perform an initial launch of the OV3600 network management solution.

Use your browser to navigate to the static IP address assigned to the internal page of the OV3600. Enter the User Name and Password as **admin/admin** for your initial login, and then select **OK**.

After successful authentication, your browser launches the OV3600 **Home > Overview** page.

NOTE

OV3600 pages are protected via SSL. Some browsers will display a confirmation dialog for your self-signed certificate. Signing your certificate will prevent this dialog from displaying. Alcatel-Lucent recommends changing the default login and password on the **OV3600 Setup > Users** page. Refer to "Creating OV3600 User Roles" on page 44 for additional information.

Chapter 3

Configuring OV3600

This chapter contains the following procedures to deploy initial OV3600 configuration:

- "Formatting the Top Header" on page 29
- "Customizing Columns in Lists" on page 30
- "Resetting Pagination Records" on page 30
- "Using the Pagination Widget" on page 31
- "Using CSV Export for Lists and Reports" on page 31
- "Defining Graph Display Preferences" on page 31
- "Customizing the Overview Subtab Display" on page 32
- "Setting Severe Alert Warning Behavior" on page 34
- "Defining General OV3600 Server Settings" on page 35
- "Defining OV3600 Network Settings" on page 41
- "Creating OV3600 Users" on page 43
- "Creating OV3600 User Roles" on page 44
- "Enabling OV3600 to Manage Your Devices" on page 47
- "Configuring TACACS+ and RADIUS Authentication" on page 52
- "Configuring Cisco WLSE and WLSE Rogue Scanning" on page 56
- "Configuring ACS Servers" on page 61
- "Integrating OV3600 with an Existing Network Management Solution (NMS)" on page 62
- "Auditing PCI Compliance on the Network" on page 63
- "Deploying WMS Offload" on page 66

NOTE

Additional configurations of multiple types are available after basic configuration is complete.

Before You Begin

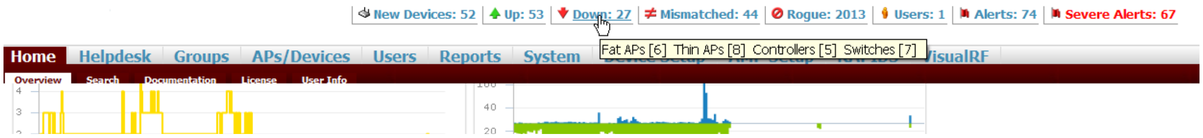
Remember to complete the required configurations in this chapter before proceeding. Alcatel-Lucent support remains available to you for any phase of OV3600 installation.

Formatting the Top Header

The OV3600 interface centers around a horizontal row of tabs with nested subtabs.

A row of statistics hyperlinks called Top Header Stats above the tabs represents many commonly used subtabs. These hyperlinks provide the ability to view certain key statistics by mousing over, such as number and type of **Down** devices, and serve as shortcuts to frequently viewed subtabs. Figure 3 illustrates the navigation bar. For more details on hyperlinks, tabs and subtabs, see "OV3600 Navigation Basics" on page 22.

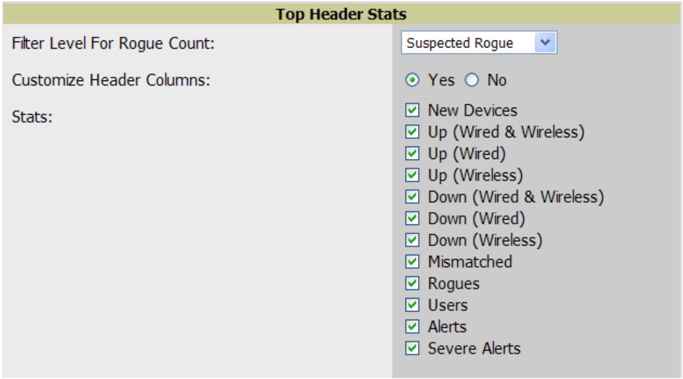
Figure 3 *Navigation Bar Displaying Home Subtabs and Down Device Statistics*



You can control which **Top Header Stats** links appear from the **OV3600 Setup > General** page, as described in "Defining General OV3600 Server Settings" on page 35. Top Header Stats can also be customized for individual user on the **Home > User Info** page. There you can select the statistics to display for certain device types, and override the **OV3600 Setup** page.

All possible display options for users are shown in Figure 4, and these fields are described in detail in "Configuring Your Own User Information with the Home > User Info Page" on page 202.

Figure 4 ***Home* > *User Info*** *Top Header Display Options*



Top Header Stats

Filter Level For Rogue Count: Suspected Rogue

Customize Header Columns: ● Yes ○ No

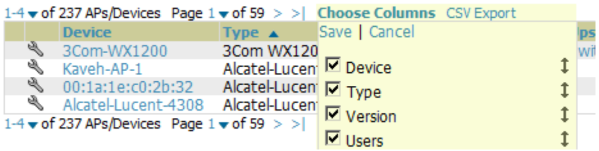
Stats:
☑ New Devices
☑ Up (Wired & Wireless)
☑ Up (Wired)
☑ Up (Wireless)
☑ Down (Wired & Wireless)
☑ Down (Wired)
☑ Down (Wireless)
☑ Mismatched
☑ Rogues
☑ Users
☑ Alerts
☑ Severe Alerts

You can also set the severity level of critical alerts displayed for a user role. For details including a description of what constitutes a severe alert, see "Setting Severe Alert Warning Behavior" on page 34.

Customizing Columns in Lists

Customize the columns for any list table selecting **Choose Columns** as shown in Figure 5. Use the up/down arrows to change the order in which the column heads appear.

Figure 5 ***Choose Columns*** *Dropdown List (highlighted for emphasis)*



1-4 ▾ of 237 APs/Devices Page 1 ▾ of 59 > >| Choose Columns CSV Export

Device	Type ▲
3Com-WX1200	3Com WX120
Kaveh-AP-1	Alcatel-Lucen
00:1a:1e:c0:2b:32	Alcatel-Lucen
Alcatel-Lucent-4308	Alcatel-Lucen

1-4 ▾ of 237 APs/Devices Page 1 ▾ of 59 > >|

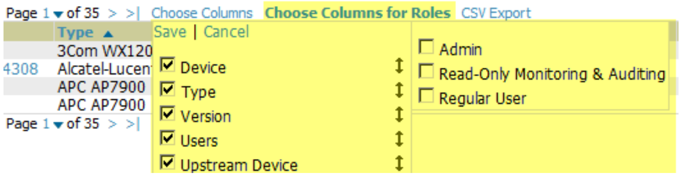
Save | Cancel
☑ Device ↕
☑ Type ↕
☑ Version ↕
☑ Users ↕

For more information on the universal list elements, see "Common List Settings" on page 26.

Users with the Admin role can also control which column heads appear for other user roles by going to **Home > User Info** and selecting **Yes** in the **Customize Columns For Other Roles** field. This exposes the **Choose Columns for Roles** dropdown menu in all tables shown in Figure 6.

The first column shows the user roles that were customized, if any. The second column allows you to establish left to right columns and order them using the arrows.

Figure 6 *Table With* ***Choose Columns for Roles*** *Menu Selected*



Page 1 ▾ of 35 > >| Choose Columns Choose Columns for Roles CSV Export

	Type ▲
	3Com WX120
4308	Alcatel-Lucen
	APC AP7900
	APC AP7900

Page 1 ▾ of 35 > >|

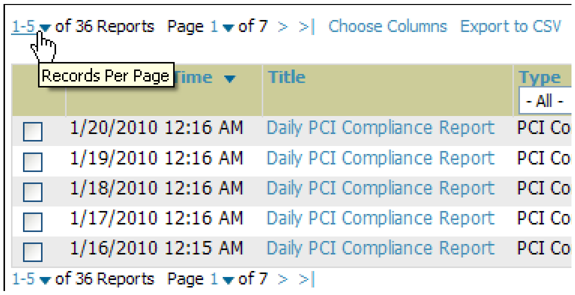
Save | Cancel
☑ Device ↕
☑ Type ↕
☑ Version ↕
☑ Users ↕
☑ Upstream Device ↕

☐ Admin
☐ Read-Only Monitoring & Auditing
☐ Regular User

Resetting Pagination Records

To control the number of records in any individual list, select the link with **Records Per Page** mouseover text at the top left of the table, as shown in Figure 7. OV3600 remembers each list table's pagination preferences.

Figure 7 ***Records Per Page*** *Drop Down Menu*



1-5 ▾ of 36 Reports Page 1 ▾ of 7 > >| Choose Columns Export to CSV

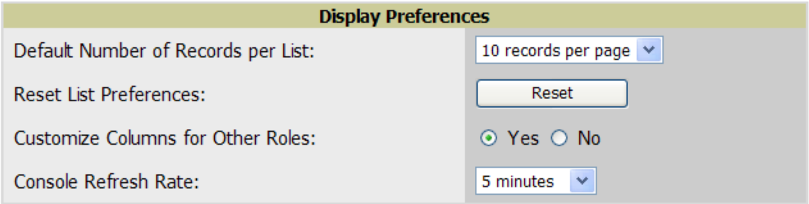
Records Per Page

	Time ▾	Title	Type - All -
□	1/20/2010 12:16 AM	Daily PCI Compliance Report	PCI Co
□	1/19/2010 12:16 AM	Daily PCI Compliance Report	PCI Co
□	1/18/2010 12:16 AM	Daily PCI Compliance Report	PCI Co
□	1/17/2010 12:16 AM	Daily PCI Compliance Report	PCI Co
□	1/16/2010 12:15 AM	Daily PCI Compliance Report	PCI Co

1-5 ▾ of 36 Reports Page 1 ▾ of 7 > >|

To reset all OV3600 list Records Per Page preferences, you can select **Reset** in the **Display Preferences** section of the **Home > User Info** page, as shown in Figure 8.

Figure 8 ***Home > User Info Display Preferences*** *section*

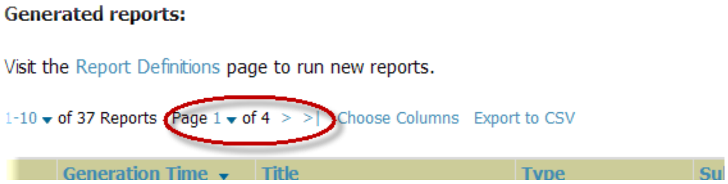


Display Preferences	
Default Number of Records per List:	10 records per page ▾
Reset List Preferences:	Reset
Customize Columns for Other Roles:	● Yes ○ No
Console Refresh Rate:	5 minutes ▾

Using the Pagination Widget

The pagination widget is located at the top and bottom of every list table, as shown in Figure 9.

Figure 9 *Pagination Widget*



Generated reports:

Visit the Report Definitions page to run new reports.

1-10 ▾ of 37 Reports Page 1 ▾ of 4 > >| Choose Columns Export to CSV

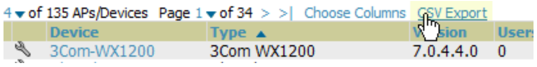
	Generation Time ▾	Title	Type	Su

Use the down arrow next to **Page 1** to see all the page numbers for that table in a dropdown menu. From here, you can jump to any portion of the table. Select the **>** symbol to jump to the next page, and **>|** to jump to the last page.

Using CSV Export for Lists and Reports

Some tables have an **CSV Export** setting you can use export the data as a spreadsheet. See Figure 10 for an example of a list with the **CSV Export** option selected.

Figure 10 *List with* ***CSV Export*** *Selected*



4 ▾ of 135 APs/Devices Page 1 ▾ of 34 > >| Choose Columns CSV Export

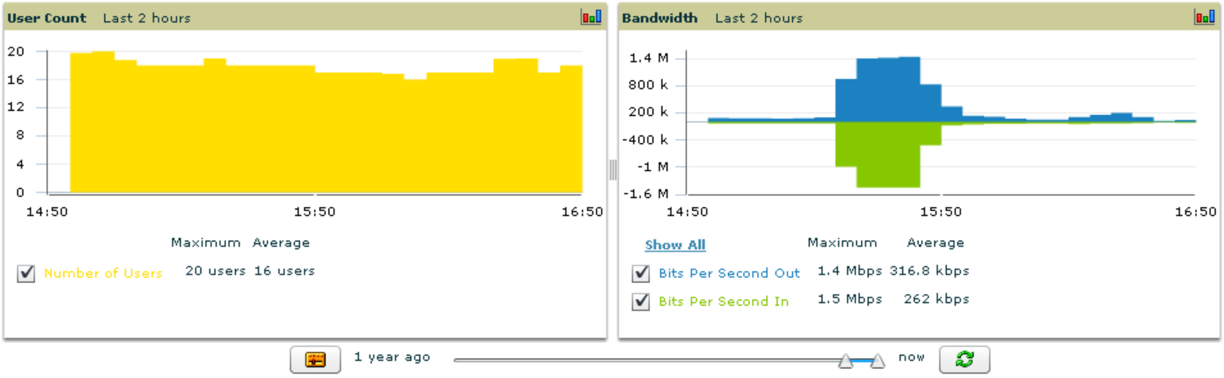
	Device	Type ▲	V sion	User
	3Com-WX1200	3Com WX1200	7.0.4.4.0	0

OV3600 also enables CSV exporting of all report types. For more information, see “Exporting Reports to XML or CSV” on page 245.

Defining Graph Display Preferences

Many of the graphs in OV3600 are Flash-based, which allows you adjust the graph settings attributes, as shown in Figure 11.

Figure 11 *Flash Graphs on the* ***Home*** *>* ***Overview*** *Page*



This Flash-enabled GUI allows for custom settings and adjustments, as follows:

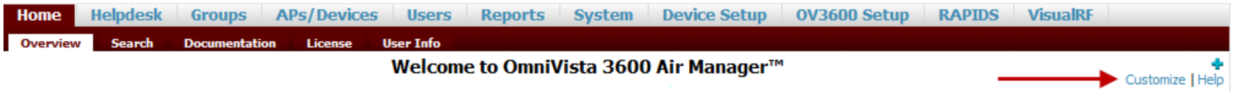
- Drag the slider at the bottom of the screen to move the scope of the graph between one year ago and the current time.
- Drag the slider between graphs to change the relative sizes of each.
- Deselect checkboxes to change the data displayed on each graph. The button with green arrows refreshes data on the graph.
- The **Show All** link displays all of the available checkboxes supporting the Flash graphs.
- Once a change to the slider bars or to the display boxes has been made, the same change can be applied to all other Flash graphs with an **apply** button (appears on mouse-over only).
- For non-Flash graphs, select the graph to open a popup window that shows historical data.

A non-Flash version of the OV3600 user page is available if desired; instead of Flash it uses the RRD graphs that were used in earlier versions of OV3600. Contact Alcatel-Lucent support for more information on activating this feature in the OV3600 database.

Customizing the Overview Subtab Display

You can rearrange or remove widgets appearing on the **Home > Overview** dashboard by selecting **Customize** to the right of this window, as shown in Figure 12.

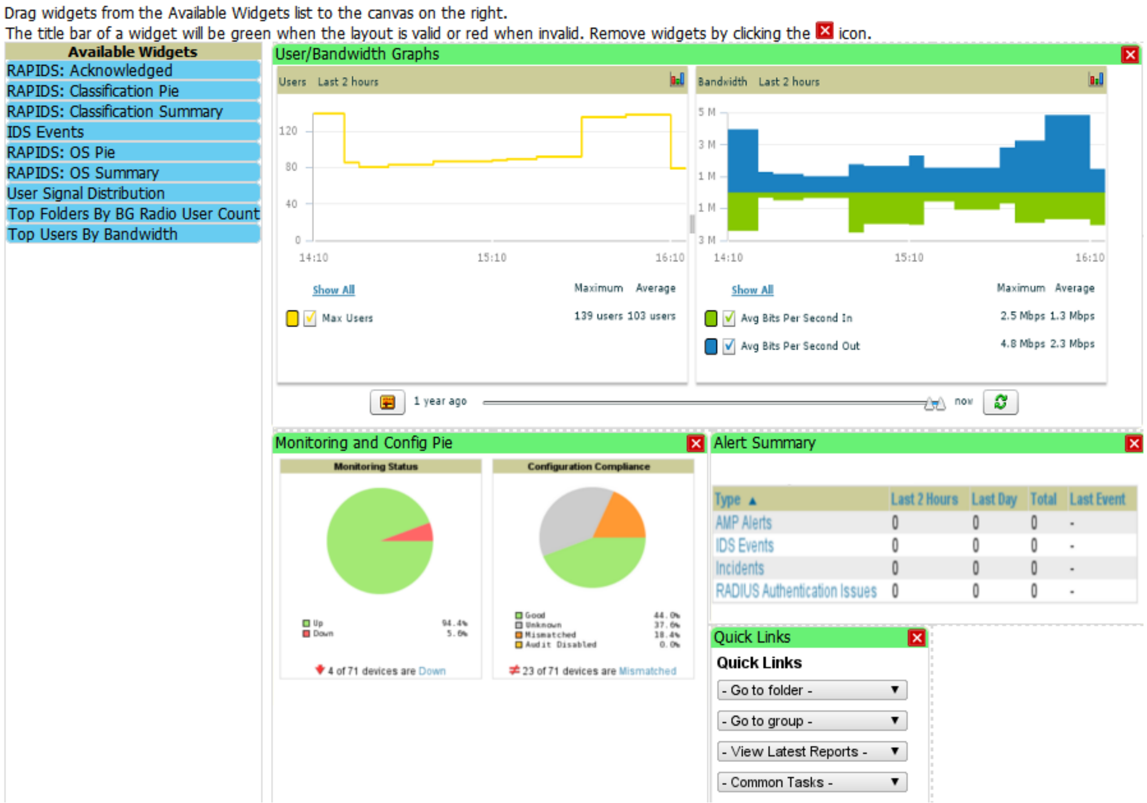
Figure 12 ***Customize*** *Button on the* ***Home*** *>* ***Overview*** *Page*



Welcome to OmniVista 3600 Air Manager™

The **Customize** workspace is shown in Figure 13.

Figure 13 ***Customize Overview*** *Page*



Drag widgets from the Available Widgets list to the canvas on the right.
The title bar of a widget will be green when the layout is valid or red when invalid. Remove widgets by clicking the ☒ icon.

Available Widgets

- RAPIDS: Acknowledged
- RAPIDS: Classification Pie
- RAPIDS: Classification Summary
- IDS Events
- RAPIDS: OS Pie
- RAPIDS: OS Summary
- User Signal Distribution
- Top Folders By BG Radio User Count
- Top Users By Bandwidth

User/Bandwidth Graphs ☒

Monitoring and Config Pie ☒

Alert Summary ☒

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	0	-
IDS Events	0	0	0	-
Incidents	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Quick Links ☒

Quick Links

- Go to folder - ▼

- Go to group - ▼

- View Latest Reports - ▼

- Common Tasks - ▼

The **Available Widgets** section on the left with no gridlines holds all possible (available) graphical elements (widgets). Select any blue widget tile with a verbal description enclosed, and it immediately turns into a graphical element with a description.

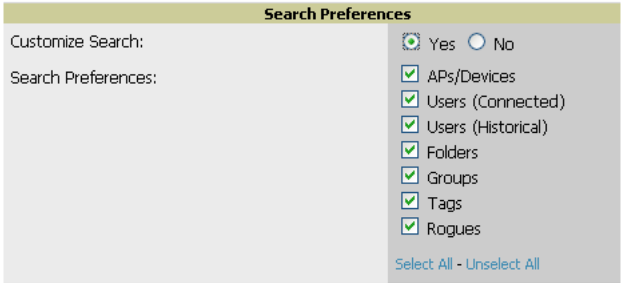
Drag the widgets you want to appear on the **Overview** dashboard across to the gridlines and arrange them in the right section, within the gridlines. A widget snaps back to the nearest available gridline if you drop it across two or more lines, and turns red if you attempt to place it over gridlines already occupied by widgets.

Green widgets are properly placed and set to appear when you select **Save**. Widgets that remain in the left section will not appear (although they can be reinstated by selecting **Restore Defaults**).

Customized Search

You can customize search results to display only desired categories of matches on the **Home > User Info** page. Go to the **Search Preferences** section and select **Yes** in the **Customize Search** field, then select or unselect categories of results and save your changes. Customized search is turned off by default, and all boxes are selected.

Figure 14 ***Home > User Info*** *Customized Search Preferences*



Search Preferences

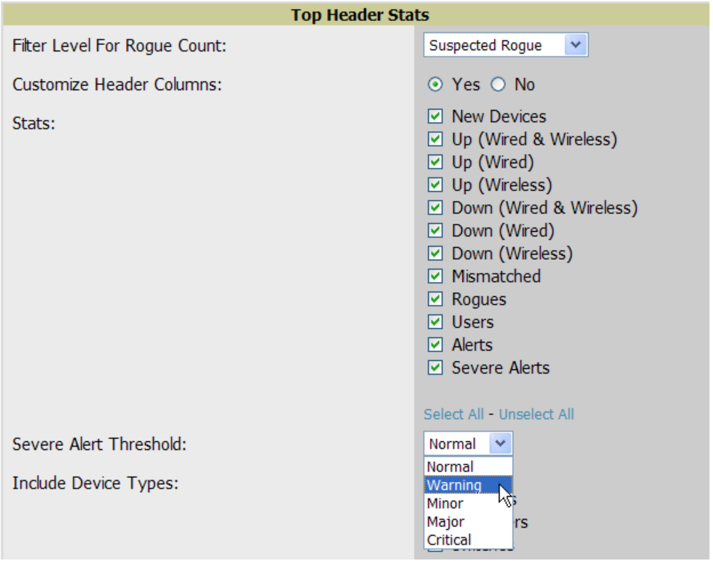
Customize Search:	● Yes ○ No
Search Preferences:	☑ APs/Devices ☑ Users (Connected) ☑ Users (Historical) ☑ Folders ☑ Groups ☑ Tags ☑ Rogues Select All - Unselect All

Setting Severe Alert Warning Behavior

You can control the alert levels users can see on the **Alerts** statistics hyperlink from the **Home > User Info** page. These settings will apply unless and until other users change settings for themselves. When a trigger is assigned a severity of **Critical**, it generates a severe alert. When a severe alert exists, a new component appears at the right of the **Status** field in bold red font.

Only users who are enabled for viewing critical alerts on the **Home > User Info** page can see severe alerts. The **Severe Alert Threshold** dropdown menu, located in the Top Header Stats section of the **Home > User Info** page is shown in Figure 15.

Figure 15 ***Home** > **User Info** > **Severe Alert Threshold** Dropdown Menu*



Top Header Stats

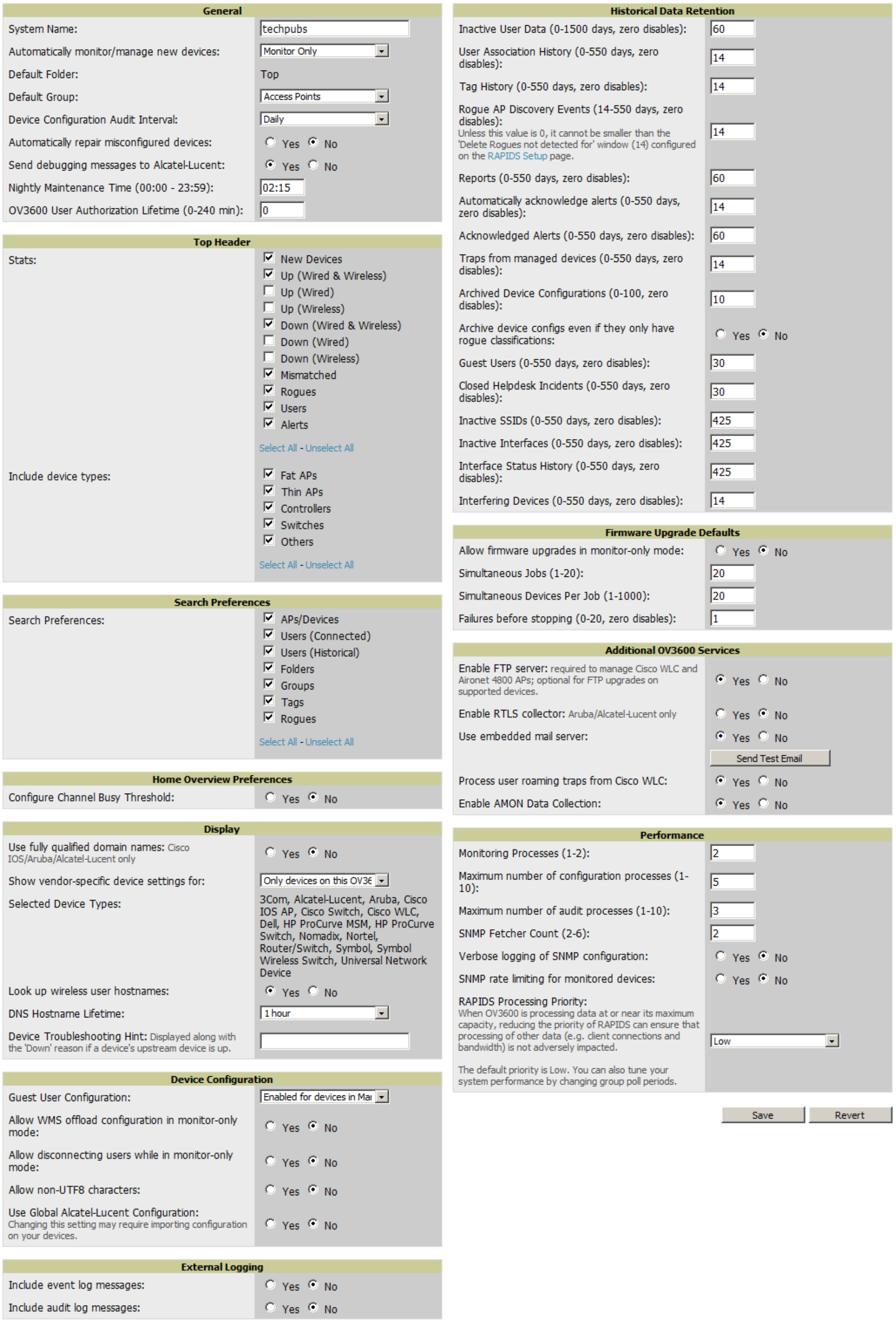
Filter Level For Rogue Count:	Suspected Rogue
Customize Header Columns:	● Yes ○ No
Stats:	☑ New Devices ☑ Up (Wired & Wireless) ☑ Up (Wired) ☑ Up (Wireless) ☑ Down (Wired & Wireless) ☑ Down (Wired) ☑ Down (Wireless) ☑ Mismatched ☑ Rogues ☑ Users ☑ Alerts ☑ Severe Alerts Select All - Unselect All
Severe Alert Threshold:	Normal
Include Device Types:	rs

Defining General OV3600 Server Settings

This section describes all pages accessed from the **OV3600 Setup** tab and describes two pages in the **Device Setup** tab—the **Communication** and **Upload Files** pages. Once required and optional configurations in this chapter are complete, continue to later chapters in this document to create and deploy device groups and device configuration and discovery on the network.

The first step in configuring OV3600 is to specify the general settings for the OV3600 server. Figure 16 illustrates the **OV3600 Setup > General** page:

Figure 16 ***OV3600 Setup*** **>** ***General*** *Page Illustration*



General

System Name:	techpubs
Automatically monitor/manage new devices:	Monitor Only
Default Folder:	Top
Default Group:	Access Points
Device Configuration Audit Interval:	Daily
Automatically repair misconfigured devices:	○ Yes ● No
Send debugging messages to Alcatel-Lucent:	● Yes ○ No
Nightly Maintenance Time (00:00 - 23:59):	02:15
OV3600 User Authorization Lifetime (0-240 min):	0

Top Header

Stats:	☑ New Devices ☑ Up (Wired & Wireless) □ Up (Wired) □ Up (Wireless) ☑ Down (Wired & Wireless) □ Down (Wired) □ Down (Wireless) ☑ Mismatched ☑ Rogues ☑ Users ☑ Alerts Select All - Unselect All
Include device types:	☑ Fat APs ☑ Thin APs ☑ Controllers ☑ Switches ☑ Others Select All - Unselect All

Search Preferences

Search Preferences:	☑ APs/Devices ☑ Users (Connected) ☑ Users (Historical) ☑ Folders ☑ Groups ☑ Tags ☑ Rogues Select All - Unselect All

Home Overview Preferences

Configure Channel Busy Threshold:	○ Yes ● No

Display

Use fully qualified domain names: Cisco IOS/Aruba/Alcatel-Lucent only	○ Yes ● No
Show vendor-specific device settings for:	Only devices on this OV36
Selected Device Types:	3Com, Alcatel-Lucent, Aruba, Cisco IOS AP, Cisco Switch, Cisco WLC, Dell, HP ProCurve MSM, HP ProCurve Switch, Nomadix, Nortel, Router/Switch, Symbol, Symbol Wireless Switch, Universal Network Device
Look up wireless user hostnames:	● Yes ○ No
DNS Hostname Lifetime:	1 hour
Device Troubleshooting Hint: Displayed along with the 'Down' reason if a device's upstream device is up.	

Device Configuration

Guest User Configuration:	Enabled for devices in Mai
Allow WMS offload configuration in monitor-only mode:	○ Yes ● No
Allow disconnecting users while in monitor-only mode:	○ Yes ● No
Allow non-UTF8 characters:	○ Yes ● No
Use Global Alcatel-Lucent Configuration: Changing this setting may require importing configuration on your devices.	○ Yes ● No

External Logging

Include event log messages:	○ Yes ● No
Include audit log messages:	○ Yes ● No

Historical Data Retention

Inactive User Data (0-1500 days, zero disables):	60
User Association History (0-550 days, zero disables):	14
Tag History (0-550 days, zero disables):	14
Rogue AP Discovery Events (14-550 days, zero disables): Unless this value is 0, it cannot be smaller than the 'Delete Rogues not detected for' window (14) configured on the RAPIDS Setup page.	14
Reports (0-550 days, zero disables):	60
Automatically acknowledge alerts (0-550 days, zero disables):	14
Acknowledged Alerts (0-550 days, zero disables):	60
Traps from managed devices (0-550 days, zero disables):	14
Archived Device Configurations (0-100, zero disables):	10
Archive device configs even if they only have rogue classifications:	○ Yes ● No
Guest Users (0-550 days, zero disables):	30
Closed Helpdesk Incidents (0-550 days, zero disables):	30
Inactive SSIDs (0-550 days, zero disables):	425
Inactive Interfaces (0-550 days, zero disables):	425
Interface Status History (0-550 days, zero disables):	425
Interfering Devices (0-550 days, zero disables):	14

Firmware Upgrade Defaults

Allow firmware upgrades in monitor-only mode:	○ Yes ● No
Simultaneous Jobs (1-20):	20
Simultaneous Devices Per Job (1-1000):	20
Failures before stopping (0-20, zero disables):	1

Additional OV3600 Services

Enable FTP server: required to manage Cisco WLC and Aironet 4800 APs; optional for FTP upgrades on supported devices.	● Yes ○ No
Enable RTLS collector: Aruba/Alcatel-Lucent only	○ Yes ● No
Use embedded mail server:	● Yes ○ No Send Test Email
Process user roaming traps from Cisco WLC:	● Yes ○ No
Enable AMON Data Collection:	● Yes ○ No

Performance

Monitoring Processes (1-2):	2
Maximum number of configuration processes (1-10):	5
Maximum number of audit processes (1-10):	3
SNMP Fetcher Count (2-6):	2
Verbose logging of SNMP configuration:	○ Yes ● No
SNMP rate limiting for monitored devices:	○ Yes ● No
RAPIDS Processing Priority: When OV3600 is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (e.g. client connections and bandwidth) is not adversely impacted. The default priority is Low. You can also tune your system performance by changing group poll periods.	Low

Perform the following steps to configure OV3600 server settings globally across the product (for all users).

1. Browse to the **OV3600 Setup > General** page, locate the **General** area, and enter the information described in Table 9:

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

Setting	Default	Description
System Name	OV3600	Defines your name for the OV3600 server, with a maximum limit of 20 alphanumeric characters.
Automatically monitor/manage new devices	No	Launches a drop-down menu that specifies the behavior OV3600 should follow when it discovers a new device. Devices are placed in the default group which is defined in the next field. Choose one of these options: ● **Monitor Only:** OV3600 compares the current configuration with the policy, and displays any discrepancies on the **APs/Devices > Audit** page, but does not change the configuration of the device. ● **Manage Read/Write:** OV3600 compares the device's current configuration settings with the Group configuration settings and automatically updates the device's configuration to match the Group policy. Automatically placing devices in **Managed Read/Write** mode will overwrite the configuration with the desired configuration in OV3600, and should only be used when you are certain OV3600 has the correct configuration. This can be risky, and generally, devices should be placed in **Monitor Only** mode as the default. ● **Thin APs Only**: Only thin APs will be automatically authorized in **Monitor Only** mode. This setting is ideal for mixed environments of thin and autonomous APs, or for very large subnets in which you don't want to auto-monitor all switches.
Default Group	Access Points	Sets the device group that this OV3600 server uses as the default for device-level configuration. Select a device group from the drop-down menu. A group must first be defined on the **Groups > List** page to appear in this drop-down menu. For additional information, refer to Chapter 4, "Configuring and Using Device Groups in OV3600" on page 69.
Device Configuration Audit Interval	Daily	If enabled, this setting defines the interval of queries which compares actual device settings to the Group configuration policies stored in the OV3600 database. If the settings do not match, the AP is flagged as mismatched and OV3600 sends an alert via email, log, or SNMP. Alcatel-Lucent recommends enabling this feature with a frequency of Daily or more frequently to ensure that your AP configurations comply with your established policies.
Automatically Repair Misconfigured Devices	Disabled	If enabled, this setting automatically reconfigures the settings on the device when the device is in **Manage** mode and OV3600 detects a variance between actual device settings and the Group configuration policy in the OV3600 database.
Send Debugging Messages	Enabled	If enabled, OV3600 automatically emails any system errors to Alcatel-Lucent Support to assist in debugging.
Nightly Maintenance Time (00:00 - 23:59)	04:15	Specifies the local time of day OV3600 should perform daily maintenance. During maintenance, OV3600 cleans the database, performs backups, and completes a few other housekeeping tasks. Such processes should not be performed during peak hours of demand.
OV3600 User Authorization Lifetime (0-240 min)	120	Sets the amount of time, in minutes, that an OV3600 user session lasts before the user must authenticate when a new browser window is opened. Setting the lifetime to **0** requires the user to log in every time a new browser window is opened.
Check for Software Updates	Yes	Enables OV3600 to check automatically for multiple update types. Check daily for OV3600 updates, to include enhancements, device template files, important security updates, and other important news. This setting requires a direct internet connection via OV3600.

2. Select the **Top Header Stats** to be displayed at the top of the interface. For more detailed information about each option, refer to Table 6 on page 22.

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

NOTE

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

Table 10 describes the settings and default values in this section.

Table 10 *OV3600* ***Setup*** *>* ***General*** *>* ***Display Options*** *Fields and Default Values*

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

4. On the **OV3600 Setup > General** page, locate the **Device Configuration** section and adjust settings for whether certain changes can be pushed to devices in **Monitor Only** mode. Table 11 describes the settings and default values of this section.

Table 11 ***OV3600 Setup*** *>* ***General*** *>* ***Device Configuration*** *Section Fields and Default Values*

Setting	Default	Description
Guest User Configuration	Disabled	Enables or prevents guest users to/from pushing configurations to devices. Options are **Disabled** (default), **Enabled for Devices in Manage (Read/Write)**, **Enabled for all Devices**.
Allow WMS offload configuration in monitor-only mode	No	When **Yes** is selected, you can enable the AOS-W WMS offload feature on the **Groups > Basic** page for WLAN switches in **Monitor Only** mode. Enabling WMS offload does not cause a controller to reboot. This option is supported only for Aruba Networks and Alcatel-Lucent devices.
Allow disconnecting users while in monitor-only mode	No	Sets whether you can deauthenticate a user for a device in monitor-only mode. If set to **No**, the **Deauthenticate User** button for in a **Users > User Detail** page is enabled only for Managed devices.

Table 11 ***OV3600 Setup** > **General** > **Device Configuration*** *Section Fields and Default Values (Continued)*

Setting	Default	Description
Allow non-UTF8 characters	No	Whether OV3600 can use character sets other than UTF-8 for configuration settings.
Use Global Alcatel-Lucent Configuration	Yes	Enables Alcatel-Lucent configuration profile settings to be globally configured and then assigned to device groups. If disabled, settings can be defined entirely within **Groups > Dell PowerConnect W Config** instead of globally. **NOTE:** Changing this setting may require importing configuration on your devices. When an existing Alcatel-Lucent configuration setup is to be converted from global to group, follow these steps: 1. Set all the devices to Monitor Only mode before setting the flag. 2. Each device Group will need to have an import performed from the Audit page of some controller in the OV3600 group. 3. All of the thin APs need to have their settings imported after the device group settings have finished importing. 4. If the devices were set to Monitor Only mode, set them back to Managed mode.

5. On the **OV3600 Setup > General** page, locate the **External Logging** section and adjust settings to send audit and system events to an external syslog server. Table 12 describes these settings and default values.

Table 12 ***OV3600 Setup** > **General** > **External Syslog Section*** *Fields and Default Values*

Setting	Default	Description
Syslog Server	N/A	Enter the IP address of the syslog server.
Syslog Port	N/A	Enter the port of the syslog server.
Include event log messages	No	Select **Yes** to send event log messages to an external syslog server.
Event log facility	local1	Select the facility for the event log from the drop-down menu.
Include audit log messages	No	Select **Yes** to send audit log messages to an external syslog server.
Audit log facility	local1	Select the facility for the audit log from the drop-down menu.

6. On the **OV3600 Setup > General** page, locate the **Historical Data Retention** section and specify the number of days you wish to keep client session records and rogue discovery events. Table 13 describes the settings and default values of this section. Many settings can be set to have no expiration date.

Table 13 ***OV3600 Setup** > **General** > **Historical Data Retention*** *Fields and Default Values*

Setting	Default	Description
Inactive User Data (2-1500 days)	60	Defines the number of days OV3600 stores basic information about inactive users. Alcatel-Lucent recommends a shorter setting of 60 days for customers with high user turnover such as hotels. The longer you store inactive user data, the more hard disk space you require.
User Association History (2-550 days)	14	Defines the number of days OV3600 stores client session records. The longer you store client session records, the more hard disk space you require.
Tag History (2-550 days)	14	Sets the number of days OV3600 retains location history for Wi-Fi tags.
Rogue AP Discovery Events (2-550 days)	14	Defines the number of days OV3600 stores Rogue Discovery Events. The longer you store discovery event records, the more hard disk space you require.
Reports (2-550 days)	60	Defines the number of days OV3600 stores Reports. Large numbers of reports, over 1000, can cause the **Reports > List** page to be slow to respond.

Table 13 ***OV3600 Setup > General > Historical Data Retention*** *Fields and Default Values (Continued)*

Setting	Default	Description
Automatically Acknowledged Alerts (0-550 days, zero disables)	14	Defines automatically acknowledged alerts as the number of days OV3600 retains alerts that have been automatically acknowledged. Setting this value to 0 disables this function, and alerts will never expire or be deleted from the database.
Acknowledged Alerts (2-550 days)	60	Defines the number of days OV3600 retains information about acknowledged alerts. Large numbers of Alerts, over 2000, can cause the **System > Alerts** page to be slow to respond.
Traps from managed devices (0-550 days, zero disables)	14	Defines the number of days OV3600 retains information about SNMP traps from Managed Devices. Setting this value to **0** disables this function, and the trap information will never expire or be deleted from the database.
Archived Device Configurations (1-100)	10	Sets the number of archived configurations to retain for each device.
Guest Users (0-550 days, zero disables)	30	Sets the number of days that OV3600 is to support any guest user. A value of **0** disables this function, and guest users will never expire or be deleted from the OV3600 database.
Closed Helpdesk Incidents (0-550 days, zero disables)	30	Sets the number of days that OV3600 is to retain records of closed Helpdesk incidents once closed. Setting this value to **0** disables this function, and Helpdesk information will never expire or be deleted from the database.
Inactive SSIDs (0-550 days, zero disables)	425	Sets the number of days OV3600 retains historical information after OV3600 last saw a client on a specific SSID. Setting this value to **0** disables this function, and inactive SSIDs will never expire or be deleted from the database.
Inactive Interfaces (0-550 days, zero disables)	425	Sets the number of days OV3600 retains inactive interface information after the interface has been removed or deleted from the device. Setting this value to **0** disables this function, and inactive interface information will never expire or be deleted from the database.
Interface Status History (0-550 days, zero disables)	425	Sets the number of days OV3600 retains historical information on interface status. Setting this value to **0** disables this function.
Interfering Devices (0-550 days, zero disables)	14	Sets the number of days OV3600 retains historical information on interfering devices. Setting this value to **0** disables this function.

7. On the **OV3600 Setup > General** page, locate the **Default Firmware Upgrade Options** section and adjust settings as required. This section allows you to configure the default firmware upgrade behavior for OV3600. Table 14 describes the settings and default values of this section.

Table 14 ***OV3600 Setup > General > Default Firmware Upgrade Options*** *Fields and Default Values*

Setting	Default	Description
Allow Firmware Upgrades in Monitor Only mode	No	If **Yes** is selected, OV3600 upgrades the firmware for APs in **Monitor Only** mode. When OV3600 upgrades the firmware in this mode, the desired configuration are not be pushed to OV3600. Only the firmware is applied. The firmware upgrade may result in configuration changes. OV3600 does not correct those changes when the AP is in **Monitor Only** mode.
Simultaneous Jobs (1-20)	20	Defines the number of jobs OV3600 runs at the same time. A job can include multiple APs.
Simultaneous Devices Per Job (1-1000)	20	Defines the number of devices that can be in the process of upgrading at the same time. OV3600 only runs one TFTP transfer at a time. As soon as the transfer to a device has completed, the next transfer begins, even if the first device is still in the process of rebooting or verifying configuration.

Table 14 *OV3600 Setup > General > Default Firmware Upgrade Options Fields and Default Values (Continued)*

Setting	Default	Description
Failures Before Stopping (0-20)	1	Sets the default number of upgrade failures before OV3600 pauses the upgrade process. User intervention is required to resume the upgrade process. Setting this value to **0** disables this function.

8. On the **OV3600 Setup > General** page, locate the **Additional OV3600 Services** section, and adjust settings as required. Table 15 describes the settings and default values of this section.

Table 15 *OV3600 Setup > General > Additional OV3600 Services Fields and Default Values*

Setting	Default	Description
Enable FTP Server	No	Enables or disables the FTP server on OV3600. The FTP server is only used to manage Cisco Aironet 4800 APs. Alcatel-Lucent recommends disabling the FTP server if you do not have any Cisco Aironet 4800 APs in the network.
Enable RTLS Collector	No	Enables or disables the RTLS Collector, which is used to allow AOS-W switches to send signed and encrypted RTLS (real time locating system) packets to VisualRF-- in other words, OV3600 becomes the acting RTLS server. The RTLS server IP address must be configured on each switch. This function is used for VisualRF to improve location accuracy and to locate chirping asset tags. This function is supported only for Dell PowerConnect W, Alcatel-Lucent and Aruba Networks devices. With selection of **Yes**, the following additional fields appear, which you should populate to match the settings configured on the switch: ● **RTLS Port**—Specify the port for the OV3600 RTLS server. ● **RTLS Username**—Enter the user name used by the switch to decode RTLS messages. ● **RTLS Password**—Enter the RTLS server password that matches the switches' value.
Use Embedded Mail Server	Yes	Enables or disables the embedded mail server that is included with OV3600.This field supports a **Send Test Email** button for testing server functionality. This button prompts you with a **To** and **From** field in which you must enter valid email addresses, and a button to send a test email.
Process User Roaming Traps from Cisco WLC	Yes	OV3600 now parses client association and authentication traps from Cisco WLC controllers to give real time information on users connected to the wireless network.
Enable AMON data collection	Yes	Allows OV3600 to collect enhanced data from Alcatel-Lucent devices on certain firmware versions; see the *Best Practices Guide* for more details.

9. On the **OV3600 Setup > General** page, locate the **Performance** section. Performance tuning is unlikely to be necessary for many OV3600 implementations, and likely provides the most improvements for customers with extremely large Pro or Enterprise installations. Please contact Alcatel-Lucent support if you think you might need to change any of these settings. Table 16 describes the settings and default values of this section.

Table 16 *OV3600 Setup > General > Performance Fields and Default Values*

Setting	Default	Description
Monitoring Processes	Based on the number of cores for your server	Optional setting configures the throughput of monitoring data. Increasing this setting allows OV3600 to process more data per second, but it can take resources away from other OV3600 processes. Please contact Alcatel-Lucent support if you think you might need to increase this setting for your network.
Maximum Number of Configuration Processes	5	Increases the number of processes that are pushing configurations to your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Please contact Alcatel-Lucent support if you think you might need to increase this setting for your network.

Table 16 *OV3600 Setup > General > Performance Fields and Default Values (Continued)*

Setting	Default	Description
Maximum Number of Audit Processes	3	Increases the number of processes that audit configurations for your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Contact Alcatel-Lucent support if you are considering increasing this setting for your network.
Verbose Logging of SNMP Configuration	No	Enables or disables logging detailed records of SNMP configuration information.
SNMP Rate Limiting for Monitored Devices	No	When enabled, OV3600 fetches SNMP data more slowly, potentially reducing device CPU load. Alcatel-Lucent recommends enabling this global setting when monitoring Alcatel-Lucent switches only if your network contains a majority of legacy switches (800, 2400, 5000, switches that use Supervisor Module II). If your network mainly uses newer processors (3000 series, 600 series, the M3 module in the 6000 series), Alcatel-Lucent strongly recommends disabling this setting.
RAPIDS Processing Priority	Low	Defines the processing and system resource priority for RAPIDS in relation to OV3600 as a whole. When OV3600 is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (such as client connections and bandwidth) is not adversely impacted. The default priority is **Low**. You can also tune your system performance by changing group poll periods.

10. Select **Save** when the **General Server** settings are complete and whenever making subsequent changes.

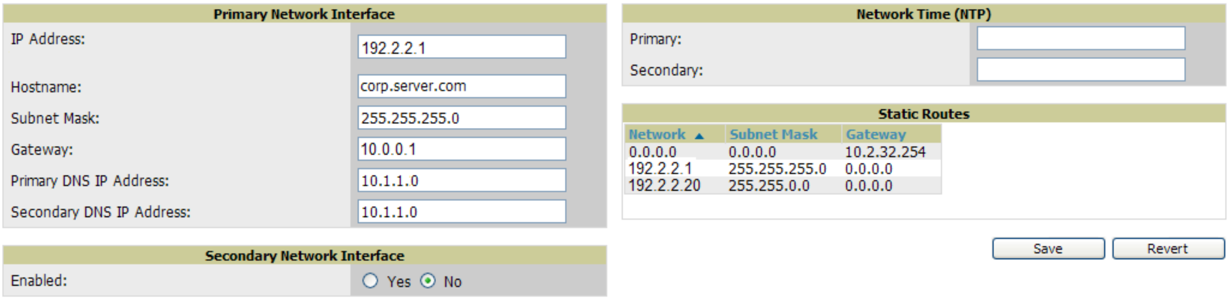
What Next?

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

Defining OV3600 Network Settings

The next step in configuring OV3600 is to confirm the OV3600 network settings. Define these settings by navigating to the **OV3600 Setup > Network** page. Figure 17 illustrates the contents of this page.

Figure 17 **OV3600** *Setup > Network Page Illustration*



Primary Network Interface

IP Address:	192.2.2.1
Hostname:	corp.server.com
Subnet Mask:	255.255.255.0
Gateway:	10.0.0.1
Primary DNS IP Address:	10.1.1.0
Secondary DNS IP Address:	10.1.1.0

Secondary Network Interface

Enabled: ○ Yes ● No

Network Time (NTP)

Primary:

Secondary:

Static Routes

Network ▲	Subnet Mask	Gateway
0.0.0.0	0.0.0.0	10.2.32.254
192.2.2.1	255.255.255.0	0.0.0.0
192.2.2.20	255.255.0.0	0.0.0.0

Perform the following steps to define the OV3600 network settings:

1. Locate the **Primary** and **Secondary Network Interface** sections. The information in these sections should match what you defined during initial network configuration and should not require changes. Table 17 describes the settings and default values.

Table 17 ***Primary and Secondary Network Interface** Fields and Default Values*

Setting	Default	Description
IP Address	None	Sets the IP address of the OV3600 network interface. This address must be a static IP address.
Hostname	None	Sets the DNS name assigned to the OV3600 server.
Subnet Mask	None	Sets the subnet mask for the primary network interface.
Gateway	None	Sets the default gateway for the network interface.
Primary DNS IP	None	Sets the primary DNS IP address for the network interface.
Secondary DNS IP	None	Sets the secondary DNS IP address for the network interface.
Secondary Network Interface	No	Select **Yes** to enable a secondary network interface. You must also define the IP address and subnet mask.

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

NOTE

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

To disable NTP services, clear both the **Primary** and **Secondary** NTP server fields. Any problem related to communication between OV3600 and the NTP servers creates an entry in the event log. Table 18 describes the settings and default values in more detail. For more information on ensuring that OV3600 servers have the correct time, please see http://support.ntp.org/bin/view/Servers/NTPPoolServers.

Table 18 ***OV3600 Setup** > **Network** > **Secondary Network** Fields and Default Values*

Setting	Default	Description
Primary	ntp1.yourdomain.com	Sets the IP address or DNS name for the primary NTP server.
Secondary	ntp2.yourdomain.com	Sets the IP address or DNS name for the secondary NTP server.

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

NOTE

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

4. Select **Save** when you have completed all changes on the **OV3600 Setup > Network** page, or select **Revert** to return to the last settings. **Save** restarts any affected services and may temporarily disrupt your network connection.

What Next?

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

Creating OV3600 Users

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

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

Each general user that you add needs a **Username**, a **Password,** and a **Role**. Use unique and meaningful user names as they are recorded in the log files when you or other users make changes in OV3600.

NOTE

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

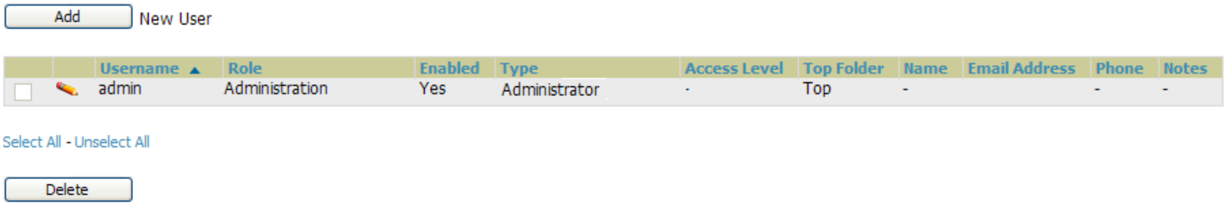
The user *role* defines the user type, access level, and the top folder for that user. User roles are defined on the **OV3600 Setup > Roles** page. Refer to the next procedure in this chapter for additional information, “Creating OV3600 User Roles” on page 44.

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

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

1. Go to the **OV3600 Setup > Users** page. This page displays all users currently configured in OV3600. Figure 18 illustrates the contents and layout of this page.

Figure 18 ***OV3600 Setup > Users*** *Page Illustration*



Add New User

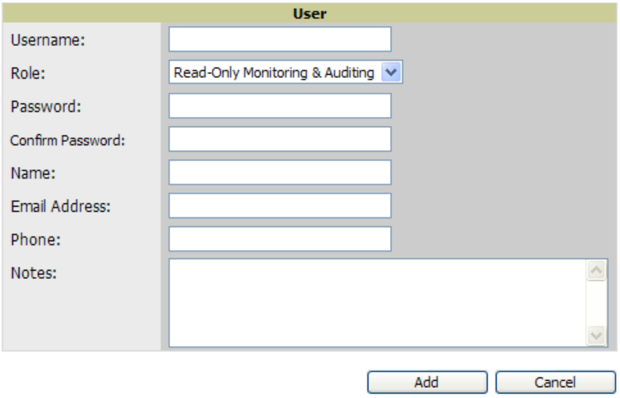
		Username ▲	Role	Enabled	Type	Access Level	Top Folder	Name	Email Address	Phone	Notes
□	✎	admin	Administration	Yes	Administrator	-	Top	-		-	-

Select All - Unselect All

Delete

2. Select **Add** to create a new user, select the pencil icon to edit an existing user, or select a user and select **Delete** to remove that user from OV3600. When you select **Add** or the edit icon, the **Add User** page appears, illustrated in Figure 19.

Figure 19 ***OV3600 Setup > Users > Add/Edit User*** *Page Illustration*



User

Username:

Role: Read-Only Monitoring & Auditing

Password:

Confirm Password:

Name:

Email Address:

Phone:

Notes:

Add Cancel

3. Enter or edit the settings on this page. Table 19 describes these settings in additional detail.

Table 19 *OV3600 Setup > User > Add/Edit User* *Fields and Default Values*

Setting	Default	Description
Username	None	Sets the username as an alphanumeric string. The Username is used when logging in to OV3600 and appears in OV3600 log files.
Role	None	Specifies the **User Role** that defines the Top viewable folder, type and access level of the user specified in the previous field. The **admin** user defines user roles on the **OV3600 Setup > Roles** page, and each user in the system is assigned to a role.
Password	None	Sets the password for the user being created or edited. Enter an alphanumeric string without spaces, and enter the password again in the **Confirm Password** field. **NOTE:** Because the default user's password is identical to the name, Alcatel-Lucent strongly recommends that your change this password.
Name	None	Allows you to define an optional and alphanumeric text field that takes note of the user's actual name.
Email Address	None	Allows you to specify a specific email address that will propagate throughout many additional pages in OV3600 for that user, including reports, triggers, and alerts.
Phone	None	Allows you to enter an optional phone number for the user.
Notes	None	Enables you to cite any additional notes about the user, including the reason they were granted access, the user's department, or job title.

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

NOTE

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

What Next?

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

Creating OV3600 User Roles

The **OV3600 Setup > Roles** page defines the viewable devices, the operations that can be performed on devices, and general OV3600 access. **VisualRF** uses the same user roles as defined for OV3600—users can see floor plans that contain an AP to which they have access in OV3600, although only visible APs appear on the floor plan.

Users can also see any building that contains a visible floor plan, and any campus that contains a visible building.

NOTE

In **VisualRF > Setup > Server Settings**, a new flag added in OV3600 7.2 allows you to restrict the visibility of empty floor plans to the role of the user who created them. In previous versions, a floor plan without APs could be visible to all users. By default, this setting is set to No.

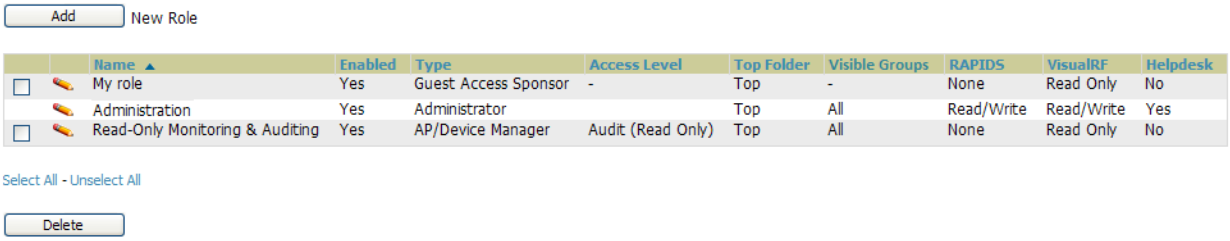
When a new role is added to OV3600, VisualRF must be restarted for the new user to be enabled. Refer to the *VisualRF User Guide* for additional information.

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

Perform the following steps to view, add, edit, or delete user **roles**:

1. Go to the **OV3600 Setup > Roles** page. This page displays all roles currently configured in OV3600. Figure 20 illustrates the contents and layout of this page.

Figure 20 ***OV3600 Setup > Roles*** *Page Illustration*



Add New Role

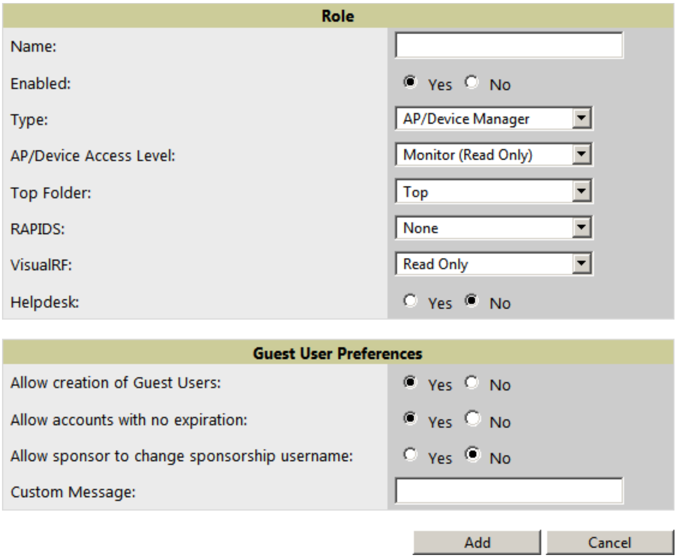
		Name ▲	Enabled	Type	Access Level	Top Folder	Visible Groups	RAPIDS	VisualRF	Helpdesk
□	✎	My role	Yes	Guest Access Sponsor	-	Top	-	None	Read Only	No
	✎	Administration	Yes	Administrator		Top	All	Read/Write	Read/Write	Yes
□	✎	Read-Only Monitoring & Auditing	Yes	AP/Device Manager	Audit (Read Only)	Top	All	None	Read Only	No

Select All - Unselect All

Delete

2. Select **Add** to create a new role, select the pencil icon to edit an existing role, or select a checkbox and select **Delete** to remove that role from OV3600. When you select **Add** or the edit icon, the **Add/Edit Role** page appears, illustrated in Figure 21.

Figure 21 ***OV3600 Setup > Roles > Add/Edit Role*** *Page Illustration*



Role	
Name:	
Enabled:	● Yes ○ No
Type:	AP/Device Manager
AP/Device Access Level:	Monitor (Read Only)
Top Folder:	Top
RAPIDS:	None
VisualRF:	Read Only
Helpdesk:	○ Yes ● No

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

Add Cancel

3. Enter or edit the settings on this page. Table 20 describes these settings in additional detail.

   As explained earlier in this section, **Roles** define the type of user-level access, the user-level privileges, and the view available to the user for device groups and devices in OV3600. Table 20 describes the settings and default values of this section.

Table 20 ***OV3600 Setup > Roles > Add/Edit Roles*** *Fields and Default Values*

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

Table 20 ***OV3600 Setup > Roles > Add/Edit Roles*** *Fields and Default Values (Continued)*

Setting	Default	Description
Type	AP/Device Manager	Defines the type of role. OV3600 supports the following role types: ● **OV3600 Administrator**—The OV3600 Administrator has full access to OV3600 and all of the devices. Only the OV3600 Administrator can create new users or access the **OV3600 Setup** page. ● **AP/Device Manager**—AP/Device Managers have access to a limited number of devices and groups based on the Top folder and varying levels of control based on the Access Level. ● **AirWave Management Client**—The AirWave Management Client (AMC) software allows WiFi-enabled devices to serve as additional sensors to gather data for RAPIDS. Use this role type to set up a client to be treated as a user with the AMC role. The user information defined in AMC must match the user with the Alcatel-Lucent Management Client type. ● **Guest Access Sponsor**—Limited-functionality role to allow helpdesk or reception desk staff to grant wireless access to temporary personnel. This role only has access to the defined top folder of APs.
AP/Device Access Level	None	Defines the privileges the role has over the viewable APs. OV3600 supports three privilege levels, as follows: ● **Manage (Read/Write)**—Manage users can view and modify devices and Groups. ● **Audit (Read Only)**—Audit users have read only access to the viewable devices and Groups. Audit users have access to the **APs/Devices > Audit** page, which may contain sensitive information including AP passwords. ● **Monitor (Read Only)**—Monitor users have read-only access to devices and groups and VisualRF. Monitor users cannot view the **APs/Devices > Audit** page which may contain sensitive information, including passwords.
Top Folder	None	Defines the Top viewable folder for the role. The role is able to view all devices and groups contained by the Top folder. The top folder and its subfolders must contain all of the devices in any of the groups it can view. **NOTE:** OV3600 enables user roles to be created with access to folders within multiple branches of the overall hierarchy. This feature assists non-administrator users who support *a subset of accounts or sites* within a single OV3600 deployment, such as help desk or IT staff. User roles can be restricted to multiple folders within the overall hierarchy, even if they do not share the same top-level folder. Non-administrator users are only able to see data and users for devices within their assigned subset of folders.
RAPIDS	None	Sets the RAPIDS privileges, which are set separately from the APs/Devices. This field specifies the RAPIDS privileges for the role, and options are as follows: ● **None**— Cannot view the RAPIDS tab or any Rogue APs. ● **Read Only**—The user can view the RAPIDS pages but cannot make any changes to rogue APs or perform OS scans. ● **Read/Write**—The user may ignore, delete, override scores and perform OS scans.
Helpdesk	No	Sets the role to support helpdesk users, with parameters that are specific to the needs of helpdesk personnel supporting users on a wireless network.
Enable Adobe Flash	Yes	Enables the Adobe Flash application for all users who are assigned this role. Adobe Flash supports dynamic graphics on the **Home > Overview** page, VisualRF, Quickview functions, and additional OV3600 pages. **NOTE:** This field is only visible if a specific flag is set in the OV3600 database. By default this option is hidden and Flash is enabled for all users.
Allow creation of Guest Users	Yes	If this option is enabled, users with an assigned role of Monitoring or Audit can be given access to guest user account creation along with the option to allow a sponsor to change its username. A custom message can also be included. The **Guest User Preferences** section does not apear if Guest User Configuration is disabled in **OV3600 Setup > General**.

What Next?

- Go to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.

- *Complete the required configurations in this chapter before proceeding.* Alcatel-Lucent support remains available to you for any phase of OV3600 installation.

Enabling OV3600 to Manage Your Devices

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

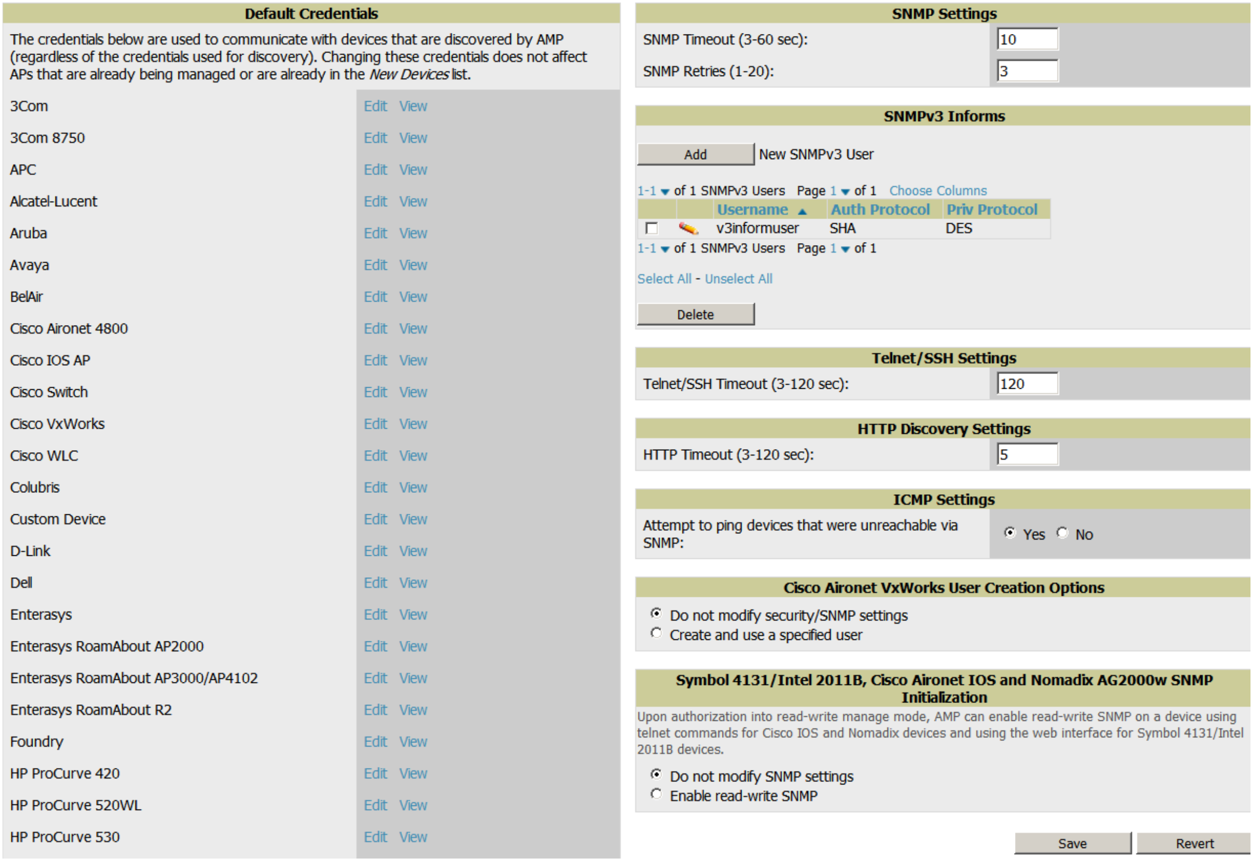
This section contains the following procedures:

- Configuring Communication Settings for Discovered Devices
- Loading Device Firmware onto OV3600 (Optional)
  - Overview of the Device Setup > Upload Firmware & Files Page
  - Loading Firmware Files to OV3600

Configuring Communication Settings for Discovered Devices

To configure OV3600 to communicate with your devices, to define the default shared secrets, and to set SNMP polling information, navigate to the **Device Setup > Communication** page, illustrated in Figure 22.

Figure 22 ***Device Setup > Communication*** *Page Illustration*



Default Credentials

The credentials below are used to communicate with devices that are discovered by AMP (regardless of the credentials used for discovery). Changing these credentials does not affect APs that are already being managed or are already in the *New Devices* list.

3Com	Edit View
3Com 8750	Edit View
APC	Edit View
Alcatel-Lucent	Edit View
Aruba	Edit View
Avaya	Edit View
BelAir	Edit View
Cisco Aironet 4800	Edit View
Cisco IOS AP	Edit View
Cisco Switch	Edit View
Cisco VxWorks	Edit View
Cisco WLC	Edit View
Colubris	Edit View
Custom Device	Edit View
D-Link	Edit View
Dell	Edit View
Enterasys	Edit View
Enterasys RoamAbout AP2000	Edit View
Enterasys RoamAbout AP3000/AP4102	Edit View
Enterasys RoamAbout R2	Edit View
Foundry	Edit View
HP ProCurve 420	Edit View
HP ProCurve 520WL	Edit View
HP ProCurve 530	Edit View

SNMP Settings

SNMP Timeout (3-60 sec): 10

SNMP Retries (1-20): 3

SNMPv3 Informs

Add New SNMPv3 User

1-1 ▾ of 1 SNMPv3 Users Page 1 ▾ of 1 Choose Columns

		Username ▲	Auth Protocol	Priv Protocol
□	✎	v3informuser	SHA	DES

1-1 ▾ of 1 SNMPv3 Users Page 1 ▾ of 1

Select All - Unselect All

Delete

Telnet/SSH Settings

Telnet/SSH Timeout (3-120 sec): 120

HTTP Discovery Settings

HTTP Timeout (3-120 sec): 5

ICMP Settings

Attempt to ping devices that were unreachable via SNMP: ● Yes ○ No

Cisco Aironet VxWorks User Creation Options

● Do not modify security/SNMP settings
○ Create and use a specified user

Symbol 4131/Intel 2011B, Cisco Aironet IOS and Nomadix AG2000w SNMP Initialization

Upon authorization into read-write manage mode, AMP can enable read-write SNMP on a device using telnet commands for Cisco IOS and Nomadix devices and using the web interface for Symbol 4131/Intel 2011B devices.

● Do not modify SNMP settings
○ Enable read-write SNMP

Save Revert

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

1. On the **Device Setup > Communication** page, locate the **Default Credentials** area. Enter the credentials for each device model on your network. The default credentials are assigned to all newly discovered APs.

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

NOTE

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

2. Browse to the **Device Setup > Communication** page, locate the **SNMP Settings** section, and enter or revise the following information. Table 21 lists the settings and default values.

Table 21 ***Device Setup > Communication > SNMP Settings*** *Fields and Default Values*

Setting	Default	Description
SNMP Timeout	3	Sets the time, in seconds, that OV3600 waits for a response from a device after sending an SNMP request.
SNMP Retries	3	Sets the number of times OV3600 tries to poll a device when it does not receive a response within the **SNMP Timeout Period** or the Group's **Missed SNMP Poll Threshold** setting (1-100). If OV3600 does not receive an SNMP response from the device after the specified number of retries, OV3600 classifies that device as **Down**.

3. Locate the **SNMP v3 Informs** section. Select **Add New SNMP v3 User** to reveal its configuration section. OV3600 users will need to configure all v3 users that are configured on the controller; the SNMP Inform receiver in the OV3600 will be restarted when users are changed or added to the controller.
   - **Username** - Username of the SNMP v3 user as configured on the controller.
   - **Auth Protocol** - Can be MD5 or SHA. The default setting is SHA.
   - **Auth and Priv Passphrases** - Enter the auth and priv passphrases for the user as configured on the controller.
   - **Priv Protocol** - Can be DES or AES. The default setting is DES.
4. Locate the **Telnet/SSH Settings** section, and complete or adjust the default value for the field in this section. Table 22 lists the setting and default value.

Table 22 ***Telnet/SSH Settings*** *Fields and Default Values*

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

5. On the **Device Setup > Communication** page, locate the **HTTP Discovery Settings** section. Complete or revise the default values for the settings in this section. Table 23 lists these settings and default values.

Table 23 ***HTTP Discovery Settings*** *Fields and Default Values*

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

6. On the **Device Setup > Communication** page, locate the **ICMP Settings** section. Complete the setting or revise the default value as required. Table 24 itemizes the setting and default value.

Table 24 ***Device Setup** > **Communication** > **ICMP Settings** Fields and Default Values*

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

7. On the **Device Setup > Communication** page, locate the **Cisco Aironet VxWorks User Creation Options** section. You only need to provide this information if you use VxWorks-based Cisco APs on your network, as follows:

   - Aironet 340
   - Aironet 350
   - Aironet 1200

   Select one of the three options listed. Table 25 describes the settings and default values of this section.

Table 25 ***Cisco Aironet VxWorks User Creation Options** Fields and Default Values*

Setting	Default	Description
Do not modify security/SNMP settings	N/A	Enables OV3600 using only an existing user account on the AP, as defined in the **Cisco VxWorks Username/Password** section in the **Default Secrets** area. This user account must have all permissions set.
Create and use specified user	N/A	Enables OV3600 to create a new user account, specified below, on each AP with all permissions enabled.

8. On the **Device Setup > Communication** page, locate the **Symbol 4131 and Cisco Aironet IOS SNMP Initialization** area. You only need to provide this information if you use Symbol 4131 or Cisco Aironet IOS access points. Select one of the options listed. Table 26 describes the settings and default values.

Loading Device Firmware onto OV3600 (Optional)

Table 26 ***Device Setup** > **Communications** Fields and Default Values*

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

Overview of the Device Setup > Upload Firmware & Files Page

OV3600 enables automated firmware distribution to the devices on your network. Once you have downloaded the firmware files from the vendor, you can upload this firmware to OV3600 for distribution to devices via the **Device Setup > Upload Firmware & Files** page.

This page lists all firmware files on OV3600 with file information. This page also enables you to add new firmware files, to delete firmware files, and to add **New Web Auth Bundle** files.

The following additional pages support firmware file information:

- Firmware files uploaded to OV3600 appear as options in the drop-down menus on the **Group > Firmware** page and on individual **APs/Devices > Manage** pages.
- Use the **OV3600 Setup** page to configure OV3600-wide default firmware options.

Table 27 below itemizes the contents, settings, and default values for the **Upload Firmware & Files** page.

Table 27 ***Device Setup** > **Upload Firmware & Files** Fields and Default Values*

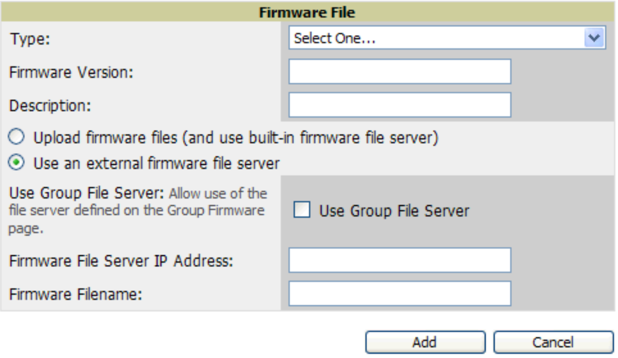
Setting	Default	Description
Type	None	Displays a drop-down list of the primary AP makes and models that OV3600 supports with automated firmware distribution.
Owner Role	None	Displays the user role that uploaded the firmware file. This is the role that has access to the file when an upgrade is attempted.
Description	None	Displays a user-configurable text description of the firmware file.
Server Protocol	None	Displays the file transfer protocol by which the firmware file was obtained from the server.
Use Group File Server	None	Displays the name of the file server supporting the group.
Firmware Filename	None	Displays the name of the file that was uploaded to OV3600 and to be transferred to an AP when the file is used in an upgrade.
Firmware Version	None	Displays the firmware version number. This is a user-configurable field.
Firmware MD5 Checksum	None	Displays the MD5 checksum of the file after it was uploaded to OV3600. The MD5 checksum is used to verify that the file was uploaded to OV3600 without issue. The checksum should match the checksum of the file before it was uploaded.
Firmware File Size	None	Displays the size of the firmware file in bytes.
HTML Filename	None	Supporting HTML, displays the name of the file that was uploaded to OV3600 and to be transferred to an AP when the file is used in an upgrade.
HTML Version	None	Supporting HTML, displays the version of HTML used for file transfer.
HTML MD5 Checksum	None	Supporting HTML, displays the MD5 checksum of the file after it was uploaded to OV3600. The MD5 checksum is used to verify that the file was uploaded to OV3600 without issue. The checksum should match the checksum of the file before it was uploaded.
HTML File Size	None	Supporting HTML, displays the size of the file in bytes.
Desired Firmware File for Specified Groups	None	The firmware file is set as the desired firmware version on the **Groups > Firmware Files** page of the specified groups. You cannot delete a firmware file that is set as the desired firmware version for a group.

Loading Firmware Files to OV3600

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

1. Go to the **Device Setup > Upload Firmware & Files** page.
2. Select **Add**. The **Add Firmware File** page appears. Figure 23 illustrates this page.

Figure 23 ***Device Setup > Add New Firmware*** *Page Illustration*



Firmware File

Type: Select One...

Firmware Version:

Description:

○ Upload firmware files (and use built-in firmware file server)

● Use an external firmware file server

Use Group File Server: Allow use of the file server defined on the Group Firmware page. □ Use Group File Server

Firmware File Server IP Address:

Firmware Filename:

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

NOTE

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

4. Enter the appropriate information and select **Add**. The file uploads to OV3600 and once complete, this file appears on the **Device Setup > Upload Firmware & Files** page. This file also appears on additional pages that display firmware files (such as the **Group > Firmware** page and on individual **APs/Devices > Manage** pages).
5. You can also import a CSV list of groups and their external TFTP firmware servers. Table 28 itemizes the settings of this page.

Table 28 ***Supported Firmware Versions and Features*** *Fields and Default Values*

Setting	Default	Description
Type	Alcatel-Lucent Switch	Indicates the firmware file is used with the specified type. If you select an IOS device from the **Type** drop-down menu, you have the option of choosing a server protocol of TFTP or FTP. If you choose FTP, you may later notice that the firmware files are pushed to the device more quickly. With selection of some types, particularly Cisco controllers, you can specify the boot software version.
Firmware Version	None	Provides a user-configurable field to specify the firmware version number. Appears if you did not select the default **Alcatel-Lucent Switch** type.
Description	None	Provides a user-configurable text description of the firmware file.
Upload firmware files (and use built-in firmware)	Built-in	Selects the TFTP server that access points use to download their firmware. The built-in TFTP server is recommended. If you choose to use an external TFTP server, enter the **File Server IP Address** and the **Firmware Filename**.
Use an external firmware file server	N/A	You can also choose to assign the external TFTP server on a per-group basis. If you select this option, you must enter the IP address on the **Groups > Firmware** page. Complete the **Firmware File Server IP Address** field. **NOTE:** With selection of some Types, you are prompted with the Server Protocol field that lets you select which protocol to use, and this varies from device to device. If you select FTP, OV3600 uses an anonymous user for file upload.
Use Group File Server	Disabled	If you opt to use an external firmware file server, this additional option appears. This setting instructs OV3600 to use the server that is associated with the group instead of defining a server.
Firmware File Server IP Address	None	Provides the IP address of the External TFTP Server (like SolarWinds) used for the firmware upgrade. This option displays when the user selects the **Use an external firmware file** option.
Firmware Filename	None	Enter the name of the firmware file that needs to be uploaded. Ensure that the firmware file is in the TFTP root directory. If you are using a non-external server, you select **Choose File** to find your local copy of the file.

NOTE

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

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

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

NOTE

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

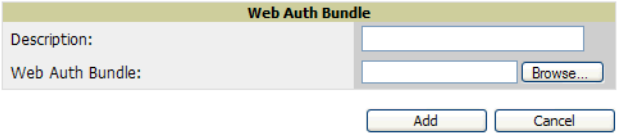
Using Web Auth Bundles in OV3600

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

Perform these steps to add or edit Web Auth bundles in OV3600.

1. Go to the **Device Setup > Upload Firmware & Files** page. This page displays any existing Web Auth bundles that are currently configured in OV3600, and allows you to add or delete Web Auth bundles.
2. Scroll to the bottom of the page. Select **Add New Web Auth Bundle** to create a new Web Auth bundle (see Figure 24), or select the pencil icon next to an existing bundle to edit. You may also delete Web Auth bundles by selecting that bundle with the checkbox, and selecting **Delete**.

Figure 24 ***Add Web Auth Bundle** Page Illustration*



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

For additional information and a case study that illustrates the use of Web Auth bundles with Cisco WLC controllers, refer to the following document on Cisco.com:

- Wireless LAN controller Web Authentication Configuration Example, Document ID: 69340

  http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008067489f.shtml

Configuring TACACS+ and RADIUS Authentication

As an optional configuration, you can set OV3600 to use an external user database to simplify password management for OV3600 administrators and users. This section contains the following procedures:

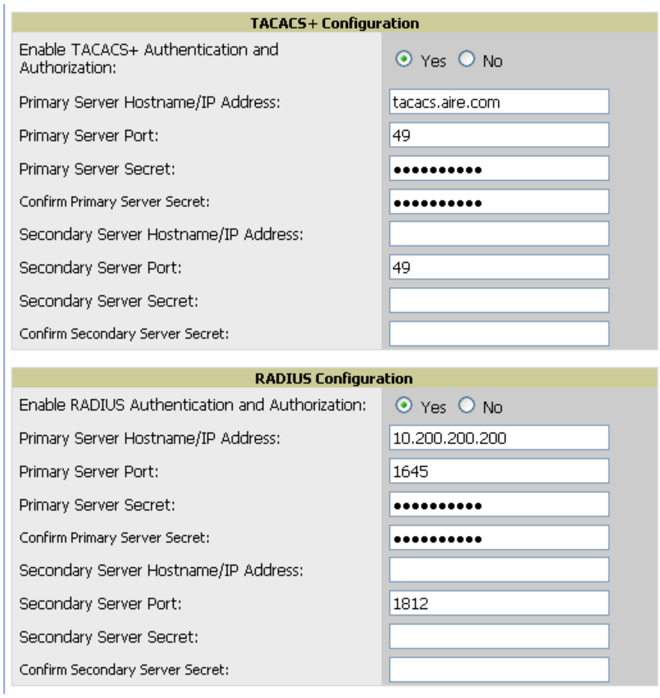
- Configuring TACACS+ Authentication
- Configuring RADIUS Authentication and Authorization
- Integrating a RADIUS Accounting Server

Configuring TACACS+ Authentication

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

1. Go to the **OV3600 Setup > Authentication** page. This page displays current status of TACACS+. Figure 25 illustrates this page when neither TACACS+ nor RADIUS authentication is enabled in OV3600.

Figure 25 ***OV3600 Setup > Authentication*** *Page Illustration*



TACACS+ Configuration

Enable TACACS+ Authentication and Authorization:	● Yes ○ No
Primary Server Hostname/IP Address:	tacacs.aire.com
Primary Server Port:	49
Primary Server Secret:	••••••••••
Confirm Primary Server Secret:	••••••••••
Secondary Server Hostname/IP Address:	
Secondary Server Port:	49
Secondary Server Secret:	
Confirm Secondary Server Secret:	

RADIUS Configuration

Enable RADIUS Authentication and Authorization:	● Yes ○ No
Primary Server Hostname/IP Address:	10.200.200.200
Primary Server Port:	1645
Primary Server Secret:	••••••••••
Confirm Primary Server Secret:	••••••••••
Secondary Server Hostname/IP Address:	
Secondary Server Port:	1812
Secondary Server Secret:	
Confirm Secondary Server Secret:	

2. Select **No** to disable or **Yes** to enable TACACS+ authentication. If you select **Yes**, several new fields appear. Complete the fields described in Table 29.

Table 29 ***OV3600 Setup > Authentication*** *Fields and Default Values*

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

3. Select **Save** and continue with additional steps.
4. To configure Cisco ACS to work with OV3600, you must define a new service named **OV3600** that uses https on the ACS server.
    - The OV3600 https service is added to the **TACACS+** (Cisco) interface under the **Interface Configuration** tab.
    - Select a checkbox for a new service.
    - Enter **OV3600** in the service column and **https** in the protocol column.

- Select **Save**.

5. Edit the existing groups or users in TACACS to use the “OV3600 service” and define a role for the group or user.
   - The role defined on the **Group Setup** page in ACS must match the exact name of the role defined on the **OV3600 Setup > Roles** page.
   - The defined role should use the following format: **`role=`**<*`name_of_OV3600_role`*>. One example is as follows:

     ```
     role=DormMonitoring
     ```

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

NOTE

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

What Next?

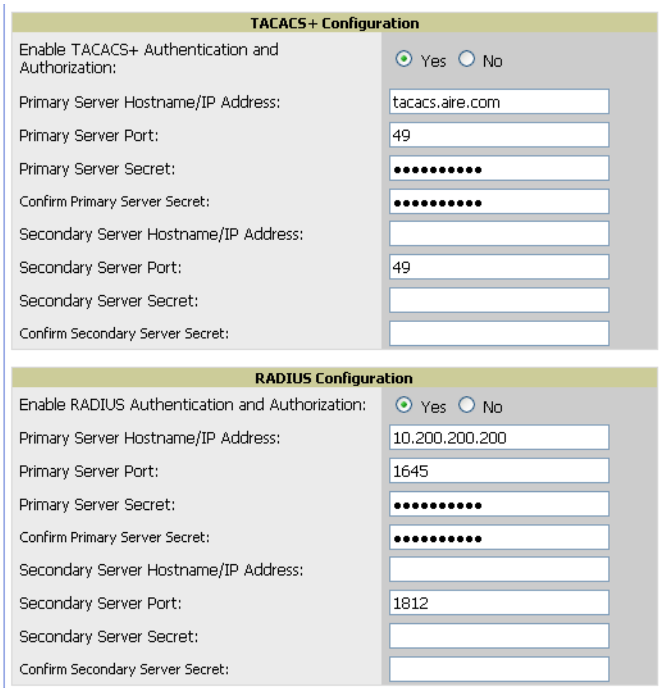
- Go to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* Alcatel-Lucent support remains available to you for any phase of OV3600 installation.

Configuring RADIUS Authentication and Authorization

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

1. Go to the **OV3600 Setup > Authentication** page. This page displays current status of RADIUS. Figure 26 illustrates this page.

Figure 26 ***OV3600 Setup* > *Authentication*** *Page Illustration*



TACACS+ Configuration

Enable TACACS+ Authentication and Authorization:	● Yes ○ No
Primary Server Hostname/IP Address:	tacacs.aire.com
Primary Server Port:	49
Primary Server Secret:	••••••••••
Confirm Primary Server Secret:	••••••••••
Secondary Server Hostname/IP Address:	
Secondary Server Port:	49
Secondary Server Secret:	
Confirm Secondary Server Secret:	

RADIUS Configuration

Enable RADIUS Authentication and Authorization:	● Yes ○ No
Primary Server Hostname/IP Address:	10.200.200.200
Primary Server Port:	1645
Primary Server Secret:	••••••••••
Confirm Primary Server Secret:	••••••••••
Secondary Server Hostname/IP Address:	
Secondary Server Port:	1812
Secondary Server Secret:	
Confirm Secondary Server Secret:	

2. Select **No** to disable or **Yes** to enable TACACS+ or RADIUS authentication. If you select **Yes**, several new fields appear. Complete the fields described in Table 30.

Table 30 ***OV3600 Setup* > *Authentication*** *Fields and Default Values*

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

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

Integrating a RADIUS Accounting Server

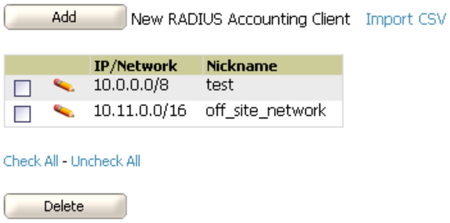
NOTE

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

Optionally, you can configure RADIUS server accounting on **OV3600 Setup > RADIUS Accounting.** This capability is not required for basic OV3600 operation, but can increase the user-friendliness of OV3600 administration in large networks. Figure 27 illustrates the settings of this optional configuration interface.

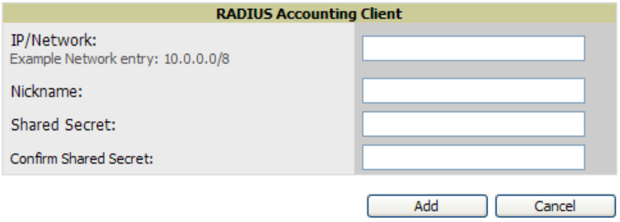
Perform the following steps and configurations to enable OV3600 to receive accounting records from a separate RADIUS server. Figure 27 illustrates the display of RADIUS accounting clients already configured, and Figure 28 illustrates the **Add RADIUS Accounting Client** page.

Figure 27 ***OV3600 Setup* > *RADIUS Accounting*** *Page Illustration*



		IP/Network	Nickname
□	✎	10.0.0.0/8	test
□	✎	10.11.0.0/16	off_site_network

Figure 28 ***OV3600 Setup* > *RADIUS* > *Add RADIUS Accounting Client*** *Page Illustration*



RADIUS Accounting Client

IP/Network:
Example Network entry: 10.0.0.0/8

Nickname:

Shared Secret:

Confirm Shared Secret:

1. To specify the RADIUS authentication server or network, browse to the **OV3600 Setup > RADIUS Accounting** page and select **Add**, illustrated in Figure 28, and provide the information in Table 31.
2. Select **Add**.

Table 31 ***OV3600 Setup* > *Radius Accounting*** *Fields and Default Values*

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

What Next?

- For more information about configuring WLAN Gateways or WLAN controllers such as BlueSocket, ReefEdge, or ProCurve wireless gateways, refer to "Third-Party Security Integration for OV3600" on page 257.
- Go to additional subtabs in **OV3600 Setup** to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* Alcatel-Lucent support remains available to you for any phase of OV3600 installation.

Configuring Cisco WLSE and WLSE Rogue Scanning

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

- Introduction to Cisco WLSE
- Configuring WLSE Initially in OV3600
- Configuring IOS APs for WDS Participation

- Configuring ACS for WDS Authentication
- Configuring Cisco WLSE Rogue Scanning

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

Introduction to Cisco WLSE

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

Table 32 *Cisco SWAN Architecture Components*

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

Configuring WLSE Initially in OV3600

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

- Adding an ACS Server for WLSE
- Enabling Rogue Alerts for Cisco WLSE
- Configuring WLSE to Communicate with APs
- Discovering Devices
- Managing Devices
- Inventory Reporting
- Defining Access
- Grouping
- WDS Participation
- Primary or Secondary WDS

Adding an ACS Server for WLSE

1. Go to the **Devices > Discover > AAA Server** page.
2. Select **New** from the drop-down list.
3. Enter the **Server Name**, **Server Port** (default 2002), **Username**, **Password**, and **Secret.**
4. Select **Save**.

Enabling Rogue Alerts for Cisco WLSE

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

Additional information about rogue device detection is available in "Configuring Cisco WLSE Rogue Scanning" on page 60.

Configuring WLSE to Communicate with APs

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

Discovering Devices

There are three methods to discover access points within WLSE, as follows:

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

Perform these steps to discover access points.

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

Managing Devices

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

NOTE

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

Use these pages to make such configurations:

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

Inventory Reporting

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

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

Defining Access

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

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

Grouping

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

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

Configuring IOS APs for WDS Participation

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

- Primary WDS
- Backup WDS
- WDS Member

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

NOTE

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

WDS Participation

Perform these steps to configure WDS participation.

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

Primary or Secondary WDS

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

1. Go to the **Wireless Services > WDS > General Setup** page.
2. If the AP is the Primary or Backup WDS, select **Use the AP as Wireless Domain Services**.
   - Select **Priority** (set **200** for Primary, **100** for Secondary).
   - Configure the **Wireless Network Manager** (configure the IP address of WLSE).
3. If the AP is Member Only, leave all options unchecked.
4. Go to the **Security > Server Manager** page.
5. Enter the **IP address** and **Shared Secret** for the ACS server and select **Apply**.
6. Go to the **Wireless Services > WDS > Server Group** page.
7. Enter the WDS Group of AP.
8. Select the **ACS server** in the **Priority 1** drop-down menu and select **Apply**.

Configuring ACS for WDS Authentication

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

1. Login to the ACS.
2. Go to the **System Configuration > ACS Certificate Setup** page.
3. Install a New Certificate by selecting the **Install New Certificate** button, or skip to the next step if the certificate was previously installed.

4. Select **User Setup** in the left frame.
5. Enter the **Username** that will be used to authenticate into the WDS and select **Add/Edit**.
6. Enter the **Password** that will be used to authenticate into the WDS and select **Submit**.
7. Go to the **Network Configuration > Add AAA Client** page.
8. Add **AP Hostname**, **AP IP Address**, and **Community String** (for the key).
9. Enter the **Password** that will be used to authenticate into the WDS and select **Submit**.

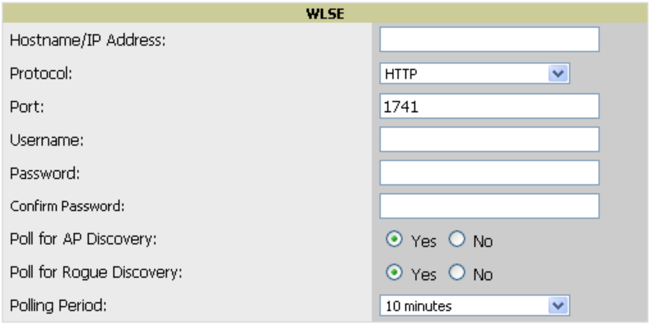
For additional and more general information about ACS, refer to "Configuring ACS Servers" on page 61.

Configuring Cisco WLSE Rogue Scanning

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

Figure 29 illustrates and itemizes the OV3600 settings for communication that is enabled between OV3600 and WLSE.

Figure 29 ***OV3600 Setup > WLSE > Add WLSE*** *Page Illustration*



WLSE

Hostname/IP Address:	
Protocol:	HTTP
Port:	1741
Username:	
Password:	
Confirm Password:	
Poll for AP Discovery:	● Yes ○ No
Poll for Rogue Discovery:	● Yes ○ No
Polling Period:	10 minutes

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

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

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

Setting	Default	Description
Hostname/IP Address	None	Designates the IP address or DNS Hostname for the WLSE server, which must already be configured on the Cisco WLSE server.
Protocol	HTTP	Specifies the protocol to be used when polling the WLSE.
Port	1741	Defines the port OV3600 uses to communicate with the WLSE server.
Username	None	Defines the username OV3600 uses to communicate with the WLSE server. The username and password must be configured the same way on the WLSE server and on OV3600. The user needs permission to display faults to discover rogues and inventory API (XML API) to discover manageable APs. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow OV3600 to pull the necessary XML APIs.
Password	None	Defines the password OV3600 uses to communicate with the WLSE server. The username and password must be configured the same way on the WLSE server and on OV3600. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow OV3600 to pull the necessary XML APIs.

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

Setting	Default	Description
Poll for AP Discovery; **Poll for Rogue Discovery**	Yes	Sets the method by which OV3600 uses WLSE to poll for discovery of new APs and/or new rogue devices on the network.
Last Contacted	None	Displays the last time OV3600 was able to contact the WLSE server.
Polling Period	10 minutes	Determines how frequently OV3600 polls WLSE to gather rogue scanning data.

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

What Next?

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

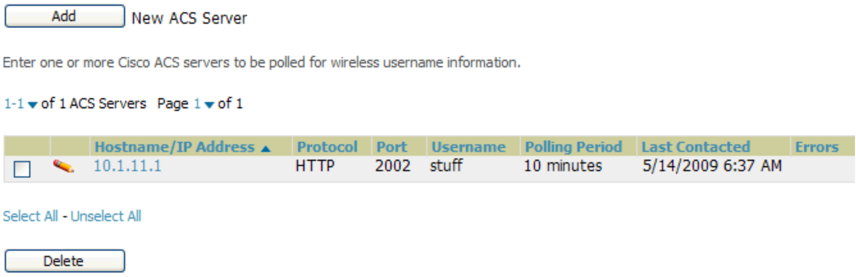
Configuring ACS Servers

This is an optional configuration. The **OV3600 Setup > ACS** page allows OV3600 to poll one or more Cisco ACS servers for wireless username information. When you specify an ACS server, OV3600 gathers information about your wireless users. Refer to "Configuring TACACS+ and RADIUS Authentication" on page 52 if you want to use your ACS server to manage your OV3600 users.

Perform these steps to configure ACS servers:

1. Go to the **OV3600 Setup > ACS** page. This page displays current ACS setup, as illustrated in Figure 30.

Figure 30 ***OV3600 Setup > ACS** Page Illustration*



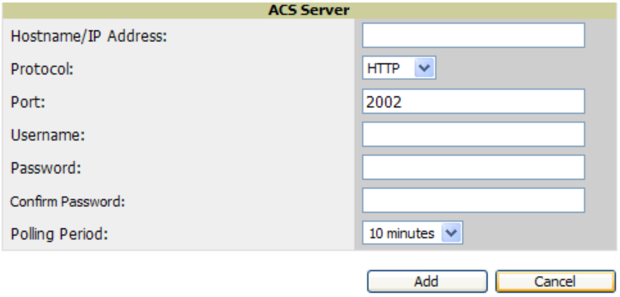
Enter one or more Cisco ACS servers to be polled for wireless username information.

1-1 ▾ of 1 ACS Servers Page 1 ▾ of 1

		Hostname/IP Address ▲	Protocol	Port	Username	Polling Period	Last Contacted	Errors
□	✎	10.1.11.1	HTTP	2002	stuff	10 minutes	5/14/2009 6:37 AM	

2. Select **Add** to create a new ACS server, or select a pencil icon to edit an existing server. To delete an ACS server, select that server and select **Delete**. When selecting **Add** or edit, the **Details** page appears, as illustrated in Figure 31.

Figure 31 ***OV3600 Setup > ACS > Add/Edit Details** Page Illustration*



ACS Server	
Hostname/IP Address:	
Protocol:	HTTP ▾
Port:	2002
Username:	
Password:	
Confirm Password:	
Polling Period:	10 minutes ▾

3. Complete the settings on **OV3600 Setup > ACS > Add/Edit Details**. Table 34 describes these fields:

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

Field	Default	Description
IP/Hostname	None	Sets the DNS name or the IP address of the ACS Server.
Protocol	HTTP	Launches a drop-down menu specifying the protocol OV3600 uses when it polls the ACS server.
Port	2002	Sets the port through which OV3600 communicates with the ACS. OV3600 generally communicates via SNMP traps on port 162.
Username	None	Sets the Username of the account OV3600 uses to poll the ACS server.
Password	None	Sets the password of the account OV3600 uses to poll the ACS server.
Polling Period	10 min	Launches a drop-down menu that specifies how frequently OV3600 polls the ACS server for username information.

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

What Next?

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

Integrating OV3600 with an Existing Network Management Solution (NMS)

This is an optional configuration. The **OV3600 Setup > NMS** configuration page allows OV3600 to integrate with other Network Management Solution (NMS) consoles. This configuration enables advanced and interoperable functionality as follows:

- OV3600 can forward WLAN-related SNMP traps to the NMS, or OV3600 can send SNMPv1 or SNMPv2 traps to the NMS.
- OV3600 can be used in conjunction with Hewlett-Packard's ProCurve Manager.
- The necessary files for either type of NMS interoperability are downloaded from the **OV3600 Setup > NMS** page as follows. For additional information, contact support.

Perform these steps to configure NMS support in OV3600:

1. Go to **OV3600 Setup > NMS**, illustrated in Figure 32.

Figure 32 ***OV3600 Setup > NMS*** *Page Illustration*

2. Select **Add** to integrate a new NMS server, or select the pencil icon to edit an existing server. Provide the information described in Table 35:

Table 35 ***OV3600 Setup > NMS Integration Add/Edit*** *Fields and Default Values*

Setting	Default	Description
Hostname	None	Cites the DNS name or the IP address of the NMS.

Table 35 ***OV3600 Setup > NMS Integration Add/Edit*** *Fields and Default Values (Continued)*

Setting	Default	Description
Port	162	Sets the port OV3600 uses to communicate with the NMS. **NOTE:** OV3600 generally communicates via SNMP traps on port 162.
Community String	None	Sets the community string used to communicate with the NMS.
SNMP Version	v2C	Sets the SNMP version of the traps sent to the Host.
Enabled	Yes	Enables or disables trap logging to the specified NMS.
Send Configuration Traps	Yes	Enables NMS servers to transmit SNMP configuration traps.

3. The **NMS Integration Add/Edit** page includes the **Netcool/OMNIbus Integration** link to information and instructions. The IBM Tivoli Netcool/OMNIbus operations management software enables automated event correlation and additional features resulting in optimized network uptime.
4. The **NMS Integration Add/Edit** page includes the **HP ProCurve Manager Integration** link. Select this link for additional information, zip file download, and brief instructions for installation with OV3600. Select **Add** to finish creating the NMS server, or **Save** to configure an existing NMS server.

What Next?

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

Auditing PCI Compliance on the Network

This section describes PCI requirements and auditing functions in OV3600, with the following topics:

- Introduction to PCI Requirements
- PCI Auditing in the OV3600 Interface
- Enabling or Disabling PCI Auditing

Introduction to PCI Requirements

OV3600 supports wide security standards and functions in the wireless network. One component of network security is the optional deployment of Payment Card Industry (PCI) Auditing.

The Payment Card Industry (PCI) Data Security Standard (DSS) establishes multiple levels in which payment cardholder data is protected in a wireless network. OV3600 supports PCI requirements according to the standards and specifications set forth by the following authority:

- Payment Card Industry (PCI) Data Security Standard (DSS)
  - PCI Security Standards Council Website
    https://www.pcisecuritystandards.org
  - *PCI Quick Reference Guide*, Version 1.2 (October 2008)
    https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

PCI Auditing in the OV3600 Interface

PCI Auditing in OV3600 allows you to monitor, audit, and demonstrate PCI compliance on the network. There are five primary pages in which you establish, monitor, and access PCI auditing, as follows:

- The **OV3600 Setup > PCI Compliance** page enables or disables PCI Compliance monitoring on the network, and displays the current compliance status on the network. See "Enabling or Disabling PCI Auditing" on page 65.

- The **Reports > Definitions** page allows you to create custom-configured and custom-scheduled PCI Compliance reports. See "Reports > Definitions Page Overview" on page 219.
- The **Reports > Generated** page lists PCI Compliance reports currently available, and allows you to generate the latest daily version of the PCI Compliance Report with a single select. Refer to "Reports > Generated Page Overview" on page 221.
- The **APs/Devices > PCI Compliance** page enables you to analyze PCI Compliance for any specific device on the network. This page is accessible when you select a specific device from the **APs/Devices > Monitor** page. First, you must enable this function through **OV3600 Setup**. See "Enabling or Disabling PCI Auditing" on page 65.
- The **PCI Compliance Report** offers additional information. Refer to "Using the PCI Compliance Report" on page 234. This report not only contains **Pass** or **Fail** status for each PCI requirement, but cites the action required to resolve a **Fail** status when sufficient information is available.

NOTE

When any PCI requirement is enabled on OV3600, then OV3600 grades the network as pass or fail for the respective PCI requirement. Whenever a PCI requirement is not enabled in OV3600, then OV3600 does not monitor the network's status in relation to that requirement, and cannot designate Pass or Fail network status. OV3600 servers without a RAPIDS license and users without RAPIDS enabled will not see the 11.1 PCI requirements in the PCI Compliance Report.

Table 36 *PCI Requirements and Support in OV3600*

Requirement	Description
1.1	Monitoring configuration standards for network firewall devices When Enabled: PCI Requirement 1.1 establishes firewall and router configuration standards. A device fails Requirement 1.1 if there are mismatches between the desired configuration and the configuration on the device. When Disabled: firewall router and device configurations are not checked for PCI compliance, and Pass or Fail status is not reported or monitored.
1.2.3	Monitoring firewall installation between any wireless networks and the cardholder data environment When Enabled: A device passes requirement 1.2.3 if it can function as a stateful firewall. When Disabled: firewall router and device installation are not checked for PCI compliance.
2.1	Monitoring the presence of vendor-supplied default security settings When Enabled: PCI Requirement 2 establishes the standard in which all vendor-supplied default passwords are changed prior to a device's presence and operation in the network. A device fails requirement 2.1 if the username, passwords or SNMP credentials being used by OV3600 to communicate with the device are on a list of forbidden default credentials. The list includes common vendor default passwords, for example. When Disabled: device passwords and other vendor default settings are not checked for PCI compliance.
2.1.1	Changing vendor-supplied defaults for wireless environments When Enabled: A device fails requirement 2.1.1 if the passphrases, SSIDs, or other security-related settings are on a list of forbidden values that OV3600 establishes and tracks. The list includes common vendor default passwords. The user can input new values to achieve compliance. When Disabled: network devices are not checked for forbidden information and PCI Compliance is not established.
4.1.1	Using strong encryption in wireless networks When Enabled: PCI Requirement 4 establishes the standard by which payment cardholder data is encrypted prior to transmission across open public networks. PCI disallows WEP encryption as an approved encryption method after June 20, 2010. A device fails requirement 4.1.1 if the desired or actual configuration reflect that WEP is enabled on the network, or if associated users can connect with WEP. When Disabled: OV3600 cannot establish a pass or fail status with regard to PCI encryption requirements on the network.

Table 36 *PCI Requirements and Support in OV3600*

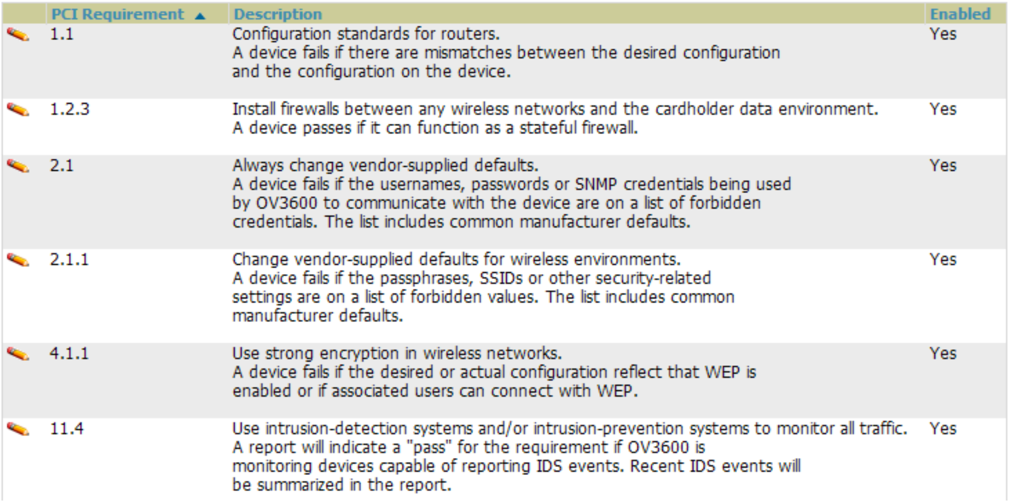
Requirement	Description
11.4	Using intrusion-detection or intrusion-prevention systems to monitor all traffic When Enabled: OV3600 reports pass or fail status when monitoring devices capable of reporting IDS events. Recent IDS events are summarized in the PCI Compliance report or the IDS Report. When Disabled: OV3600 does not monitor the presence of PCI-compliant intrusion detection or prevention systems, nor can it report **Pass** or **Fail** status with regard to IDS events.

Enabling or Disabling PCI Auditing

Perform these steps to verify status and to enable or disable OV3600 support for PCI 1.2 requirements. enabling one or all PCI standards on OV3600 enables real-time information and generated reports that advise on Pass or Fail status. The PCI auditing supported in OV3600 is reported in Table 36.

1. To determine what PCI Compliance standards are enabled or disabled on OV3600, navigate to the **OV3600 Setup > PCI Compliance** page, illustrated in Figure 33.

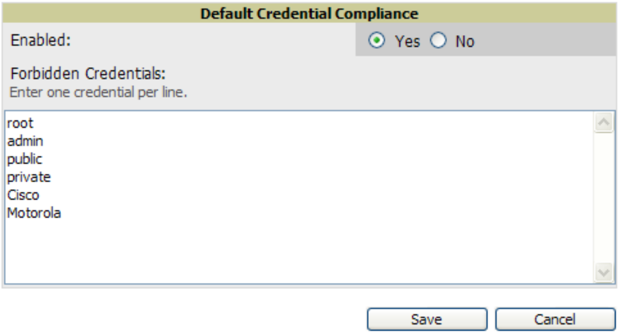
Figure 33 ***OV3600 Setup > PCI Compliance** Page Illustration*



	PCI Requirement ▲	Description	Enabled
✎	1.1	Configuration standards for routers. A device fails if there are mismatches between the desired configuration and the configuration on the device.	Yes
✎	1.2.3	Install firewalls between any wireless networks and the cardholder data environment. A device passes if it can function as a stateful firewall.	Yes
✎	2.1	Always change vendor-supplied defaults. A device fails if the usernames, passwords or SNMP credentials being used by OV3600 to communicate with the device are on a list of forbidden credentials. The list includes common manufacturer defaults.	Yes
✎	2.1.1	Change vendor-supplied defaults for wireless environments. A device fails if the passphrases, SSIDs or other security-related settings are on a list of forbidden values. The list includes common manufacturer defaults.	Yes
✎	4.1.1	Use strong encryption in wireless networks. A device fails if the desired or actual configuration reflect that WEP is enabled or if associated users can connect with WEP.	Yes
✎	11.4	Use intrusion-detection systems and/or intrusion-prevention systems to monitor all traffic. A report will indicate a "pass" for the requirement if OV3600 is monitoring devices capable of reporting IDS events. Recent IDS events will be summarized in the report.	Yes

2. To enable, disable, or edit any category of PCI Compliance monitoring in OV3600, select the pencil icon next to the category. The **Default Credential Compliance** page displays for the respective PCI standard.
3. Create changes as required. Specific credentials can be cited in the **Forbidden Credentials** section of any **Edit** page to enforce PCI requirements in OV3600. Figure 34 shows one example.

Figure 34 ***Default Credential Compliance** for PCI Requirements*



Default Credential Compliance

Enabled: ● Yes ○ No

Forbidden Credentials:
Enter one credential per line.

root
admin
public
private
Cisco
Motorola

4. Select **Save**.

5. To view and monitor PCI auditing on the network, use generated or daily reports. See Chapter 9, "Creating, Running, and Emailing Reports" . In addition, you can view the real-time PCI auditing of any given device online. Perform these steps:
   a. Go to the **APs/Devices > List** page, select a specific device, and the **Monitor** page for that device displays. The **Monitor** page displays a **PCI Compliance** subtab in the menu bar.
   b. Select **PCI Compliance** to view complete PCI compliance auditing for that specific device.

What Next?

- For more information about configuring WLAN Gateways or WLAN controllers such as BlueSocket, ReefEdge, or ProCurve wireless gateways, refer to "Third-Party Security Integration for OV3600" on page 257.
- Go to other tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* Alcatel-Lucent support remains available to you in any phase of OV3600 installation.

Deploying WMS Offload

Overview of WMS Offload in OV3600

This section describes the Wireless LAN Management Server (WMS) offload infrastructure. WMS Offload is supported with the following two requirements:

- AOS-W Version 2.5.4 or later
- OV3600 Version 6.0 or later

The WMS feature is an enterprise-level hardware device and server architecture with managing software for security and network policy. There are three primary components of the WMS deployment:

- Air Monitor AP devices establish and monitor RF activity on the network.
- The WMS server manages devices and network activity, to include rogue AP detection and enforcement of network policy.
- The OV3600 graphical user interface (GUI) allows users to access and use the WMS functionality.

WMS Offload is the ability to place the burden of the WMS server data and GUI functions on OV3600. WMS master switches provide this data so that OV3600 can support rigorous network monitoring capabilities.

General Configuration Tasks Supporting WMS Offload in OV3600

WMS Offload must be enabled with a six-fold process and related configuration tasks, as follows:

1. Configure WLAN switches for optimal OV3600 monitoring.
   - Disable debugging.
   - Ensure OV3600 server is a trap receiver host.
   - Ensure proper traps are enabled.
2. Configure OV3600 to optimally monitor the Alcatel-Lucent infrastructure.
   - Enable WMS offload.
   - Configure SNMP communication.
   - Create a proper policy for monitoring Alcatel-Lucent infrastructure.
   - Discover the infrastructure.
3. Configure device classification.
   - Set up rogue classification.

   - Set up rogue classification override.
   - Establish user classification override devices.
4. Deploy AOS-W-specific monitoring features.
   - Enable remote AP and wired network monitoring.
   - View switch license information.
5. Convert existing floor plans to VisualRF, to include the following elements:
   - MMS
   - AOS-W
   - RF Plan
6. Use RTLS for increasing location accuracy (optional).
   - Enable RTLS service on the OV3600 server.
   - Enable RTLS on AOS-W Infrastructure.

Additional Information Supporting WMS Offload

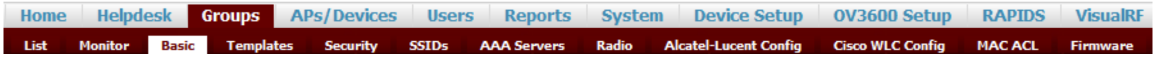
For additional information, including detailed concepts, configuration procedures, restrictions, AOS-W infrastructure, and OV3600 version differences in support of WMS Offload, refer to the *Alcatel-Lucent Best Practices Guide*.

Chapter 4

Configuring and Using Device Groups in OV3600

This chapter describes the deployment of device groups within OV3600. The section below describes the pages or focused subtabs available on the Groups tab. Note that the available subtabs can vary significantly from one device group to another—one or more subtabs may not appear, depending on the types of devices you add to OV3600.

Figure 35 *Subtabs under the **Group** tab*



- **List**—This page is the default page in the **Groups** section of OV3600. It lists all groups currently configured in OV3600 and provides the foundation for all group-level configurations. See "Viewing All Defined Device Groups" on page 71.
- **Monitor**—This page displays user and bandwidth information, lists devices in a given group, provides an **Alert Summary** table for monitoring alerts for the group, and provides a detailed **Audit Log** for group-level activity.

NOTE

The **Incidents** portion of the **Alert Summary** table only increments the counter for incidents that are open and associated to an AP in that group, associated with the group itself. It does not include incidents associated with any folder. To view all incidents including those not associated to an AP, go to the **Helpdesk > Incidents** page.

- **Basic**—This page appears when you create a new group on the **Groups > List** page. Once you define a group name, OV3600 displays the **Basic** page from which you configure many group-level settings. This page remains available for any device group configured in OV3600. Refer to "Configuring Basic Group Settings" on page 72.
- **Templates**—This page manages templates for any device group. Templates allow you to manage the configuration of Dell PowerConnect W, 3Com, Alcatel-Lucent, Aruba Networks, Cisco Aironet IOS, Cisco Catalyst switches, Enterasys, HP, Nomadix, Nortel, Symbol and Trapeze devices in a given group using a configuration file. Variables in such templates configure device-specific properties, such as name, IP address and channel. Variables also define group-level properties. For additional information about using the **Templates** page, refer to Chapter 6, "Creating and Using Templates" on page 147.
- **Security**—This page defines general security settings for device groups, to include RADIUS, encryption, and additional security settings on devices. Refer to "Configuring Group Security Settings" on page 80.
- **SSIDs**—This page sets SSIDs, VLANs, and related parameters in device groups. Refer to "Configuring Group SSIDs and VLANs" on page 83.
- **AAA Servers**—This page configures authentication, authorization, and accounting settings in support of RADIUS servers for device groups. Refer to "Adding and Configuring Group AAA Servers" on page 79.
- **Radio**—This page defines general 802.11 radio settings for device groups. Refer to "Configuring Radio Settings for Device Groups" on page 86.
- **Alcatel-Lucent Config**—This page manages AOS-W Device Groups, AP Overrides, and other profiles specific to Alcatel-Lucent devices on the network. Use this page as an alternative to the **Device Setup > Alcatel-Lucent Configuration** page. The apperance of this page varies depending on whether OV3600 is configured for global configuration or group configuration. For additional information, refer to the *Alcatel-Lucent Configuration Guide.*
- **Cisco WLC Config**—This page consolidates controller-level settings from the Group Radio, Security, SSIDs, Cisco WLC Radio and AAA Server pages into one navigation tree that is easier to navigate, and has familiar layout and terminology. Bulk configuration for per-thin AP settings, previously configured

on the Group LWAPP APs tab, can now be performed from Modify Devices on the **APs/Devices > List** page. Refer to "Configuring Cisco Controller Settings" on page 95.

- **PTMP**—This page defines settings specific to Proxim MP devices when present. Refer to "Configuring Group PTMP Settings" on page 97.
- **Proxim Mesh**—This page defines mesh AP settings specific to Proxim devices when present. Refer to "Configuring Proxim Proxim Mesh" on page 97.
- **MAC ACL**—This page defines MAC-specific settings that apply to Proxim, Cisco VxWorks, Symbol, and Procurve520 devices when present. Refer to "Configuring Group MAC Access Control Lists" on page 99.
- **Firmware**—This page manages firmware files for many devices. "Specifying Minimum Firmware Versions for APs in a Group" on page 99.
- **Compare**—This page allows you to compare line item-settings between two device groups. On the **Groups > List** page, select **Compare Two Groups**, select the two groups from the drop-down menus, then select **Compare**. "Comparing Device Groups" on page 100.

This chapter also provides the following additional procedures for group-level configurations:

- "Deleting a Group" on page 101
- "Changing Multiple Group Configurations" on page 101
- "Modifying Multiple Devices" on page 103
- "Using Global Groups for Group Configuration" on page 105

OV3600 Groups Overview

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 efficiently at 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 may 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 may be from different vendors or hardware models. All devices within a Group share certain basic configuration settings.

Typical group configuration variables include basic settings (SSID, SNMP polling interval, and so forth), security settings (VLANs, WEP, 802.1x, ACLs, and so forth), and some 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. Such changes must be applied with every device in **Managed** mode. **Monitor** mode is the more common mode.

CAUTION

Always review the **Audit** page before pushing configuration to a device or group.

Individual device settings—such as device name, RF channel selection, RF transmission power, antenna settings, and so forth—typically should not be managed at a group level and must be individually configured for optimal performance. Individual AP settings are configured on the **APs/Devices > Manage** page.

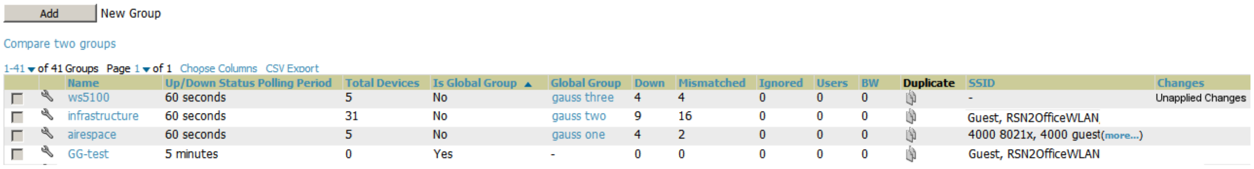
You can create as many different groups as required. Administrators usually establish groups that range in size from five to 100 wireless devices.

Group configuration can be enhanced with the OV3600 **Global Groups** feature, which lets you create Global Groups with configurations that are pushed to individual Subscriber Groups.

Viewing All Defined Device Groups

To display a list of all defined groups, browse to the **Groups > List** page, illustrated in Figure 36.

Figure 36 ***Groups > List*** *Page Illustration*



Add New Group

Compare two groups

1-41 ▾ of 41 Groups Page 1 ▾ of 1 Choose Columns CSV Export

		Name	Up/Down Status Polling Period	Total Devices	Is Global Group ▲	Global Group	Down	Mismatched	Ignored	Users	BW	Duplicate	SSID	Changes
□		ws5100	60 seconds	5	No	gauss three	4	4	0	0	0		-	Unapplied Changes
□		infrastructure	60 seconds	31	No	gauss two	9	16	0	0	0		Guest, RSN2OfficeWLAN	
□		airespace	60 seconds	5	No	gauss one	4	2	0	0	0		4000 8021x, 4000 guest(more...)	
□		GG-test	5 minutes	0	Yes	-	0	0	0	0	0		Guest, RSN2OfficeWLAN	

Table 37 describes the columns in the **Groups > List** page.

Table 37 ***Groups > List*** *Columns*

Column	Description
Add New Group	Launches a page that enables you to add a new group by name and to define group parameters for devices in that group. For additional information, refer to "Configuring Basic Group Settings" on page 72.
Manage (wrench icon)	Goes to the **Groups > Basic** configuration page for that group. Hover your mouse over the icon to see a list of shortcuts to group-specific subtabs that would appear across the navigation section if this group is selected.
Name	Uniquely identifies the group by location, vendor, department or any other identifier (such as "Accounting APs," "Floor 1 APs," "Cisco devices," "802.1x APs," and so forth).
Up/Down Status Polling Period	The time between Up/Down SNMP polling periods for each device in the group. Detailed SNMP polling period information is available on the **Groups > Basic** configuration page. Note that by default, most polling intervals do not match the up/down period.
Is Global Group	If a group is designated as global, it may not contain APs but it may be used as a template for other groups. This column may also indicate **Yes** if this group has been pushed to the OV3600 from a Master Console.
Global Group	Specifies which group this Subscriber Group is using as its template.
SSID	The SSID assigned to supported device types within the group.
Total Devices	Total number of devices contained in the group including APs, controllers, routers, or switches.
Down	The number of access points within the group that are not reachable via SNMP or are no longer associated to a controller. Note that thin APs are not directly polled with SNMP, but are polled through the controller. That controller may report that the thin AP is down or is no longer on the controller. At this point, OV3600 classifies the device as down.
Mismatched	The number of devices within the group that are in a mismatched state.
Ignored	The number of ignored devices in that group.
Users	The number of mobile users associated with all access points within the group. To avoid double counting of users, users are only listed in the group of the AP with which they are associated. Note that device groups with only controllers in them report no users.
BW	Bandwidth: A running average of the sum of bytes in and bytes out for the managed radio page.
Duplicate	Creates a new group with the name **Copy of <Group Name>** with configuration settings. (Alcatel-Lucent configuration settings will have to be manually added back.)
Changes	Whether the group has unapplied changes.

NOTE

When you first configure OV3600, there is only one default group labeled **Access Points**. If you have no other groups configured, refer to "Configuring Basic Group Settings" on page 72.

Configuring Basic Group Settings

The first default device group that OV3600 sets up is the **Access Points** group, but you can use this procedure to add and configure any device group. Perform these steps to configure basic group settings, then continue to additional procedures to define additional settings as required.

1. Go to the **Groups > List** page. Existing device groups appear on this page.
2. To create a new group, select **Add**. Enter a group name and select **Add**. The **Groups > Basic** page appears.

   To edit an existing device group, select the **manage** (wrench) icon next to the group. The **Groups > Basic** page appears. If you mouse over an existing group's wrench, a popup menu allows you to select **Basic**, **Templates**, **Security**, **SSIDs**, **AAA Servers**, **Radio**, **Alcatel-Lucent Config** or **Cisco WLC Config** to edit those pages as desired, as illustrated in Figure 37.

Figure 37 *Pop-up When Hovering over Wrench Icon in Groups > List*

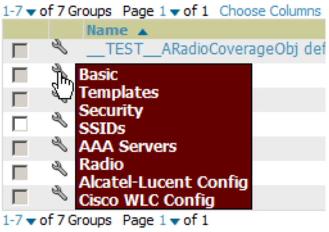
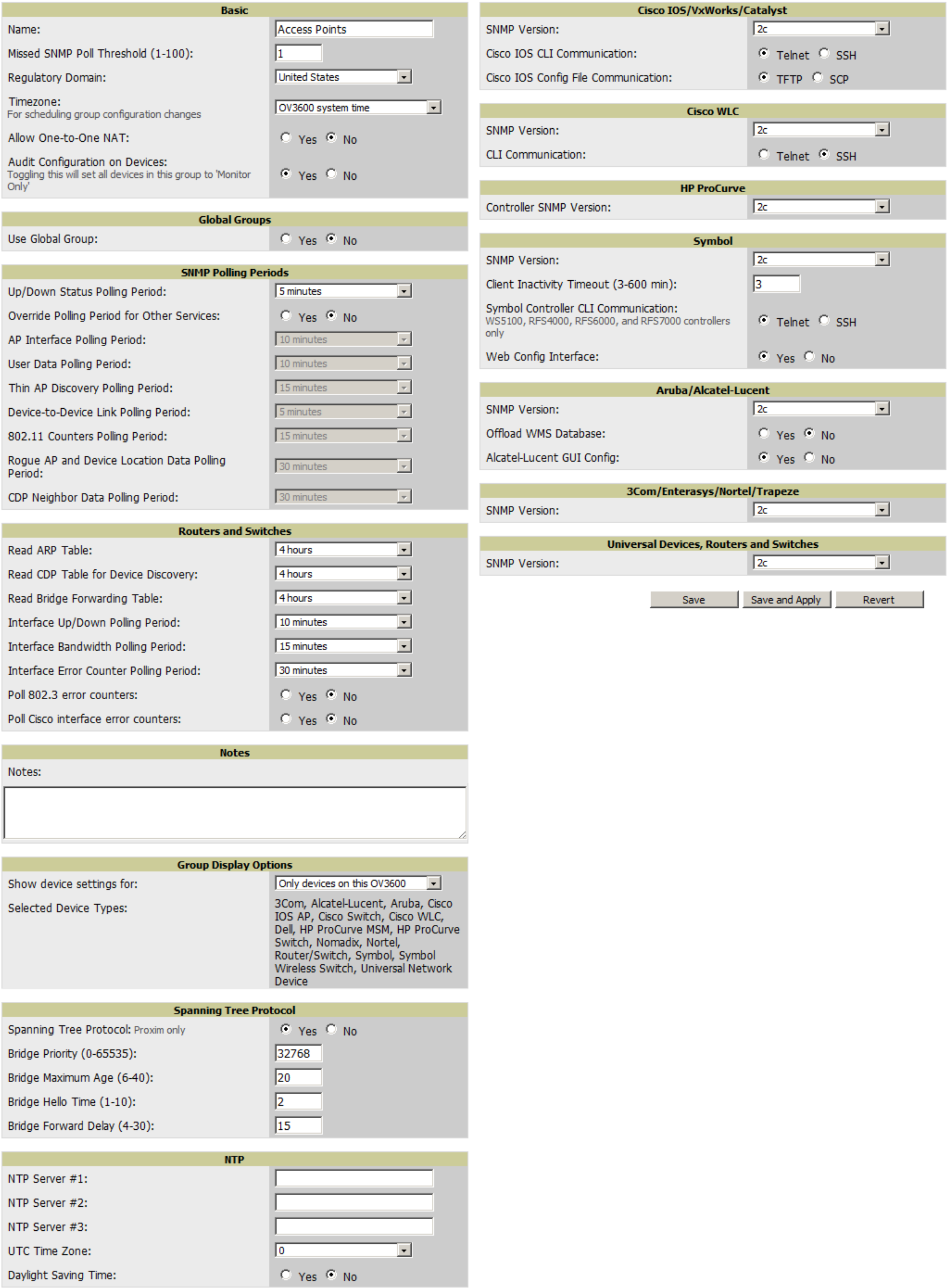

1-7 ▾ of 7 Groups Page 1 ▾ of 1 Choose Columns
Name ▲
__TEST__ARadioCoverageObj def
Basic
Templates
Security
SSIDs
AAA Servers
Radio
Alcatel-Lucent Config
Cisco WLC Config
1-7 ▾ of 7 Groups Page 1 ▾ of 1

Figure 38 illustrates an example **Groups > Basic** page.

Figure 38 ***Groups > Basic*** *Page Illustration*



Basic

Name:	Access Points
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	United States
Timezone: For scheduling group configuration changes	OV3600 system time
Allow One-to-One NAT:	○ Yes ● No
Audit Configuration on Devices: Toggling this will set all devices in this group to 'Monitor Only'	● Yes ○ No

Global Groups

Use Global Group:	○ Yes ● No

SNMP Polling Periods

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

Routers and Switches

Read ARP Table:	4 hours
Read CDP Table for Device Discovery:	4 hours
Read Bridge Forwarding Table:	4 hours
Interface Up/Down Polling Period:	10 minutes
Interface Bandwidth Polling Period:	15 minutes
Interface Error Counter Polling Period:	30 minutes
Poll 802.3 error counters:	○ Yes ● No
Poll Cisco interface error counters:	○ Yes ● No

Notes

Notes:

Group Display Options

Show device settings for:	Only devices on this OV3600
Selected Device Types:	3Com, Alcatel-Lucent, Aruba, Cisco IOS AP, Cisco Switch, Cisco WLC, Dell, HP ProCurve MSM, HP ProCurve Switch, Nomadix, Nortel, Router/Switch, Symbol, Symbol Wireless Switch, Universal Network Device

Spanning Tree Protocol

Spanning Tree Protocol: Proxim only	● Yes ○ No
Bridge Priority (0-65535):	32768
Bridge Maximum Age (6-40):	20
Bridge Hello Time (1-10):	2
Bridge Forward Delay (4-30):	15

NTP

NTP Server #1:	
NTP Server #2:	
NTP Server #3:	
UTC Time Zone:	0
Daylight Saving Time:	○ Yes ● No

Cisco IOS/VxWorks/Catalyst

SNMP Version:	2c
Cisco IOS CLI Communication:	● Telnet ○ SSH
Cisco IOS Config File Communication:	● TFTP ○ SCP

Cisco WLC

SNMP Version:	2c
CLI Communication:	○ Telnet ● SSH

HP ProCurve

Controller SNMP Version:	2c

Symbol

SNMP Version:	2c
Client Inactivity Timeout (3-600 min):	3
Symbol Controller CLI Communication: WS5100, RFS4000, RFS6000, and RFS7000 controllers only	● Telnet ○ SSH
Web Config Interface:	● Yes ○ No

Aruba/Alcatel-Lucent

SNMP Version:	2c
Offload WMS Database:	○ Yes ● No
Alcatel-Lucent GUI Config:	● Yes ○ No

3Com/Enterasys/Nortel/Trapeze

SNMP Version:	2c

Universal Devices, Routers and Switches

SNMP Version:	2c

3. Define the settings in the **Basic** and **Global Group** sections. Table 38 describes some typical settings and default values of this **Basic** section.

Table 38 *Basic* and *Global Group* Fields and Default Values

Setting	Default	Description
Name	Defined when first adding the group	Displays or changes the group name. As desired, use this field to set the name to uniquely identify the group by location, vendor, department, or any other identifier (such as “Accounting APs,” “Cisco devices,” “802.1x APs,” and so forth).
Missed SNMP Poll Threshold	1	Sets the number of Up/Down SNMP polls that must be missed before OV3600 considers a device to be down. The number of SNMP retries and the SNMP timeout of a poll can be set on the **Device Setup > Communication** page.
Regulatory Domain	United States	Sets the regulatory domain in OV3600, limiting the selectable channels for APs in the group.
Timezone	OV3600 system time	Allows group configuration changes to be scheduled relative to the time zone in which the devices are located. This setting is used for scheduling group-level configuration changes.
Allow One-to-One NAT	No	Allows OV3600 to talk to the devices on a different IP address than the one configured on the device. **NOTE:** If enabled, the LAN IP Address listed on the **AP/Devices > Manage** configuration page under the **Settings** area is different than the IP Address under the **Device Communication** area.
Audit Configuration on Devices	Yes	Auditing and pushing of configuration to devices can be disabled on all the devices in the group. Once disabled, all the devices in the groups will not be counted towards mismatched devices.
Use Global Group	No	When enabled, this field allows you to define the device group to be a Global Group. Refer to “Using Global Groups for Group Configuration” on page 105.

4. Complete the **SNMP Polling Periods** section. The information in this section overrides default settings. Table 39 describes the SNMP polling settings.

Table 39 *SNMP Polling Periods* Fields and Default Values

Setting	Default	Description
Up/Down Status Polling Period	5 minutes	Sets time between Up/Down SNMP polling for each device in the group. The Group SNMP Polling Interval overrides the global parameter configured on the **Device Setup > Communication** page. An initial polling interval of **5** minutes is best for most networks.
Override Polling Period for Other Services	No	Enables or disables overriding the base SNMP Polling Period. If you select **Yes**, the other settings in the SNMP Polling Periods section are activated, and you can override default values.
AP Interface Polling Period	5 minutes	Sets the interval at which OV3600 polls for radio monitoring and bandwidth being used by a device.
User Data Polling Period	5 minutes	Sets time between SNMP polls for User Data for devices in the group.
Thin AP Discovery Polling Period	5 minutes	Sets time between SNMP polls for Thin AP Device Discovery. Controllers are the only devices affected by this polling interval.
Device-to-Device link Polling Period	5 minutes	Sets time between SNMP polls for Device-to-Device link polling. Mesh APs are the only devices affected by this polling interval.
802.11 Counters Polling Period	5 minutes	Sets time between SNMP polls for 802.11 Counter information.
Rogue AP and Device Location Data Polling Period	5 minutes	Sets time between SNMP polls for Rogue AP and Device Location Data polling.
CDP Neighbor Data Polling Period	30 minutes	Sets the frequency in which this group polls the network for Cisco Discovery Protocol (CDP) neighbors.

5. Record additional information and comments about the group in the **Notes** section.

6. To configure which options and tabs are visible for the group, complete the settings in the **Group Display Options** section. Table 40 describes the settings and default values.

Table 40 ***Group Display Options*** *Fields and Default Values*

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

7. To assign dynamically a range of static IP addresses to new devices as they are added into the group, locate the **Automatic Static IP Assignment** section on the **Groups > Basic** configuration page. If you select **Yes** in this section, additional fields appear. Complete these fields as required. Table 41 describes the settings and default values. This section is only relevant for a small number of device types, and will appear when they are present.

Table 41 ***Automatic Static IP Assignment*** *Fields and Default Values*

Setting	Default	Description
Assign Static IP Addresses to Devices	No	Enables OV3600 to statically assign IP addresses from a specified range to all devices in the Group.
Start IP Address	Blank	Sets the first address OV3600 assigns to the devices in the Group.
Number of Addresses	Blank	Sets the number of addresses in the pool from which OV3600 can assign IP addresses.
Subnet Mask	Blank	Sets the subnet mask to be assigned to the devices in the Group.
Subnet Gateway	Blank	Sets the gateway to be assigned to the devices in the Group.
Next IP Address	Blank	Defines the next IP address queued for assignment. This field is disabled for the initial Access Points group.

8. To configure Spanning Tree Protocol on WLC devices and Proxim APs, locate the Spanning Tree Protocol section on the **Groups > Basic** configuration page. Adjust these settings as required. Table 42 describes the settings and default values.

Table 42 ***Spanning Tree Protocol*** *Fields and Default Values*

Setting	Default	Description
Spanning Tree Protocol	No	Enables or disables Spanning Tree Protocol on WLSE devices and Proxim APs.

Table 42 ***Spanning Tree Protocol*** *Fields and Default Values (Continued)*

Setting	Default	Description
Bridge Priority	32768	Sets the priority for the AP. Values range from 0 to 65535. Lower values have higher priority. The lowest value is the root of the spanning tree. If all devices are at default the device with the lowest MAC address will become the root.
Bridge Maximum Age	20	Sets the maximum time, in seconds, that the device stores protocol information. The supported range is from 6 to 40.
Bridge Hello Time	2	Sets the time, in seconds, between Hello message broadcasts.
Bridge Forward Delay	15	Sets the time, in seconds, that the port spends in listening and learning mode if the spanning tree has changed.

9. To configure NTP settings locate the **NTP** section and adjust these settings as required. Table 43 describes the settings and default values.

Table 43 ***NTP*** *Fields and Default Values*

Setting	Default	Description
NTP Server #1,2,3	None	Sets the IP address of the NTP server to be configured on the AP.
UTC Time Zone	0	Sets the hour offset from UTC time to local time for the AP. Times displayed in OV3600 graphs and logs use the time set on the OV3600 server.
Daylight Saving Time	No	Enables or disables the advanced daylight saving time settings in the Proxim and HP ProCurve 420 sections of the **Groups > Basic** configuration page.

10. To configure settings specific to Cisco IOS/VxWorks, locate the **Cisco IOS/VxWorks** section and adjust these settings as required. Table 44 describes the settings and default values.

Table 44 ***Cisco IOS/VxWorks/Catalyst*** *Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	The version of SNMP used by OV3600 to communicate to the AP.
Cisco IOS CLI Communication	Telnet	The protocol OV3600 uses to communicate with Cisco IOS devices. Selecting **SSH** uses the secure shell for command line page (CLI) communication. Selecting **Telnet** sends the data in clear text via Telnet.
Cisco IOS Config File Communication	TFTP	The protocol OV3600 uses to communicate with Cisco IOS devices. Selecting **SCP** uses the secure copy protocol for file transfers. Selecting **TFTP** will use the insecure trivial file transfer protocol. The SCP login and password should be entered in the Telnet username and password fields.
Track Usernames on Cisco Aironet VxWorks APs	No	Configures VxWorks APs to send SNMP packets to OV3600.

11. To configure settings specific to Cisco WLC, locate the **Cisco WLC** section and adjust these settings as required. Table 45 describes the settings and default values.

Table 45 ***Cisco WLC*** *Fields and Default Values*

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

NOTE

When configuring Cisco WLC controllers, refer to "Configuring Wireless Parameters for Cisco Controllers" on page 95.

12. To configure Proxim/Avaya specific settings locate the **Proxim/Avaya** section and adjust these settings as required. Table 46 describes the settings and default values.

Table 46 ***Proxim/Avaya*** *Fields and Default Values*

Setting	Default	Description
SNMP Version	1	Sets the version of SNMP used by OV3600 to communicate to the AP.
Enable DNS Client	No	Enables the DNS client on the AP. Enabling the DNS client allows you to set some values on the AP by hostname instead of IP address. If you select **Yes** for this setting, additional DNS fields display.
Primary DNS server	Blank	Sets the IP address of the Primary DNS server.
Secondary DNS server	Blank	Sets the IP address of the Secondary DNS server.
Default DNS domains	Blank	Sets the default DNS domain used by the AP.
HTTP Server Port	80	Sets this port as the HTTP server port on all Proxim APs in the group.
Country Code	United States	Configures OV3600 to derive its time settings based on the country of location, as specified in this field.

13. To configure HP ProCurve specific settings, locate the **HP ProCurve** section and adjust these settings as required. Table 47 describes the settings and default values.

Table 47 ***HP ProCurve*** *Fields and Default Values*

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

NOTE

DST Start Month, Start Day, End Month, End Day, and DST Offset are only visible if Daylight Saving Time is enabled in the NTP section of the **Groups > Basic** configuration page.

14. To configure Symbol settings, locate the **Symbol** section and adjust these settings as required. Table 48 describes the settings and default values of this section.

Table 48 ***Symbol** Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	Specifies the version of SNMP used by OV3600 to communicate to the device.
Symbol Client Inactivity Timeout (3-600 min)	3	Sets the minutes of inactivity after which a client associated to a Symbol AP will be considered "inactive." A lower value typically provides a more accurate representation of current WLAN usage. **NOTE:** For other APs, OV3600 has more precise methods to determine when inactive clients are no longer associated to an AP.
Symbol Controller CLI Communication	Telnet	The connection type to support the command-line interface (CLI) connection. The options are **Telnet** and secure shell (**SSH**). This is supported for WS5100, RFS4000, RFS6000 and RFS7000 devices only.
Web Config Interface	Yes	Enables or disables the **http/https** configuration page for the Symbol 4131 devices.

15. To configure settings specific to AOS-W, locate the **Aruba/Alcatel-Lucent** section and adjust these settings as required. Table 49 describes the settings and default values of this section.

Table 49 ***AOS-W** Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	The version of SNMP used by OV3600 to communicate to the AP.
Offload WMS database	No	Configures commands previously documented in the *Best Practices Guide*. When enabled, this feature allows OV3600 to display historical information for WLAN switches. Changing the setting to **Yes** pushes commands via SSH to all WLAN switches in Monitor Only mode without rebooting the switch. The command can be pushed to switches in manage mode (also without rebooting the switch) if the **Allow WMS Offload** setting on **OV3600 Setup > General** is changed to **Yes**.
Aruba/Alcatel-Lucent GUI Config	Yes	This setting selects whether you'd like to configure your Alcatel-Lucent devices using the **Groups > Alcatel-Lucent Config** method (either global or group) or using Templates.

16. To configure settings for 3Com, Enterasys, Nortel, or Trapeze devices, locate the **3Com/Enterasys/Nortel/Trapeze** section and define the version of SNMP to be supported.

17. To configure support for universal devices, routers, and switches in the group, locate the **Routers and Switches** section and adjust these settings as required. This section defines the frequency in which all devices in the group polled. These settings can be disabled entirely. Table 50 describes the settings and default values of this section.

Table 50 ***Routers and Switches** Fields and Default Values*

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

Table 50 ***Routers and Switches*** *Fields and Default Values (Continued)*

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

18. To configure settings for universal devices on the network, including routers and switches that support both wired and wireless networks, locate the **Universal Devices, Routers and Switches** section of the **Groups > Basic** page and define the version of SNMP to be supported.
19. Select **Save** when the configurations of the **Groups > Basic** configuration page are complete to retain these settings, but without pushing these settings to all devices in the group. **Save** is a good option if you intend to make additional device changes in the group, and wish to wait until all configurations are complete before you push all configurations at one time.

    Select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.

What Next?

Continue to additional sections in this chapter to create new groups or to edit existing groups.

Once general group-level configurations are complete, continue to later chapters in this document to add or edit additional device-level configurations and to use several additional OV3600 functions.

Adding and Configuring Group AAA Servers

Configure RADIUS servers on the **Groups > AAA Servers** page.

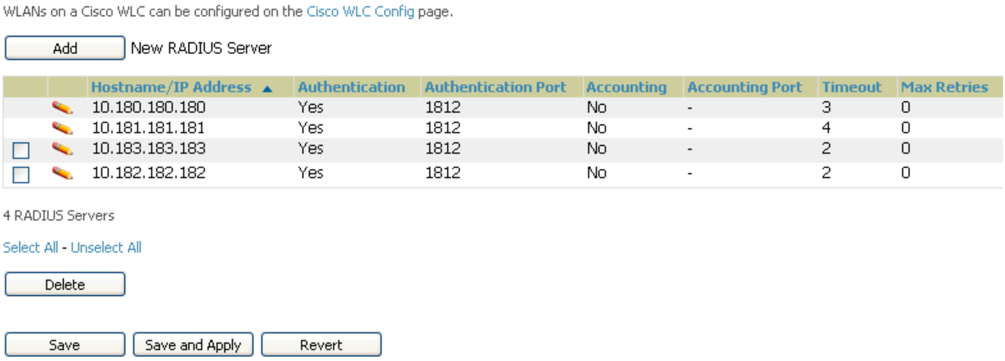
Once defined on this page, RADIUS servers are selectable in the drop-down menus on the **Groups > Security and Groups > SSIDs** configuration pages. Perform these steps to create RADIUS servers.

NOTE

TACACS+ servers are configurable only for Cisco WLC devices. Refer to "Configuring Security Parameters and Functions" on page 96.

1. Go to the **Groups > List** page and select the group for which to define AAA servers by selecting the group name. The **Monitor** page appears.
2. Select the **AAA Servers** page. The **AAA Servers** page appears, enabling you to add a RADIUS server. Figure 39 illustrate this page for AAA RADIUS Servers:

Figure 39 ***Groups > AAA Servers** Page Illustration*


WLANs on a Cisco WLC can be configured on the Cisco WLC Config page.

		Hostname/IP Address ▲	Authentication	Authentication Port	Accounting	Accounting Port	Timeout	Max Retries
	✎	10.180.180.180	Yes	1812	No	-	3	0
	✎	10.181.181.181	Yes	1812	No	-	4	0
□	✎	10.183.183.183	Yes	1812	No	-	2	0
□	✎	10.182.182.182	Yes	1812	No	-	2	0

4 RADIUS Servers

3. To add a RADIUS server or edit an existing server, select **Add New RADIUS Server** or the corresponding pencil icon to edit an existing server. Table 51 describes the settings and default values of the **Add/Edit** page.

Table 51 ***Adding a RADIUS Server** Fields and Default Values*

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

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

   OV3600 supports reports for subsequent RADIUS Authentication. These are viewable by selecting **Reports > Generated**, scrolling to the bottom of the page, and selecting **Latest RADIUS Authentication Issues Report**.

5. To make additional RADIUS configurations for device groups, use the **Groups > Security** page and continue to the next topic.

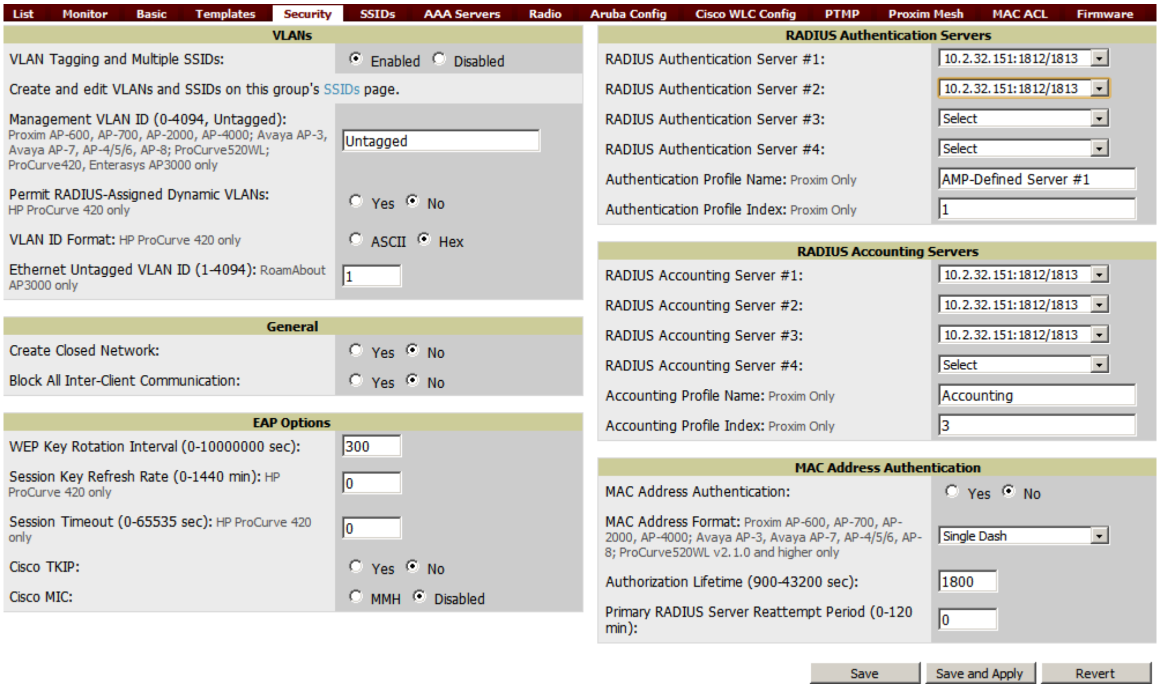
Configuring Group Security Settings

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

1. Select the device group for which to define security settings from the **Groups > List** page.

2. Go to **Groups > Security**. Some controls on this page interact with additional OV3600 pages. Figure 40 illustrates this page and Table 52 explains the fields and default values.

Figure 40 ***Groups*** **>** ***Security*** *Page Illustration*



VLANs

VLAN Tagging and Multiple SSIDs:	● Enabled ○ Disabled
Create and edit VLANs and SSIDs on this group's SSIDs page.	
Management VLAN ID (0-4094, Untagged): Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL; ProCurve420, Enterasys AP3000 only	Untagged
Permit RADIUS-Assigned Dynamic VLANs: HP ProCurve 420 only	○ Yes ● No
VLAN ID Format: HP ProCurve 420 only	○ ASCII ● Hex
Ethernet Untagged VLAN ID (1-4094): RoamAbout AP3000 only	1

General

Create Closed Network:	○ Yes ● No
Block All Inter-Client Communication:	○ Yes ● No

EAP Options

WEP Key Rotation Interval (0-10000000 sec):	300
Session Key Refresh Rate (0-1440 min): HP ProCurve 420 only	0
Session Timeout (0-65535 sec): HP ProCurve 420 only	0
Cisco TKIP:	○ Yes ● No
Cisco MIC:	○ MMH ● Disabled

RADIUS Authentication Servers

RADIUS Authentication Server #1:	10.2.32.151:1812/1813
RADIUS Authentication Server #2:	10.2.32.151:1812/1813
RADIUS Authentication Server #3:	Select
RADIUS Authentication Server #4:	Select
Authentication Profile Name: Proxim Only	AMP-Defined Server #1
Authentication Profile Index: Proxim Only	1

RADIUS Accounting Servers

RADIUS Accounting Server #1:	10.2.32.151:1812/1813
RADIUS Accounting Server #2:	10.2.32.151:1812/1813
RADIUS Accounting Server #3:	10.2.32.151:1812/1813
RADIUS Accounting Server #4:	Select
Accounting Profile Name: Proxim Only	Accounting
Accounting Profile Index: Proxim Only	3

MAC Address Authentication

MAC Address Authentication:	○ Yes ● No
MAC Address Format: Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL v2.1.0 and higher only	Single Dash
Authorization Lifetime (900-43200 sec):	1800
Primary RADIUS Server Reattempt Period (0-120 min):	0

Table 52 ***Groups*** **>** ***Security*** *Page Fields and Default Values*

Setting	Default	Description
VLANs Section		
VLAN Tagging and Multiple SSIDs	Enabled	This field enables support for VLANs and multiple SSIDs on the wireless network. If this setting is enabled, define additional VLANs and SSIDs on the **Groups > SSIDs** page. Refer to "Configuring Group SSIDs and VLANs" on page 83.
Management VLAN ID	Untagged	This setting sets the ID for the management VLAN when VLANs are enabled in OV3600. This setting is supported only for the following devices: ● Proxim AP-600, AP-700, AP-2000, AP-4000 ● Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8 ● ProCurve520WL; ProCurve420 ● Enterasys AP3000
Permit RADIUS-Assigned Dynamic VLANs	No	This setting enables dynamic VLANs to be assigned by the RADIUS server. This setting is supported only for HP ProCurve 420.
VLAN ID Format	Hex	This setting defines the naming convention for VLANs to be supported in OV3600. The supported naming formats are ASCII and Hexadecimal.
Ethernet Untagged VLAN ID (1-4094)	1	This field defines the VLAN that will use untagged Ethernet. The VLAN must be a number between 1 and 4094, and defines the untagged VLAN ID for the RoamAbout AP3000.
General Section		
Create Closed Network	No	If enabled, the APs in the Group do not broadcast their SSIDs. **NOTE:** Creating a closed network will make it more difficult for intruders to detect your wireless network.

Table 52 ***Groups > Security*** *Page Fields and Default Values (Continued)*

Setting	Default	Description
Block All Inter-Client Communication	No	If enabled, this setting blocks client devices associated with an AP from communicating with other client devices on the wireless network. **NOTE:** This option may also be identified as PSPF (Publicly Secure Packet Forwarding), which can be useful for enhanced security on public wireless networks.
EAP Options Section		
WEP Key Rotation Interval	300	Sets the frequency at which the Wired Equivalent Privacy (WEP) keys are rotated in the device group being configured. The supported range is from 0 to 10,000,000 seconds.
Session Key Refresh Rate	0	Sets the frequency at which the general session key is refreshed in the device group being configured. The supported range is from 1 to 40 minutes. This setting is supported only for HP ProCurve 420.
Session Timeout	0	Sets the time at which the session times out for the device group being configured. The supported range is from 0 to 65,535 seconds. This setting is supported only for HP ProCurve 420.
Cisco TKIP	No	Sets the device group to use the Cisco Temporal Key Integrity Protocol (TKIP). If enabled, TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP. **NOTE:** TKIP can only be enabled when EAP-based security is used.
Cisco MIC	Disabled	Sets the device group to use the Cisco Message Integrity Check (MIC). Selecting MMH encryption enables this function. If enabled, Message Integrity Check (MIC) adds several bytes per packet to make it more difficult to tamper with the packets.
RADIUS Authentication Servers Section		
RADIUS Authentication Server #1 - #4	Not selected	Defines one or more RADIUS Authentication servers to be supported in this device group. Select up to four RADIUS authentication servers from the four drop-down menus.
Authentication Profile Name	OV3600-Defined Server #1	For Proxim devices only, this field sets the name of the authentication profile to be supported in this device group.
Authentication Profile Index	1	For Proxim devices only, this field sets the name of the authentication profile index to be supported in this device group.
RADIUS Accounting Servers Section		
RADIUS Accounting Server #1 - #4	Not selected	Defines one or more RADIUS Accounting servers to be supported in this device group. Select up to four RADIUS accounting servers from the four drop-down menus.
Authentication Profile Name	Accounting	For Proxim devices only, this field sets the name of the accounting profile to be supported in this device group.
Authentication Profile Index	3	For Proxim devices only, this field sets the name of the accounting profile index to be supported in this device group.
MAC Address Authentication Section		
MAC Address Authentication	No	If enabled, only MAC addresses known to the RADIUS server are permitted to associate to APs in the Group.
MAC Address Format	Single Dash	Allows selection of the format for MAC addresses used in RADIUS authentication and accounting requests: ■ Dash Delimited: xx-xx-xx-xx-xx-xx (default) ■ Colon Delimited: xx:xx:xx:xx:xx:xx ■ Single-Dash: xxxxxx-xxxxxx ■ No Delimiter: xxxxxxxxxxxx This option is supported only for the devices listed on the interface.
Authorization Lifetime	1800	Sets the amount of time a user can be connected before reauthorization is required. The supported range is from 900 to 43,200 seconds.

Table 52 *Groups* > *Security Page Fields and Default Values (Continued)*

Setting	Default	Description
Primary RADIUS Server Reattempt Period	0	Specifies the time (in minutes) that the AP awaits responses from the primary RADIUS server before communicating with the secondary RADIUS server, and so forth

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

Configuring Group SSIDs and VLANs

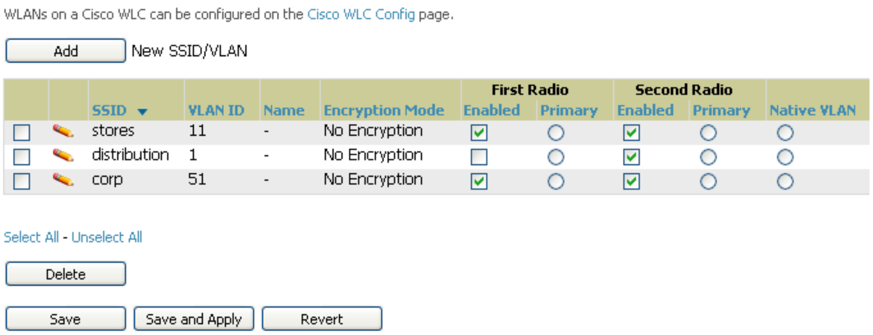
The **Groups > SSIDs** configuration page allows you to create and edit SSIDs and VLANs that apply to a device group. Perform these steps to create or edit VLANs and to set SSIDs.

NOTE

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

Figure 41 illustrates an example of the **Groups > SSIDs** page.

Figure 41 *Groups > SSIDs Page Illustration*



WLANs on a Cisco WLC can be configured on the Cisco WLC Config page.

						First Radio		Second Radio		
		SSID ▼	VLAN ID	Name	Encryption Mode	Enabled	Primary	Enabled	Primary	Native VLAN
□	✎	stores	11	-	No Encryption	☑	○	☑	○	○
□	✎	distribution	1	-	No Encryption	□	○	☑	○	○
□	✎	corp	51	-	No Encryption	☑	○	☑	○	○

NOTE

OV3600 reports users by radio and by SSID. Graphs on the AP and controller monitoring pages display bandwidth in and out based on SSID. OV3600 reports can also be run and filtered by SSID. An option on the **OV3600 Setup > General** page can age out SSIDs and their associated graphical data; by default, this is set to 365 days.

1. Go to **Groups > List** and select the group name for which to define SSIDs/VLANs.
2. Select the **Groups > SSIDs** configuration page. Table 53 describes the information that appears for SSIDs and VLANs that are currently configured for the device group.

Table 53 *Groups > SSIDs Fields and Descriptions*

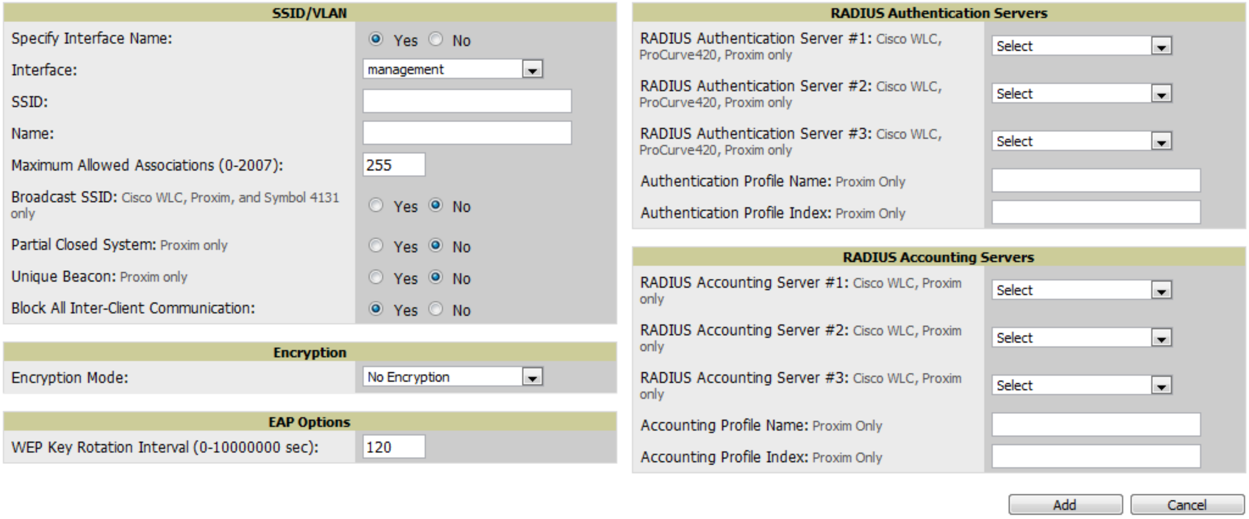
Field	Description
SSID	Displays the SSID associated with the VLAN.
VLAN ID	Identifies the number of the primary VLAN SSID on which encrypted or unencrypted packets can pass between the AP and the switch.
Name	Displays the name of the VLAN.
Encryption Mode	Displays the encryption on the VLAN.
First or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

Table 53 *Groups > SSIDs Fields and Descriptions*

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

3. Select **Add** to create a new SSID or VLAN, or select the pencil icon next to an existing SSID/VLAN to edit that existing SSID or VLAN. The **Add SSID/VLAN** configuration page appears as illustrated in Figure 42 and explained in Table 54.

Figure 42 ***Groups > SSIDs > Add SSID/VLAN*** *Page Illustration*



SSID/VLAN

Specify Interface Name: ● Yes ○ No
Interface: management
SSID:
Name:
Maximum Allowed Associations (0-2007): 255
Broadcast SSID: Cisco WLC, Proxim, and Symbol 4131 only ○ Yes ● No
Partial Closed System: Proxim only ○ Yes ● No
Unique Beacon: Proxim only ○ Yes ● No
Block All Inter-Client Communication: ● Yes ○ No

Encryption

Encryption Mode: No Encryption

EAP Options

WEP Key Rotation Interval (0-10000000 sec): 120

RADIUS Authentication Servers

RADIUS Authentication Server #1: Cisco WLC, ProCurve420, Proxim only: Select
RADIUS Authentication Server #2: Cisco WLC, ProCurve420, Proxim only: Select
RADIUS Authentication Server #3: Cisco WLC, ProCurve420, Proxim only: Select
Authentication Profile Name: Proxim Only
Authentication Profile Index: Proxim Only

RADIUS Accounting Servers

RADIUS Accounting Server #1: Cisco WLC, Proxim only: Select
RADIUS Accounting Server #2: Cisco WLC, Proxim only: Select
RADIUS Accounting Server #3: Cisco WLC, Proxim only: Select
Accounting Profile Name: Proxim Only
Accounting Profile Index: Proxim Only

4. Locate the **SSID/VLAN** section on the **Groups > SSIDS** configuration page and adjust these settings as required. This section encompasses the basic VLAN configuration. Table 54 describes the settings and default values. Note that the displayed settings can vary.

Table 54 ***Groups > SSIDs > SSID/VLAN*** *Section Fields and Default Values*

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

Table 54 ***Groups > SSIDs > SSID/VLAN*** *Section Fields and Default Values (Continued)*

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

5. Locate the **Encryption** area on the **Groups > SSIDs** page and adjust these settings as required. Table 55 describes the settings and default values.

Table 55 ***Groups > SSIDs > Encryption*** *Section Fields and Default Values*

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

6. Locate the **EAP Options** area on the **Groups > SSIDS** page, and complete the settings. Table 56 describes the settings and default values.

Table 56 ***Groups > SSIDs > EAP Options*** *Section Fields and Default Values*

Setting	Default	Description
WEP Key Rotation Interval	120	Time (in seconds) between WEP key rotation on the AP.
Cisco TKIP	No	If enabled, Cisco Temporal Key Integrity Protocol (TKIP) provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP. **NOTE:** TKIP can only be enabled when EAP-based security is used.
Cisco MIC	Disabled	If enabled, Cisco Message Integrity Check (MIC) adds several bytes per packet to make it more difficult to tamper with the packets.

7. Locate the **RADIUS Authentication Servers** area on the **Groups > SSIDS** configuration page and define the settings. Table 57 describes the settings and default values.

Table 57 ***Groups > SSIDs > RADIUS Authentication Servers*** *Fields and Default Values*

Setting	Default	Description
RADIUS Authentication Server 1-3 (ProCurve420, Proxim only)	None	Drop-down menu to select RADIUS Authentication servers previously entered on the **Groups > RADIUS** configuration page. These RADIUS servers dictate how wireless clients authenticate onto the network.
Authentication Profile Name (Proxim Only)	None	Sets the Authentication Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000.
Authentication Profile Index (Proxim Only)	None	Sets the Authentication Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000.

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

NOTE

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

9. Locate the **RADIUS Accounting Servers** area on the **Groups > SSIDS** configuration page and define the settings. Table 58 describes the settings and default values.

Table 58 ***Groups > SSIDs > Radius Accounting Servers*** *Fields and Default Values*

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

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

Configuring Radio Settings for Device Groups

The **Groups > Radio** configuration page allows you to specify detailed RF-related settings for devices in a particular group.

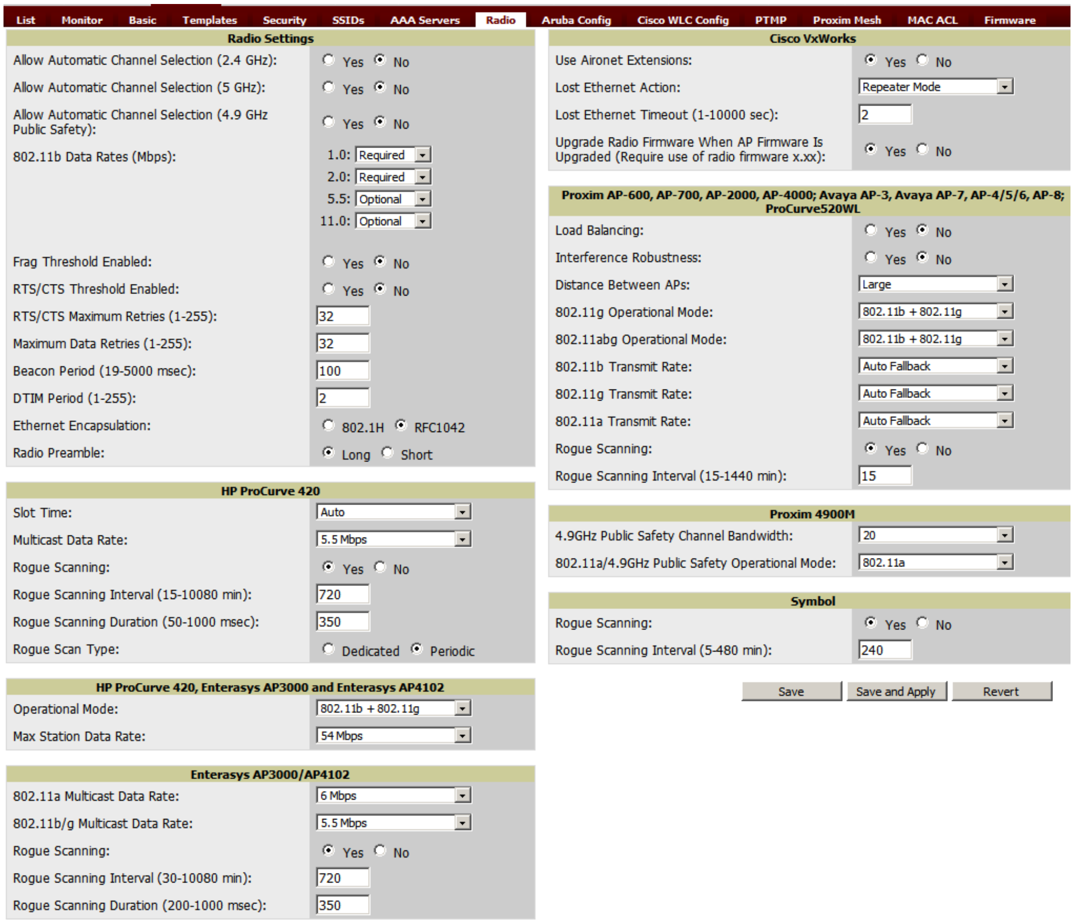
NOTE

If you have existing deployed devices, you may want to use the current RF settings on those devices as a guide for configuring the settings in your default Group.

Perform the following steps to define RF-related radio settings for groups.

1. Go to the **Groups > List** page and select the group for which to define radio settings by selecting the group name. Alternatively, select **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Go to the **Groups > Radio** page. Figure 43 illustrates this page.

Figure 43 ***Groups > Radio*** *Page Illustration*



Radio Settings

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

HP ProCurve 420

Slot Time:	Auto
Multicast Data Rate:	5.5 Mbps
Rogue Scanning:	● Yes ○ No
Rogue Scanning Interval (15-10080 min):	720
Rogue Scanning Duration (50-1000 msec):	350
Rogue Scan Type:	○ Dedicated ● Periodic

HP ProCurve 420, Enterasys AP3000 and Enterasys AP4102

Operational Mode:	802.11b + 802.11g
Max Station Data Rate:	54 Mbps

Enterasys AP3000/AP4102

802.11a Multicast Data Rate:	6 Mbps
802.11b/g Multicast Data Rate:	5.5 Mbps
Rogue Scanning:	● Yes ○ No
Rogue Scanning Interval (30-10080 min):	720
Rogue Scanning Duration (200-1000 msec):	350

Cisco VxWorks

Use Aironet Extensions:	● Yes ○ No
Lost Ethernet Action:	Repeater Mode
Lost Ethernet Timeout (1-10000 sec):	2
Upgrade Radio Firmware When AP Firmware Is Upgraded (Require use of radio firmware x.xx):	● Yes ○ No

Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL

Load Balancing:	○ Yes ● No
Interference Robustness:	○ Yes ● No
Distance Between APs:	Large
802.11g Operational Mode:	802.11b + 802.11g
802.11abg Operational Mode:	802.11b + 802.11g
802.11b Transmit Rate:	Auto Fallback
802.11g Transmit Rate:	Auto Fallback
802.11a Transmit Rate:	Auto Fallback
Rogue Scanning:	● Yes ○ No
Rogue Scanning Interval (15-1440 min):	15

Proxim 4900M

4.9GHz Public Safety Channel Bandwidth:	20
802.11a/4.9GHz Public Safety Operational Mode:	802.11a

Symbol

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

3. Locate the **Radio Settings** area and adjust these settings as required. Table 59 describes the settings and default values.

Table 59 ***Groups > Radio*** *Fields and Default Values*

Setting	Default	Description
Allow Automatic Channel Selection (2.4, 5 GHz and 4.9GHz)	No	If enabled, whenever the AP is rebooted it uses its radio to scan the airspace and select its optimal RF channel based on observed signal strength from other radios. **NOTE:** If you enable this feature, OV3600 automatically reboots the APs in the group when the change is implemented.
802.11b Data Rates (Mbps)	Required: ● 1.0 ● 2.0 Optional: ● 5.5 ● 11.0	Displays pull-down menus for various data rates for transmitting data. **NOTE:** This setting does not apply to Cisco LWAPP devices. The three values in each of the pull-down menus are as follows: ● ***Required***—The AP transmits only unicast packets at the specified data rate; multicast packets are sent at a higher data rate set to optional. (Corresponds to a setting of **yes** on Cisco devices.) ● ***Optional***—The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of **basic** on Cisco devices.) ● ***Not Used***—The AP does not transmit data at the specified data rate. (Corresponds to a setting of **no** on Cisco devices.)
Frag Threshold Enabled	No	If enabled, this setting enables packets to be sent as several pieces instead of as one block. In most cases, leave this option disabled.
Threshold Value	2337	If Fragmentation Threshold is enabled, this specifies the size (in bytes) at which packets are fragmented. A lower **Fragmentation Threshold** setting might be required if there is a great deal of radio interference.

Table 59 ***Groups > Radio*** *Fields and Default Values (Continued)*

Setting	Default	Description
RTS/CTS Threshold Enabled	No	If enabled, this setting configures the AP to issue a RTS (Request to Send) before sending a packet. In most cases, leave this option disabled.
RTS/CTS Threshold Value	2338	If RTS/CTS is enabled, this specifies the size of the packet (in bytes) at which the AP sends the RTS before sending the packet.
RTS/CTS Maximum Retries	32	If RTS/CTS is enabled, this specifies the maximum number of times the AP issues an RTS before stopping the attempt to send the packet through the radio. Acceptable values range from **1** to **128**.
Maximum Data Retries	32	The maximum number of attempts the AP makes to send a packet before giving up and dropping the packet. Acceptable values range from **1** to **255.**
Beacon Period (19-5000 msec)	100	Time between beacons (in microseconds).
DTIM Period (1-255)	2	DTIM alerts power-save devices that a packet is waiting for them. This setting configures DTIM packet frequency as a multiple of the number of beacon packets. The DTIM Interval indicates how many beacons equal one cycle.
Ethernet Encapsulation	RFC1042	This setting selects either the RFC1042 or 802.1h Ethernet encapsulation standard for use by the group.
Radio Preamble	Long	This setting determines whether the APs uses a **short** or **long** preamble. The preamble is generated by the AP and attached to the packet prior to transmission. The short preamble is 50 percent shorter than the long preamble and thus may improve wireless network performance. **NOTE:** Because older WLAN hardware may not support the "short" preamble, the "long" preamble is recommended as a default setting in most environments.

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

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

NOTE

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

5. To configure HP ProCurve 420 settings exclusively, locate the **HP ProCurve 420** section and adjust these settings as required. Table 60 describes the settings and default values.

Table 60 ***HP ProCurve 420*** *Fields and Default Values*

Setting	Default	Description
Slot Time	Auto	Short-slot-time mechanism, if used on a pure 802.11g deployment, improves WLAN throughput by reducing wait time for transmitter to assure clear channel assessment.
Multicast Data Rate	5.5Mbps	Sets the maximum data rate of the multicast data packets.
Rogue Scanning	Enabled	If enabled the 420 APs in the group will scan for rogues.
Rogue Scanning Interval (15-10080 min)	720	If rogue scanning is enabled, this setting controls the frequency with which scans are conducted (in minutes). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan. **NOTE:** This setting only applies to Periodic scans.

Table 60 *HP ProCurve 420 Fields and Default Values (Continued)*

Setting	Default	Description
Rogue Scanning Duration (50-1000 msec)	350	Specifies the amount of time, in milliseconds, the AP should spend performing the rogue scan. If the duration is set too high users may start to experience connectivity issues. **NOTE:** This setting only applies to periodic scans.
Rogue Scan Type	Periodic	Specifies the Rogue Scanning mode. When set to **Dedicated**, users are unable to associate to the AP.

6. To configure the HP ProCurve 240, Enterasys AP 3000 and AP 4102 Operational Mode and Max Station Data Rate, locate the **HP ProCurve 240, Enterasys AP 3000** and **AP 4102** section and define the settings. Table 61 describes the settings and default values of this page.

Table 61 *HP ProCurve 240, Enterasys AP 3000 and AP 4102 Fields and Default Values*

Setting	Default	Description
Operational Mode	802.11b + 802.11g	Sets the radio operational mode for all of the ProCurve 420s, Enterasys 3000s and 4102s in the group to either b only, g only, or b + g.
Max Station Data Rate	54 Mbps	The maximum data rate at which a user can connect to the AP.

7. To configure settings specific to Enterasys AP3000 and Enterasys AP4102, locate the **Enterasys AP3000** and **Enterasys AP4102** section and define the settings. Table 62 describes the settings and default values of this page.

Table 62 *Enterasys AP3000 and Enterasys AP4102 Fields and Default Values*

Setting	Default	Description
802.11a Multicast Data Rate	6 Mbps	Drop-down menu that specifies the a radio multicast data rate.
802.11b/g Multicast Data Rate	5.5 Mbps	Drop-down menu that specifies the b/g multicast data rate.
Rogue Scanning	Enabled	If enabled AP 3000s and 4102s in the group with firmware 3.1.20 or newer will passively scan for rogue access points at the specified interval for the specified amount of time. This rogue scan will not break users' association to the network.
Rogue Scan Interval (30-10080 min)	720	Specifies the time, in minutes, between rogue scans.
Rogue Scan Duration (200-1000 msec)	350	Specifies the amount of time, in milliseconds, the AP listens to rogues before returning to normal operation.

8. To configure radio settings for Cisco VxWorks devices in the group, locate the **Groups > VxWorks** section and adjust these settings as required. Table 63 describes the settings and default values of this page.

Table 63 *Groups > VxWorks Fields and Default Values*

Setting	Default	Description
Use Aironet Extensions	Yes	When enabled, this option allows Cisco devices to provide functionality not supported by 802.11 IEEE standards, including the following: ● **Load balancing**—Allows the access point to direct Aironet clients to the optimum access point. ● **Message Integrity Check (MIC)**—Protects against bit-flip attacks. ● **Temporal Key Integrity Protocol (TKIP)**—Key hashing algorithm that protects against IV attacks.

Table 63 ***Groups > VxWorks** Fields and Default Values (Continued)*

Setting	Default	Description
Lost Ethernet Action	Repeater Mode	Pull-down menu that specifies the action to take when the Lost Ethernet Timeout threshold is exceeded: ● **No Action**—No action taken by the AP. ● **Repeater Mode**—The AP converts to a repeater, disassociating all its clients while the backbone is unavailable. If the AP can communicate with another root AP on the same SSID, its clients will be able to re-associate and connect to the backbone. If the AP cannot communicate with another root AP, clients are not allowed to re-associate. ● **Disable Radio**—The AP disassociates its clients and disables the radio until it can establish communication with the backbone. ● **Restrict SSID**—The AP disassociates all clients and then allows clients to re-associate with current SSID.
Lost Ethernet Timeout (1-1000 secs)	2	Specifies the time (in seconds) the AP waits prior to taking action when its backbone connectivity is down. Actions are defined in the **Lost Ethernet Action** field.
Upgrade Radio Firmware When AP Firmware Is Upgraded	Yes	If enabled, this setting mandates that the radio firmware be upgraded to a firmware version compatible with the current version of AP firmware.

9. To configure settings specific to the Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3/4/5/6//7/8, and ProCurve 520WL, locate the appropriate section of **Groups > Radio** page and define the required fields. Table 64 describes the settings and default values.

Table 64 ***Groups > Proxim/Avaya/Procurve APs** Fields and Default Values*

Setting	Default	Description
Load Balancing	No	If enabled, this setting allows client devices associating to an AP with two radio cards to determine which card to associate with, based on the load (# of clients) on each card. **NOTE:** This feature is only available when two 802.11b wireless cards are used in an AP-2000.
Interference Robustness	No	If enabled, this option will fragment packets greater than 500 bytes in size to reduce the impact of radio frequency interference on wireless data throughput.
Distance Between APs	Large	This setting adjusts the receiver sensitivity. Reducing receiver sensitivity from its maximum may help reduce the amount of crosstalk between wireless stations to better support roaming users. Reducing the receiver sensitivity, user stations will be more likely to connect with the nearest access point.
802.11g Operational Mode	802.11b +802.11g	This setting sets the operational mode of all g radios in the group to either b only, g only or b + g.
802.11abg Operational Mode	802.11b +802.11g	This setting sets the operational mode of all a/b/g radios in the group to either a only, b only, g only or b + g.
802.11b Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
802.11g Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
802.11a Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
Rogue Scanning	Yes	If enabled, any ORiNOCO or Avaya APs in the group (with the appropriate firmware) will passively scan for rogue access points at the specified interval. This rogue scan will not break users' association to the network. **NOTE:** This feature can affect the data performance of the access point.

Table 64 ***Groups > Proxim/Avaya/Procurve APs*** *Fields and Default Values (Continued)*

Setting	Default	Description
Rogue Scan Interval	15 minutes	If rogue scanning is enabled, this setting controls the frequency with which scans are conducted (in minutes). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan.

10. To configure settings specific to Proxim 4900M, locate the **Proxim 4900M** section and define the required fields. Table 65 describes the settings and default values.

Table 65 ***Proxim 4900*** *Fields and Default Values*

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

11. To configure Symbol-only settings, locate the **Symbol** section and define the required fields. Table 66 describes the settings and default values.

Table 66 ***Symbol****-only Fields and Default Values*

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

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

An Overview of Cisco WLC Configuration

The **Groups > Cisco WLC Config** page consolidates the settings for Cisco WLC devices from all group pages. The **Groups > SSIDs** subtab applies to all device types except for Cisco WLC, which have WLANs configured on the **Cisco WLC Config** page. It is not recommended to have HP Procurve 420s, Symbol 4131 and Proxim APs in the same group as Cisco devices. Also, it is recommended that users set device preferences to **Only devices in this group**. This topic describes how to access and navigate the **Groups > Cisco WLC Config** page.

Accessing Cisco WLC Configuration

Go to the **Cisco WLC Config** page in one of these two ways:

1. In **Groups > List**, select a group that has been defined to support Cisco devices and the **Cisco WLC Config** option appears in the subtabs.
2. In **Groups > List**, create a new group to support Cisco devices with these steps:
   - Select **Add** from the **Groups > List** page to create a new group, enter a group name, and select **Add**.
   - Once OV3600 prompts you with the **Groups > Basic** page, ensure that you enable device-specific settings for **Cisco WLC**.

- Once you select **Save** or **Save and Apply**, then the **Groups > Cisco WLC Config** subtab appears in the navigation pane at the top in association with that group.

Navigating Cisco WLC Configuration

The navigation pane on the left side of the **Groups > Cisco WLC Config** page is expandable, and displays the Cisco configurations supported and deployed. Figure 44 and Figure 45 illustrate this navigation pane.

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

Figure 44 ***Groups** > **Cisco WLC Config** Page Illustration, collapsed view*

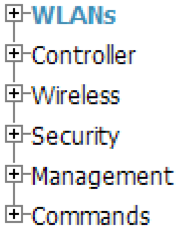
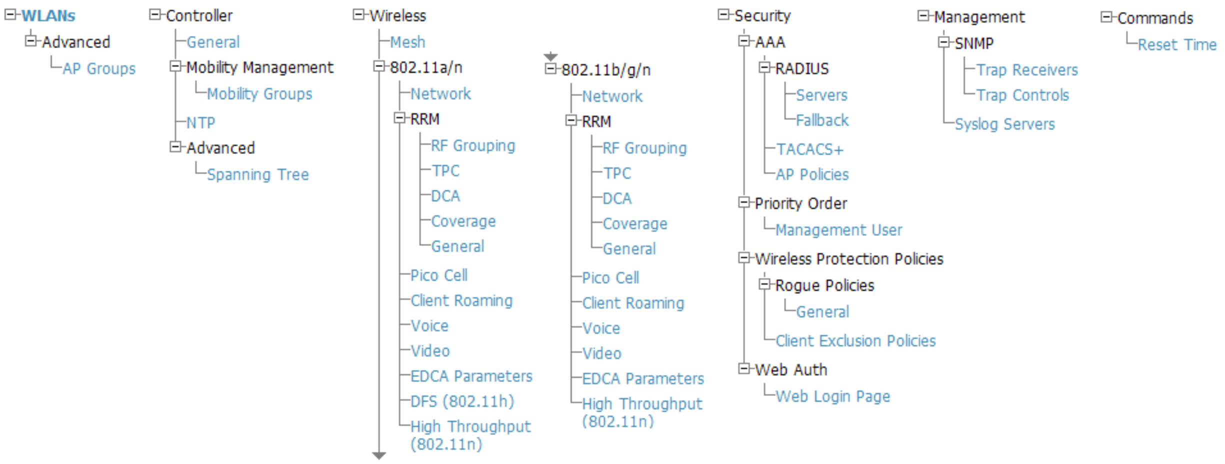


Figure 45 ***Groups** > **Cisco WLC Config** Page Illustration, expanded view*

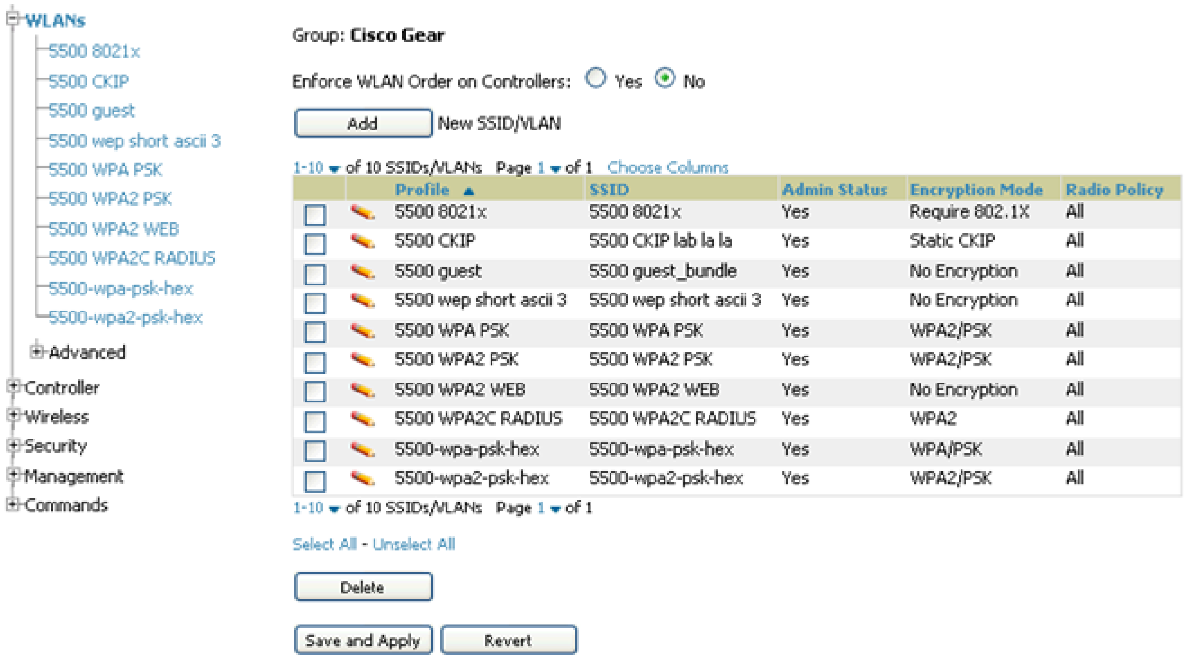


Configuring WLANs for Cisco WLC Devices

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

1. Go to the **Groups > Cisco WLC Config** page, and select **WLANs** in the navigation pane at left. This page displays the SSIDs or VLANs that are available for use with Cisco WLC devices, and enables you to define new SSIDs or VLANs. Figure 46 illustrates this page.
2. To change the ID/position of a WLAN on the controller by dragging and dropping, set the toggle to **yes**. Note that the by setting this flag to **yes**, OV3600 will display a mismatch if the WLANs in the desired and device config differ only on the order.

Figure 46 ***Groups* > *Cisco WLC Config* > *WLANS*** *page illustration*



- WLANs
  - 5500 8021x
  - 5500 CKIP
  - 5500 guest
  - 5500 wep short ascii 3
  - 5500 WPA PSK
  - 5500 WPA2 PSK
  - 5500 WPA2 WEB
  - 5500 WPA2C RADIUS
  - 5500-wpa-psk-hex
  - 5500-wpa2-psk-hex
  - Advanced
- Controller
- Wireless
- Security
- Management
- Commands

Group: **Cisco Gear**

Enforce WLAN Order on Controllers: ○ Yes ● No

Add New SSID/VLAN

1-10 of 10 SSIDs/VLANs Page 1 of 1 Choose Columns

		Profile ▲	SSID	Admin Status	Encryption Mode	Radio Policy
□	✎	5500 8021x	5500 8021x	Yes	Require 802.1X	All
□	✎	5500 CKIP	5500 CKIP lab la la	Yes	Static CKIP	All
□	✎	5500 guest	5500 guest_bundle	Yes	No Encryption	All
□	✎	5500 wep short ascii 3	5500 wep short ascii 3	Yes	No Encryption	All
□	✎	5500 WPA PSK	5500 WPA PSK	Yes	WPA2/PSK	All
□	✎	5500 WPA2 PSK	5500 WPA2 PSK	Yes	WPA2/PSK	All
□	✎	5500 WPA2 WEB	5500 WPA2 WEB	Yes	No Encryption	All
□	✎	5500 WPA2C RADIUS	5500 WPA2C RADIUS	Yes	WPA2	All
□	✎	5500-wpa-psk-hex	5500-wpa-psk-hex	Yes	WPA/PSK	All
□	✎	5500-wpa2-psk-hex	5500-wpa2-psk-hex	Yes	WPA2/PSK	All

1-10 of 10 SSIDs/VLANs Page 1 of 1

Select All - Unselect All

Delete

Save and Apply Revert

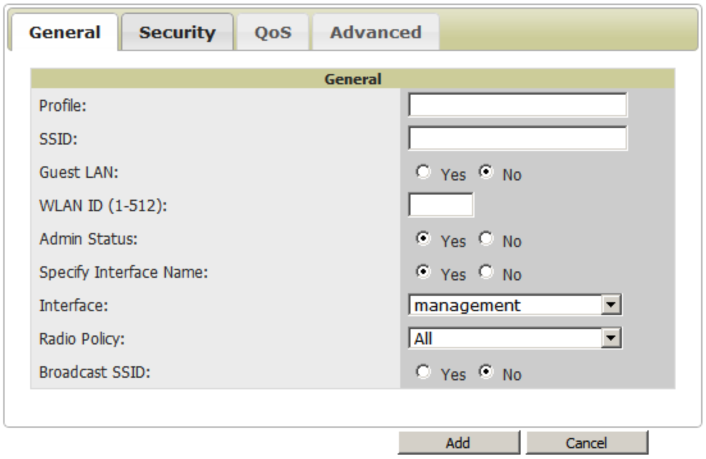
3. To add or edit SSIDs or VLANs that are dedicated to Cisco WLC devices, either select the **Add New SSID/VLAN** button, or select the pencil icon for an existing SSID/VLAN. A new page appears comprised of four tabs, as follows:

   - **General**—Defines general administrative parameters for the Cisco WLC WLAN.
   - **Security**—Defines encryption and RADIUS servers.
   - **QoS**—Defines quality of service (QoS) parameters for the Cisco WLC WLAN.
   - **Advanced**—Defines advanced settings that are available only with Cisco WLC devices, for example, AAA override, coverage, DHCP and DTIM period.

NOTE

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

Figure 47 ***Groups* > *Cisco WLC Config* > *WLANs* > *Add New SSID/VLAN* > *General*** *Tab Illustration*



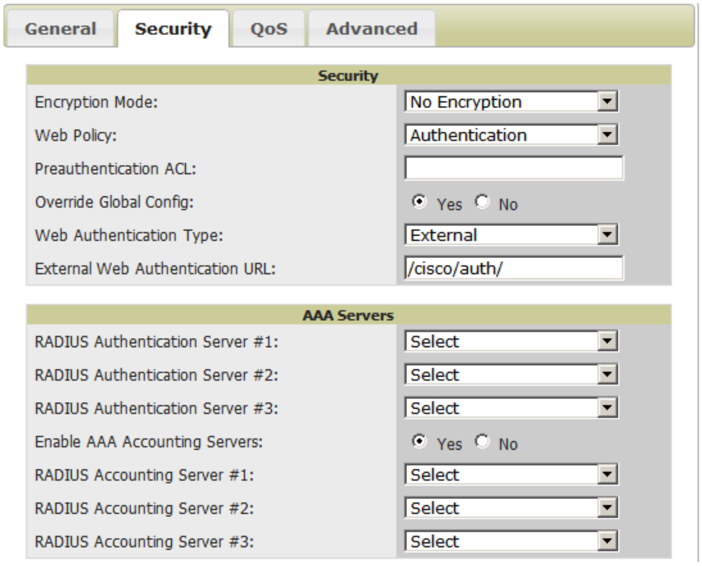
General | Security | QoS | Advanced

General

Profile:	
SSID:	
Guest LAN:	○ Yes ● No
WLAN ID (1-512):	
Admin Status:	● Yes ○ No
Specify Interface Name:	● Yes ○ No
Interface:	management
Radio Policy:	All
Broadcast SSID:	○ Yes ● No

Add Cancel

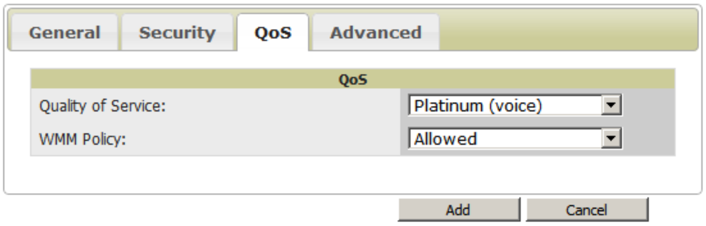
Figure 48 ***Groups* > *Cisco WLC Config* > *WLANs* > *Add New SSID/VLAN* > *Security*** *Tab Illustration*



Security	
Encryption Mode:	No Encryption
Web Policy:	Authentication
Preauthentication ACL:	
Override Global Config:	● Yes ○ No
Web Authentication Type:	External
External Web Authentication URL:	/cisco/auth/

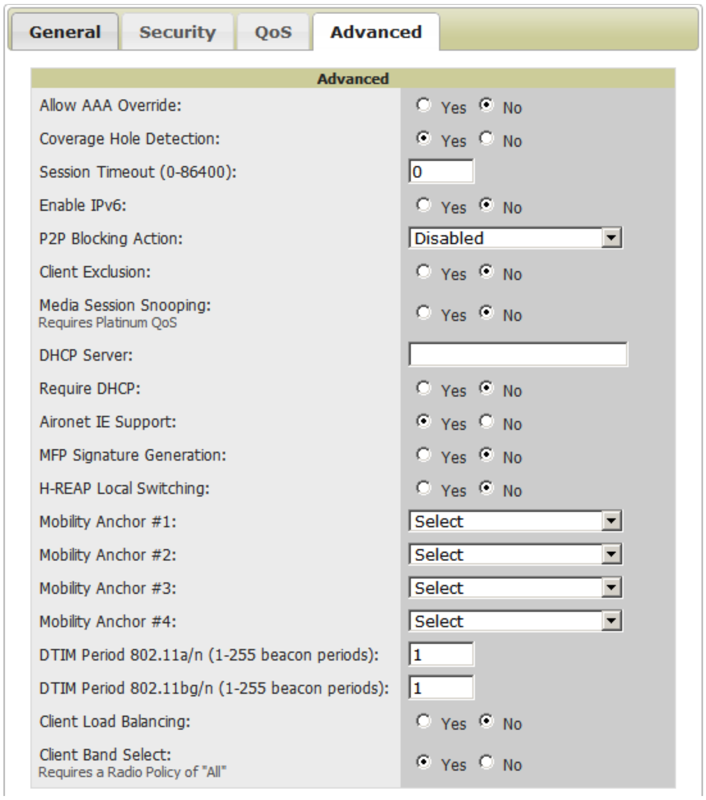
AAA Servers	
RADIUS Authentication Server #1:	Select
RADIUS Authentication Server #2:	Select
RADIUS Authentication Server #3:	Select
Enable AAA Accounting Servers:	● Yes ○ No
RADIUS Accounting Server #1:	Select
RADIUS Accounting Server #2:	Select
RADIUS Accounting Server #3:	Select

Figure 49 ***Groups* > *Cisco WLC Config* > *WLANs* > *Add New SSID/VLAN* > *QoS*** *Tab Illustration*



QoS	
Quality of Service:	Platinum (voice)
WMM Policy:	Allowed

Figure 50 ***Groups* > *Cisco WLC Config* > *WLANs* > *Add New SSID/VLAN* > *Advanced*** *Tab Illustration*



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

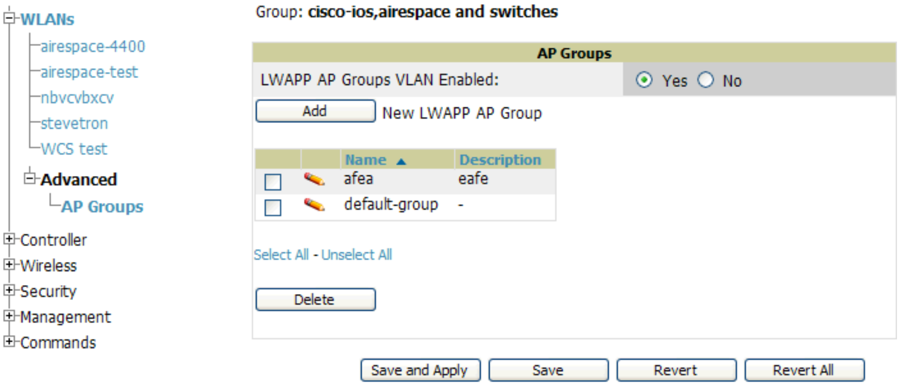
Defining and Configuring LWAPP AP Groups for Cisco Devices

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

Viewing and Creating AP Groups

1. Go to the **Groups > Cisco WLC Config** page, and select **WLANs > Advanced > AP Groups** in the navigation pane at left. This page displays the configured LWAPP APs. Figure 51 illustrates this page.

Figure 51 ***Groups** > **Cisco WLC Config** > **WLANS** > **Advanced** > **AP Groups** Page Illustration*



Group: cisco-ios,airespace and switches

AP Groups

LWAPP AP Groups VLAN Enabled: ● Yes ○ No

New LWAPP AP Group

		Name ▲	Description
□	✎	afea	eafe
□	✎	default-group	-

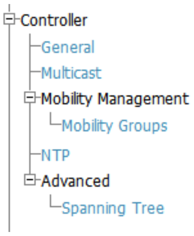
2. To add a new LWAPP AP group, select **Yes** in the **AP Groups** section. Additional controls appear.
3. Select **Add** to create a new LWAPP AP group. To edit an existing LWAPP AP group, select the pencil icon next to that group. Add one or more SSIDs and the interface/VLAN ID mapping on the **Add/Edit**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

Configuring Cisco Controller Settings

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

Go to the **Groups > Cisco WLC Config > Controller** page. This navigation is illustrated in Figure 52.

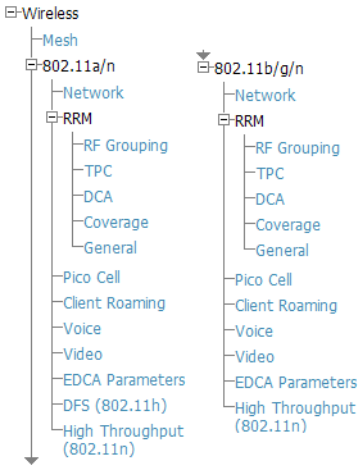
Figure 52 ***Groups** > **Cisco WLC Config** > **Controller** Navigation*



Configuring Wireless Parameters for Cisco Controllers

This section illustrates the configuration of **Wireless** settings in support of Cisco WLC controllers. The navigation for Wireless settings is illustrated in Figure 53.

Figure 53 ***Groups* > *Cisco WLC Config* > *Wireless*** *Navigation Illustration*



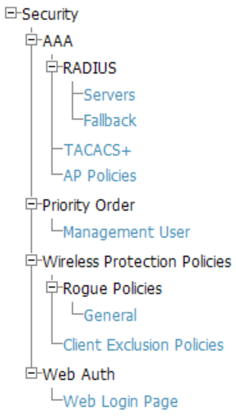
Configuring Security Parameters and Functions

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

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

Figure 54 illustrates these components and this navigation:

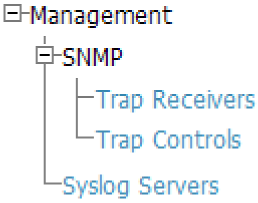
Figure 54 ***Groups* > *Cisco WLC Config* > *Security*** *Navigation Illustration*



Configuring Management Settings for Cisco

OV3600 allows you to configure of SNMP and Syslog Server settings for Cisco WLC controllers. Users should be able to configure up to four trap receivers on the Cisco WLC including the OV3600 IP that can be used in Global Groups. To define SNMP and server settings, go to the **Groups > Cisco WLC Config > Management** page, illustrated in Figure 55.

Figure 55 ***Groups* > *Cisco WLC Config* > *Management*** *Navigation Illustration*



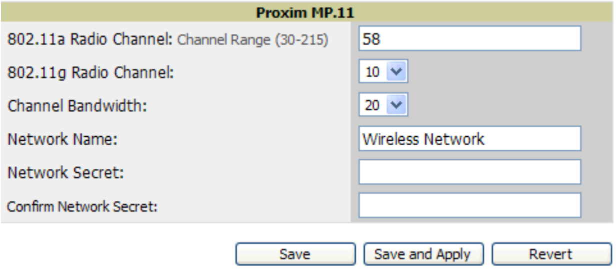
Configuring Group PTMP Settings

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

Perform the following steps to configure these functions.

1. Go to the **Groups > List** page and select the group for which to define PTMP settings by selecting the group name. Alternatively, select **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Select the PTMP tab in the OV3600 navigation menu. Figure 56 illustrates this page.

Figure 56 ***Groups* > *PTMP*** *Page Illustration*



Proxim MP.11

802.11a Radio Channel: Channel Range (30-215)	58
802.11g Radio Channel:	10
Channel Bandwidth:	20
Network Name:	Wireless Network
Network Secret:	
Confirm Network Secret:	

3. Define the settings on this page. Table 67 describes the settings and default values.

Table 67 ***Groups* > *PTMP*** *Fields and Default Values*

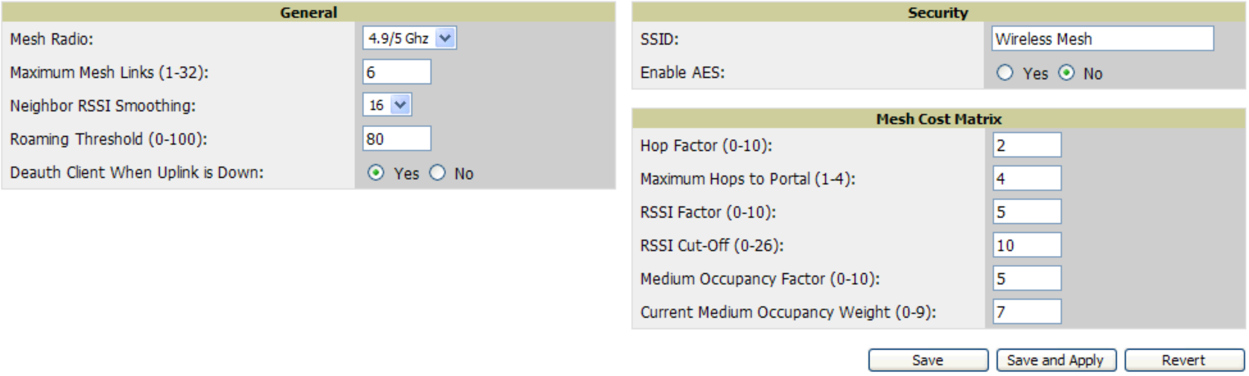
Setting	Default	Description
802.11a Radio Channel	58	Selects the channel used for 802.11a radios by the devices in this group.
802.11g Radio Channel	10	Selects the channel used for 802.11g radios by the devices in this group.
Channel Bandwidth	20	Defines the channel bandwidth used by the devices in this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

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

Configuring Proxim Proxim Mesh

1. Go to the **Groups > Proxim Mesh** configuration page to configure Mesh-specific radio settings.
2. Define the settings as required for your network. Figure 57 illustrates this page. Table 68 and Table 69 describe the settings and default values.

Figure 57 ***Groups* > *Proxim Mesh*** *Page Illustration*



General

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

Security

SSID:	Wireless Mesh
Enable AES:	○ Yes ● No

Mesh Cost Matrix

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

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

Table 68 ***Groups* > *Proxim Mesh* > *General*** *Fields and Default Values*

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

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

Table 69 ***Groups* > *Proxim Mesh* > *Security*** *Fields and Default Values*

Setting	Default	Description
SSID	None	Sets the SSID used by the Mesh Radio to connect to the mesh network.
Enable AES	No	Enable or Disable AES encryption.

3. The **Mesh Cost Matrix** configuration section contains settings for hop factor and maximum hops to portal, RSSI factor and cut-off, medium occupancy factor and current medium occupancy weight. Adjust these settings as required for your network. Table 70 describes these settings and default values.

Table 70 ***Groups* > *Proxim Mesh* > *Mesh Cost Matrix*** *Fields and Default Values*

Setting	Default	Description
Hop Factor	5	Sets the factor associated with each hop when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
Maximum Hops to Portal	4	Set the maximum number of hops for the AP to reach the Portal AP.
RSSI Factor	5	Sets the factor associated with the RSSI values used when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
RSSI Cutoff	10	Specifies the minimum RSSI needed to become a mesh neighbor.

Table 70 ***Groups > Proxim Mesh > Mesh Cost Matrix*** *Fields and Default Values (Continued)*

Setting	Default	Description
Medium Occupancy Factor	5	Sets the factor associated with Medium Occupancy when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
Current Medium Occupancy Weight	7	Specifies the importance given to the most recently observed Medium Occupancy against all of the previously viewed medium occupancies. Lower values place more importance on previously observed Medium Occupancies.

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

Configuring Group MAC Access Control Lists

This configuration is optional. If you use Symbol 4121/4131, Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP-3/4/5/6/7/8, or ProCurve 520WL wireless access points, OV3600 enables you to specify the MAC Addresses of devices that are permitted to associate with APs in the Group. Other devices are not able to associate to APs in the Group, even if the users of those devices are authorized users on the network.

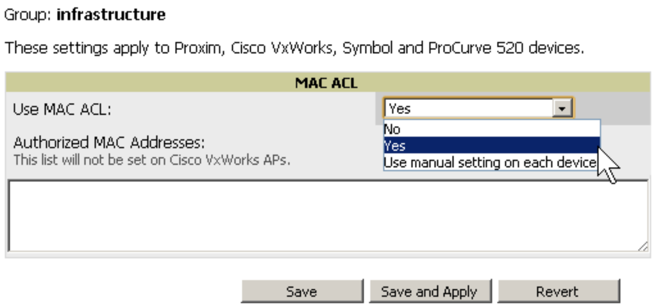
NOTE

If **Use MAC ACL** is enabled for Cisco VxWorks, OV3600 does not disable this feature on the AP; but the MAC list entered is not populated on the AP. The individual MAC addresses must be entered manually on the AP. If you have APs from other vendors in the Group, the ACL restrictions do not apply to those APs.

Perform the following steps to use the MAC ACL function.

1. Browse to the **Groups > MAC ACL** configuration page. Figure 58 illustrates this page.

Figure 58 ***Groups > MAC ACL*** *Page Illustration*



Group: **infrastructure**

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

MAC ACL

Use MAC ACL: Yes

Authorized MAC Addresses:
This list will not be set on Cisco VxWorks APs.

2. Select **Yes** on the **Use MAC ACL** drop-down menu. Enter all authorized MAC addresses, separated by white spaces.

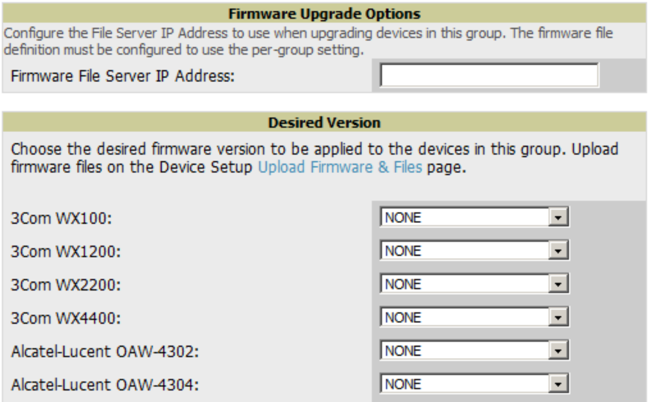
3. Select **Save** when configurations are complete to retain these settings. Select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.

Specifying Minimum Firmware Versions for APs in a Group

This configuration is optional. OV3600 allows you the option of defining the minimum firmware version for each AP type in a group on the **Groups > Firmware** configuration page. At the time that you define the minimum version, OV3600 automatically upgrades all eligible APs. When you add APs into the group in the future, you will be able to upgrade APs in manual fashion. The firmware for an AP is not upgraded automatically when it is added to a group. Perform the following steps to make this firmware configuration.

1. Browse to the **Groups > Firmware** configuration page. Figure 59 illustrates this page.

Figure 59 ***Groups > Firmware*** *Page Illustration*



Firmware Upgrade Options

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

Firmware File Server IP Address:	

Desired Version

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

3Com WX100:	NONE
3Com WX1200:	NONE
3Com WX2200:	NONE
3Com WX4400:	NONE
Alcatel-Lucent OAW-4302:	NONE
Alcatel-Lucent OAW-4304:	NONE

2. For each device type in the group, specify the minimum acceptable firmware version. If no firmware versions are listed, go to the **Device Setup > Firmware** configuration page to upload the firmware files to OV3600.
3. Select **Upgrade** to apply firmware preferences to devices in the group. Refer to the firmware upgrade help under **APs/Devices > Manage** configuration page for detailed help on Firmware job options.
4. Select **Save** to save the firmware file as the desired version for the group.
5. If you have opted to assign an external TFTP server on a per-group basis on the **Device Setup > Firmware** configuration page, you can enter the IP address in the **Firmware Upgrade Options** field on the top of this configuration page.
6. Once you have defined your first group, you can configure that group to be the **default** group on your network. When OV3600 discovers new devices that need to be assigned to a management group, the default group appears at the top of all drop-down menus and lists. Newly discovered devices are place automatically in the default group if OV3600 is set to **Automatically Monitor/Manage New Devices** on **OV3600 Setup > General**.
7. Browse to the **Groups > List** configuration page.
8. From the list of groups, check the **Default** radio button next to the desired default group.

Comparing Device Groups

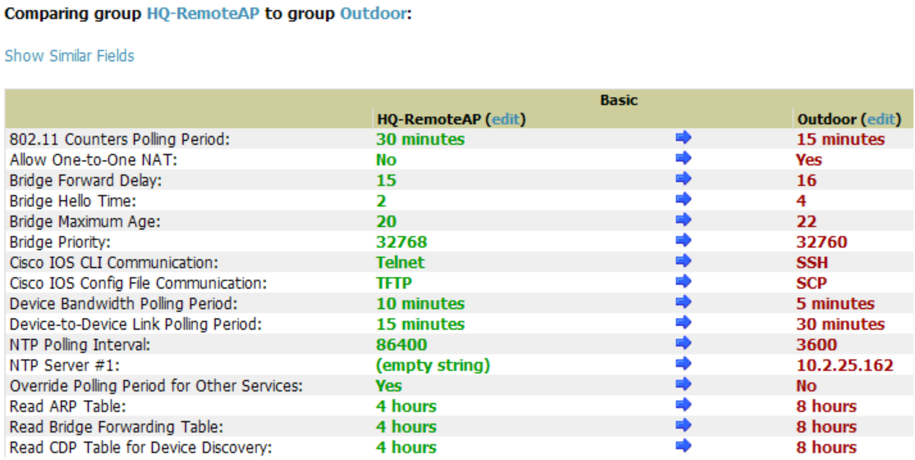
You can compare two existing device groups with a detailed line-item comparison. Group comparison allows several levels of analysis to include the following:

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

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

1. From the **Groups > List** page, select **Compare two groups**. Two drop-down menus appear.
2. Select the two groups to compare to each other in the drop-down menus, and select **Compare**. The **Compare** page appears, displaying some configuration categories. Figure 60 illustrates this page.

Figure 60 *Comparing Two Devices Groups on the* ***Groups > List > Compare*** *Page (Partial View)*



Comparing group HQ-RemoteAP **to group** Outdoor**:**

Show Similar Fields

	Basic		
	HQ-RemoteAP (edit)		**Outdoor** (edit)
802.11 Counters Polling Period:	30 minutes	➡	15 minutes
Allow One-to-One NAT:	No	➡	Yes
Bridge Forward Delay:	15	➡	16
Bridge Hello Time:	2	➡	4
Bridge Maximum Age:	20	➡	22
Bridge Priority:	32768	➡	32760
Cisco IOS CLI Communication:	Telnet	➡	SSH
Cisco IOS Config File Communication:	TFTP	➡	SCP
Device Bandwidth Polling Period:	10 minutes	➡	5 minutes
Device-to-Device Link Polling Period:	15 minutes	➡	30 minutes
NTP Polling Interval:	86400	➡	3600
NTP Server #1:	(empty string)	➡	10.2.25.162
Override Polling Period for Other Services:	Yes	➡	No
Read ARP Table:	4 hours	➡	8 hours
Read Bridge Forwarding Table:	4 hours	➡	8 hours
Read CDP Table for Device Discovery:	4 hours	➡	8 hours

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

Deleting a Group

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

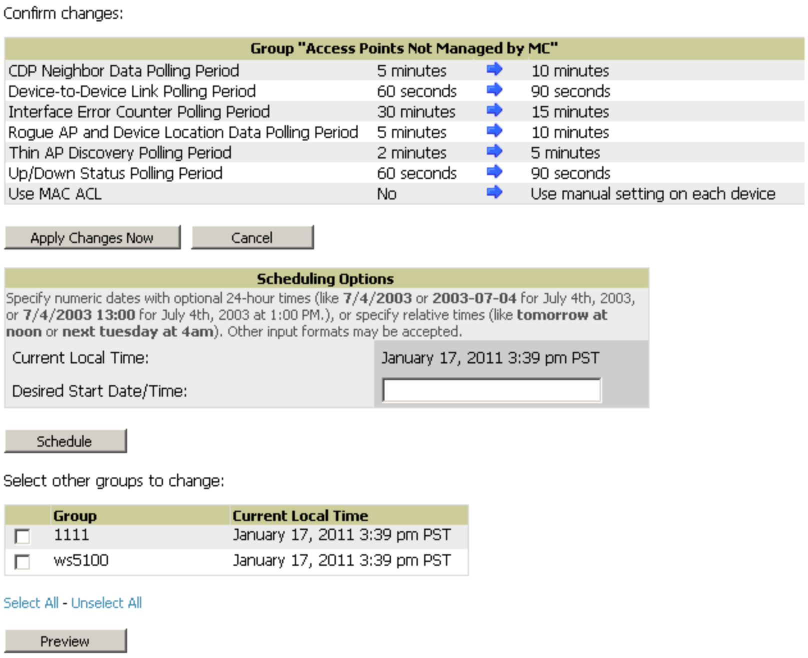
1. Browse to the **Groups > List** configuration page.
2. Ensure that the Group you wish to delete is not marked as the **default** group. OV3600 does not permit you to delete the current default Group.
3. Ensure that there are no devices in the Group you wish to delete. OV3600 does not permit you to delete a Group that still contains managed devices. You must move all devices to other Groups before deleting a Group.
4. Ensure that the Group is not a Global Group which has Subscriber Groups, and is not a Group that was pushed from a Master Console. OV3600 will not delete a Group in which either of those is true.
5. Select the checkbox and select **Delete**.

Changing Multiple Group Configurations

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

1. Browse to the **Groups > List** configuration page.
2. Select the **Manage** link (the pencil icon) for the group you wish to edit. The **Groups > Basic** configuration page appears.
3. Select the fields to be edited on the **Basic** configuration page or go to **Radio**, **Security**, **VLANs**, or **MAC ACL** configuration page and edit the fields. Use the **Save** button to store the changes prior to applying them.
4. When all changes for the group are complete select the **Save and Apply** button to make the changes permanent. Figure 61 illustrates the confirmation message that appears.

Figure 61 ***Groups > Basic** Configuration Change Confirmation Page Illustration*



Confirm changes:

Group "Access Points Not Managed by MC"			
CDP Neighbor Data Polling Period	5 minutes	➡	10 minutes
Device-to-Device Link Polling Period	60 seconds	➡	90 seconds
Interface Error Counter Polling Period	30 minutes	➡	15 minutes
Rogue AP and Device Location Data Polling Period	5 minutes	➡	10 minutes
Thin AP Discovery Polling Period	2 minutes	➡	5 minutes
Up/Down Status Polling Period	60 seconds	➡	90 seconds
Use MAC ACL	No	➡	Use manual setting on each device

Scheduling Options

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

Current Local Time:	January 17, 2011 3:39 pm PST
Desired Start Date/Time:	

Select other groups to change:

	Group	Current Local Time
□	1111	January 17, 2011 3:39 pm PST
□	ws5100	January 17, 2011 3:39 pm PST

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

NOTE

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

   - **Schedule** — Schedules the changes to be applied to this group in the future. Enter the desired change date in the **Start Date/Time field**. OV3600 takes the time zone into account for the group if a time zone other than **OV3600 System Time** has been configured on the **Groups > Basic** configuration page.
   - **Cancel** — Cancels the application of changes (immediately or scheduled).

NOTE

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

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

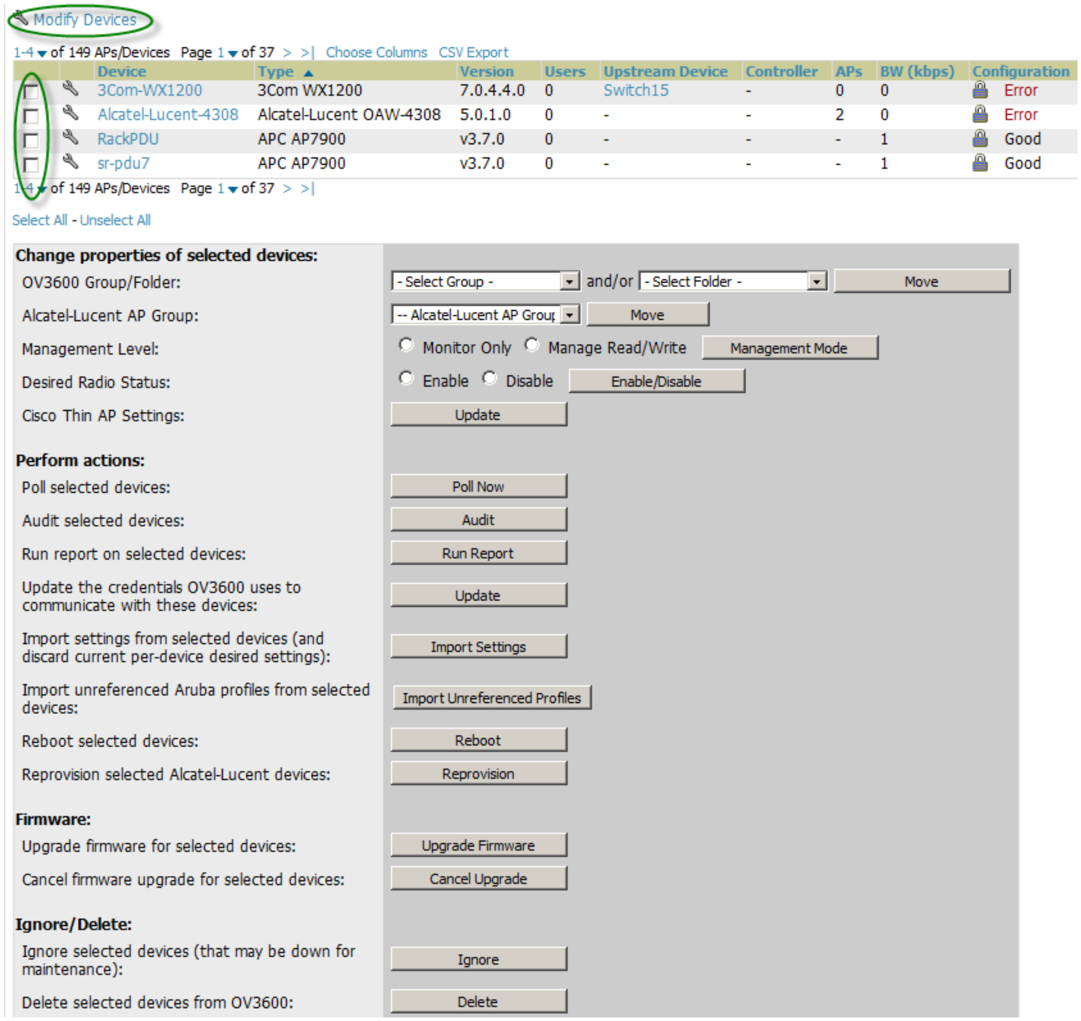
Modifying Multiple Devices

OV3600 provides a very powerful utility that modifies all APs or a subset of access points unrelated to the typical OV3600 group construct. This utility provides the ability to delete simultaneously multiple devices, migrate multiple devices to another group and/or folder, update credentials and optimize channels. Perform these steps to modify multiple devices.

1. To modify multiple devices, go to one of the following pages with a device list:
   - **APs/Devices > List**
   - **APs/Devices > Up**
   - **APs/Devices > Down**
   - **APs/Devices > Mismatched**
   - **Groups > Monitor** configuration pages

   Each of these pages displays a list of devices. Controller monitoring pages also have lists of their thin APs which can be modified using **Modify Devices**.
2. Select **Modify Devices** to make the checkboxes at the left of all devices appear. In addition, a new section appears in this page location to display various settings that can be configured for multiple devices at one time (some operations cannot be performed on the selected devices). Figure 62 illustrates this page.

Figure 62 ***Modify Multiple Devices*** *Section Illustration*



Modify Devices

1-4 ▾ of 149 APs/Devices Page 1 ▾ of 37 > >| Choose Columns CSV Export

		Device	Type ▲	Version	Users	Upstream Device	Controller	APs	BW (kbps)	Configuration
□	🔧	3Com-WX1200	3Com WX1200	7.0.4.4.0	0	Switch15	-	0	0	🔒 Error
□	🔧	Alcatel-Lucent-4308	Alcatel-Lucent OAW-4308	5.0.1.0	0	-	-	2	0	🔒 Error
□	🔧	RackPDU	APC AP7900	v3.7.0	0	-	-	-	1	🔒 Good
□	🔧	sr-pdu7	APC AP7900	v3.7.0	0	-	-	-	1	🔒 Good

1-4 ▾ of 149 APs/Devices Page 1 ▾ of 37 > >|

Select All - Unselect All

Change properties of selected devices:	
OV3600 Group/Folder:	- Select Group - ▾ and/or - Select Folder - ▾ [Move]
Alcatel-Lucent AP Group:	-- Alcatel-Lucent AP Grour ▾ [Move]
Management Level:	○ Monitor Only ○ Manage Read/Write [Management Mode]
Desired Radio Status:	○ Enable ○ Disable [Enable/Disable]
Cisco Thin AP Settings:	[Update]
Perform actions:	
Poll selected devices:	[Poll Now]
Audit selected devices:	[Audit]
Run report on selected devices:	[Run Report]
Update the credentials OV3600 uses to communicate with these devices:	[Update]
Import settings from selected devices (and discard current per-device desired settings):	[Import Settings]
Import unreferenced Aruba profiles from selected devices:	[Import Unreferenced Profiles]
Reboot selected devices:	[Reboot]
Reprovision selected Alcatel-Lucent devices:	[Reprovision]
Firmware:	
Upgrade firmware for selected devices:	[Upgrade Firmware]
Cancel firmware upgrade for selected devices:	[Cancel Upgrade]
Ignore/Delete:	
Ignore selected devices (that may be down for maintenance):	[Ignore]
Delete selected devices from OV3600:	[Delete]

3. Select one or more devices that are to share the configurations. Select the checkbox for each device to modify.
4. In the **Modify Multiple Devices** section, select any button or use any drop-down menu for the supported changes. Any action you take applies to all selected devices. Each action you take will direct you to a new configuration page, or prompt you with a confirmation page to confirm your changes.
5. You are taken to a confirmation configuration page that allows you to schedule the change for a time in the future. Enter a start date and time in the scheduling field and select when the change should occur from the drop-down menu (one time is the default, but you may select recurring options for many of the actions). Scheduled jobs can be viewed and edited in the **System > Configuration Change Jobs** tab.
6. Using the neighbor lists, OV3600 is able to optimize channel selection for APs. Select the APs to optimize and OV3600 minimizes the channel interference while giving channel priority to the most heavily used APs. Table 71 describes these action and controls.

Table 71 ***Modify Multiple Devices Section*** *Fields and Default Values*

Action	Description
Set Group/Folder	Move the selected devices to a new group or folder. If the AP is in managed mode when it is moved to a new group, it will be reconfigured.
Move to AOS-W AP Group	Moves the selected APs to a new group or folder. If the AP is in managed mode when it is moved to a new group it will be reconfigured.
Desired Radio Status	Enables or disables the radios on the selected device. Does *not* apply Cisco IOS APs.
Update Cisco Thin AP Settings	Bulk configuration for per-thin AP settings, previously configured on the **Group LWAPP AP** tab, can be performed from **Modify Devices** on the **APs/Devices List** page. Make changes to LWAPP AP groups, including the option that was under Modify Devices.
Poll now	Polls selected devices for current user count and bandwidth data; overrides default poll settings for the group. Polling numerous devices may create a temporary performance load on your OV3600 server.
Audit selected devices	Fetches the current configuration from the device and compares it to the desired OV3600 configuration. The audit action updates the Configuration Status.
Run report on selected devices	Takes you to the **Reports > Definitions** page where you can define or run a custom report for selected devices. For more details and a procedure, see "Using Custom Reports" on page 223.
Update the credentials OV3600 uses to communicate with these devices	**Update** changes the credentials OV3600 uses to communicate with the device. It does *not* change the credentials on the AP.
Import settings from selected devices (and discard current pre-device desired settings)	Audit updates a number of the AP specific settings OV3600 initially read off of the AP including channel, power, antenna settings and SSL certifications. OV3600 recommends using this setting if APs have been updated outside of OV3600. Most settings on the **APs/Devices Manage** configuration page are set to the values currently read off of the devices.
Reboot selected devices	Reboots the selected devices. Use caution when rebooting devices because this can disrupt wireless users.
Reprovision selected AOS-W devices	Configures the switch to send provisioning parameters such as radio, antenna, and IP address settings to the selected APs. Please note that APs will be rebooted as part of reprovisioning.
Upgrade firmware for selected devices	Upgrades firmware for the selected devices. Refer to the firmware upgrade help under **APs/Devices > Manage** configuration page for detailed help on Firmware job options.
Cancel firmware upgrade for selected devices	Cancels any firmware upgrades that are scheduled or in progress for the selected APs.

Table 71 ***Modify Multiple Devices Section** Fields and Default Values*

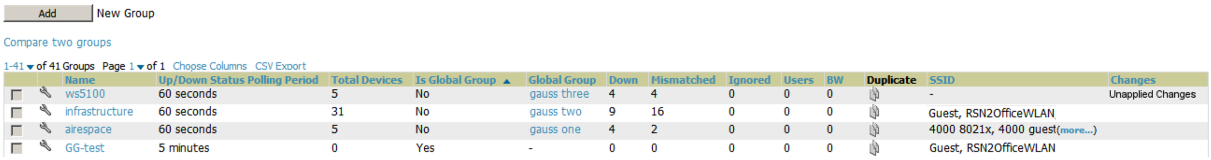
Action	Description
Ignore selected devices	Ignores selected APs, preventing OV3600 from generating any alerts or including the AP in an up/down count. The device's history is preserved but it will not be polled. Ignored devices can be seen and taken out of ignore status by navigating to the **New Devices** configuration page and selecting **View Ignored Devices** link at the bottom.
Delete selected devices from OV3600	Removes the selected APs from OV3600. The deletes will be performed in the background and may take a minute to be removed from the list.

Using Global Groups for Group Configuration

To apply group configurations using the OV3600 Global Groups feature, first go to the **Groups > List** configuration page. Select **Add** to add a new group, or select the name of the group to edit settings for an existing group. Select the **Duplicate** icon to create a new group with identical configuration to an existing group.

- To have Global Group status, a group must contain no devices; accordingly, access points can never be added to a Global Group. Global groups are visible to users of all roles, so they may not contain devices, which can be made visible only to certain roles. Figure 63 illustrates the **Groups > List** page.

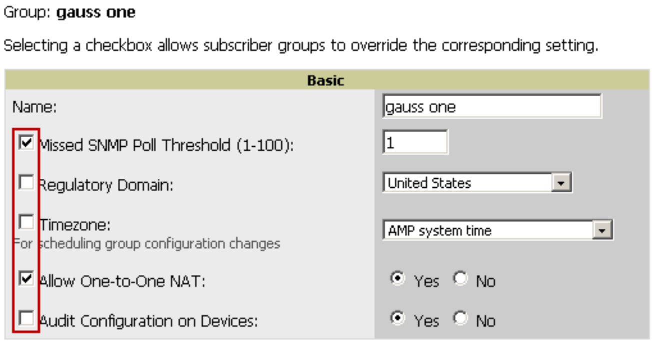
Figure 63 ***Groups** > **List** Page Illustration*



		Name	Up/Down Status Polling Period	Total Devices	Is Global Group ▲	Global Group	Down	Mismatched	Ignored	Users	BW	Duplicate	SSID	Changes
□		ws5100	60 seconds	5	No	gauss three	4	4	0	0	0		-	Unapplied Changes
□		infrastructure	60 seconds	31	No	gauss two	9	16	0	0	0		Guest, RSN2OfficeWLAN	
□		airespace	60 seconds	5	No	gauss one	4	2	0	0	0		4000 8021x, 4000 guest(more...)	
□		GG-test	5 minutes	0	Yes	-	0	0	0	0	0		Guest, RSN2OfficeWLAN	

- To set a group as a Global Group, go to the **Groups > Basic** configuration page for an existing or a newly created group. Select **Yes** for the **Is Global Group** field under the Global Group section.
- When the change is saved and applied, the group will have a checkbox next to fields. Figure 64 illustrates this configuration page.

Figure 64 ***Groups** > **Basic Page** for a Global Group (partial view)*



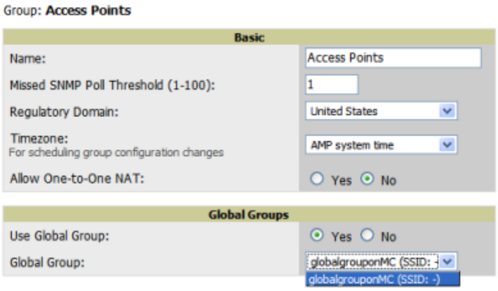
Group: **gauss one**

Selecting a checkbox allows subscriber groups to override the corresponding setting.

Basic	
Name:	gauss one
☑ Missed SNMP Poll Threshold (1-100):	1
□ Regulatory Domain:	United States
□ Timezone: For scheduling group configuration changes	AMP system time
☑ Allow One-to-One NAT:	● Yes ○ No
□ Audit Configuration on Devices:	● Yes ○ No

- When a Global Group configuration is pushed to Subscriber Groups, all settings are static except for settings with the checkbox selected; for fields with checkboxes selected, the value or setting can be changed on the corresponding tab for each managed group. In the case of the **Groups > SSIDs** configuration page, override options are available only on the **Add** configuration page (go to the **Groups > SSIDs** configuration page and select **Add**). Global templates are also configurable as part of Global Groups; see "Creating and Using Templates" on page 147 for more information.
- Once Global Groups have been configured, groups may be created or configured to subscribe to a particular Global Group. Go to the **Groups > Basic** configuration page of a group and locate the **Use Global Groups** section. Select the **Yes** radio button and select the name of the Global Group from the drop-down menu. Then select **Save and Apply** to make the changes permanent. Figure 65 illustrates this page.

Figure 65 ***Groups*** ***> Basic > Managed*** *Page Illustration*



Group: **Access Points**

Basic	
Name:	Access Points
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	United States
Timezone: For scheduling group configuration changes	AMP system time
Allow One-to-One NAT:	○ Yes ● No
Global Groups	
Use Global Group:	● Yes ○ No
Global Group:	globalgrouponMC (SSID: -) globalgrouponMC (SSID: -)

- Once the configuration is pushed, the unchecked fields from the Global Group appears on the Subscriber Group as static values and settings. Only fields that had the override checkbox selected in the Global Group appear as fields that can be set at the level of the Subscriber Group. Any changes to a static field must be made on the Global Group.
- If a Global Group has Subscriber Groups, it cannot be changed to a non-Global Group. A Global Group without Subscriber Groups can be changed to a regular Group by updating the setting on the **Groups > Basic** configuration interface. The Global Groups feature can also be used with the Master Console. For more information about this feature, refer to "Supporting OV3600 Servers with the Master Console" on page 210.

Chapter 5

Discovering, Adding, and Managing Devices

This chapter describes how to add, configure and monitor devices, both wired and wireless, and contains the following sections, corresponding to features of the **Device Setup** and **APs/Devices** tabs:

Device Discovery Overview

Once you have deployed OV3600 on the network, the next step is to discover all existing devices connected to your network.

OV3600 allows device discovery in the following ways, all of which are described in this chapter:

- **SNMP/HTTP discovery scanning**—This is the primary method to discover devices on your network, configured in the **Device Setup > Discovery** page. See "SNMP/HTTP Scanning" on page 107.
- **Cisco Discovery Protocol (CDP)**—OV3600 enhances support for CDP by discovering a Cisco device's CDP neighbors. See "Enabling Cisco Discovery Protocol (CDP)" on page 111.
- **Manual device entry**—This admin-supported method of discovery applies when you know of devices that are already on your network. See the following sections for information and procedures:
  - "Manually Adding Individual Devices" on page 112
  - "Adding Multiple Devices from a CSV File" on page 115
  - "Adding Universal Devices" on page 116
- **Controller-driven device discovery**—Thin APs will automatically be discovered in the network and added to the **New Devices** list when you add their controller to OV3600. To add the thin APs, refer to "Authorizing Devices to OV3600 from APs/Devices > New Page" on page 111.

Discovering and Adding Devices

This section describes the following topics:

- SNMP/HTTP Scanning
- Enabling Cisco Discovery Protocol (CDP)
- Authorizing Devices to OV3600 from APs/Devices > New Page
- Manually Adding Individual Devices

SNMP/HTTP Scanning

SNMP/HTTP discovery scanning is the primary method for discovering devices on your network, including rogue devices. Enable this scanning method from the **Device Setup > Discover** page.

SNMP/HTTP scanning information is provided in these sections:

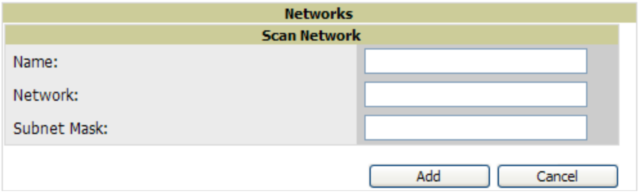
- Adding Networks for SNMP/HTTP Scanning—explains how to enable networks that have been defined for scanning.
- Adding Credentials for SNMP/HTTP Scanning—explains how to define network credentials for scanning. Credentials must be defined before using them in scan sets.
- Defining a SNMP/HTTP Scan Set—explains how to create a scan set by combining networks and credentials when scanning for devices.
- Running a Scan Set—provides a procedure for running a scan set.

Adding Networks for SNMP/HTTP Scanning

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

1. Go to the **Device Setup > Discover** page, and locate the **Networks** section.
2. In the **Networks** section, select **Add New Scan Network**. The **Scan Network** page appears, as shown in Figure 66. Alternatively, you can edit an existing scan network by selecting the corresponding pencil icon. The **New/Edit Networks** page also appears in this instance.

Figure 66 ***Device Setup > Discover > New Network*** *Section Illustration*



Networks

Scan Network

Name:	
Network:	
Subnet Mask:	

3. In the **Name** field, provide a name for the network to be scanned (for example, **Accounting Network**).
4. In the **Network** field, define the IP network range, or the first IP address on the network, to be scanned. One example would be 10.52.0.0.
5. Enter the **Subnet Mask** for the network to be scanned (for example, 255.255.252.0). The largest subnet OV3600 supports is 255.255.0.0.
6. Select **Add**.
7. Repeat these steps to add as many networks for which to enable device scanning. All network segments configured in this way appear in the **Network** section of the **Device Setup > Discover** page.
8. Complete the configuration of scan credentials, then combine scan networks and scan credentials to create scan sets. The next two procedures in this section describe these tasks.

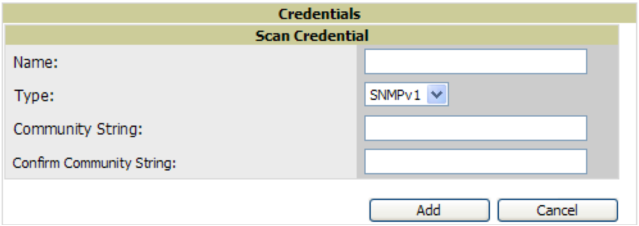
Adding Credentials for SNMP/HTTP Scanning

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

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

1. Locate the **Credentials** section on the **Device Setup > Discover** page. This page displays scan sets, networks, and credentials that have been configured so far, and allows you to define new elements for device scanning.
2. To create a new scan credential, select **Add New Scan Credential**. Figure 67 illustrates this page.

Figure 67 ***Device Setup > Discover > Add/Edit New Scan Credential*** *Section Illustration*



Credentials

Scan Credential

Name:

Type: SNMPv1

Community String:

Confirm Community String:

3. Enter a name for the credential in the **Name** field (for example, **Default**). This field supports alphanumeric characters, both upper and lower case, blank spaces, hyphens, and underscore characters.
4. Choose the type of scan to be completed (**SNMPv1, SNMPv2,** or **HTTP**). In most cases, perform scans using SNMP for device discovery, but consider the following factors in your decision:
   - SNMPv1 and SNMP v2 differ between in their supported traps, supported MIBs, and network query elements used in device scanning.
   - HTTP discovers devices using the HyperText Transfer Protocol in communications between servers and additional network components. HTTP is not as robust in processing network events as is SNMP, but HTTP may be sufficient, simpler, or preferable in certain scenarios.
5. Define and confirm the **Community String** to be used during scanning. In this section, the community string used can be either **read-only** or **read/write**, as OV3600 only uses it for discovering APs. To bring APs under management, OV3600 uses the credentials supplied in the **Device Setup > Communication SNMP** section. Once the device is authorized, it will use the non-scanning credentials.

NOTE

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

6. Select **Add**. The **Device Setup > Discover** page displays the new scan credential or credentials just created or edited.
7. Repeat these steps to add as many credentials as you require.
8. Once scan networks and scan credentials are defined, combine them by creating scan sets using the next procedure: "Defining a SNMP/HTTP Scan Set" on page 109.

Defining a SNMP/HTTP Scan Set

Once you have defined at least one network and one scan credential, you can create a scan set that combines the two for device discovery. Perform these steps to create a scan set.

1. Locate the **Scan Set** area at the top of the **Device Setup > Discover** page.
2. Select **Add New Scan Set** to see all scan components configured so far. If you wish to create a new network, or new scanning credentials, you can select **Add** in either of these fields to create new components prior to creating a scan set.
3. Select the **Network**(s) to be scanned and the **Credential(s)** to be used. OV3600 defines a unique scan for each **Network-Credential** combination.
4. Select **Add** to create the selected scans, which then appear in a list at the top of the **Device Setup > Discover** page.
5. To edit an existing scan, select the pencil icon next to the scan on the **Device Setup > Discover** page.

6. When ready, proceed to the next task, "Running a Scan Set" on page 110.

NOTE

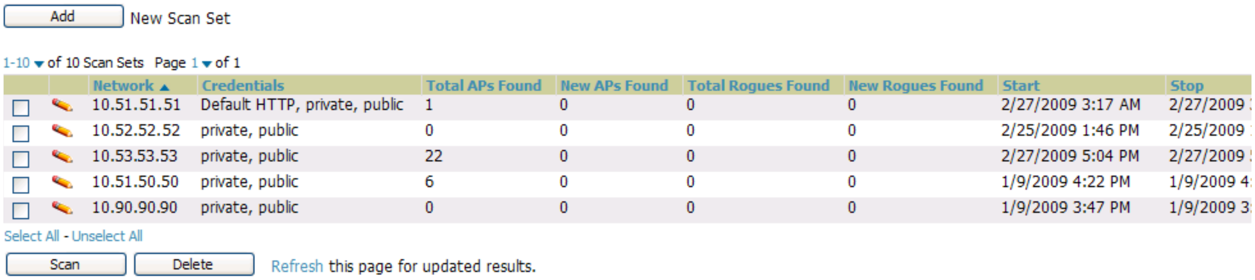
Scheduling an HTTP scan to run daily on your network can help you to discover rogues. Some consumer APs, like most D-Link, Linksys, and NetGear models, do not support SNMP and are found only on the wired side with an HTTP scan. These devices are discovered only if they have a valid IP address. Proper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

Running a Scan Set

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

1. Browse to the **Device Setup > Discover** page and locate the list of all scan sets that have been defined so far. Figure 68 illustrates this page.

Figure 68 ***Device Setup > Discover*** *Executing a Scan Illustration*



Add New Scan Set

1-10 ▾ of 10 Scan Sets Page 1 ▾ of 1

		Network ▲	Credentials	Total APs Found	New APs Found	Total Rogues Found	New Rogues Found	Start	Stop
□	✎	10.51.51.51	Default HTTP, private, public	1	0	0	0	2/27/2009 3:17 AM	2/27/2009
□	✎	10.52.52.52	private, public	0	0	0	0	2/25/2009 1:46 PM	2/25/2009
□	✎	10.53.53.53	private, public	22	0	0	0	2/27/2009 5:04 PM	2/27/2009
□	✎	10.51.50.50	private, public	6	0	0	0	1/9/2009 4:22 PM	1/9/2009 4
□	✎	10.90.90.90	private, public	0	0	0	0	1/9/2009 3:47 PM	1/9/2009 3

Select All - Unselect All

Scan Delete Refresh this page for updated results.

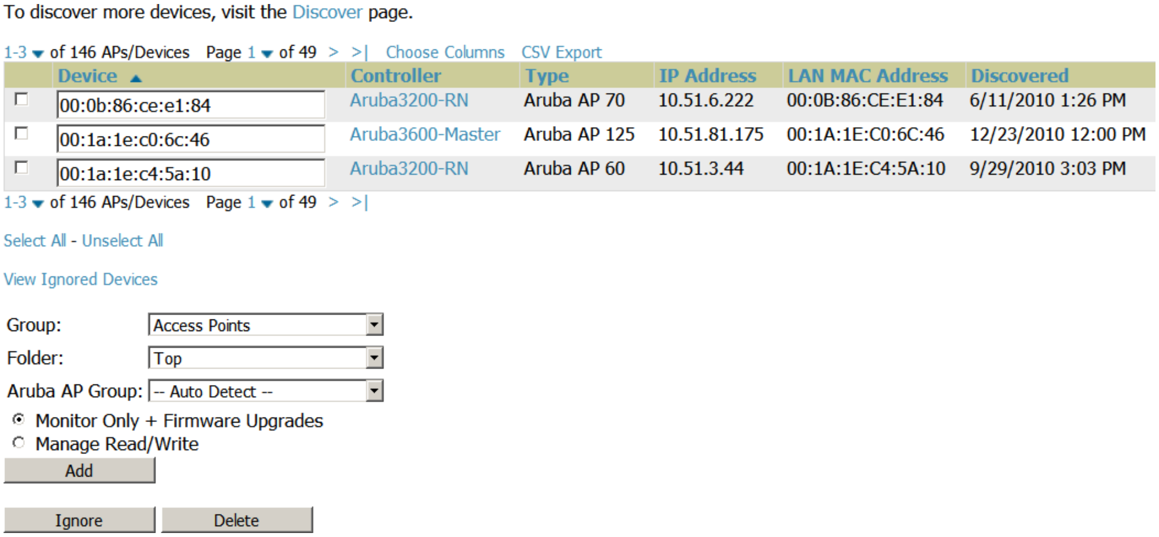
2. Check the box next to the scan(s) that you would like to execute.
3. Select **Scan** to execute the selected scans, and the scan immediately begins. The last column indicates the scan is **In Progress**.
4. For future scans, select **Show Scheduling Options** and enter the desired date and time to schedule a future scan.
5. After several minutes have passed, refresh the browser page and view the results of the scan. When the **Start** and **Stop** columns display date and time information, the scan is available to display the results.
6. Select the pencil icon for the scan to display the results. Table 72 describes the scan results and related information.

Table 72 ***Device Setup > Discover > Discovery Execution*** *Fields*

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

7. Go to the **APs/Devices > New** page to see a full list of the newly discovered devices that the scan detected. Figure 69 illustrates this page.

Figure 69 ***APs/Devices > New** Page Illustration*



To discover more devices, visit the Discover page.

1-3 ▾ of 146 APs/Devices Page 1 ▾ of 49 > >| Choose Columns CSV Export

	Device ▲	Controller	Type	IP Address	LAN MAC Address	Discovered
□	00:0b:86:ce:e1:84	Aruba3200-RN	Aruba AP 70	10.51.6.222	00:0B:86:CE:E1:84	6/11/2010 1:26 PM
□	00:1a:1e:c0:6c:46	Aruba3600-Master	Aruba AP 125	10.51.81.175	00:1A:1E:C0:6C:46	12/23/2010 12:00 PM
□	00:1a:1e:c4:5a:10	Aruba3200-RN	Aruba AP 60	10.51.3.44	00:1A:1E:C4:5A:10	9/29/2010 3:03 PM

1-3 ▾ of 146 APs/Devices Page 1 ▾ of 49 > >|

Select All - Unselect All

View Ignored Devices

Group: Access Points

Folder: Top

Aruba AP Group: -- Auto Detect --

● Monitor Only + Firmware Upgrades

○ Manage Read/Write

What Next?

- To authorize one or more devices to a group, see "Authorizing Devices to OV3600 from APs/Devices > New Page" on page 111.
- To delete a device altogether from OV3600, select the corresponding check box for each device, and select **Delete**.
- Alcatel-Lucent thin APs can have Alcatel-Lucent AP Group specified and Cisco thin APs can have LWAPP AP Group specified when they are authorized.

Enabling Cisco Discovery Protocol (CDP)

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

Authorizing Devices to OV3600 from APs/Devices > New Page

Once you have discovered devices on your network, add these devices to a group and specify whether the device is to be placed in **Manage Read/Write** or **Monitor Only** mode. To configure a new group, refer to "Configuring and Using Device Groups in OV3600" on page 69.

In **Manage Read/Write** mode, OV3600 compares the device's current configuration settings with the Group configuration settings and automatically updates the device's configuration to match the Group policy.

In **Monitor Only** mode, OV3600 updates the firmware, compares the current configuration with the policy, and displays any discrepancies on the **APs/Devices > Audit** page, but does not change the configuration of the device.

CAUTION

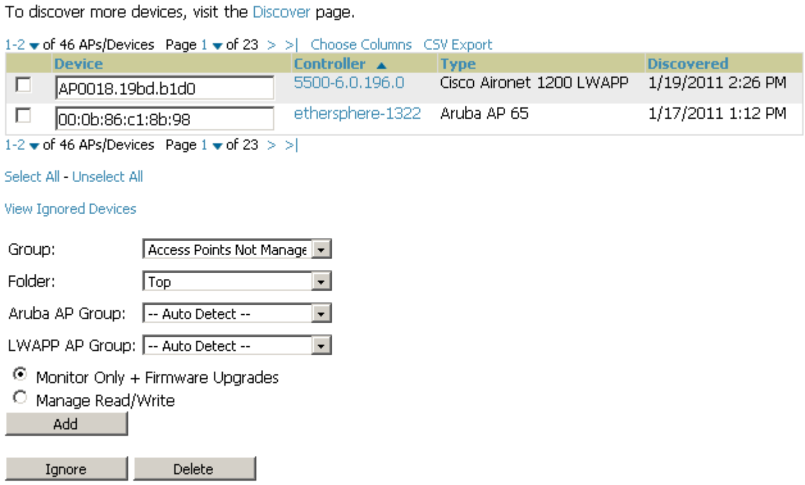
Put devices in Monitor Only mode when they are added to a newly established device group. This avoids overwriting any important existing configuration settings.

Once you have added several devices to the Group, and verified that no unexpected or undesired configuration changes will be made to the devices, you can begin to put the devices in **Manage Read/Write** mode using the **APs/Devices > Manage** or the **Modify these devices** link on any list page.

Perform the following steps to add a newly discovered device to a group:

1. Browse to the **APs/Devices > New** page. The **APs/Devices > New** page displays all newly discovered devices, the related controller (when known/applicable) and the device vendor, model, LAN MAC Address, IP Address, and the date/time of discovery. Figure 70 illustrates this page.

Figure 70 ***APs/Devices > New*** *Page Illustration*



To discover more devices, visit the Discover page.

1-2 ▾ of 46 APs/Devices Page 1 ▾ of 23 > >| Choose Columns CSV Export

	Device	Controller ▲	Type	Discovered
□	AP0018.19bd.b1d0	5500-6.0.196.0	Cisco Aironet 1200 LWAPP	1/19/2011 2:26 PM
□	00:0b:86:c1:8b:98	ethersphere-1322	Aruba AP 65	1/17/2011 1:12 PM

1-2 ▾ of 46 APs/Devices Page 1 ▾ of 23 > >|

Select All - Unselect All

View Ignored Devices

Group:	Access Points Not Manage ▾
Folder:	Top ▾
Aruba AP Group:	-- Auto Detect -- ▾
LWAPP AP Group:	-- Auto Detect -- ▾

● Monitor Only + Firmware Upgrades
○ Manage Read/Write

2. Select the group and folder to which the device will be added from the drop-down menu (the default group appears at the top of the **Group** listing). Devices cannot be added to a Global Group; groups designated as Global Groups cannot contain access points.

3. Select either the **Monitor Only** or the **Manage Read/Write** radio button and select **Add**.

   At this point, you can go to the **APs/Devices > List** page and select the folder(s) to which you have assigned one or more devices to verify that your device has been properly assigned. If you wish to assign a device to the **Ignored** page, or delete it entirely from OV3600, go to step 4.

NOTE

If you select **Manage Select Devices**, OV3600 automatically overwrites existing device settings with the specified Group settings. Alcatel-Lucent strongly recommends placing newly discovered devices in Monitor mode until you can confirm that all group configuration settings are appropriate for that device.

4. If you do not wish to manage or monitor a discovered device, you may select the device(s) from the list and select either **Ignore Selected Devices** or **Delete Selected Devices**. If you choose to **Ignore** the devices, they will not be displayed in the **APs/Devices > New** list, even if they are discovered in subsequent scans. You can view a list of all Ignored devices on the **APs/Devices > Ignored** page. If you choose to **Delete** the device, it will be listed on the **APs/Devices > New** list if discovered by OV3600 in a subsequent scan. Refer to "Assigning Devices to the Ignored Page" on page 116.

Manually Adding Individual Devices

Some deployment situations 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.

This section describes the following procedures:

- Adding Devices with the Device Setup > Add Page
- Adding Multiple Devices from a CSV File
- Adding Universal Devices

Adding Devices with the Device Setup > Add Page

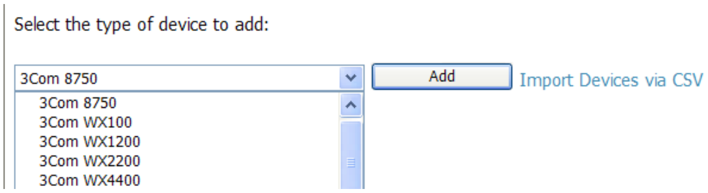
Manually adding devices from the **Device Setup > Add** page to OV3600 is an option for adding all device types. You only need to select device vendor information from a drop down menu for Cisco and Alcatel-

Lucent devices, and OV3600 automatically finds and adds specific make and model information into its database.

Perform these steps to manually add devices to OV3600:

1. The first step to add a device manually is to select the vendor and model. Browse to the **Device Setup > Add** page and select the vendor and model of the device to add. Figure 71 illustrates this page.

Figure 71 ***Device Setup > Add*** *Page Illustration*



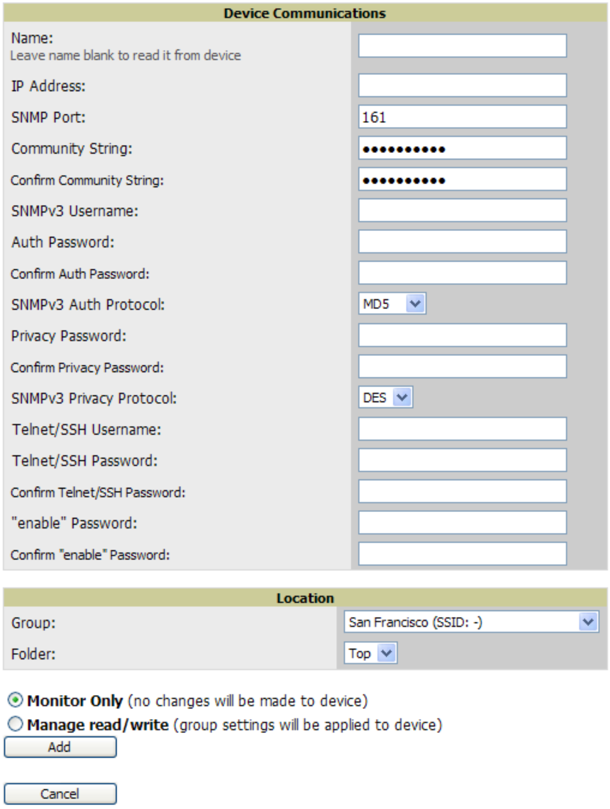
Select the type of device to add:

3Com 8750 [Add] Import Devices via CSV

3Com 8750
3Com WX100
3Com WX1200
3Com WX2200
3Com WX4400

2. Select **Add**, and the **Device Communications** and **Location** sections appear, illustrated in Figure 72.

Figure 72 ***Device Setup > Add > Device Communications*** *and* ***Location*** *Sections*



Device Communications	
Name: Leave name blank to read it from device	
IP Address:	
SNMP Port:	161
Community String:	••••••••••
Confirm Community String:	••••••••••
SNMPv3 Username:	
Auth Password:	
Confirm Auth Password:	
SNMPv3 Auth Protocol:	MD5
Privacy Password:	
Confirm Privacy Password:	
SNMPv3 Privacy Protocol:	DES
Telnet/SSH Username:	
Telnet/SSH Password:	
Confirm Telnet/SSH Password:	
"enable" Password:	
Confirm "enable" Password:	

Location	
Group:	San Francisco (SSID: -)
Folder:	Top

● **Monitor Only** (no changes will be made to device)
○ **Manage read/write** (group settings will be applied to device)

3. Complete these **Device Communications** and **Location** settings for the new device. Table 73 further describes the contents of this page. Settings may differ from device to device. In several cases, the default values from any given device derive from the **Device Setup > Communication** page.

Table 73 ***Device Communications and Location*** *Fields and Default Values*

Setting	Default	Description
Name	None	User-configurable name for the AP (maximum of 20 characters).
IP Address	None	IP address of the device. This field is required.
SNMP Port	161	Port OV3600 uses to communicate with the AP using SNMP.

Table 73 ***Device Communications and Location*** *Fields and Default Values*

Setting	Default	Description
Community String (Confirm)	Taken from **Device Setup > Communication**	Community string used to communicate with the AP. **NOTE:** The **Community String** should have RW (Read-Write) capability. New, out-of-the-box Cisco devices typically have SNMP disabled and a blank username and password combination for HTTP and Telnet. Cisco supports multiple community strings per AP.
SNMPv3 Username	Taken from **Device Setup > Communication**	If you are going to manage configuration for the device, this field provides a read-write user account (SNMP, HTTP, and Telnet) within the Cisco Security System for access to existing APs. OV3600 initially uses this username and password combination to control the Cisco AP. OV3600 creates a user-specified account with which to manage the AP if the **User Creation Options** are set to **Create** and user Specified as User.
Auth Password (Confirm)		
Privacy Password (Confirm)	Taken from **Device Setup > Communication**	SNMPv3 privacy password.
SNMPv3 Auth Protocol	Taken from **Device Setup > Communication**	Drop-down menu that allows you to enable the SNMPv3 authentication protocol to the device being added.
SNMPv3 Privacy Protocol	Taken from **Device Setup > Communication**	Drop-down menu that allows you to enable SNMPv3 privacy protocol to the device being added.
Telnet/SSH Username & Password (Confirm)	Taken from **Device Setup > Communication**	Telnet username and password for existing Cisco IOS APs. OV3600 uses the Telnet username/password combination to manage the AP and to enable SNMP if desired. **NOTE:** New, out-of-the-box Cisco IOS-based APs typically have SNMP disabled with a default telnet username of ***Cisco*** and default password of ***Cisco***. This value is required for management of any existing Cisco IOS-based APs.
"enable" Password (Confirm)	Taken from **Device Setup > Communication**	Password that allows OV3600 to enter **enable** mode on the device.
HTTP Username & Password	Taken from **Device Setup > Communication**	HTTP password used to manage the device initially, and to enable SNMP if desired.
Auth Password	Taken from **Device Setup > Communication**	SNMPv3 authentication password. **NOTE:** SNMPv3 supports three security levels: (1) no authentication and no encryption, (2) authentication and no encryption, and (3) authentication and encryption. OV3600 currently only supports authentication and encryption.
Privacy Password	Taken from **Device Setup > Communication**	SNMPv3 privacy password. **NOTE:** SNMPv3 supports three security levels: (1) no authentication and no encryption, (2) authentication and no encryption, and (3) authentication and encryption. OV3600 currently only supports authentication and encryption.

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** radio button. The choice depends on whether or not you wish to overwrite the **Group** settings for the device being added. For more information and a detailed procedure, see "Authorizing Devices to OV3600 from APs/ Devices > New Page" on page 111.

NOTE

If you select **Manage read/write**, OV3600 overwrites existing device settings with the **Group** settings. Alcatel-Lucent recommends placing newly discovered devices in **Monitor read/only** mode to enable auditing of actual settings instead of Group Policy settings.

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

Adding Multiple Devices from a CSV File

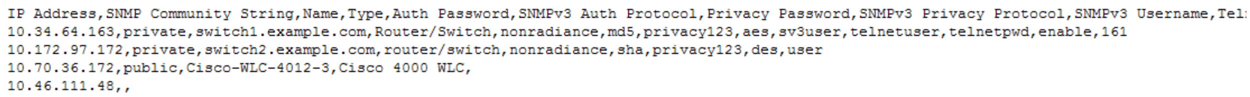
You can add devices in bulk from a CSV file to OV3600. Here you also have the option of specifying vendor name only, and OV3600 will automatically determine the correct type while bringing up the device. If your CSV file includes make and model information, OV3600 will add the information provided in the CSV file as it did before. 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 Username
- Telnet Username
- Telnet Password
- Enable Password
- SNMP Port

You can download a CSV file and customize it as you like. A sample CSV file is illustrated in Figure 73.

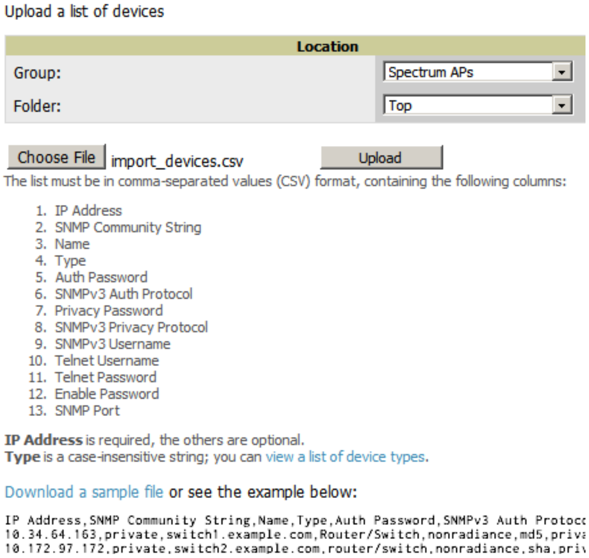
Figure 73 *Sample CSV File*



```
IP Address,SNMP Community String,Name,Type,Auth Password,SNMPv3 Auth Protocol,Privacy Password,SNMPv3 Privacy Protocol,SNMPv3 Username,Tel
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,,
```

1. To import a CSV file, go to the **Device Setup > Add** page.
2. Select the **Import Devices via CSV** link. The **Upload a list of devices** page displays as illustrated in Figure 74.

Figure 74 ***Device Setup*** **>** ***Add*** **>** ***Import Devices via CSV*** *Page Illustration*



Upload a list of devices

Location	
Group:	Spectrum APs
Folder:	Top

import_devices.csv

The list must be in comma-separated values (CSV) format, containing the following columns:

1. IP Address
2. SNMP Community String
3. Name
4. Type
5. Auth Password
6. SNMPv3 Auth Protocol
7. Privacy Password
8. SNMPv3 Privacy Protocol
9. SNMPv3 Username
10. Telnet Username
11. Telnet Password
12. Enable Password
13. 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 Protoc
10.34.64.163,private,switch1.example.com,Router/Switch,nonradiance,md5,priva
10.172.97.172,private,switch2.example.com,router/switch,nonradiance,sha,priv
```

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

5. Select **Upload** to add the list of devices into OV3600.

Adding Universal Devices

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

Perform the same steps to add universal devices to OV3600 that were detailed in "Adding Devices with the Device Setup > Add Page" on page 112.

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

By selecting the pencil icon next to an interface, you can assign it to be non-monitored or monitored as Interface 1 or 2. OV3600 collects this information and displays it on the **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.

Assigning Devices to the Ignored Page

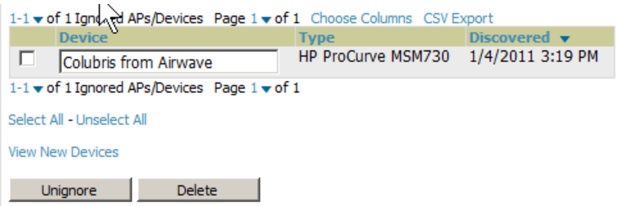
There are two ways a device can be assigned to the **Ignored** page: from the **APs/Devices > New** page, or from the **APs/Devices > Manage** page. The advantage of having the device be designated in this way, as in the case of a device that is temporarily down for a known reason, is that when you take it off the ignored list, it returns immediately to the location in OV3600 where it had resided before it was marked **Ignored**.

- Ignored devices are *not* displayed in **APs/Devices > New** if discovered in subsequent scans.
- Deleted devices *will* be listed on the **APs/Devices > New** if discovered in subsequent scans.

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

1. To view all devices that are ignored, go to the **APs/Devices > Ignored** page, illustrated in Figure 75.

Figure 75 ***APs/Devices > Ignored*** *Page Illustration*



1-1 ▾ of 1 Ignored APs/Devices Page 1 ▾ of 1

	Device	Type	Discovered ▾
□	Colubris from Airwave	HP ProCurve MSM730	1/4/2011 3:19 PM

1-1 ▾ of 1 Ignored APs/Devices Page 1 ▾ of 1

This page provides the following information for any ignored device:

- device name or MAC address, when known
- controller associated with that device
- device type
- device IP address
- LAN MAC address for the LAN on which the device is located
- date and time of device discovery

2. To change the device parameters for a given device, select its checkbox and adjust group, folder, monitor, and manage settings as desired.

3. Select **Add** to add the device to OV3600 so that it appears on the **APs/Devices > New** list. The **Unignore** button will either return the device to its regular folder or group, or send it to the **APs/ Devices > New** page.

Monitoring Devices

This section discusses various device monitoring options and includes the following sections:

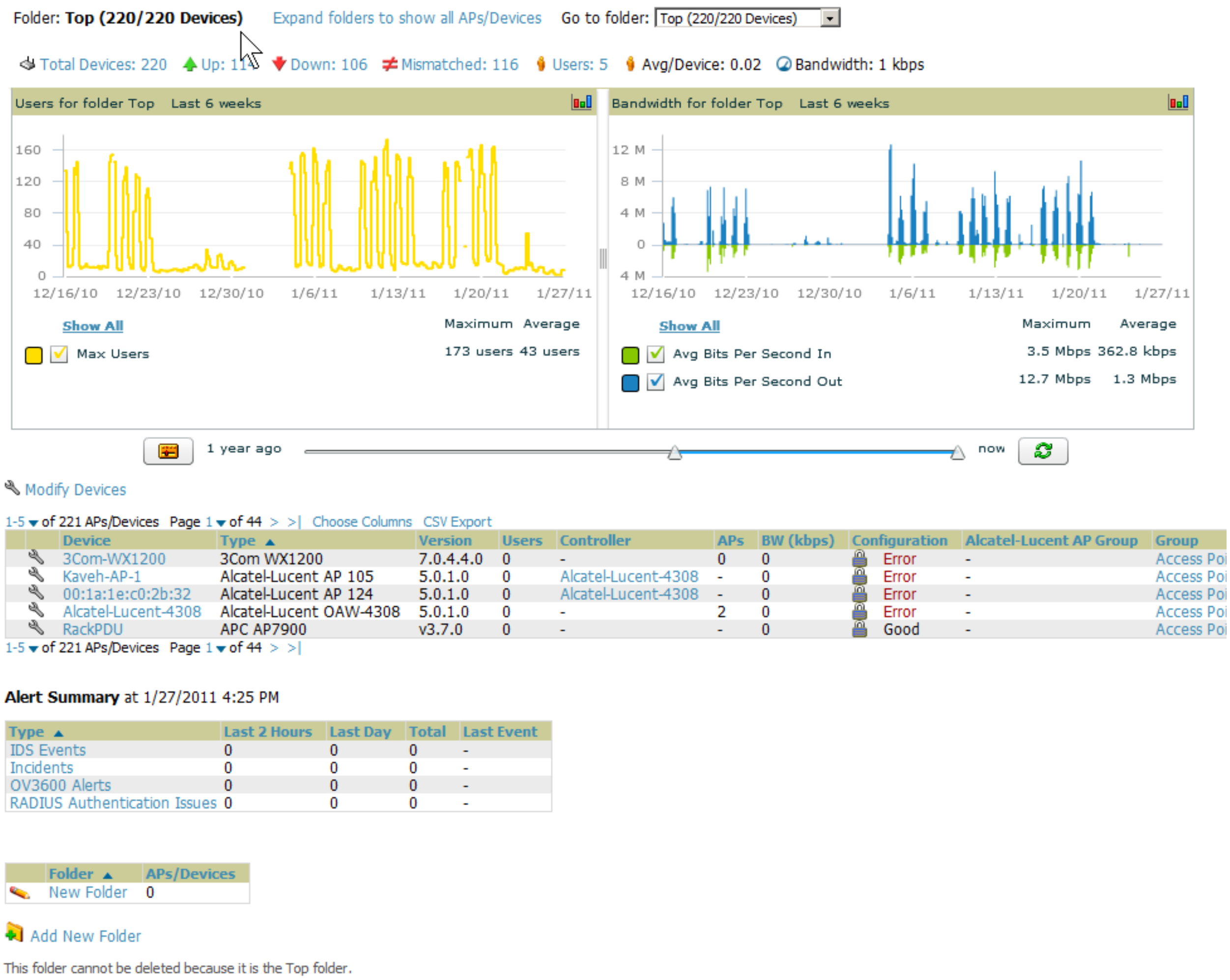
- Viewing Device Monitoring Statistics
- Auditing Device Configuration

Viewing Device Monitoring Statistics

You can view many useful device monitoring statistics in the **APs/Devices > List** page.

1. Go to the **APs/Devices > List** page, which lists all devices that are managed or monitored by OV3600. Using the **Go to folder** field, you can determine whether to view all devices or only the devices from a specified folder. A lock icon in the **Configuration** column indicates that the device is in **Monitor only** mode. Figure 76 illustrates this page.

Figure 76 ***APs/Devices > List*** *(partial view)*



Folder: **Top (220/220 Devices)** Expand folders to show all APs/Devices Go to folder: Top (220/220 Devices)

Total Devices: 220 Up: 114 Down: 106 Mismatched: 116 Users: 5 Avg/Device: 0.02 Bandwidth: 1 kbps

		Maximum	Average
🟨	☑ Max Users	173 users	43 users

		Maximum	Average
🟩	☑ Avg Bits Per Second In	3.5 Mbps	362.8 kbps
🟦	☑ Avg Bits Per Second Out	12.7 Mbps	1.3 Mbps

Modify Devices

1-5 of 221 APs/Devices Page 1 of 44 > >| Choose Columns CSV Export

	Device	Type ▲	Version	Users	Controller	APs	BW (kbps)	Configuration	Alcatel-Lucent AP Group	Group
	3Com-WX1200	3Com WX1200	7.0.4.4.0	0	-	0	0	Error	-	Access Poi
	Kaveh-AP-1	Alcatel-Lucent AP 105	5.0.1.0	0	Alcatel-Lucent-4308	-	0	Error	-	Access Poi
	00:1a:1e:c0:2b:32	Alcatel-Lucent AP 124	5.0.1.0	0	Alcatel-Lucent-4308	-	0	Error	-	Access Poi
	Alcatel-Lucent-4308	Alcatel-Lucent OAW-4308	5.0.1.0	0	-	2	0	Error	-	Access Poi
	RackPDU	APC AP7900	v3.7.0	0	-	-	0	Good	-	Access Poi

1-5 of 221 APs/Devices Page 1 of 44 > >|

Alert Summary at 1/27/2011 4:25 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
IDS Events	0	0	0	-
Incidents	0	0	0	-
OV3600 Alerts	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

	Folder ▲	APs/Devices
	New Folder	0

Add New Folder

This folder cannot be deleted because it is the Top folder.

2. Verify that the devices you added are now appearing in the devices list with a Status of **Up**.

NOTE

Newly added devices will be status **Down** until they have been polled the first time. They will be configuration **Unknown** until they have finished verification. The **Up** status is not contingent on verification.

The same section also appears on the **Groups > Monitor** page, and is hyperlinked from a controller's monitoring interface.

3. Go to the **Alert Summary** section of **APs/Devices > List**, which cites the number of events that have occurred in the last two hours, the last 24 hours, and total. There are four categories of alerts as listed below:
   - OV3600 Alerts
   - IDS Events
   - Incidents
   - RADIUS Authentication Issues

NOTE

The **Alerts Summary** table is also a feature of the **Home > Overview** page, and has the same links in that location.

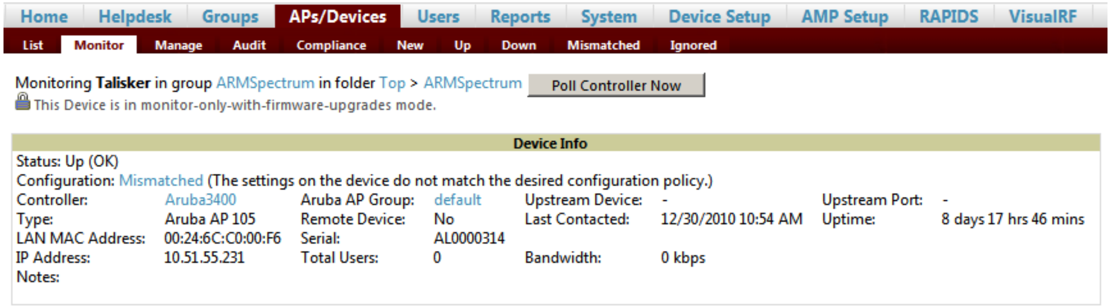
For more information on the **Alert Summary** table, refer to “Viewing Alerts” on page 185.

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

You can quickly go to any device’s monitoring page once 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 77.

Figure 77 ***Monitoring*** *Page Top Level Data Common to All Device Types*



Monitoring **Talisker** in group ARMSpectrum in folder Top > ARMSpectrum

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

Device Info

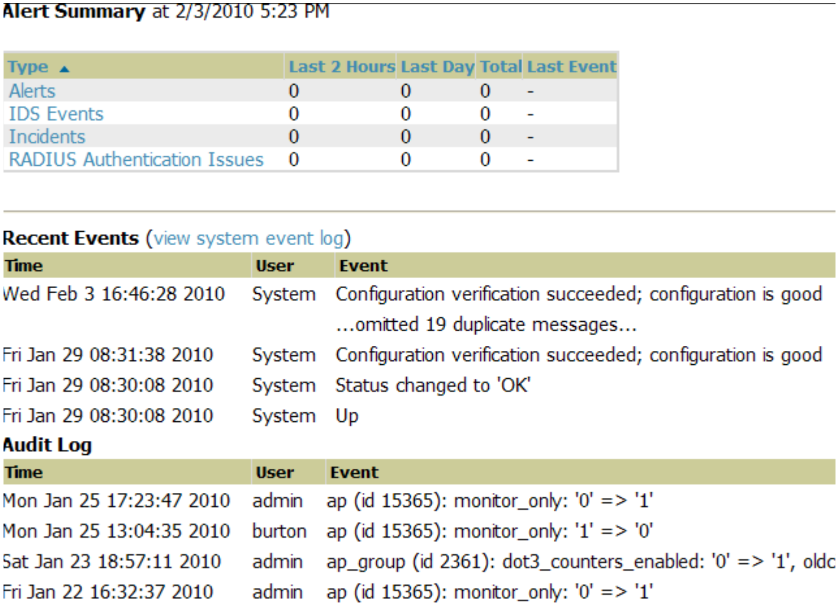
Status: Up (OK)

Configuration: Mismatched (The settings on the device do not match the desired configuration policy.)

Controller:	Aruba3400	Aruba AP Group:	default	Upstream Device:	-	Upstream Port:	-
Type:	Aruba AP 105	Remote Device:	No	Last Contacted:	12/30/2010 10:54 AM	Uptime:	8 days 17 hrs 46 mins
LAN MAC Address:	00:24:6C:C0:00:F6	Serial:	AL0000314				
IP Address:	10.51.55.231	Total Users:	0	Bandwidth:	0 kbps		
Notes:							

The alert summary, events and audit log sections are also the same regardless of device type and these sections appear at the bottom of these pages, a portion of which is shown in Figure 78.

Figure 78 ***Monitoring*** *Page Bottom Level Data Common to All Device Types*



Alert Summary at 2/3/2010 5:23 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
Alerts	0	0	0	-
IDS Events	0	0	0	-
Incidents	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Recent Events (view system event log)

Time	User	Event
Wed Feb 3 16:46:28 2010	System	Configuration verification succeeded; configuration is good
		...omitted 19 duplicate messages...
Fri Jan 29 08:31:38 2010	System	Configuration verification succeeded; configuration is good
Fri Jan 29 08:30:08 2010	System	Status changed to 'OK'
Fri Jan 29 08:30:08 2010	System	Up

Audit Log

Time	User	Event
Mon Jan 25 17:23:47 2010	admin	ap (id 15365): monitor_only: '0' => '1'
Mon Jan 25 13:04:35 2010	burton	ap (id 15365): monitor_only: '1' => '0'
Sat Jan 23 18:57:11 2010	admin	ap_group (id 2361): dot3_counters_enabled: '0' => '1', oldc
Fri Jan 22 16:32:37 2010	admin	ap (id 15365): monitor_only: '0' => '1'

Monitoring pages vary slightly according to whether they are wired routers/switches or controllers/WLAN switches, or thin or fat APs. These differences are discussed in the sections that follow.

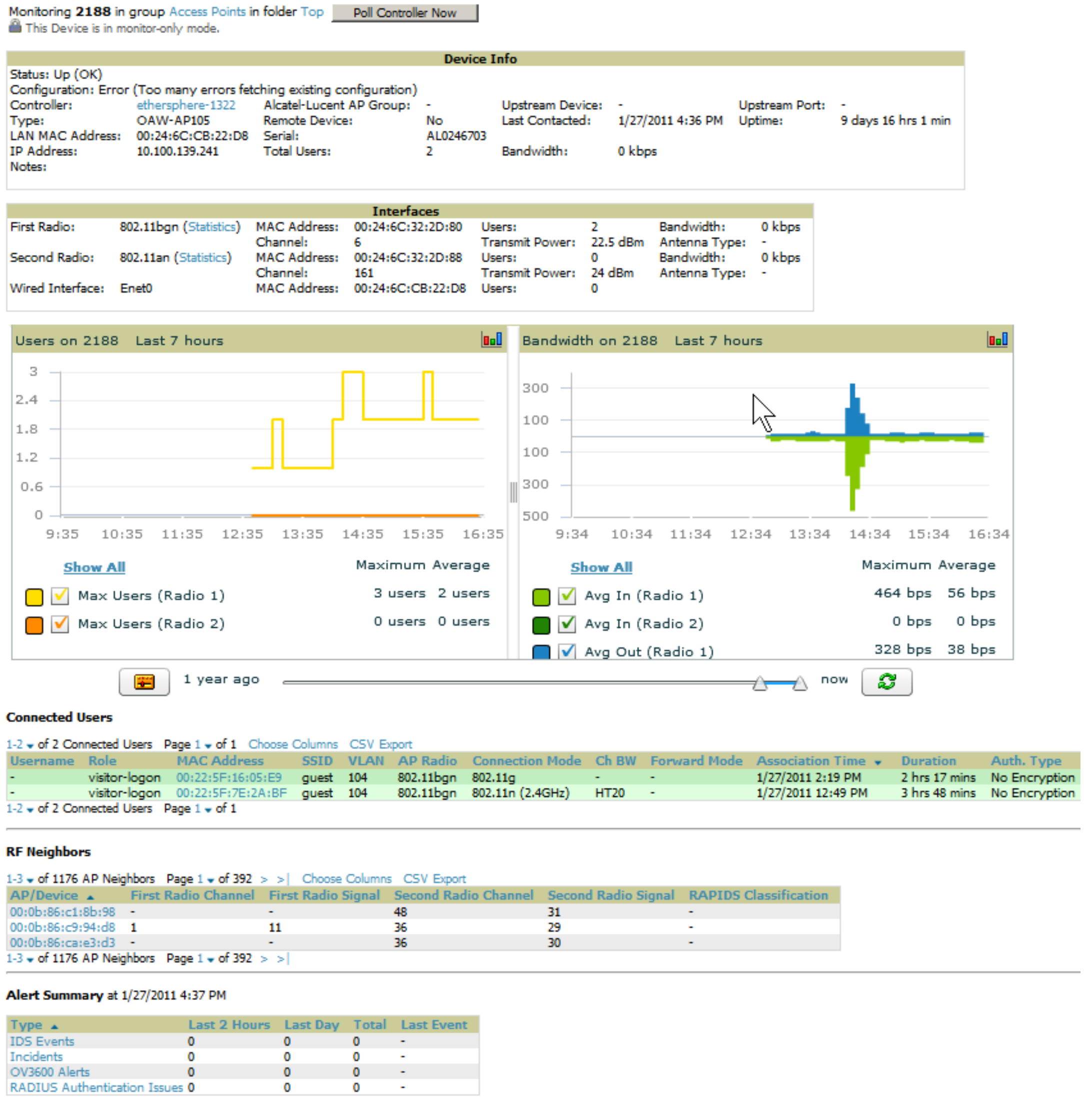
Monitoring Data Specific to Wireless Devices

The **APs/Devices > Monitor** page for controllers and APs include a graph for users and bandwidth. The controller graph lists the APs connected to it, while the APs include a list of users it has connected.

When available, lists of CDP and RF neighbors are also listed.

A sample monitoring page for wireless devices is shown in Figure 79.

Figure 79 ***APs/Devices > Monitor*** *Page for Wireless Devices (partial view of an AP)*



Monitoring **2188** in group Access Points in folder Top [Poll Controller Now]
This Device is in monitor-only mode.

Device Info

Status: Up (OK)
Configuration: Error (Too many errors fetching existing configuration)

Controller:	ethersphere-1322	Alcatel-Lucent AP Group:	-	Upstream Device:	-	Upstream Port:	-
Type:	OAW-AP105	Remote Device:	No	Last Contacted:	1/27/2011 4:36 PM	Uptime:	9 days 16 hrs 1 min
LAN MAC Address:	00:24:6C:CB:22:D8	Serial:	AL0246703				
IP Address:	10.100.139.241	Total Users:	2	Bandwidth:	0 kbps		
Notes:							

Interfaces

First Radio:	802.11bgn (Statistics)	MAC Address:	00:24:6C:32:2D:80	Users:	2	Bandwidth:	0 kbps
		Channel:	6	Transmit Power:	22.5 dBm	Antenna Type:	-
Second Radio:	802.11an (Statistics)	MAC Address:	00:24:6C:32:2D:88	Users:	0	Bandwidth:	0 kbps
		Channel:	161	Transmit Power:	24 dBm	Antenna Type:	-
Wired Interface:	Enet0	MAC Address:	00:24:6C:CB:22:D8	Users:	0		

Users on 2188 Last 7 hours
3
2.4
1.8
1.2
0.6
0
9:35
10:35
11:35
12:35
13:35
14:35
15:35
16:35
Show All
Maximum Average
Max Users (Radio 1) 3 users 2 users
Max Users (Radio 2) 0 users 0 users
Bandwidth on 2188 Last 7 hours
300
100
100
300
500
9:34
10:34
11:34
12:34
13:34
14:34
15:34
16:34
Show All
Maximum Average
Avg In (Radio 1) 464 bps 56 bps
Avg In (Radio 2) 0 bps 0 bps
Avg Out (Radio 1) 328 bps 38 bps
1 year ago
now

Connected Users

1-2 of 2 Connected Users Page 1 of 1 Choose Columns CSV Export

Username	Role	MAC Address	SSID	VLAN	AP Radio	Connection Mode	Ch BW	Forward Mode	Association Time	Duration	Auth. Type
-	visitor-logon	00:22:5F:16:05:E9	guest	104	802.11bgn	802.11g	-	-	1/27/2011 2:19 PM	2 hrs 17 mins	No Encryption
-	visitor-logon	00:22:5F:7E:2A:BF	guest	104	802.11bgn	802.11n (2.4GHz)	HT20	-	1/27/2011 12:49 PM	3 hrs 48 mins	No Encryption

1-2 of 2 Connected Users Page 1 of 1

RF Neighbors

1-3 of 1176 AP Neighbors Page 1 of 392 > >| Choose Columns CSV Export

AP/Device	First Radio Channel	First Radio Signal	Second Radio Channel	Second Radio Signal	RAPIDS Classification
00:0b:86:c1:8b:98	-	-	48	31	-
00:0b:86:c9:94:d8	1	11	36	29	-
00:0b:86:ca:e3:d3	-	-	36	30	-

1-3 of 1176 AP Neighbors Page 1 of 392 > >|

Alert Summary at 1/27/2011 4:37 PM

Type	Last 2 Hours	Last Day	Total	Last Event
IDS Events	0	0	0	-
Incidents	0	0	0	-
OV3600 Alerts	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Table 74 describes the fields and information displayed in the **Device Info** section. The displayed fields vary from device to device.

Table 74 ***APs/Devices > Monitor > Device Info*** *Fields and Default Values*

Field	Description
Poll Now	Button immediately polls the individual AP or the controller for a thin AP; this overrides the group's preset polling intervals to force an immediate update of all data except for rogue information. Shows “attempt” status and last polling times.
Status	Displays ability of OV3600 to connect to the AP. **Up** (no issue) means everything is working as it should. **Down** (SNMP “get” failed) means OV3600 can get to the device but not speak with it using SNMP. Check the SNMP credentials OV3600 is using the view secrets link on the **APs/ Devices > Manage** page and verify SNMP is enabled on the AP. Many APs ship with SNMP disabled. **Down** (ICMP ping failed after SNMP get failed) means OV3600 is unable to connect to the AP using SNMP and is unable to ping the AP. This usually means OV3600 is blocked from connecting to the AP or the AP needs to be rebooted or reset.
Configuration	**Good** means all the settings on the AP agree with the settings OV3600 wants them to have. **Mismatched** means there is a configuration mismatch between what is on the AP and what OV3600 wants to push to the AP. The **Mismatched** link directs you to this specific **APs/ Devices > Audit** page where each mismatch is highlighted. **Unknown** means the device configuration has not yet been fetched (possible issue with credentials). **Verifying** means it's fetching configuration to be compared to desired settings.
Firmware	Displays the firmware version running on the AP.

Table 74 ***APs/Devices* > *Monitor* > *Device Info*** *Fields and Default Values (Continued)*

Field	Description
Licenses	Appears for Alcatel-Lucent switches. Selecting this link opens a pop-up window that lists the licenses installed for this device, and whether they have expired.
Switch	Appears for APs. Displays the controller for the associated AP device. Select the controller name hyperlink to display the **APs/Devices > Monitor** page, which contains detailed controller information. Controller information includes **Status**, operational metrics, **Controller Client Count by SSID**, **Thin APs**, **Switch Bandwidth by SSID**, **CPU Utilization**, **Memory Utilization**, **APs Managed by this Controller**, **Alerts**, and **Recent Events**. Figure 79 illustrates the **Controller** page.
Portal *	Specifies the mesh AP acting as the wired connection to the network.
Mesh Mode *	Specifies whether the AP is a portal device or a mesh AP. The portal device is connected to the network over a wired connection. A mesh AP is a device downstream of the portal that uses wireless connections to reach the portal device.
Hop Count *	Displays the number of mesh links between this AP and the portal.
Type	Displays the make and model of the device.
Last Contacted	Displays the most recent time OV3600 has polled the AP for information. The polling interval can be set on the **Groups > Basic** page.
Uptime	Displays the amount of time since the AP has been rebooted. This is the amount of time the AP reports and is not based on any connectivity with OV3600.
LAN MAC Address	Displays the MAC address of the Ethernet interface on the device.
Serial	Displays the serial number of the device.
Radio Serial	Displays the serial number of the radios in the device. **NOTE:** This field is not available for all APs.
Location	Displays the SNMP location of the device.
Contact	Displays the SNMP contact of the device.
IP Address	Displays the IP address that OV3600 uses to communicate to the device. This number is also a link to the AP web interface. When the link is moused over a pop-up menu will appear allowing you to http, https, telnet or SSH to the device.
SSIDs	Appears for some APs. Displays the SSID(s) of the radio(s).
Total Users	Displays the total number of users associated to the AP regardless of which radio they are associated to, at the time of the last polling.

*This field is only available for mesh APs.

Table 75 describes the information in the **Interfaces** table for APs:

Table 75 ***APs/Devices* > *Monitor* > *Interface*** *Page Illustration*

Field	Description
First Radio	Displays the Radio type of the first radio (802.11a, 802.11b or 802.11g). If a (Statistics) link appears next to the radio, refer to "Evaluating Radio Statistics for an AP" on page 123.
Second Radio	Displays the Radio type of the second radio (802.11a, 802.11b or 802.11g.
Transmit Power	Some devices report transmit power reduction rather than transmit power; no value is reported for those devices.
Antenna Type	Indicates internal or external radio. For devices where antenna type is defined per AP, including Alcatel-Lucent devices, the same antenna type will be listed for each radio.
Channel	Displays the channel of the corresponding radio.
Users	Displays the number of users associated to the corresponding radio at the time of the last polling.
Bridge Links	Displays the number of bridge links for devices that are point-to-multi-point (see the **Groups > PTMP** page for more details).

Table 75 ***APs/Devices* > *Monitor* > *Interface*** *Page Illustration*

Field	Description
Mesh Links *	Displays the total number of mesh links to the device including uplinks and downlinks.
Bandwidth	Displays the amount of bandwidth being pushed through the corresponding radio interface or device at the time of the last polling.
MAC Address *	Displays the MAC address of the corresponding radio in the AP.
Last RAD Scan	Displays the last time the device performed a wireless rogue scan and the number of devices discovered during the scan.
Notes	A free-form text field for entering fixed asset numbers or other device information. This information is printed on the nightly inventory report. Notes can be entered on the **APs/Devices > Manage** page.

Table 76 describes graph information displayed in the **Graphical Data** section.

Table 76 ***APs/Devices* > *Monitor* > *Graphical Data*** *Fields and Default Values*

Graph	Description
User	Shows the max and average user count reported by the device radios for a configurable period of time. User count for controllers are the sum of the user count on the associated APs. Checkboxes below the graph can be used to limit the data displayed.
Bandwidth	Shows the bandwidth in and out reported by the device for a configurable period of time. Bandwidth for controllers is the sum of the associated APs. Checkboxes below the graph can be used to limit the data displayed.
CPU Utilization *(controllers only)*	Reports overall CPU utilization (not on a per-CPU basis) of the controller.
Memory Utilization *(controllers only)*	Reports average used and free memory and average max memory for the controller.
Channel Utilization *(Alcatel-Lucent and Cisco WLC thin APs on supported firmware versions only)*	Displays max and average percentages per-radio for busy, interfering receiving and transmitting signals. Special configuration on the controller is required to enable this data; consult the *Alcatel-Lucent Best Practices Guide* for details.

Table 77 describes the fields and information displayed for the **Connected Users** display.

Table 77 ***APs/Devices* > *Monitor* > *Connected Users*** *Fields and Default Values*

Field	Description
User	Provides the name of the User associated to the AP. OV3600 gathers this data in a variety of ways. It can be taken from RADIUS accounting data or traps.
MAC Address	Displays the Radio MAC address of the user associated to the AP. Also provides a link that redirects to the **Users > Detail** page.
Radio	Displays the radio to which the user is associated.
Association Time	Displays the first time OV3600 recorded the MAC address as being associated.
Duration	Displays the length of time the MAC address has been associated.

Table 77 ***APs/Devices* > *Monitor* > *Connected Users*** *Fields and Default Values (Continued)*

Field	Description
Auth. Type	Displays the type of authentication employed by the user. Supported auth types are as follows: - **EAP**—Extensible Authentication Protocol, only reported by Cisco VxWorks using SNMP traps. - **RADIUS accounting**—RADIUS accounting servers integrated with OV3600 provide the RADIUS Accounting Auth type. - **Authenticated**—a general category supporting additional authentication types. OV3600 considers all other types as not authenticated. The information OV3600 displays in **Auth Type** and **Cipher** columns depends on what information the server receives from the devices it is monitoring. The client devices may all be similar, but if the APs to which they are associated are of different models, or if security is set up differently between them, then different **Auth Type** or **Cipher** values may be reported to OV3600. If all APs are the same model and all are set up the same way, then another reason for differing **Auth Types** might be the use of multiple VLANs or SSIDs. One client device might authenticate on one SSID using one **Auth Type** and another client device might authenticate on a second SSID using a different **Auth Type**.
Cipher	Displays the encryption or decryption cipher supporting the user, when this information is available. The client devices may all be similar, but if the APs to which they are associated are of different models, or if security is set up differently between them, then different **Auth Type** or **Cipher** values may be reported to the OV3600 server.
Auth. Time	Shows when the user authenticated.
Signal Quality	Displays the average signal quality the user experienced.
BW	Displays the average bandwidth consumed by the MAC address.
Location	Displays the QuickView box allows users to view features including heatmap for a device and location history for a user.
LAN IP	Displays the IP assigned to the user MAC. This information is not always available. OV3600 can gather it from the ARP cache of switches discovered by OV3600.
VPN IP	Displays the VPN IP of the user MAC. This information can be obtained from VPN servers that send RADIUS accounting packets to OV3600.

The **Recent Events** area lists the most recent events specific to the AP. This information also appears on the **System > Events Log** page. Table 78 describes the fields in this page that display.

Table 78 ***APs/Devices* > *Monitor* > *Recent Events*** *Fields and Default Values*

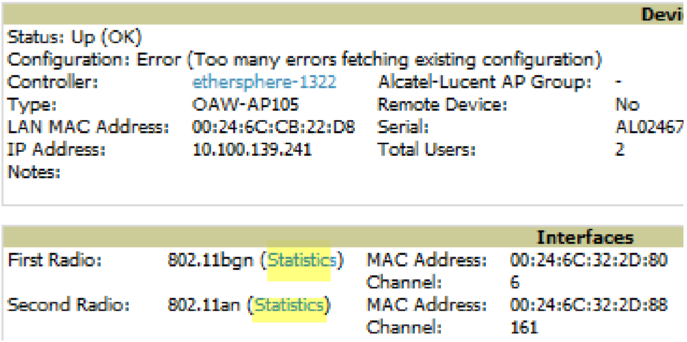
Field	Description
Time	Displays the day and time the event was recorded.
User	Displays the user that triggered the event. Configuration changes are logged as the OV3600 user that submitted them. Automated OV3600 events are logged as the System user.
Event	Displays a short text description of the event.

Evaluating Radio Statistics for an AP

The **APs/Devices > Monitor > Radio Statistics** page contains useful data for pinpointing network issues at the AP radio level for Alcatel-Lucent APs and Cisco WLC thin APs (firmware 4.2 or greater).

To see radio statistics details, navigate to the **APs/Devices > Monitoring** page for a supported AP and select the **Statistics** link in the **Interfaces** section, as illustrated in Figure 80.

Figure 80 *Statistics link on **APs/Devices** > **Monitoring** for an AP*



Devi

Status: Up (OK)
Configuration: Error (Too many errors fetching existing configuration)

Controller:	ethersphere-1322	Alcatel-Lucent AP Group:	-
Type:	OAW-AP105	Remote Device:	No
LAN MAC Address:	00:24:6C:CB:22:D8	Serial:	AL02467
IP Address:	10.100.139.241	Total Users:	2
Notes:			

Interfaces

First Radio:	802.11bgn (Statistics)	MAC Address:	00:24:6C:32:2D:80
		Channel:	6
Second Radio:	802.11an (Statistics)	MAC Address:	00:24:6C:32:2D:88
		Channel:	161

Overview of the Radio Statistics Page

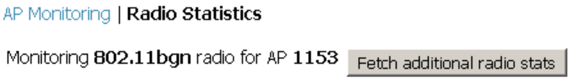
The Radio Statistics page displays transmit and receive statistics about the communication quality of individual radios. Depending on the AP, assigned group profiles, and recent activity on this radio, this data gives visibility into recent and historical changes in the network, fetches real-time statistics from the AP's controller, indicates actively interfering devices (requires Alcatel-Lucent APs set to Spectrum mode -- see "Setting up Alcatel-Lucent Spectrum Analysis in OV3600" on page 143), and summarizes major issues.

Viewing Real-Time ARM Statistics

Alcatel-Lucent AP Groups that have the **Adaptive Radio Management** (**ARM**) feature enabled continuously optimize each AP to use the best channel and transmission power settings available. An AP configured with ARM will automatically adjust to a better channel if it reaches a configured threshold for noise, MAC errors, or PHY errors; additionally, it can attenuate transmit power and switch between radio modes as needed. See the ARM chapter in the *AOS-W User Guide* for more information.

Complete ARM statistics from Alcatel-Lucent switches can be retrieved from the Radio Statistics page by selecting the new **Fetch additional radio stats** button, as illustrated in Figure 81.

Figure 81 *Fetch additional radio stats button*



AP Monitoring | **Radio Statistics**

Monitoring **802.11bgn** radio for AP **1153**

When this button is selected, a new browser window launches with the statistics in plain text. Other ARM-tracked metrics are visible in the **Radio Statistics** page for Alcatel-Lucent APs.

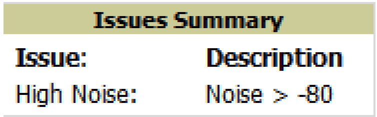
Issues Summary section

The **Issues Summary** section only displays when noise, user count, non-802.11 interfering devices, channel utilization, bandwidth, and MAC and PHY errors reach a certain threshold of concern, as described in Table 79 and illustrated in Figure 82:

Table 79 *Issues Summary labels and Thresholds*

Issue	Triggering Threshold
High Noise	> -80
High Number of Users	> 15
High Channel Utilization	> 75%
High Bandwidth	> 75% of max
Interfering Devices Detected	Detected within the last 5 minutes
High MAC/Phy Errors	> 1000 frames/sec

Figure 82 *Issues Summary Section Illustration*



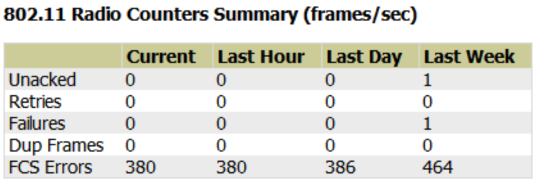
Issues Summary	
Issue:	**Description**
High Noise:	Noise > -80

These issues highlighted in this section can be examined in detail using the corresponding interactive graphs on the same page. See the Radio Statistics Interactive graphs section of this chapter for details.

802.11 Radio Counters Summary

This table appears for radios with 802.11 counters and summarizes the number of times an expected acknowledgement frame was not received, the number of duplicate frames, the number of frames containing Frame Check Sequence (FCS) errors, and the number of frame/packet transmission retries and failures. These aggregate error counts are broken down by Current, Last Hour, Last Day, and Last Week time frames, as illustrated in Figure 83.

Figure 83 *802.11 Radio Counters Summary table*



802.11 Radio Counters Summary (frames/sec)

	Current	Last Hour	Last Day	Last Week
Unacked	0	0	0	1
Retries	0	0	0	0
Failures	0	0	0	1
Dup Frames	0	0	0	0
FCS Errors	380	380	386	464

The frame- per-second rate of these and other 802.11 errors over time are tracked and compared in the **802.11 Counters** graph on the same page.

Radio Statistics Interactive graphs

Time-series graphs for the radio are displayed across a tabbed, dual-pane interface to show changes recorded at every polling interval over time. Users and Bandwidth data are polled based on the AP's group's User Data Polling Period. Channel, Noise, and Power are based on AP Interface Polling Period. 802.11 Counters data are based on the AP's group's **802.11 Counters Polling Period**.

You can adjust the attributes of these graphs as follows:

- Drag the horizontal slider under the graphs to move the scope of all graphs between one year ago and the current time.
- Drag the vertical slider between graphs to change the relative width of each.
- The **Show All** link displays all of the available data series.
- The bar-graph icon on the upper right-hand corner of each graph opens a new window and displays all data series for the selected graph over the last two hours, last day, last week, last month, and last year in one page. The graphs that display depend on the AP and/or its controller.

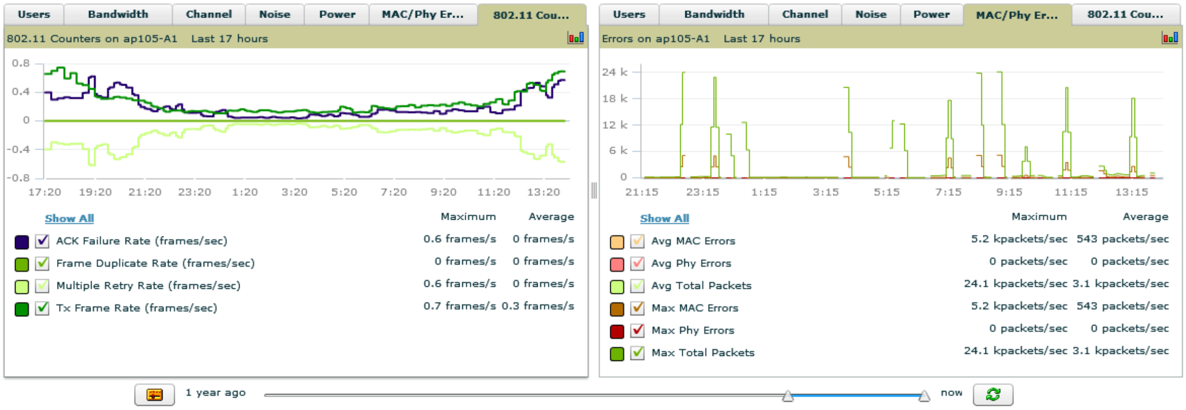
The two graph panes enable simultaneous display of two different information sets, as detailed in Table 80:

Table 80 *Radio Statistics Interactive Graphs Descriptions*

Graph Title	Description
Users	A line graph that displays the maximum users associated to the corresponding radio at polling intervals over the time range set in the slider. Select **Show All** for other metrics such as average users and max users for various individual devices.
Bandwidth	An area graph displaying the average bandwidth in each direction for the radio. Select **Show All** for other metrics such as max bandwidth in and out, average and max mesh/overhead or overhead bandwidth, and average/max Enet0.

Graph Title	Description
Channel	An area graph that displays the channel changes (if any) of the radio over time. Frequent, regular channel changes on an Alcatel-Lucent or Cisco WLC AP radio usually indicate that the Adaptive Radio Management feature (ARM) in AOS-W is compensating for high noise levels from interfering devices.
Noise	An area graph that displays signal interference (noise floor) levels in units of dBm. Noise from interfering devices above your AP's noise threshold can result in dropped packets. For ARM-enabled Alcatel-Lucent APs, crossing the noise threshold triggers an automatic channel change.
Power	A line graph that displays the average and maximum radio transmit power, between 0 and 30 dBm, over the time range set in the slider. You can adjust the transmit power manually in the **APs/Devices > Manage** page for this radio's AP, or enable ARM on Alcatel-Lucent APs to dynamically adjust the power toward your acceptable Coverage Index as needed. See the "Adaptive Radio Management" chapter of the *AOS-W User Guide* for more information.
MAC/Phy Errors	A line graph displaying the frame reception rate, physical layer error rate (resulting from poor signal reception or broken antennas), and the data link (MAC) layer (corrupt frames, driver decoding issues) for the radio.
802.11 Counters	A line graph that displays statistics such as frame rate, fragment rate, retry rate, duplicate frame rate, and other metrics tracked by 802.11 counters. Select the checkbox next to any metric to remove its data from the graph. Select **Collapse** to remove unchecked metrics from the legend, and **Show All** to restore them.

Figure 84 *Radio Statistics Interactive Graphs Illustration – Bandwidth and 802.11 Counters displayed*



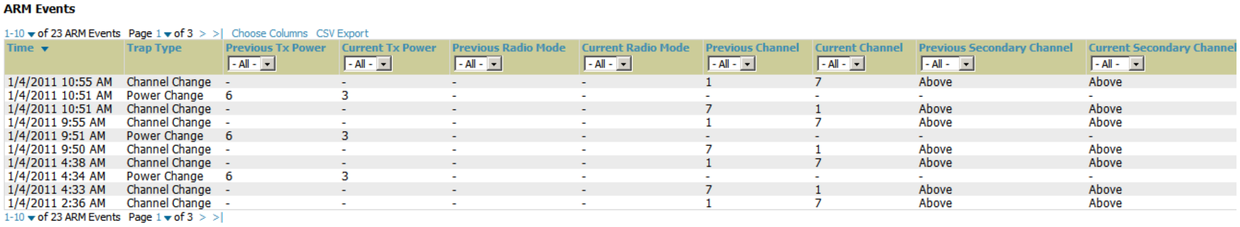
Show All	Maximum	Average
☑ ACK Failure Rate (frames/sec)	0.6 frames/s	0 frames/s
☑ Frame Duplicate Rate (frames/sec)	0 frames/s	0 frames/s
☐ Multiple Retry Rate (frames/sec)	0.6 frames/s	0 frames/s
☑ Tx Frame Rate (frames/sec)	0.7 frames/s	0.3 frames/s

Show All	Maximum	Average
☐ Avg MAC Errors	5.2 kpackets/sec	543 packets/sec
☑ Avg Phy Errors	0 packets/sec	0 packets/sec
☐ Avg Total Packets	24.1 kpackets/sec	3.1 kpackets/sec
☑ Max MAC Errors	5.2 kpackets/sec	543 packets/sec
☑ Max Phy Errors	0 packets/sec	0 packets/sec
☑ Max Total Packets	24.1 kpackets/sec	3.1 kpackets/sec

Recent ARM Events Log

If this radio references an active and enabled ARM profile, and if your OV3600 is enabled as a trap host (see *Best Practices Guide* for instructions), ARM-initiated events such as automatic channel changes, power changes, and mode changes are collected and parsed by OV3600. Any recent ARM changes will be displayed in this table with the original and modified values; these values can be selected for filtering the results. The ARM Events table can be exported in CSV format. The columns and values are described in Table 81, and illustrated in Figure 85.

Figure 85 ***ARM Events*** *Table Illustration*



ARM Events

1-10 ▾ of 23 ARM Events Page 1 ▾ of 3 > >| Choose Columns CSV Export

Time ▾	Trap Type	Previous Tx Power - All - ▾	Current Tx Power - All - ▾	Previous Radio Mode - All - ▾	Current Radio Mode - All - ▾	Previous Channel - All - ▾	Current Channel - All - ▾	Previous Secondary Channel - All - ▾	Current Secondary Channel - All - ▾
1/4/2011 10:55 AM	Channel Change	-	-	-	-	1	7	Above	Above
1/4/2011 10:51 AM	Power Change	6	3	-	-	-	-	-	-
1/4/2011 10:51 AM	Channel Change	-	-	-	-	7	1	Above	Above
1/4/2011 9:55 AM	Channel Change	-	-	-	-	1	7	Above	Above
1/4/2011 9:51 AM	Power Change	6	3	-	-	-	-	-	-
1/4/2011 9:50 AM	Channel Change	-	-	-	-	7	1	Above	Above
1/4/2011 4:38 AM	Channel Change	-	-	-	-	1	7	Above	Above
1/4/2011 4:34 AM	Power Change	6	3	-	-	-	-	-	-
1/4/2011 4:33 AM	Channel Change	-	-	-	-	7	1	Above	Above
1/4/2011 2:36 AM	Channel Change	-	-	-	-	1	7	Above	Above

1-10 ▾ of 23 ARM Events Page 1 ▾ of 3 > >|

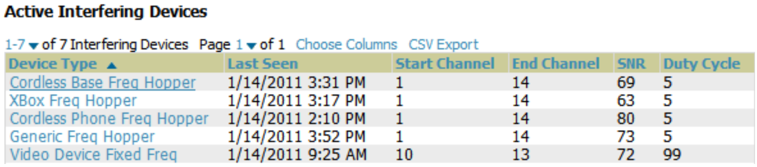
Table 81 ***ARM Events*** *Table Columns and Values*

Column	Description
Time	The time of the ARM event.
Trap Type	The type of trap that delivered the change information. Current ARM trap types that display in OV3600 are: ● Power Change ● Mode Change ● Channel Change Values that display in the following columns depend on the Trap Type.
Previous Tx Power	Old value for transmit power before the Power Change event took place.
Current Tx Power	New transmit power value after the change.
Previous Radio Mode	Old value for radio mode before the Mode Change event took place.
Current Radio Mode	New radio mode value after the change.
Previous Channel	Old primary channel value before the Channel Change event took place.
Current Channel	New primary channel value after the change.
Previous Secondary Channel	Old secondary channel value (for 40Mhz channels on 802.11n devices) before the Channel Change event took place.
Current Secondary Channel	New secondary channel value after the change.
Change Reason	If the noise and interference cause for the change can be determined, they will be displayed here. Mode change reasons are not yet tracked.

Active Interfering Devices Table

For Alcatel-Lucent APs running in Spectrum mode (refer to "Setting up Alcatel-Lucent Spectrum Analysis in OV3600" on page 143), the same non-802.11 interfering devices identified in the **Issues Summary** section are classified in the Active Interfering Devices table along with the timestamp of its last detection, the start and end channels of the interference, the signal to noise ratio, and the percentage of time the interference takes place, as illustrated in Figure 86. This table can be exported to CSV format, and the displayed columns can be moved or hidden as needed.

Figure 86 ***Active Interfering Devices*** *Table Illustration*



Active Interfering Devices

1-7 ▾ of 7 Interfering Devices Page 1 ▾ of 1 Choose Columns CSV Export

Device Type ▲	Last Seen	Start Channel	End Channel	SNR	Duty Cycle
Cordless Base Freq Hopper	1/14/2011 3:31 PM	1	14	69	5
XBox Freq Hopper	1/14/2011 3:17 PM	1	14	63	5
Cordless Phone Freq Hopper	1/14/2011 2:10 PM	1	14	80	5
Generic Freq Hopper	1/14/2011 3:52 PM	1	14	73	5
Video Device Fixed Freq	1/14/2011 9:25 AM	10	13	72	99

Possible device types for the Active Interfering Devices table are:

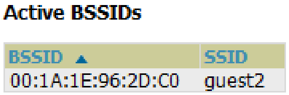
- Wi-Fi
- Microwave
- Bluetooth
- Generic Fixed Freq
- Cordless Phone Fixed Freq
- Video Device Fixed Freq
- Audio Device Fixed Freq
- Generic Freq Hopper
- Cordless Phone Freq Hopper
- XBox Freq Hopper

- Microwave Inverter
- Cordless Base Freq Hopper
- Unknown

Active BSSIDs

The Active BSSIDs table maps the BSSIDs on a radio with the SSID it broadcasts to the network, as illustrated in Figure 87. This table appears only for Alcatel-Lucent AP radios.

Figure 87 ***Active BSSIDs*** *Table Illustration*



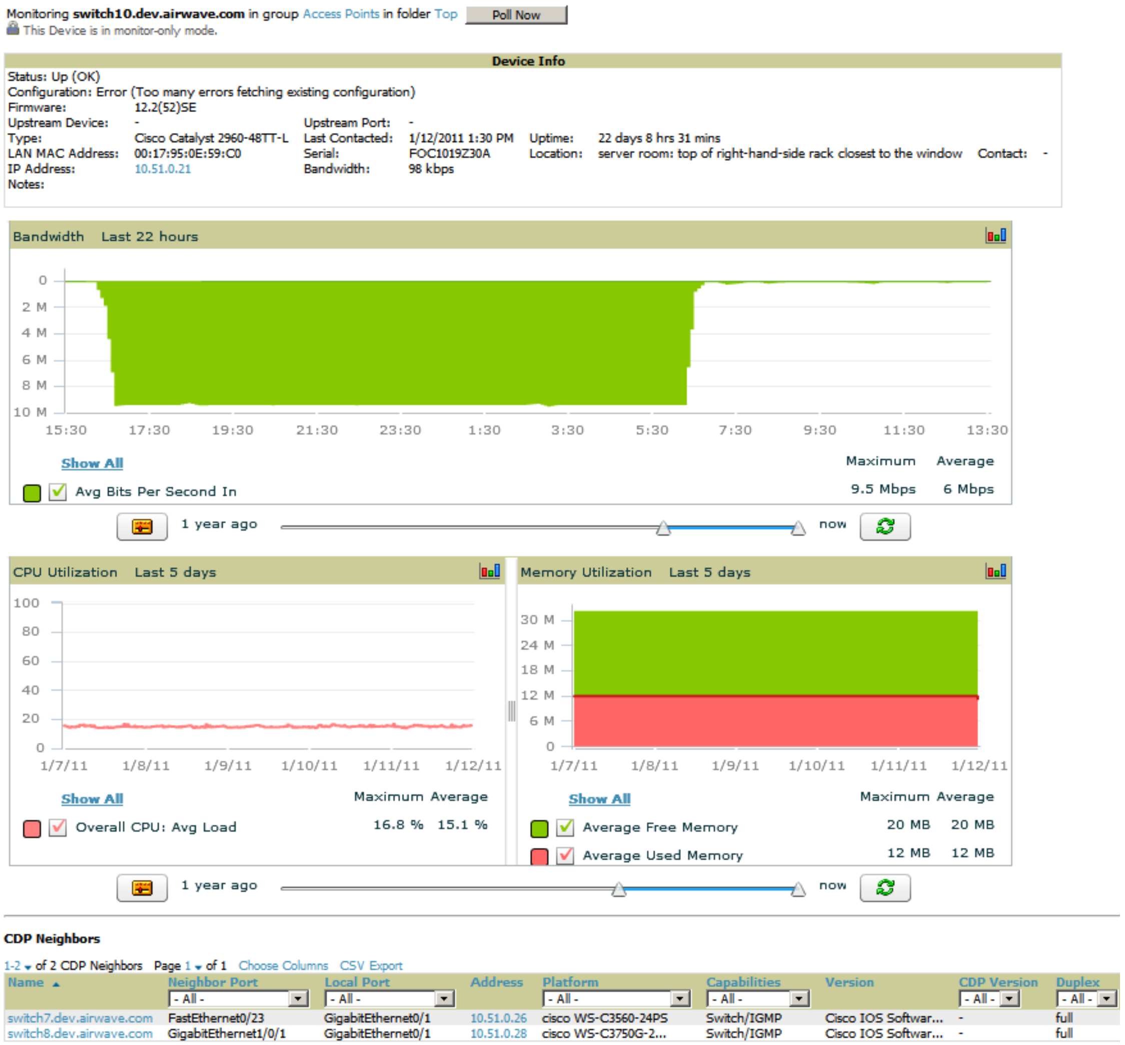
Active BSSIDs

BSSID ▲	SSID
00:1A:1E:96:2D:C0	guest2

Monitoring Data for Wired Devices (Routers and Switches)

The monitoring page for routers and switches includes basic device information at the top, a bandwidth graph depicting the sum of all the physical interfaces, and beneath that, CPU/Memory usage graphs as shown in Figure 88.

Figure 88 ***APs/Devices > Monitor*** *Page for Wired Devices*



Monitoring **switch10.dev.airwave.com** in group Access Points in folder Top

This Device is in monitor-only mode.

Device Info

Status: Up (OK)

Configuration: Error (Too many errors fetching existing configuration)

Firmware:	12.2(52)SE						
Upstream Device:	-	Upstream Port:	-				
Type:	Cisco Catalyst 2960-48TT-L	Last Contacted:	1/12/2011 1:30 PM	Uptime:	22 days 8 hrs 31 mins		
LAN MAC Address:	00:17:95:0E:59:C0	Serial:	FOC1019Z30A	Location:	server room: top of right-hand-side rack closest to the window	Contact:	-
IP Address:	10.51.0.21	Bandwidth:	98 kbps				
Notes:							

		Maximum	Average
🟩	☑ Avg Bits Per Second In	9.5 Mbps	6 Mbps

		Maximum	Average
🟥	☑ Overall CPU: Avg Load	16.8 %	15.1 %

		Maximum	Average
🟩	☑ Average Free Memory	20 MB	20 MB
🟥	☑ Average Used Memory	12 MB	12 MB

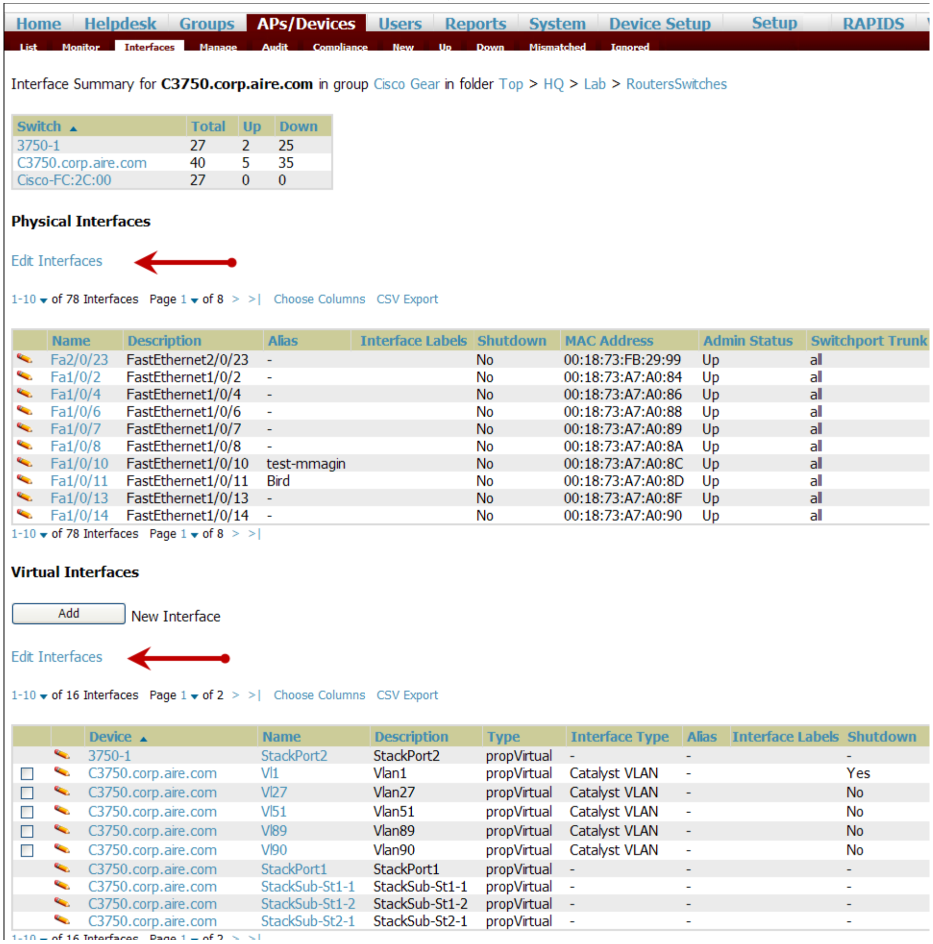
CDP Neighbors

1-2 ▾ of 2 CDP Neighbors Page 1 ▾ of 1 Choose Columns CSV Export

Name ▲	Neighbor Port	Local Port	Address	Platform	Capabilities	Version	CDP Version	Duplex
	- All -	- All -		- All -	- All -		- All -	- All -
switch7.dev.airwave.com	FastEthernet0/23	GigabitEthernet0/1	10.51.0.26	cisco WS-C3560-24PS	Switch/IGMP	Cisco IOS Softwar...	-	full
switch8.dev.airwave.com	GigabitEthernet1/0/1	GigabitEthernet0/1	10.51.0.28	cisco WS-C3750G-2...	Switch/IGMP	Cisco IOS Softwar...	-	full

All managed wired devices also include an **Interfaces** subtab, as shown in Figure 89.

Figure 89 ***APs/Devices*** **> *Interfaces*** *Page for Wired Devices (partial view).*



Interface Summary for **C3750.corp.aire.com** in group Cisco Gear in folder Top > HQ > Lab > RoutersSwitches

Switch ▲	Total	Up	Down
3750-1	27	2	25
C3750.corp.aire.com	40	5	35
Cisco-FC:2C:00	27	0	0

Physical Interfaces

Edit Interfaces

1-10 ▾ of 78 Interfaces Page 1 ▾ of 8 > >| Choose Columns CSV Export

	Name	Description	Alias	Interface Labels	Shutdown	MAC Address	Admin Status	Switchport Trunk
✎	Fa2/0/23	FastEthernet2/0/23	-		No	00:18:73:FB:29:99	Up	all
✎	Fa1/0/2	FastEthernet1/0/2	-		No	00:18:73:A7:A0:84	Up	all
✎	Fa1/0/4	FastEthernet1/0/4	-		No	00:18:73:A7:A0:86	Up	all
✎	Fa1/0/6	FastEthernet1/0/6	-		No	00:18:73:A7:A0:88	Up	all
✎	Fa1/0/7	FastEthernet1/0/7	-		No	00:18:73:A7:A0:89	Up	all
✎	Fa1/0/8	FastEthernet1/0/8	-		No	00:18:73:A7:A0:8A	Up	all
✎	Fa1/0/10	FastEthernet1/0/10	test-mmagin		No	00:18:73:A7:A0:8C	Up	all
✎	Fa1/0/11	FastEthernet1/0/11	Bird		No	00:18:73:A7:A0:8D	Up	all
✎	Fa1/0/13	FastEthernet1/0/13	-		No	00:18:73:A7:A0:8F	Up	all
✎	Fa1/0/14	FastEthernet1/0/14	-		No	00:18:73:A7:A0:90	Up	all

1-10 ▾ of 78 Interfaces Page 1 ▾ of 8 > >|

Virtual Interfaces

Add New Interface

Edit Interfaces

1-10 ▾ of 16 Interfaces Page 1 ▾ of 2 > >| Choose Columns CSV Export

		Device ▲	Name	Description	Type	Interface Type	Alias	Interface Labels	Shutdown
	✎	3750-1	StackPort2	StackPort2	propVirtual	-	-		-
□	✎	C3750.corp.aire.com	Vl1	Vlan1	propVirtual	Catalyst VLAN	-		Yes
□	✎	C3750.corp.aire.com	Vl27	Vlan27	propVirtual	Catalyst VLAN	-		No
□	✎	C3750.corp.aire.com	Vl51	Vlan51	propVirtual	Catalyst VLAN	-		No
□	✎	C3750.corp.aire.com	Vl89	Vlan89	propVirtual	Catalyst VLAN	-		No
□	✎	C3750.corp.aire.com	Vl90	Vlan90	propVirtual	Catalyst VLAN	-		No
	✎	C3750.corp.aire.com	StackPort1	StackPort1	propVirtual	-	-		-
	✎	C3750.corp.aire.com	StackSub-St1-1	StackSub-St1-1	propVirtual	-	-		-
	✎	C3750.corp.aire.com	StackSub-St1-2	StackSub-St1-2	propVirtual	-	-		-
	✎	C3750.corp.aire.com	StackSub-St2-1	StackSub-St2-1	propVirtual	-	-		-

1-10 ▾ of 16 Interfaces Page 1 ▾ of 2 > >|

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

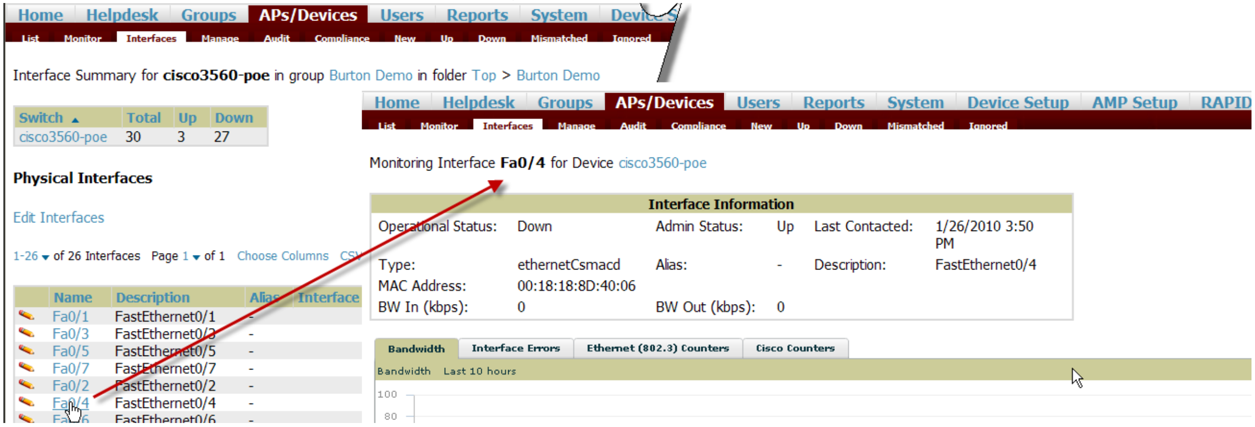
OV3600 now monitors **Up/Down** status and bandwidth information on all interfaces. You can edit multiple interfaces concurrently by selecting one of the two **Edit Interfaces** hyperlinks as shown using red arrows in Figure 89 above. You can edit both monitoring and configuration settings this way.

Interface labels are used to group one or more interfaces for the purpose of defining interface bandwidth triggers. For more information on interface bandwidth triggers, see ""Backing Up OV3600" on page 215" on page 179.

Understanding the APs/Devices > Interfaces Page

"Monitoring Data for Wired Devices (Routers and Switches)" on page 128 showed you how to view high level interface information for all physical and virtual interfaces on an entire router or switch. Select any interface hotlink in the **Name** column of the Physical or Virtual Interfaces tables on the stacked switches to go to an **Interfaces** page displaying data relevant to that specific interface, as shown Figure 90.

Figure 90 ***Individual Interface Monitoring*** *Page.*



Interface Summary for **cisco3560-poe** in group Burton Demo in folder Top > Burton Demo

Switch ▲	Total	Up	Down
cisco3560-poe	30	3	27

Physical Interfaces

Edit Interfaces

1-26 ▾ of 26 Interfaces Page 1 ▾ of 1 Choose Columns CSV

	Name	Description	Alias	Interface
✎	Fa0/1	FastEthernet0/1	-	
✎	Fa0/3	FastEthernet0/3	-	
✎	Fa0/5	FastEthernet0/5	-	
✎	Fa0/7	FastEthernet0/7	-	
✎	Fa0/2	FastEthernet0/2	-	
✎	Fa0/4	FastEthernet0/4	-	
✎	Fa0/6	FastEthernet0/6	-	

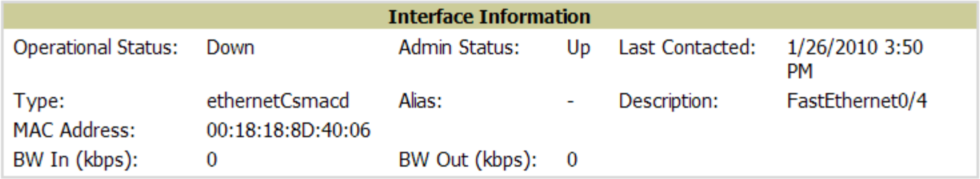
Monitoring Interface **Fa0/4** for Device cisco3560-poe

Interface Information

Operational Status:	Down	Admin Status:	Up	Last Contacted:	1/26/2010 3:50 PM
Type:	ethernetCsmacd	Alias:	-	Description:	FastEthernet0/4
MAC Address:	00:18:18:8D:40:06				
BW In (kbps):	0	BW Out (kbps):	0		

An individual **Interface** monitoring page includes is comprised of 2 sections. Specifics of the interface are in the upper section, as depicted in Figure 91.

Figure 91 *Individual* ***Interface Information*** *Section.*



Interface Information

Operational Status:	Down	Admin Status:	Up	Last Contacted:	1/26/2010 3:50 PM
Type:	ethernetCsmacd	Alias:	-	Description:	FastEthernet0/4
MAC Address:	00:18:18:8D:40:06				
BW In (kbps):	0	BW Out (kbps):	0		

Bandwidth, and various standard and enterprise specific error counting information is displayed in the lower section in a tabbed graph.

What Next?

All device lists in OV3600 act as portals to management pages if you have the proper read/write privileges. Selecting the wrench or pencil icon next to a device table entry, or selecting **Modify Devices** where appropriate above a device table, will take you to the appropriate Management page (**APs/Devices > Manage**). See "Configuring and Managing Devices" on page 132 for more information.

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. See "Individual Device Support and Firmware Upgrades" on page 141 for more details.

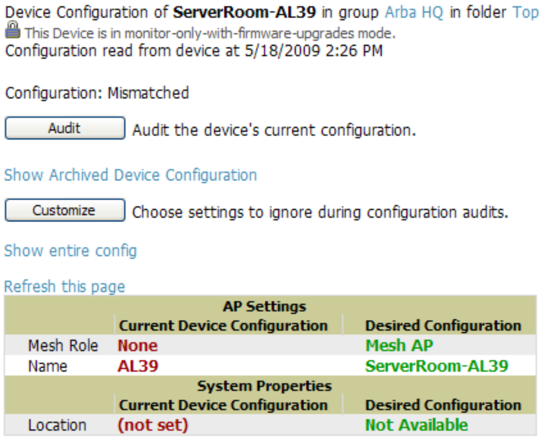
Perform these steps to verify the device configuration status:

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 do 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. The **APs/Devices > Audit** page lists detailed information on 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. Figure 92 illustrates this page.

Figure 92 ***APs/Devices > Audit*** *Page Illustration*



Device Configuration of **ServerRoom-AL39** in group Arba HQ in folder Top
This Device is in monitor-only-with-firmware-upgrades mode.
Configuration read from device at 5/18/2009 2:26 PM

Configuration: Mismatched

Audit — Audit the device's current configuration.

Show Archived Device Configuration

Customize — Choose settings to ignore during configuration audits.

Show entire config

Refresh this page

	Current Device Configuration	Desired Configuration
AP Settings		
Mesh Role	None	Mesh AP
Name	AL39	ServerRoom-AL39
System Properties		
	Current Device Configuration	**Desired Configuration**
Location	(not set)	Not Available

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.

Using Device Folders (Optional)

The devices on the **APs/Devices List** pages include **List, Up, Down,** and **Mismatched** fields. These devices are arranged in groups 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 OV3600 users can see.

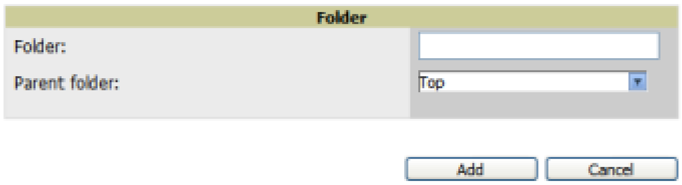
Folder views are persistent in OV3600. If you select the **Top** folder and then select the **Down** link at the top of the page, you are taken to all of the down devices in the folder.

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 an additional column that lists the folder containing the AP.

Perform the following steps to add a device folder to OV3600.

1. To add a folder, select the **Add New Folder** link in **APs/Devices > List**. Figure 93 illustrates the page that appears.

Figure 93 *Folder Creation Page Illustration*



Folder	
Folder:	
Parent folder:	Top

2. Enter the name of the new folder.
3. Select the **Parent** folder.
4. Select **Add**.

Once a new folder has been created, devices can be moved into it using the **Modify Devices** link or when **New Devices** are added into OV3600.

Configuring and Managing Devices

This section contains the following topics describing individual device configuration within device groups:

- "Moving a Device from Monitor Only to Manage Read/Write Mode" on page 132
- "Configuring AP Settings" on page 133
- "Configuring Device Interfaces for Cisco Catalyst Switches" on page 138
- "Individual Device Support and Firmware Upgrades" on page 141

While most device configuration settings can be efficiently managed by OV3600 at a Group level, certain settings must be managed at the individual device level. For example, because devices within a Group are often contiguous with one another, and have overlapping coverage areas, it makes sense to manage these devices individually to avoid RF interference.

NOTE

Any changes made at an individual device level will automatically override Group level settings.

OV3600 automatically saves the last 10 device configurations for reference and compliance purposes. Archived device configurations are linked on the **APs/Devices > Audit** page and identified by name. By default, configuration is tracked by the date and time it was created; device configurations are also archived by date.

It is not possible to push archived configurations to devices, but archived configurations can be compared to the current configuration, the desired configuration, or to other archived configurations using the drop-down menus on the **APs/Devices > Audit** page. This applies to startup or to running configuration files.

Compare two configurations to highlight the specific lines that are mismatched. The Audit page provides links to the OV3600 pages where any mismatched settings can be configured.

NOTE

These procedures assume you are familiar with the function buttons available to save, apply, revert, and so on. For details on button functions, see "Buttons and Icons" on page 26.

Moving a Device from Monitor Only to Manage Read/Write Mode

Once the device configuration status is **Good** on the **APs/Devices > List** page, or once you have verified all changes that will be applied to the device on the **APs/Devices > Audit** page, you can safely shift the device from **Monitor Only** mode to **Manage Read/Write** mode.

NOTE

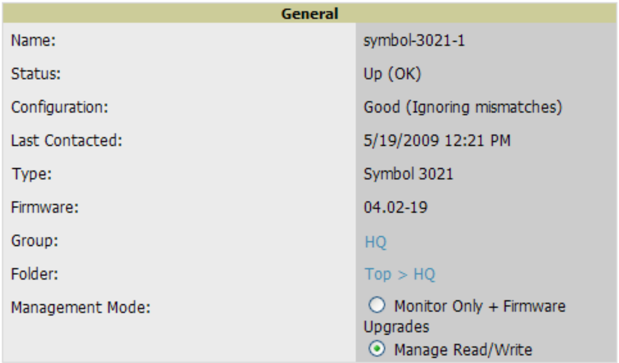
Once a device is in Manage mode, OV3600 will push a new configuration to the device in the event that the actual device configuration does not match the OV3600 configuration for that device.

To move a device from **Monitor Only** to **Manage Read/Write** mode, perform the following steps.

1. Go to the **APs/Devices > List** page and select the wrench icon next to the name of the AP to be shifted from **Monitor Only** mode to **Manage Read/Write** mode. This directs you to the **APs/Devices > Manage** page.

2. Locate the **General** area as shown in Figure 94.

Figure 94 ***APs/Devices > Manage > General*** *Section Illustration*



General	
Name:	symbol-3021-1
Status:	Up (OK)
Configuration:	Good (Ignoring mismatches)
Last Contacted:	5/19/2009 12:21 PM
Type:	Symbol 3021
Firmware:	04.02-19
Group:	HQ
Folder:	Top > HQ
Management Mode:	○ Monitor Only + Firmware Upgrades ● Manage Read/Write

3. Select **Manage Read/Write** on the **Management Mode** field.

4. Select **Save and Apply**, then **Confirm Edit** on the confirmation page to retain these settings and to push configuration to the device.

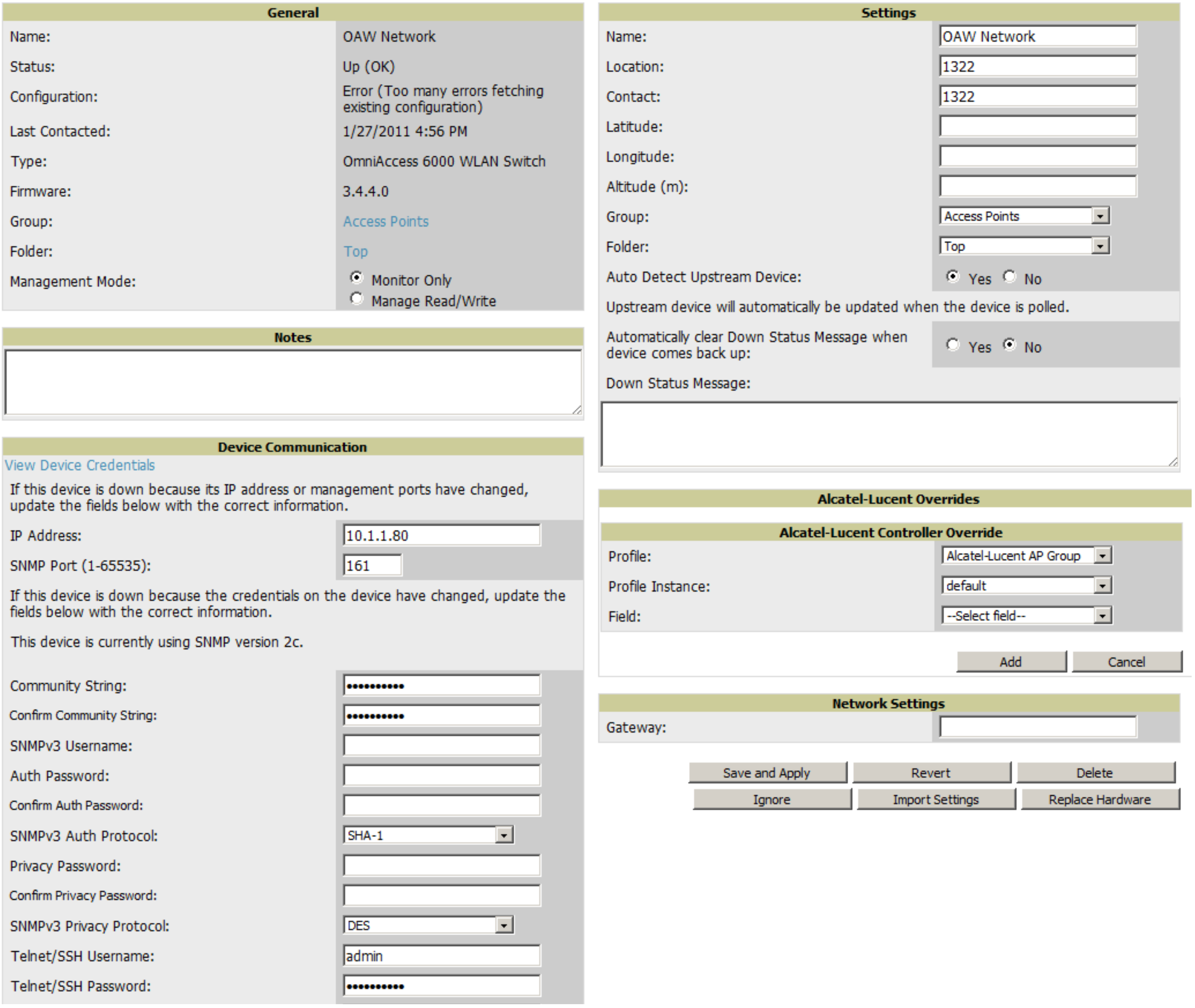
5. For device configuration changes that require the device to reboot, use the **Schedule** function to push the changes at a time when WLAN users will not be affected.

6. To move multiple devices into managed mode at once, use the **Modify these devices** link. Refer to "Modifying Multiple Devices" on page 103 for more information.

Configuring AP Settings

1. Browse to the **APs/Devices > List** page and select the wrench icon next to the device whose AP settings you want to edit. This directs you to the **Manage** page for that device. Figure 95 illustrates this page.

Figure 95 ***APs/Devices* > *Manage*** *Page Illustration*



General

Name:	OAW Network
Status:	Up (OK)
Configuration:	Error (Too many errors fetching existing configuration)
Last Contacted:	1/27/2011 4:56 PM
Type:	OmniAccess 6000 WLAN Switch
Firmware:	3.4.4.0
Group:	Access Points
Folder:	Top
Management Mode:	● Monitor Only ○ Manage Read/Write

Notes

Device Communication

View Device Credentials

If this device is down because its IP address or management ports have changed, update the fields below with the correct information.

IP Address:	10.1.1.80
SNMP Port (1-65535):	161

If this device is down because the credentials on the device have changed, update the fields below with the correct information.

This device is currently using SNMP version 2c.

Community String:	••••••••••
Confirm Community String:	••••••••••
SNMPv3 Username:	
Auth Password:	
Confirm Auth Password:	
SNMPv3 Auth Protocol:	SHA-1
Privacy Password:	
Confirm Privacy Password:	
SNMPv3 Privacy Protocol:	DES
Telnet/SSH Username:	admin
Telnet/SSH Password:	••••••••••

Settings

Name:	OAW Network
Location:	1322
Contact:	1322
Latitude:	
Longitude:	
Altitude (m):	
Group:	Access Points
Folder:	Top
Auto Detect Upstream Device:	● Yes ○ No

Upstream device will automatically be updated when the device is polled.

Automatically clear Down Status Message when device comes back up:	○ Yes ● No

Down Status Message:

Alcatel-Lucent Overrides

Alcatel-Lucent Controller Override

Profile:	Alcatel-Lucent AP Group
Profile Instance:	default
Field:	--Select field--

Network Settings

Gateway:	

If any changes are scheduled for this AP, they appear in a **Scheduled Changes** section at the top of the page above the other fields. The linked name of the job takes you to its **System > Configuration Change Job Detail** page.

2. Locate the **General** section for information about the APs current status. Table 82 describes the fields, information, and settings.

Table 82 ***APs/Devices* > *Manage* > *General*** *Fields and Descriptions*

Field	Description
Name	Displays the name currently set on the device.
Status	Displays the current status of an AP. If an AP is **Up**, then OV3600 is able to ping it and fetch SNMP information from the AP. If the AP is listed **Down** then OV3600 is either unable to ping the AP or unable to read the necessary SNMP information from the device.
Configuration	Displays the current configuration status of the AP. To update the status, select **Audit** on the **APs/Devices > Audit** page.
Last Contacted	Displays the last time OV3600 successfully contacted the AP.
Type	Displays the type of AP.
Firmware	Displays the version of firmware running on the AP.
Group	Links to the **Group > Monitoring** page for the AP.

Table 82 ***APs/Devices* > *Manage*** > ***General*** *Fields and Descriptions (Continued)*

Field	Description
Template	Displays the name of the group template currently configuring the AP. Also displays a link to the **Groups > Template** page. This is only visible for APs that are managed by templates.
Folder	Displays the name of the folder containing the AP. Also displays a link to the **APs/Devices > List** page for the folder.
Management Mode	Displays the current management mode of the AP. No changes are made to the AP when it is in **Monitor Only** mode. OV3600 pushes configurations and makes changes to an AP when it is in **Manage Read/Write** mode.
Notes	Provides a free-form text field to describe device information.

3. Review and provide the following information in the **Settings** area. Devices with dual radios display radio-specific settings in the Slot A and Slot B area. If a device is dual-radio capable but only has one device installed, OV3600 manages that device as if it were a single slot device.

NOTE

Devices from different vendors have different RF settings and capabilities. The fields in the **Settings** section of the **APs/Devices > Manage** page are context-sensitive and only present the information relevant for the particular device vendor and model.

Table 83 describes field settings, default values, and information for the **Settings** section of this page.

Table 83 ***APs/Devices* > *Manage* > *Settings*** *Fields and Default Values*

Setting	Default	Device Type	Description
Name	None	All	User-configurable name for the device (max. 20 characters)
Domain Name	None	IOS	Field populated upon initial device discovery or upon refreshing settings. Enable this option from **OV3600 Setup > Network** page to display this field on the **APs/Devices > Manage** page, with fully-qualified domain names for IOS APs. This field is used in conjunction with **Domain** variable in IOS templates.
Location	Read from the device	All	The SNMP location set on the device.
Latitude	None	All	Text field for entering the latitude of the device. The latitude is used with the Google Earth integration.
Longitude	None	All	Text field for entering the longitude of the device. The longitude is used with the Google Earth integration.
Altitude (meters)	None	All	Text field for entering the altitude of the device when known. This setting is used with the Google Earth integration. Specify altitude in meters.
Group	Default Group	All	Drop-down menu that can be used to assign the device to another Group.
Folder	Top	All	Drop-down menu that can be used to assign the device to another Group.
Auto Detect Upstream Device	Yes	All	Selecting **Yes** enables automatic detection of upstream device, which is automatically updated when the device is polled. Selecting **No** displays a drop-down menu of upstream devices.
Down Status Message	None	All	Enter a text message that provides information to be conveyed if the device goes down.
Administrative Status	Enable	All	Enables or disables administrative mode for the device.

Table 83 ***APs/Devices* > *Manage* > *Settings*** *Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
Mode	Local	All	Designates the mode in which the device should operate. Options include the following: ● Local ● H-REAP ● Monitor ● Rogue Detector ● Sniffer

4. Complete additional settings on the **APs/Devices > Manage** page, to include H-REAP, certificates, radio settings, and network settings. Table 84 describes many of the possible fields.

NOTE

For complete listing and discussion of settings applicable only to Alcatel-Lucent devices, see the *Alcatel-Lucent Configuration Guide* for this release.

Table 84 ***APs/Devices* > *Manage*** *Page Illustration, Additional Settings*

Setting	Default	Device Type	Description
Mesh Role	Mesh AP	Mesh Devices	Drop-down menu specifies the mesh role for the AP as shown: ● **Mesh AP** —The AP will act like a mesh client. It will use other APs as its uplink to the network. ● **Portal AP** —The AP will become a portal AP. It will use a wired connection as its uplink to the network and serve it over the radio to other APs. ● **None** —The AP will act like a standard AP. It will not perform any meshing functions
Mesh Mobility	Static	Mesh Devices	Select **Static** if the AP is static, as in the case of a device mounted on a light pole or in the ceiling. Select **Roaming** if the AP is mobile. Two examples would be an AP mounted in a police car or utility truck.
Receive Antenna	Diversity	Cisco	Drop-down menu for the receive antenna provides three options: **Diversity** —Device will use the antenna that receives the best signal. If the device has two fixed (non-removable) antennas, the **Diversity** setting should be used for both receive and transmit antennas. **Right** —If your device has removable antennas and you install a high-gain antenna on the device's right connector (the connector on the right side when viewing the back panel of the device), use this setting for both receive and transmit. **Left** —If your device has removable antennas and you install a high-gain antenna on the device's left connector, use this setting for both receive and transmit.
Transmit Antenna	Diversity	Cisco	See description in **Receive Antenna** above.
Antenna Diversity	Primary Only	Symbol 4131	Drop-down menu provides the following options: **Full Diversity**—The AP receives information on the antenna with the best signal strength and quality. The AP transmits on the antenna from which it last received information. **Primary Only**—The AP transmits and receives on the primary antenna only. Secondary Only: The AP transmits and receives on the secondary antenna only. **Rx Diversity**—The AP receives information on the antenna with the best signal strength and quality. The AP transmits information on the primary antenna only.
Transmit Power Reduction	0	Proxim	Transmit Power Reduction determines the APs transmit power. The max transmit power is reduced by the number of decibels specified.

Table 84 ***APs/Devices* > *Manage*** *Page Illustration, Additional Settings*

Setting	Default	Device Type	Description
Channel	6	All	Represents the AP's current RF channel setting. The number relates to the center frequency output by the AP's RF synthesizer. Contiguous APs should be set to different channels to minimize crosstalk, which occurs when the signals from APs overlap and interfere with each other. This RF interference negatively influences WLAN performance. 802.11b's 2.4-GHz range has a total bandwidth of 80-MHz separated into 11 center channels. Of these channels, only 3 are non-overlapping (1, 6, and 11). In the United States, most organizations use only these non-overlapping channels.
Transmit Power Level	Highest power level supported by the radio in the regulatory domain (country)	Cisco, Symbol, Proxim AP-600, AP-700, AP-2000 (802.11g)	Determines the power level of radio transmission. Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device. You can increase the coverage radius of the access point by increasing the Transmit Power Level. However, while this increases the zone of coverage, it also makes it more likely that the AP will interfere with neighboring APs. Supported values are: **Cisco (100mW, 50mW, 30mW, 20mW, 5mW, 1mW) Symbol (Full or 50mW, 30mW, 15mW, 5mW, 1mW)**
Radio (Enable/ Disable)	Enable	All	The Radio option allows you to disable the radio's ability to transmit or receive data while still maintaining Ethernet connectivity to the network. OV3600 will still monitor the Ethernet page and ensure the AP stays online. Customers typically use this option to temporarily disable wireless access in particular locations. This setting can be scheduled at an AP-Level or Group-Level.
DHCP	Yes	All	If enabled, the AP will be assigned a new IP address using DHCP. If disabled, the AP will use a static IP address. For improved security and manageability, Alcatel-Lucent recommends disabling DHCP and using static IP addresses.
LAN IP	None	All	The IP Address of the AP Ethernet interface. If One-to-One NAT is enabled, OV3600 will communicate with the AP on a different address (the IP Address defined in the "Device Communication" area). If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.
Subnet Mask	None	All	Provides the IP subnet mask to identify the sub-network so the IP address can be recognized on the LAN. If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.
Gateway	None	All	The IP address of the default internet gateway. If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.

5. Locate the **Template Options** area on the **APs/Devices > Manage** page.

NOTE

This field only appears for IOS APs, Symbol controllers, and Alcatel-Lucent switches in groups with Alcatel-Lucent GUI Config disabled.

Table 85 describes field settings, default values, and additional information for this page.

Table 85 ***APs/Devices* > *Manage* > *IOS Template Options*** *Fields and Default Values*

Setting	Default	Device Type	Description
WDS Role	Client	Cisco IOS Wireless LAN Controllers only	Set the WDS role for this AP. Select Master for the WDS master APs and Client for the WDS Client. Once this is done you can use the %if wds_role= % to push the client, master, or backup lines to appropriate WDS APs.
SSL Certificate	None	Cisco IOS	OV3600 will read the SSL Certificate off of the AP when it comes UP in OV3600. The information in this field will defines what will be used in place of %certificate%.
Extra Device Commands	None	Cisco IOS	Defines the lines that will replace the %ap_include_1% variable in the IOS template. This field allows for unique commands to be run on individual APs. If you have any settings that are unique per AP like a MOTD you can set them here.

Table 85 ***APs/Devices > Manage > IOS Template Options*** *Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
switch_command	None	Cisco Catalyst switches	Defines lines included for each of the members in the stack. This field appears only on the master's **Manage** page. The information in this field will determine what is used in place of the %switch_command% variable.

6. For Cisco WLC devices, go to the interfaces section of the **AP > Manage** page. Select **Add new Interface** to add another controller interface, or select the pencil icon to edit an existing controller interface. Figure 96 describes the settings and default values. For detailed descriptions of Cisco WLC devices supported by OV3600, refer to the Cisco WLC product documentation.

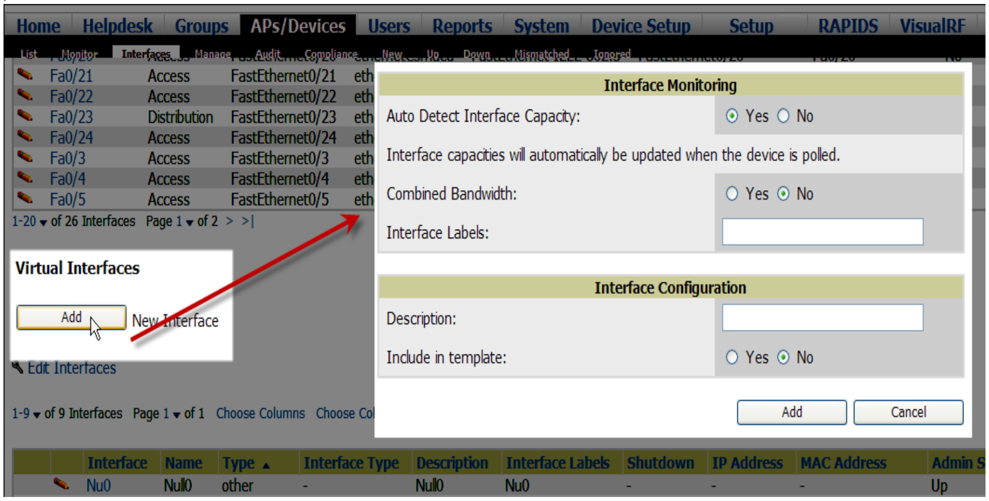
Figure 96 ***APs/Devices > Manage > Interface*** *Fields and Descriptions for Cisco WLC Devices*

Field	Default	Description
Name	None	The name of the interface on the controller.
VLAN ID	None	The VLAN ID for the interface on the controller.
Port	None	The port on the controller to access the interface.
IP Address	None	The IP address of the controller.
Subnet Mask	None	The subnet mask for the controller.
Gateway	None	The controller's gateway.
Primary and Secondary DHCP Servers	None	The DHCP servers for the controller.
Guest LAN	Disabled	Indicates a guest LAN.
Quarantine VLAN ID	Disabled	Enabled indicates it is a quarantine VLAN; used only for H-REAP-associated clients.
Dynamic Device Management	Enabled	When enabled, makes the interface an AP-manager interface. Cisco calls this feature Dynamic AP Management.

Configuring Device Interfaces for Cisco Catalyst Switches

When you go to the APs/Devices > Interfaces page for a Cisco Catalyst switch, you can add a Virtual interface by selecting **Add** and entering the appropriate information in the page that then appears, as shown in Figure 97.

Figure 97 ***Add Virtual Interfaces*** *Page for Wired Devices*



Fa0/21	Access	FastEthernet0/21	eth
Fa0/22	Access	FastEthernet0/22	eth
Fa0/23	Distribution	FastEthernet0/23	eth
Fa0/24	Access	FastEthernet0/24	eth
Fa0/3	Access	FastEthernet0/3	eth
Fa0/4	Access	FastEthernet0/4	eth
Fa0/5	Access	FastEthernet0/5	eth

1-20 of 26 Interfaces Page 1 of 2 > >|

Interface Monitoring

Auto Detect Interface Capacity: ● Yes ○ No

Interface capacities will automatically be updated when the device is polled.

Combined Bandwidth: ○ Yes ● No

Interface Labels:

Interface Configuration

Description:

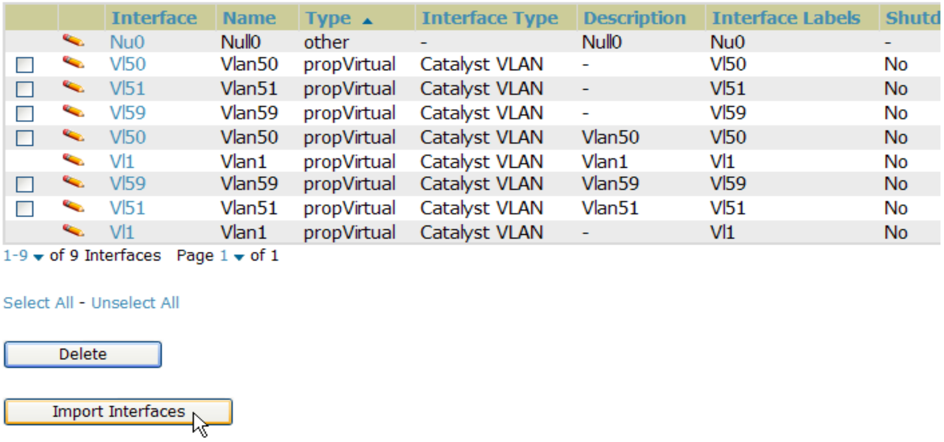
Include in template: ○ Yes ● No

1-9 of 9 Interfaces Page 1 of 1

Interface	Name	Type ▲	Interface Type	Description	Interface Labels	Shutdown	IP Address	MAC Address	Admin S
Nu0	Null0	other	-	Null0	Nu0	-	-	-	Up

New physical and virtual interfaces are discovered using SNMP polling as described in "SNMP/HTTP Scanning" on page 107. To refresh and reload all current interface information from a device, select **Import Interfaces** on the bottom of the page as shown in Figure 98.

Figure 98 ***Import Interfaces** for Refresh and Reload (lower portion of page)*



		Interface	Name	Type ▲	Interface Type	Description	Interface Labels	Shutd
	✎	Nu0	Null0	other	-	Null0	Nu0	-
□	✎	Vl50	Vlan50	propVirtual	Catalyst VLAN	-	Vl50	No
□	✎	Vl51	Vlan51	propVirtual	Catalyst VLAN	-	Vl51	No
□	✎	Vl59	Vlan59	propVirtual	Catalyst VLAN	-	Vl59	No
□	✎	Vl50	Vlan50	propVirtual	Catalyst VLAN	Vlan50	Vl50	No
	✎	Vl1	Vlan1	propVirtual	Catalyst VLAN	Vlan1	Vl1	No
□	✎	Vl59	Vlan59	propVirtual	Catalyst VLAN	Vlan59	Vl59	No
□	✎	Vl51	Vlan51	propVirtual	Catalyst VLAN	Vlan51	Vl51	No
	✎	Vl1	Vlan1	propVirtual	Catalyst VLAN	-	Vl1	No

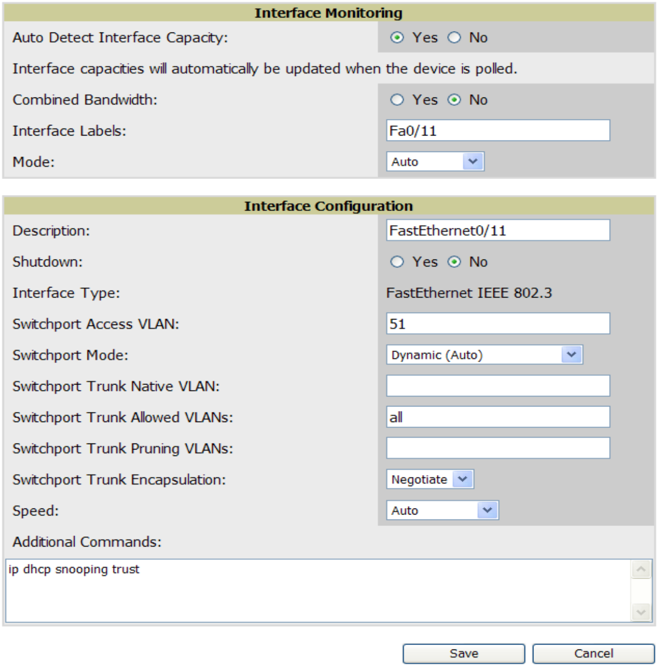
1-9 ▾ of 9 Interfaces   Page 1 ▾ of 1
Select All - Unselect All
Delete
Import Interfaces

You can view details for each interface on a wired device from its individual interface page as well. For details, see "Understanding the APs/Devices > Interfaces Page" on page 129.

You can configure interface settings individually or in groups. For individual settings, select the pencil icon next the interface name in **AP/Devices > Interfaces**.

This takes you to the **Interfaces Monitoring and Configuration** window which has a slightly different appearance depending on whether you are configuring a physical or virtual interface, as shown in Figure 99 and Figure 100.

Figure 99 ***Physical Interfaces Monitoring and Configuration** Sections*



Interface Monitoring

Auto Detect Interface Capacity:	● Yes ○ No
Interface capacities will automatically be updated when the device is polled.	
Combined Bandwidth:	○ Yes ● No
Interface Labels:	Fa0/11
Mode:	Auto

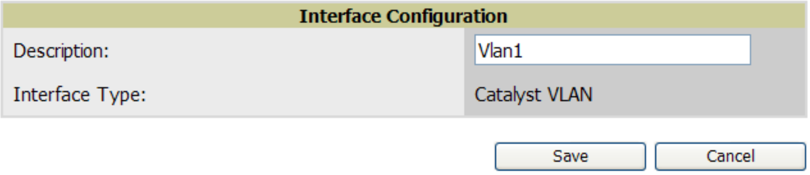
Interface Configuration

Description:	FastEthernet0/11
Shutdown:	○ Yes ● No
Interface Type:	FastEthernet IEEE 802.3
Switchport Access VLAN:	51
Switchport Mode:	Dynamic (Auto)
Switchport Trunk Native VLAN:	
Switchport Trunk Allowed VLANs:	all
Switchport Trunk Pruning VLANs:	
Switchport Trunk Encapsulation:	Negotiate
Speed:	Auto

Additional Commands:

```
ip dhcp snooping trust
```

Figure 100 ***Virtual Individual Interfaces Configuration*** *Section*

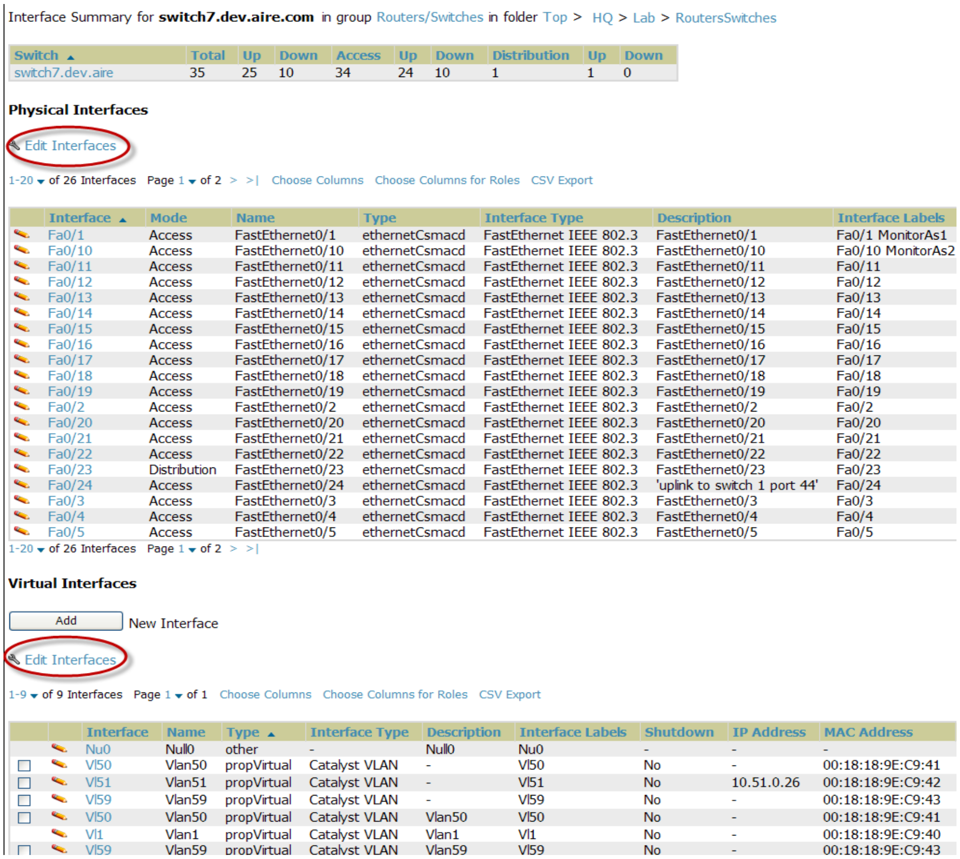


Interface Configuration

Description:	Vlan1
Interface Type:	Catalyst VLAN

To configure interfaces as a group, select **Edit Interfaces** above the Physical or Virtual Interfaces table as shown in Figure 101.

Figure 101 *Edit Multiple Interfaces*



Interface Summary for **switch7.dev.aire.com** in group Routers/Switches in folder Top > HQ > Lab > RoutersSwitches

Switch ▲	Total	Up	Down	Access	Up	Down	Distribution	Up	Down
switch7.dev.aire	35	25	10	34	24	10	1	1	0

Physical Interfaces

Edit Interfaces

1-20 ▾ of 26 Interfaces Page 1 ▾ of 2 > >| Choose Columns Choose Columns for Roles CSV Export

Interface ▲	Mode	Name	Type	Interface Type	Description	Interface Labels
Fa0/1	Access	FastEthernet0/1	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/1	Fa0/1 MonitorAs1
Fa0/10	Access	FastEthernet0/10	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/10	Fa0/10 MonitorAs2
Fa0/11	Access	FastEthernet0/11	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/11	Fa0/11
Fa0/12	Access	FastEthernet0/12	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/12	Fa0/12
Fa0/13	Access	FastEthernet0/13	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/13	Fa0/13
Fa0/14	Access	FastEthernet0/14	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/14	Fa0/14
Fa0/15	Access	FastEthernet0/15	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/15	Fa0/15
Fa0/16	Access	FastEthernet0/16	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/16	Fa0/16
Fa0/17	Access	FastEthernet0/17	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/17	Fa0/17
Fa0/18	Access	FastEthernet0/18	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/18	Fa0/18
Fa0/19	Access	FastEthernet0/19	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/19	Fa0/19
Fa0/2	Access	FastEthernet0/2	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/2	Fa0/2
Fa0/20	Access	FastEthernet0/20	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/20	Fa0/20
Fa0/21	Access	FastEthernet0/21	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/21	Fa0/21
Fa0/22	Access	FastEthernet0/22	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/22	Fa0/22
Fa0/23	Distribution	FastEthernet0/23	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/23	Fa0/23
Fa0/24	Access	FastEthernet0/24	ethernetCsmacd	FastEthernet IEEE 802.3	'uplink to switch 1 port 44'	Fa0/24
Fa0/3	Access	FastEthernet0/3	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/3	Fa0/3
Fa0/4	Access	FastEthernet0/4	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/4	Fa0/4
Fa0/5	Access	FastEthernet0/5	ethernetCsmacd	FastEthernet IEEE 802.3	FastEthernet0/5	Fa0/5

1-20 ▾ of 26 Interfaces Page 1 ▾ of 2 > >|

Virtual Interfaces

Add New Interface

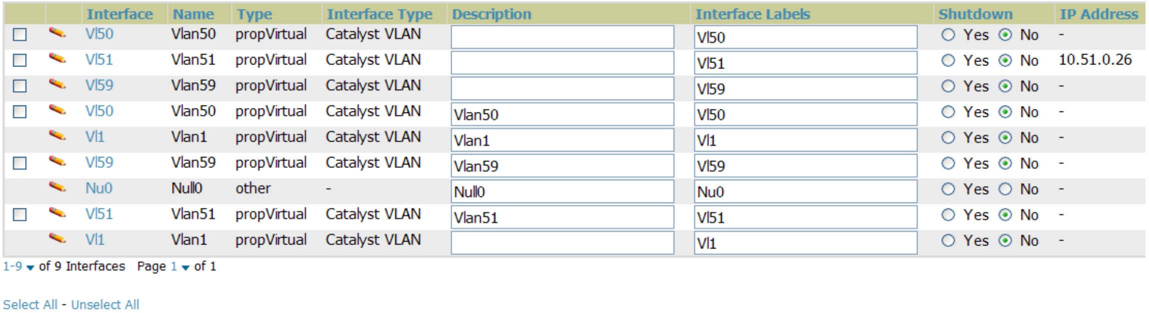
Edit Interfaces

1-9 ▾ of 9 Interfaces Page 1 ▾ of 1 Choose Columns Choose Columns for Roles CSV Export

	Interface	Name	Type ▲	Interface Type	Description	Interface Labels	Shutdown	IP Address	MAC Address
	Nu0	Null0	other	-	Null0	Nu0	-	-	-
□	Vl50	Vlan50	propVirtual	Catalyst VLAN	-	Vl50	No	-	00:18:18:9E:C9:41
□	Vl51	Vlan51	propVirtual	Catalyst VLAN	-	Vl51	No	10.51.0.26	00:18:18:9E:C9:42
□	Vl59	Vlan59	propVirtual	Catalyst VLAN	-	Vl59	No	-	00:18:18:9E:C9:43
□	Vl50	Vlan50	propVirtual	Catalyst VLAN	Vlan50	Vl50	No	-	00:18:18:9E:C9:41
	Vl1	Vlan1	propVirtual	Catalyst VLAN	Vlan1	Vl1	No	-	00:18:18:9E:C9:40
□	Vl59	Vlan59	propVirtual	Catalyst VLAN	Vlan59	Vl59	No	-	00:18:18:9E:C9:43

You will remain on the same page, but will have the option to make changes to the most commonly edited settings in batch mode, as shown in Figure 102.

Figure 102 *Multiple Interface Editing Page Illustration*



	Interface	Name	Type	Interface Type	Description	Interface Labels	Shutdown	IP Address
□	Vl50	Vlan50	propVirtual	Catalyst VLAN		Vl50	○ Yes ● No	-
□	Vl51	Vlan51	propVirtual	Catalyst VLAN		Vl51	○ Yes ● No	10.51.0.26
□	Vl59	Vlan59	propVirtual	Catalyst VLAN		Vl59	○ Yes ● No	-
□	Vl50	Vlan50	propVirtual	Catalyst VLAN	Vlan50	Vl50	○ Yes ● No	-
	Vl1	Vlan1	propVirtual	Catalyst VLAN	Vlan1	Vl1	○ Yes ● No	-
□	Vl59	Vlan59	propVirtual	Catalyst VLAN	Vlan59	Vl59	○ Yes ● No	-
	Nu0	Null0	other	-	Null0	Nu0	○ Yes ○ No	-
□	Vl51	Vlan51	propVirtual	Catalyst VLAN	Vlan51	Vl51	○ Yes ● No	-
	Vl1	Vlan1	propVirtual	Catalyst VLAN		Vl1	○ Yes ● No	-

1-9 ▾ of 9 Interfaces Page 1 ▾ of 1

Select All - Unselect All

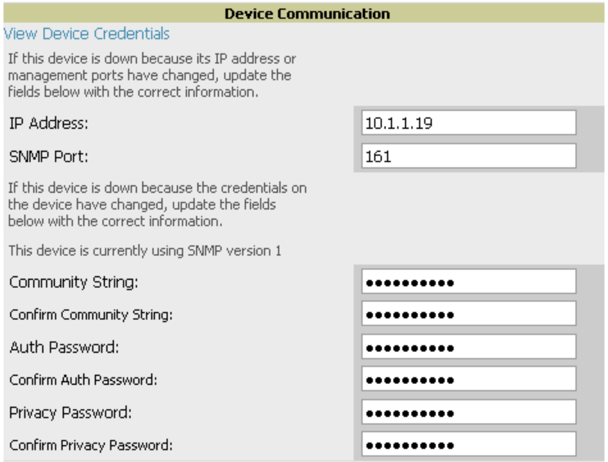
OV3600 assembles the entire running configuration using templates and your modifications to these pages. For a more detailed discussion on the use of templates, see Chapter 6, “Creating and Using Templates” on page 147.

Individual Device Support and Firmware Upgrades

Perform the following steps to configure AP communication settings for individual device types.

1. Locate the **Device Communication** area on the **APs/Devices > Manage** page.
2. Specify the credentials to be used to manage the AP. Figure 103 illustrates this page.

Figure 103 ***APs/Devices > Manage > Device Communication***



Device Communication

View Device Credentials

If this device is down because its IP address or management ports have changed, update the fields below with the correct information.

IP Address: 10.1.1.19

SNMP Port: 161

If this device is down because the credentials on the device have changed, update the fields below with the correct information.

This device is currently using SNMP version 1

Community String: ••••••••••

Confirm Community String: ••••••••••

Auth Password: ••••••••••

Confirm Auth Password: ••••••••••

Privacy Password: ••••••••••

Confirm Privacy Password: ••••••••••

NOTE

The **Device Communication** area may appear slightly different depending on the particular vendor and model of the APs being used.

3. Enter and confirm the appropriate **Auth Password** and **Privacy Password**.
4. You can disable the **View AP Credentials** link in OV3600 by the root user. Contact Alcatel support for detailed instructions to disable the link.
5. (Optional.) Enter the appropriate SSH and Telnet credentials if you are configuring Dell, Alcatel-Lucent or any Cisco device except Cisco WLAN controllers.
6. Select **Apply**, then **Confirm Edit** to apply the changes to the AP immediately, **Schedule** to schedule the changes during a specific time, or **Cancel** to return to **APs/Devices > Manage**.

NOTE

Some AP configuration changes may require the AP to be rebooted. Use the **Schedule** function to schedule these changes to occur at a time when WLAN users will not be affected.

Select **Update Firmware** to upgrade the device's firmware. Figure 104 illustrates this page and Table 86 describes the settings and default values.

NOTE

Note that for Alcatel-Lucent firmware upgrades, OV3600 does not check whether a device is in **Master** or **Local** configuration, and it does not schedule rebooting after the upgrade. OV3600 users should consult Alcatel-Lucent’s best practices for firmware upgrades and plan their upgrades using OV3600 accordingly.

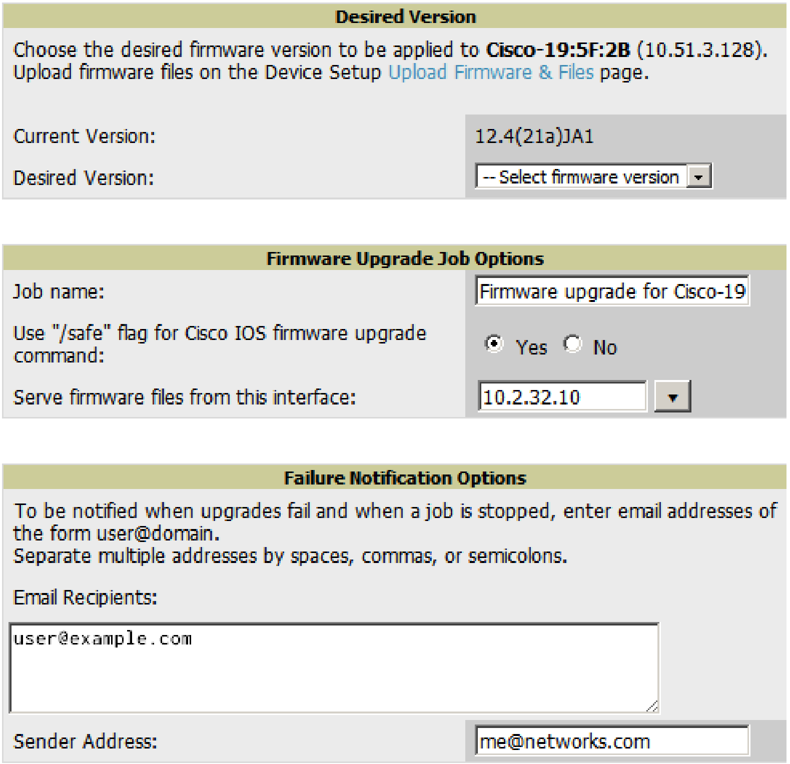
Table 86 ***APs/Devices > Manage Firmware Upgrades*** *Fields and Default Values*

Setting	Default	Description
Desired Version	None	Specifies the firmware to be used in the upgrade. Firmware can be added to this drop-down menu on the **Device Setup > Firmware Files** page.
Job Name	None	Sets a user-defined name for the upgrade job. Alcatel-Lucent recommends using a meaningful and descriptive name.

Table 86 *APs/Devices > Manage Firmware Upgrades Fields and Default Values (Continued)*

Setting	Default	Description
Use "/safe" flag for Cisco IOS firmware upgrade command	No	Enables or disables the /safe flag when upgrading IOS APs. The /**safe** flag must be disabled on older APs for the firmware file to fit in flash memory.
Email Recipients	None	Displays a list of email addresses that should receive alert emails if a firmware upgrade fails.
Sender Address	None	Displays the **From** address in the alert email.

Figure 104 *APs/Devices > Manage Firmware Upgrades*



Desired Version

Choose the desired firmware version to be applied to **Cisco-19:5F:2B** (10.51.3.128).
Upload firmware files on the Device Setup Upload Firmware & Files page.

Current Version: 12.4(21a)JA1

Desired Version: -- Select firmware version ▾

Firmware Upgrade Job Options

Job name: Firmware upgrade for Cisco-19

Use "/safe" flag for Cisco IOS firmware upgrade command: ● Yes ○ No

Serve firmware files from this interface: 10.2.32.10 ▾

Failure Notification Options

To be notified when upgrades fail and when a job is stopped, enter email addresses of the form user@domain.
Separate multiple addresses by spaces, commas, or semicolons.

Email Recipients:

user@example.com

Sender Address: me@networks.com

Troubleshooting a Newly Discovered Device with Down Status

If the device status on the **APs/Devices > List** page remains **Down** after it has been added to a group, the most likely source of the problem is an error in the SNMP community string being used to manage the device. Perform the following steps to troubleshoot this scenario.

1. Select the **Name** of the down device in the list of devices on the **APs/Devices > List** page. This automatically directs you to the **APs/Device > Monitor** page for that device.
2. Locate the **Status** field in the **Device Info** section. If the Status is **Down**, it includes a description of the cause of the problem. Some of the common system messages are as follows in Table 87:

Table 87 *Common System Messages for Down Status*

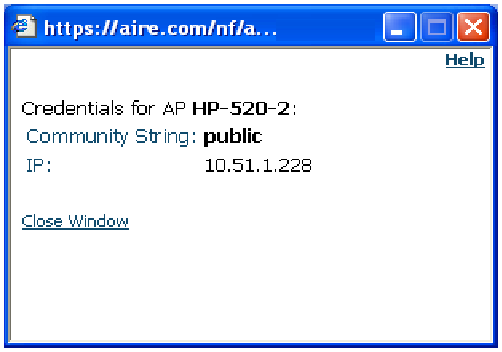
Message	Meaning
SNMP Get Failed	An incorrect SNMP community string or incorrect SNMP port is specified. If SNMP is not enabled on the device, you will also receive this message. Some APs, including Cisco and Alcatel-Lucent devices, do not have SNMP enabled by default.
Telnet Error: command timed out	Telnet username and password specified for that device is incorrect, or an incorrect telnet port is specified.

Table 87 *Common System Messages for Down Status*

Message	Meaning
ICMP Ping Failed (after SNMP Get Failed)	The device is not responding on the network and is likely non-operational.

3. If the **SNMP Get Failed** message appears, select the **APs/Devices > Manage** tab to go to the management page for that device.
4. If visible, select the **View device credentials** link in the **Device Communications** section. This displays the credentials OV3600 is using unsuccessfully to communicate with the device. This link can be removed from OV3600 for security reasons by setting a flag in OV3600. Only users with root access to the OV3600 command line can show or hide this link. To disable this feature, please contact Alcatel support. . Figure 105 illustrates this page.

Figure 105 ***View device credentials*** *Window*



Credentials for AP **HP-520-2**:
Community String: **public**
IP: 10.51.1.228

NOTE

The **View AP Credentials** message may appear slightly different depending on the vendor and model.

5. If the credentials are incorrect, return to the **Device Communications** area on the **APs/Devices > Manage** page.
6. Enter the appropriate credentials, and select **Apply**.
7. Return to the **APs/Devices > List** page to see if the device appears with a Status of **Up**.

Setting up Alcatel-Lucent Spectrum Analysis in OV3600

Overview of Spectrum Analysis

The spectrum analysis software modules on Alcatel-Lucent AP models AP-105, RAP-5WN, the AP-12x and the AP-90 Series can examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources.

The spectrum analyzer is used in conjunction with Alcatel-Lucent's Adaptive Radio Management (ARM) technology. While the spectrum analyzer identifies and classifies Wi-Fi and non-Wi-Fi sources of interference, ARM automatically ensures that APs serving clients will stay clear of interference.

Individual APs or groups of APs can be converted to dedicated spectrum monitors through the dot11a and dot11g radio profiles of that AP or AP group, or through a special spectrum override profile.

Each 802.11a and 802.11g radio profile references a spectrum profile, which identifies the spectrum band the radio will monitor and analyze, and defines the default ageout times for each monitored device type. By default, an 802.11a radio profile references a spectrum profile named **default-a** (which configures the radio to monitor the upper channels of the 5 GHz radio band), and an 802.11g radio profile references a spectrum profile named **default-g** (which configures the radio to monitor all channels the 2.4 GHz radio band).

Most interference will occur in the 2.4 GHz radio band.

For more information about Spectrum analysis as well as ARM technology, refer to the *AOS-W 6.0 User Guide.*

Spectrum Configurations and Prerequisites

The following prerequisites must be in place to configure an AP to run in spectrum mode in OV3600:

- The AP must be in **Manage Read/Write** mode.
- The AP's associated switch must have an RFprotect license, and must be running AOS-W 6.0 or later.
- Alcatel-Lucent GUI Config must be enabled for that AP's group in the **Groups > Basic** page.

There are three main situations in which you would set one or more devices to Spectrum mode in OV3600:

- Alcatel-Lucent AP Groups running permanently with the default Spectrum profile
- Individual APs running temporarily in Spectrum mode while part of an Alcatel-Lucent AP Group set to ap-mode
- Switch-level Spectrum Overrides (an alternative to creating new Alcatel-Lucent AP groups or new radio profiles for temporary changes)

Setting up a Permanent Spectrum Alcatel-Lucent AP Group

If you have multiple supported Alcatel-Lucent APs in multiple switches that you want to run in Spectrum mode over the long run, you create a special Alcatel-Lucent AP group and set up a profile that is set to **spectrum-mode** and references the default **Spectrum** profile. Set up more than one profile if you want to utilize both radio bands in Spectrum mode.

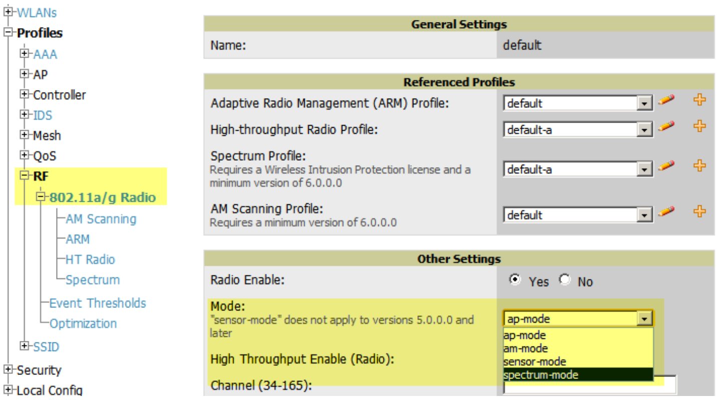
If you use an 802.11a or 802.11g radio profile to create a group of spectrum monitors, all APs in any AP group referencing that radio profile will be set to spectrum mode. Therefore, best practices are to create a new 802.11a or 802.11g radio profile just for spectrum monitors.

If you have Global Alcatel-Lucent Configuration enabled in **OV3600 Setup > General**, create the configuration below, then go to the switch's group's **Alcatel-Lucent Config** page and select the newly created Alcatel-Lucent AP Group.

Perform these steps to set the AP group to use the default Spectrum profile settings:

1. In **Groups > Alcatel-Lucent Config**, select **Add New Alcatel-Lucent AP Group**.
2. Give the new Group a name (like "Spectrum APs") and select the plus sign next to the **802.11a Radio Profile** to create a new radio profile.
3. Enter a name under the General Settings section of **Profiles > RF > 802.11a/g Radio**.
4. In the **Other Settings** section, change the **Mode** field from ap-mode to **spectrum-mode, as illustrated in** Figure 106. Then select **Save**.

Figure 106 *Spectrum mode in Alcatel-Lucent Config*



General Settings

Name: default

Referenced Profiles

Adaptive Radio Management (ARM) Profile: default

High-throughput Radio Profile: default-a

Spectrum Profile: default-a
Requires a Wireless Intrusion Protection license and a minimum version of 6.0.0.0

AM Scanning Profile: default
Requires a minimum version of 6.0.0.0

Other Settings

Radio Enable: ● Yes ○ No

Mode: ap-mode
"sensor-mode" does not apply to versions 5.0.0.0 and later

High Throughput Enable (Radio):

Channel (34-165):

The above steps will use the defaults in the referenced **Spectrum Profile**. To change the defaults, navigate to **Groups > Alcatel-Lucent Config > Profiles > RF > 802.11a/g Radio > Spectrum** and create a new Spectrum profile with non-default settings. In most cases, it is not recommended to change the settings in the default profile.

If all of the devices in this Alcatel-Lucent AP Group are managed by the same switch and you want to temporarily override one or more profile settings in your spectrum-mode APs, you can set up a switch override.

To disable spectrum mode in this group, change the referenced radio profile back to **default**.

Configuring an Individual AP to run in Spectrum Mode

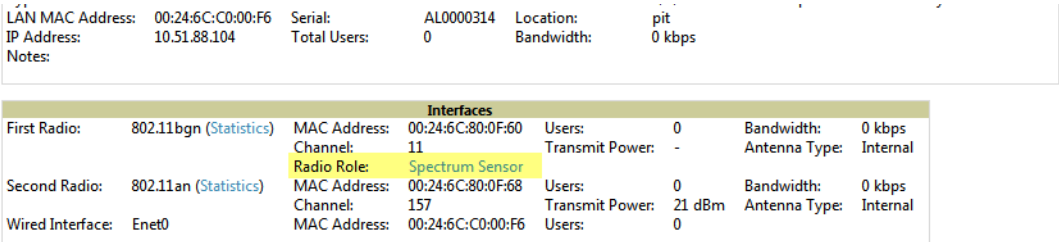
If you want to temporarily set an individual radio in an AP to run in Spectrum mode without creating or changing Alcatel-Lucent AP Groups or radio profiles, perform these steps to set up a Spectrum Override on a supported Alcatel-Lucent AP:

1. Go to the **APs/Devices > Manage** page for a Spectrum-supported Alcatel-Lucent AP (-105, -120, -90).
2. After checking the Audit page, set the AP to **Manage Read/Write** mode.
3. Select **Yes** on the **Spectrum Override** field for one or both radios, depending on the band and channels you want it to analyze.
4. Select the band that should run in spectrum. If you selected the 5GHz band in the 802.11an Radio section, choose the lower, middle, or upper range of channels that you want to be analyzed by this radio.
5. Select **Save and Apply** and confirm your edit.

This overrides the current **Mode** setting for that AP (ap-mode or am-mode).

After making this change, you can view the new **Radio Role** field that will appear in the **Interfaces** section of the **APs/Devices > Monitor** page, as illustrated in Figure 107.

Figure 107 *Spectrum Sensor Link in Interfaces Section of an AP*

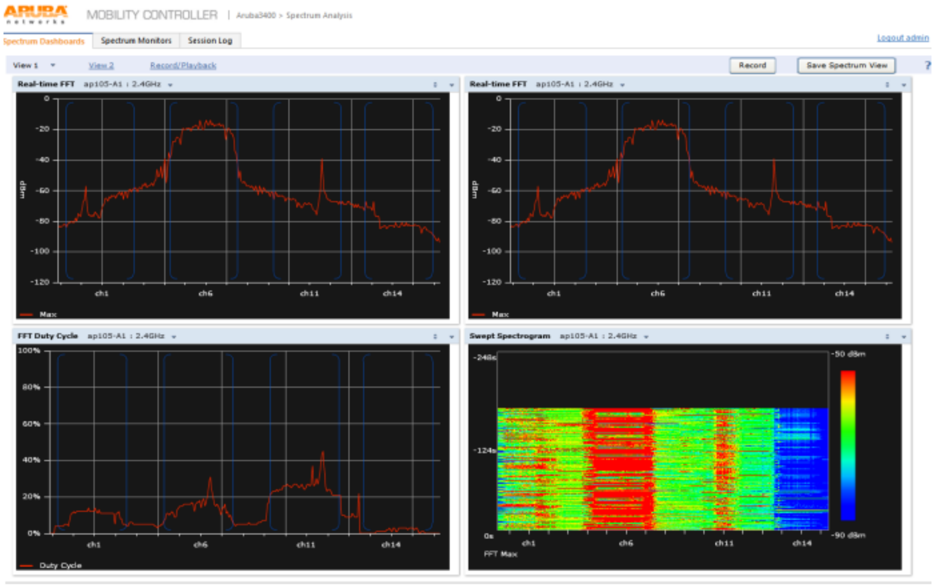


LAN MAC Address:	00:24:6C:C0:00:F6	Serial:	AL0000314	Location:	pit
IP Address:	10.51.88.104	Total Users:	0	Bandwidth:	0 kbps
Notes:					

Interfaces									
First Radio:	802.11bgn (Statistics)	MAC Address:	00:24:6C:80:0F:60	Users:	0	Bandwidth:	0 kbps
		Channel:	11	Transmit Power:	-	Antenna Type:	Internal
		Radio Role:	Spectrum Sensor				
Second Radio:	802.11an (Statistics)	MAC Address:	00:24:6C:80:0F:68	Users:	0	Bandwidth:	0 kbps
		Channel:	157	Transmit Power:	21 dBm	Antenna Type:	Internal
Wired Interface:	Enet0	MAC Address:	00:24:6C:C0:00:F6	Users:	0		

The new role, Spectrum Sensor, is a link to the Spectrum Analysis page for the switch that manages this AP, as illustrated in Figure 108.

Figure 108 *Spectrum Analysis on Switch Dashboard*

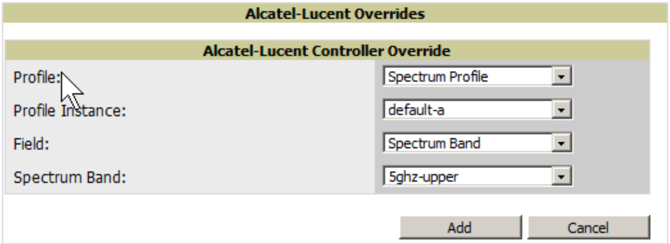


To disable Spectrum mode on this individual AP after it has collected data, return to the **APs/Devices > Manage** page for this AP and set the **Spectrum Override** field back to **No**.

Configuring a Switch to use the Spectrum Profile

You can use OV3600 to customize individual fields in the profile instance used by a particular switch without having to create a new Alcatel-Lucent AP groups and new radio profiles. To do this, you can set a switch-level override for its referenced Spectrum profile, as illustrated in Figure 109. This will affect all Spectrum-supported APs managed by this switch.

Figure 109 *Override Section of a Supported Switch's Manage Page*



Alcatel-Lucent Overrides

Alcatel-Lucent Controller Override

Profile:	Spectrum Profile
Profile Instance:	default-a
Field:	Spectrum Band
Spectrum Band:	5ghz-upper

Perform these steps to override individual profile settings for an Alcatel-Lucent switch:

1. Select a Spectrum-supported Alcatel-Lucent switch that is referencing a Spectrum profile, and go to its **APs/Devices > Manage** page. Set it to **Manage Read/Write** mode.
2. Under the **Alcatel-Lucent Overrides** section, select **Add New Alcatel-Lucent Controller Override**.
3. In the **Profile** drop-down menu, select the **Spectrum Profile** type.
4. In the **Profile Instance** drop-down menu, select the instance of the Spectrum profile being used by the switch.
5. In the **Field** drop-down menu, select the setting you would like to change (such as an Age-Out setting or a Spectrum Band), and enter the overriding value below it.
6. Select **Add** to save your changes.
7. To create more overrides for this switch, select **Add New Alcatel-Lucent Controller Override** again.
8. When you have finished, select **Save and Apply**.

You can also use the above procedure to turn on Spectrum mode for radio profiles on one particular switch, or use the overrides to point your radio profile to a non-default Spectrum profile for just this switch.

Chapter 6

Creating and Using Templates

This chapter provides an overview and several tasks supporting the use of device configuration templates in OV3600, and contains the following topics:

- "Group Templates" on page 147
- "Viewing and Adding Templates" on page 148
- "Configuring General Template Files and Variables" on page 151
- "Configuring Cisco IOS Templates" on page 156
- "Configuring Cisco Catalyst Switch Templates" on page 159
- "Configuring Symbol Controller / HP WESM Templates" on page 159
- "Configuring a Global Template" on page 161

Group Templates

Supported Device Templates

Templates are helpful configuration tools that allow OV3600 to manage virtually all device settings. A template uses variables to adjust for minor configuration differences between devices.

The **Groups > Templates** configuration page allows you to create configuration templates for the following types of devices:

- Dell PowerConnect W
- Aruba
- Alcatel-Lucent

NOTE

Alcatel-Lucent recommends using the graphical Alcatel-Lucent Config feature in support of Alcatel-Lucent devices, particularly for AOS-W 3.3.2.x and later. Refer to the *Alcatel-Lucent Configuration Guide* for additional information.

- Cisco Aironet IOS and 4800 autonomous APs
- Cisco Catalyst switches
- HP ProCurve 530 and WeSM controllers
- Nomadix
- Symbol
- Trapeze
  - 3Com
  - Nortel
  - Enterasys

Template Variables

Variables in templates configure device-specific properties, such as name, IP address and channel. Variables can also be used to configure group-level properties, such as SSID and RADIUS server, which may differ from one group to the next. The OV3600 template understands many variables including the following:

- `%ap_include_1% through %ap_include_10%`
- `%channel%`
- `%hostname%`
- `%ip_address%`
- `%ofdmpower%`

The variable settings correspond to device-specific values on the **APs/Devices > Manage** configuration page for the specific AP that is getting configured.

NOTE

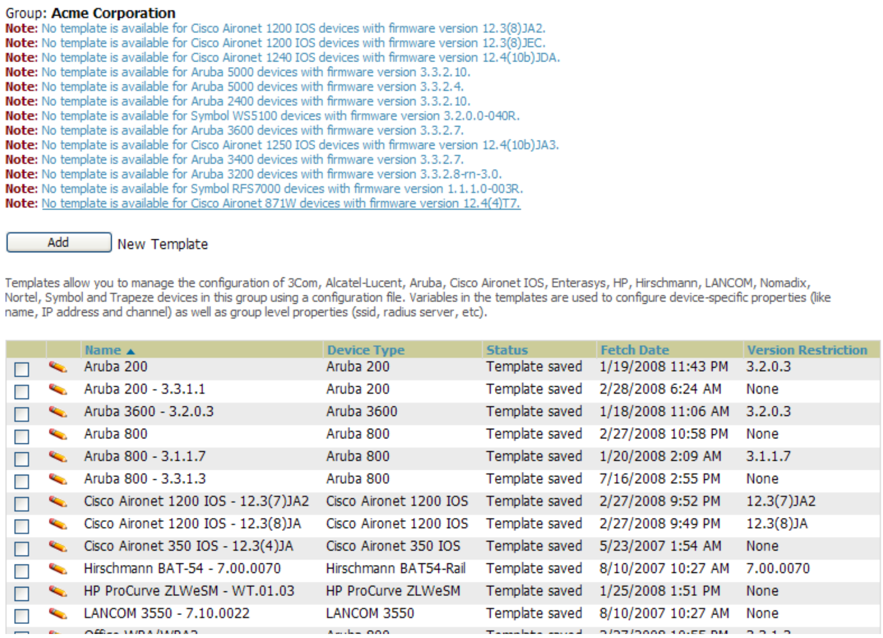
Changes made on the other **Group** pages (Radio, Security, VLANs, SSIDs, and so forth) are not applied to any APs that are configured by templates.

Viewing and Adding Templates

Perform these steps to display, add, or edit templates.

1. Go to the **Groups > List** page, and select a group for which to add or edit templates. This can be a new group, created with the **Add** button, or you can edit an existing group by selecting the corresponding pencil icon. The **Groups > Basic** page for that group appears.Additional information about adding and editing groups is described in "Configuring and Using Device Groups in OV3600" on page 69.
2. From the OV3600 navigation pane, select **Templates**. The **Templates** page appears. Figure 110 illustrates the **Groups > Templates** configuration page, and Table 88 describes the columns.

Figure 110 ***Groups > Templates*** *Page Illustration for a Sample Device Group*



Group: **Acme Corporation**

Note: No template is available for Cisco Aironet 1200 IOS devices with firmware version 12.3(8)JA2.
Note: No template is available for Cisco Aironet 1200 IOS devices with firmware version 12.3(8)JEC.
Note: No template is available for Cisco Aironet 1240 IOS devices with firmware version 12.4(10b)JDA.
Note: No template is available for Aruba 5000 devices with firmware version 3.3.2.10.
Note: No template is available for Aruba 5000 devices with firmware version 3.3.2.4.
Note: No template is available for Aruba 2400 devices with firmware version 3.3.2.10.
Note: No template is available for Symbol WS5100 devices with firmware version 3.2.0.0-040R.
Note: No template is available for Aruba 3600 devices with firmware version 3.3.2.7.
Note: No template is available for Cisco Aironet 1250 IOS devices with firmware version 12.4(10b)JA3.
Note: No template is available for Aruba 3400 devices with firmware version 3.3.2.7.
Note: No template is available for Aruba 3200 devices with firmware version 3.3.2.8-rn-3.0.
Note: No template is available for Symbol RFS7000 devices with firmware version 1.1.1.0-003R.
Note: No template is available for Cisco Aironet 871W devices with firmware version 12.4(4)T7.

Templates allow you to manage the configuration of 3Com, Alcatel-Lucent, Aruba, Cisco Aironet IOS, Enterasys, HP, Hirschmann, LANCOM, Nomadix, Nortel, Symbol and Trapeze devices in this group using a configuration file. Variables in the templates are used to configure device-specific properties (like name, IP address and channel) as well as group level properties (ssid, radius server, etc).

		Name ▲	Device Type	Status	Fetch Date	Version Restriction
□	✎	Aruba 200	Aruba 200	Template saved	1/19/2008 11:43 PM	3.2.0.3
□	✎	Aruba 200 - 3.3.1.1	Aruba 200	Template saved	2/28/2008 6:24 AM	None
□	✎	Aruba 3600 - 3.2.0.3	Aruba 3600	Template saved	1/18/2008 11:06 AM	3.2.0.3
□	✎	Aruba 800	Aruba 800	Template saved	2/27/2008 10:58 PM	None
□	✎	Aruba 800 - 3.1.1.7	Aruba 800	Template saved	1/20/2008 2:09 AM	3.1.1.7
□	✎	Aruba 800 - 3.3.1.3	Aruba 800	Template saved	7/16/2008 2:55 PM	None
□	✎	Cisco Aironet 1200 IOS - 12.3(7)JA2	Cisco Aironet 1200 IOS	Template saved	2/27/2008 9:52 PM	12.3(7)JA2
□	✎	Cisco Aironet 1200 IOS - 12.3(8)JA	Cisco Aironet 1200 IOS	Template saved	2/27/2008 9:49 PM	12.3(8)JA
□	✎	Cisco Aironet 350 IOS - 12.3(4)JA	Cisco Aironet 350 IOS	Template saved	5/23/2007 1:54 AM	None
□	✎	Hirschmann BAT-54 - 7.00.0070	Hirschmann BAT54-Rail	Template saved	8/10/2007 10:27 AM	7.00.0070
□	✎	HP ProCurve ZLWeSM - WT.01.03	HP ProCurve ZLWeSM	Template saved	1/25/2008 1:51 PM	None
□	✎	LANCOM 3550 - 7.10.0022	LANCOM 3550	Template saved	8/10/2007 10:27 AM	None

Table 88 ***Groups > Templates*** *Fields and Default Values*

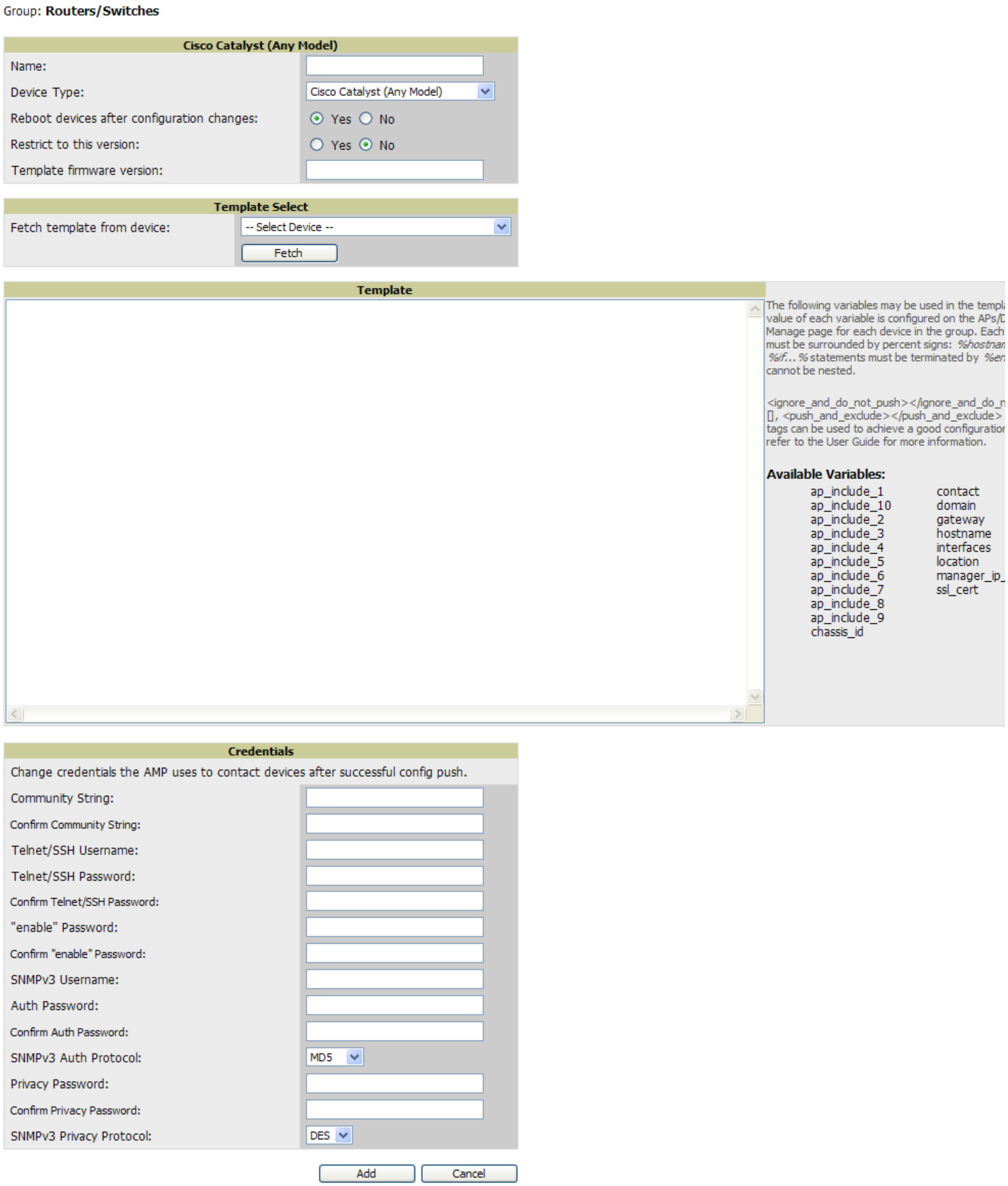
Setting	Description
Notes	When applicable, this section lists devices that are active on the network with no template available for the respective firmware. Select the link from such a note to launch the **Add Template** configuration page for that device.
Name	Displays the template name.

Table 88 ***Groups > Templates*** *Fields and Default Values (Continued)*

Setting	Description
Device Type	Displays the template that applies to APs or devices of the specified type. If **vendor (Any Model)** is selected, the template applies to all models from that vendor that do not have a version specific template defined. If there are two templates that might apply to a device, the template with the most restrictions takes precedence.
Status	Displays the status of the template.
Fetch Date	Sets the date that the template was originally fetched from a device.
Version Restriction	Designates that the template only applies to APs running the version of firmware specified. If the restriction is **None**, then the template applies to all the devices of the specified type in the group. If there are two templates that might apply to a device the template with the most restrictions takes precedence. If there is a template that matches a devices firmware it will be used instead of a template that does not have a version restriction.

3. To create a new template and add it to the OV3600 template inventory, go to the **Groups > List** page, and select the group to which you will apply the template. Select the group name, and the **Details** page appears. Select **Templates**, then **Add**.
4. Complete the configurations illustrated in Figure 111, and the settings described in Table 89.

Figure 111 ***Groups > Templates > Add Template*** *Page Illustration*



Group: **Routers/Switches**

Cisco Catalyst (Any Model)

Name:	
Device Type:	Cisco Catalyst (Any Model)
Reboot devices after configuration changes:	● Yes ○ No
Restrict to this version:	○ Yes ● No
Template firmware version:	

Template Select

Fetch template from device:	-- Select Device -- Fetch

Template

The following variables may be used in the templa
value of each variable is configured on the APs/D
Manage page for each device in the group. Each
must be surrounded by percent signs: *%hostnan*
%if... % statements must be terminated by *%en*
cannot be nested.

<ignore_and_do_not_push></ignore_and_do_n
[], <push_and_exclude></push_and_exclude>
tags can be used to achieve a good configuration
refer to the User Guide for more information.

Available Variables:

ap_include_1	contact
ap_include_10	domain
ap_include_2	gateway
ap_include_3	hostname
ap_include_4	interfaces
ap_include_5	location
ap_include_6	manager_ip_
ap_include_7	ssl_cert
ap_include_8	
ap_include_9	
chassis_id	

Credentials

Change credentials the AMP uses to contact devices after successful config push.

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

Table 89 ***Groups > Templates > Add Template*** *Fields and Default Values*

Setting	Default	Description
Use Global Template	No	Uses a global template that has been previously configured on the **Groups > Templates** configuration page. Available templates will appear in the drop-down menu. If **Yes** is selected you can also configure global template variables. For Symbol devices you can select the groups of thin APs to which the template should be applied. For more information about global templates, see the **Groups > Templates** section of the *User Guide*.

Table 89 *Groups > Templates > Add Template Fields and Default Values (Continued)*

Setting	Default	Description
Fetch	None	Selects an AP from which to fetch a configuration. The configuration will be turned into a template with basic AP specific settings like channel and power turned into variables. The variables are filled with the data on the **APs/Devices > Manage** configuration page for each AP.
Name	None	Defines the template display name.
AP Type	Cisco IOS (Any Model)	Determines that the template applies to APs or devices of the specified type. If **Cisco IOS (Any Model)** is selected, the template applies to all IOS APs that do not have a version specific template specified.
Reboot APs After Configuration Changes	No	Determines reboot when OV3600 applies the template, copied from the new configuration file to the startup configuration file on the AP. If **No** is selected, OV3600 uses the AP to merge the startup and running configurations. If **Yes** is selected, the configuration is copied to the startup configuration file and the AP is rebooted. This field is only visible for some devices.
Restrict to this version	No	Restricts the template to APs of the specified firmware version. If **Yes** is selected, the template only applies to APs on the version of firmware specified in the **Template Firmware Version** field.
Template firmware version	None	Designates that the template only applies to APs running the version of firmware specified.
Community String	None	If the template is updating the community strings on the AP, enter the new community string OV3600 should use here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
Telnet/SSH Username	None	If the template is updating the **Telnet/SSH Username** on the AP, enter the new username OV3600 should use here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
Telnet/SSH Password	None	If the template is updating the **Telnet/SSH password** on the AP, enter the new Telnet/SSH password OV3600 should use here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
"enable" Password	None	If the template is updating the enable password on the AP, enter the new enable password OV3600 should use here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Username	None	If the template is updating the **SNMP v3 Username** password on the AP, enter the new SNMP Username password here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
Auth Password	None	If the template is updating the **SNMP v3 Auth** password on the AP, enter the new SNMP Username password here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
Privacy Password	None	If the template is updating the **SNMP v3 Privacy** password on the AP, enter the new SNMP Username password here. OV3600 updates the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Auth Protocol	MD5	Specifies the **SNMPv3 Auth** protocol, either **MD5 or SHA-1**.
SNMPv3 Privacy Protocol	DES	Specifies the **SNMPv3 Privacy** protocol, either **DES or AES**.

Configuring General Template Files and Variables

This section describes the most general aspects of configuring AP device templates and the most common variables:

- Configuring General Templates
- Using Template Syntax
- Using Directives to Eliminate Reporting of Configuration Mismatches

- Using Conditional Variables in Templates
- Using Substitution Variables in Templates
- Using AP-Specific Variables

Configuring General Templates

Perform the following steps to configure Templates within a Group.

1. Select a Group to configure.

NOTE

Alcatel-Lucent recommends starting with a small group of access points and placing these APs in Monitor Only mode, which is read-only. Do this using the **Modify Devices** link until you are fully familiar with the template configuration process. This prevents configuration changes from being applied to the APs until you are sure you have the correct configuration specified.

2. Select an AP from the Group to serve as a *model* AP for the others in the Group. You should select a device that is configured currently with all the desired settings. If any APs in the group have two radios, make sure to select a model AP that has two radios and that both are configured in proper and operational fashion.
3. Go to the **Groups > Templates** configuration page. Select **Add** to add a new template.
4. Select the type of device that will be configured by this template.
5. Select the model AP from the drop-down list, and select **Fetch**.
6. OV3600 automatically attempts to replace some values from the configuration of that AP with *variables* to enable AP-specific options to be set on an AP-by-AP basis. Refer to "Using Template Syntax" on page 153

   These variables are always encapsulated between % signs. On the right side of the configuration page is the **Additional Variables** section. This section lists all available variables for your template. Variables that are in use in a template are green, while variables that are not yet in use are black. Verify these substitutions to ensure that all of the settings that you believe should be managed on an AP-by-AP basis are labeled as variables in this fashion. If you believe that any AP-level settings are not marked correctly, please contact Alcatel support before proceeding.
7. Specify the device types for the template. The templates only apply to devices of the specified type.
   - Specify whether OV3600 should reboot the devices after a configuration push. If the **Reboot Devices after Configuration Changes** option is selected, then OV3600 instructs the AP to copy the configuration from OV3600 to the startup configuration file of the AP and reboot the AP.
   - If the **Reboot Devices after Configuration Changes** option is not selected, then OV3600 instructs the AP to copy the configuration to the startup configuration file and then tell the AP to copy the startup configuration file to the running configuration file.
   - Alcatel-Lucent recommends using the **reboot** option when there are changes requiring reboot to take effect, for example, removing a new SSID from a Cisco IOS device. Copying the configuration from startup configuration file to running configuration file merges the two configurations and can cause undesired configuration lines to remain active on the AP.
8. Restrict the template to apply only to the specified version of firmware. If the template should only apply to a specific version of firmware, select Yes and enter the firmware version in the **Template Firmware Version** text field.
9. Select **Save and Apply** to push the configuration to all of the devices in the group. If the devices are in monitor-only mode (which is recommended while you are crafting changes to a template or creating a

new one), then OV3600 will audit the devices and compare their current configuration to the one defined in the template.

NOTE

If you set the reboot flag to **No**, then some changes could result in configuration mismatches until the AP is rebooted.

For example, changing the SSID on Cisco IOS APs requires the AP to be rebooted. Two other settings that require the AP to be rebooted for configuration change are Logging and NTP. A configuration mismatch results if the AP is not rebooted.

If logging and NTP service are not required according to the Group configuration, but are enabled on the AP, you would see a configuration file mismatch as follows if the AP is not rebooted:

IOS Configuration File Template:

```
…
(no logging queue-limit)
…
```

Device Configuration File on APs/Devices > Audit Configuration Page

```
…
    line con 0
    line vty 5 15
actual logging 10.51.2.1
actual logging 10.51.2.5
actual logging facility local6
actual logging queue-limit 100
actual logging trap debugging
    no service pad
actual ntp clock-period 2861929
actual ntp server 209.172.117.194
    radius-server attribute 32 include-in-access-req format %h
…
```

10. Once the template is correct and all mismatches are verified on the **AP Audit** configuration page, use the **Modify Devices** link on the **Groups > Monitor** configuration page to place the desired devices into **Management** mode. This removes the APs from Monitor mode (read-only) and instructs the AP to pull down its new startup configuration file from OV3600.

NOTE

Devices can be placed into Management mode individually from the **APs/Devices > Manage** configuration page.

Using Template Syntax

Template syntax is comprised of the following components, described in this section:

- Using AP-Specific Variables
- Using Directives to Eliminate Reporting of Configuration Mismatches
- Using Conditional Variables in Templates
- Using Substitution Variables in Templates

Using Directives to Eliminate Reporting of Configuration Mismatches

OV3600 is designed to audit AP configurations to ensure that the actual configuration of the access point exactly matches the Group template. When a configuration mismatch is detected, OV3600 generates an automatic alert and flags the AP as having a **Mismatched** configuration status on the user page.

However, when using the templates configuration function, there will be times when the running-config file and the startup-config file do not match under normal circumstances. For example, the `ntp clock-period` setting is almost never identical in the running-config file and the startup-config file. You can use directives such as **`<ignore_and_do_not_push>`** to customize the template to keep OV3600 from reporting mismatches for this type of variance.

OV3600 provides two types of directives that can be used within a template to control how OV3600 constructs the startup-config file to send to each AP and whether it reports variances between the running-config file and the startup-config file as "configuration mismatches." Lines enclosed in **<push_and_exclude>** are included in the AP startup-config file but OV3600 ignores them when verifying configurations. Lines enclosed in **<ignore_and_do_not_push>** cause OV3600 to ignore those lines during configuration verification.

Ignore_and_do_not_push Command

The `ignore and do not push` directive should typically be used when a value cannot be configured on the device, but always appears in the running-config file. Lines enclosed in the ignore and do not push directive will not be included in the startup-config file that is copied to each AP.

When OV3600 is comparing the running-config file to the startup-config file for configuration verification, it will ignore any lines in the running-config file that start with the text within the directive. Lines belonging to an ignored and unpushed line, the lines immediately below the line and indented, are ignored as well. In the example below, if you were to bracket NTP server, the NTP clock period would behave as if it were bracketed because it belongs or is associated with the NTP server line.

NOTE

The line <ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push> will cause lines starting with "ntp clock-period" to be ignored. However, the line <ignore_and_do_not_push>ntp </ignore_and_do_not_push> causes all lines starting with "ntp" to be ignored, so it is important to be as specific as possible.

Push_and_exclude Command

Instead of using the full tags you may use the parenthesis shorthand, (substring). The push and exclude directive is used to push commands to the AP that will not appear in the running-config file. For example, some **no** commands that are used to remove SSIDs or remove configuration parameters do not appear in the running-config file of a device. A command inside the push and exclude directive are included in the startup-config file pushed to a device, but OV3600 excludes them when calculating and reporting configuration mismatches.

NOTE

The opening tag may have leading spaces.

Below are some examples of using directives:

```
…
line con 0
 </push_and_exclude>no stopbits</push_and_exclude>
line vty 5 15
!
ntp server 209.172.117.194
<ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push>
end
```

Using Conditional Variables in Templates

Conditional variables allow lines in the template to be applied only to access points where the enclosed commands will be applicable and not to any other access points within the Group. For example, if a group of APs consists of dual-radio Cisco 1200 devices (802.11a/b) and single-radio Cisco 1100 (802.11b) devices, it is necessary to make commands related to the 802.11a device in the 1200 APs conditional. Conditional variables are listed in the table below.

The syntax for conditional variables is as follows, and syntax components are described in Table 90:

```
%if variable=value%
…
%endif%
```

Table 90 *Conditional Variable Syntax Components*

Variable	Values	Meaning
interface	Dot11Radio0	2.4GHz radio module is installed
	Dot11Radio1	5GHz external radio module is installed
radio_type	a	Installed 5GHz radio module is 802.11a
	b	Installed 2.4GHz radio module is 802.11b only
	g	Installed 2.4GHz radio module is 802.11g capable
wds_role	backup	The WDS role of the AP is the value selected in the dropdown menu on the **APs/Devices > Manage** configuration page for the device.
	client	
	master	
IP	Static	IP address of the device is set statically on the AP Manage configuration page.
	DHCP	IP address of the device is set dynamically using DHCP

Using Substitution Variables in Templates

Substitution variables are used to set AP-specific values on each AP in the group. It is obviously not desirable to set the IP address, hostname, and channel to the same values on every AP within a Group. The variables in Table 91 are substituted with values specified on each access point's **APs/Devices > Manage** configuration page within the **OV3600 User** page.

Sometimes, the running-config file on the AP does not include the command for one of these variables because the value is set to the default. For example, when the "transmission power" is set to maximum (the default), the line "power local maximum" will not appear in the AP running-config file, although it will appear in the startup-config file. OV3600 would typically detect and flag this variance between the running-config file and startup-config file as a configuration mismatch. To prevent OV3600 from reporting a configuration mismatch between the desired startup-config file and the running-config file on the AP, OV3600 suppresses the lines in the desired configuration when auditing the AP configuration (similar to the way OV3600 suppresses lines enclosed in parentheses, which is explained below). A list of the default values that causes lines to be suppressed when reporting configuration mismatches is shown in Table 91.

Table 91 *Substitution Variables in Templates*

Variable	Meaning	Command	Suppressed Default
hostname	Name	hostname %hostname%	-
channel	Channel	channel %channel%	-
ip_address **netmask**	IP address Subnet mask	ip address %ip_address% %netmask% or ip address dhcp …	
gateway	Gateway	ip default-gateway %gateway%	-
antenna_ receive	Receive antenna	antenna receive %antenna_receive%	diversity

Table 91 *Substitution Variables in Templates (Continued)*

Variable	Meaning	Command	Suppressed Default
antenna_transmit	Transmit antenna	antenna transmit %antenna_transmit%	diversity
cck_power	802.11g radio module CCK power level	power local cck %cck_power%	maximum
ofdm_power	802.11g radio module OFDM power level	power local ofdm %ofdm_power%	maximum
power	802.11a and 802.11b radio module power level	power local %power%	maximum
location	The location of the SNMP server.	snmp-server location %location%	-
contact	The SNMP server contact.	snmp-server contact %contact%	
certificate	The SSL Certificate used by the AP	%certificate%	-
ap include	The AP include fields allow for configurable variables. Any lines placed in the AP Include field on the **APs/Devices > Manage** configuration page replace this variable.	%ap_include_1% through %ap_include_10%	-
`chassis id`			
`domain`			
`interfaces`			
`location`			

Using AP-Specific Variables

When a template is applied to an AP all variables are replaced with the corresponding settings from the **APs/Devices > Manage** configuration page. This enables AP-specific settings (such as Channel) to be managed effectively on an AP-by-AP basis. The list of used and available variables appears on the template detail configuration page. Variables are always encapsulated between % signs. The following example illustrates this usage:

```
hostname %hostname%
…
interface Dot11Radio0
…
 power local cck %CCK_POWER%
 power local ofdm %OFDM_POWER%
 channel %CHANNEL%
…
```

The `hostname` line sets the AP hostname to the hostname stored in OV3600.

The `power` lines set the power local `cck` and `ofdm` values to the numerical values that are stored in OV3600.

Configuring Cisco IOS Templates

Cisco IOS access points have hundreds of configurable settings. OV3600 enables you to control them via the **Groups > Templates** configuration page. This page defines the startup-config file of the devices rather than using the OV3600 normal **Group** configuration pages. OV3600 no longer supports making changes for these devices via the browser-based page, but rather uses templates to configure all settings, including settings that were controlled formerly on the OV3600 **Group** configuration pages. Perform these steps to configure a Cisco IOS Template for use with one or more groups, and the associated devices.

This section includes the following topics:

- Applying Startup-config Files
- WDS Settings in Templates
- SCP Required Settings in Templates
- Supporting Multiple Radio Types via a Single IOS Template
- Configuring Single and Dual-Radio APs via a Single IOS Template

Applying Startup-config Files

OV3600 instructs each of the APs in the Group to copy its unique startup-config file from OV3600 via TFTP or SCP.

- If the **Reboot Devices after Configuration Changes** option is selected, then OV3600 instructs the AP to copy the configuration from OV3600 to the startup-config file of the AP and reboot the AP.
- If the **Reboot Devices after Configuration Changes** option is not selected, then OV3600 instructs the AP to copy the configuration to the startup-config file and then tell the AP to copy the startup config file to the running-config file. Use the reboot option when possible. Copying the configuration from startup to running merges the two configurations and can cause undesired configuration lines to remain active on the AP.

For additional information, refer to "Access Point Notes" on page 261 for a full Cisco IOS template.

NOTE

Changes made on the standard OV3600 Group configuration pages, to include Basic, Radio, Security, VLANs, and so forth, are not applied to any template-based APs.

WDS Settings in Templates

A group template supports Cisco WDS settings. APs functioning in a WDS environment communicate with the Cisco WLSE via a WDS master. IOS APs can function in Master or Slave mode. Slave APs report their rogue findings to the WDS Master (AP or WLSM which reports the data back to the WLSE. On the **APs/ Devices > Manage** configuration page, select the proper role for the AP in the WDS Role drop down menu.

The following example sets an AP as a WDS Slave with the following lines:

```
%if wds_role=client%
wlccp ap username wlse password 7 XXXXXXXXXX
%endif%
```

The following example sets an AP as a WDS Master with the following lines:

```
%if wds_role=master%
aaa authentication login method_wds group wds
aaa group server radius wds server
10.2.25.162 auth-port 1645 acct-port 1646
wlccp authentication-server infrastructure method_wds
wlccp wds priority 200 interface BVI1
wlccp ap username wlse password 7 095B421A1C
%endif%
```

The following example sets an AP as a WDS Master Backup with the following lines:

```
%if wds_role=backup%
aaa authentication login method_wds group wds
aaa group server radius wds server
10.2.25.162 auth-port 1645 acct-port 1646
wlccp authentication-server infrastructure method_wds
wlccp wds priority 250 interface BVI1
wlccp ap username wlse password 7 095B421A1C
```

```
%endif%
```

SCP Required Settings in Templates

A few things must be set up before enabling SCP on the **Groups > Basic** configuration page. The credentials used by OV3600 to login to the AP must have level 15 privileges. Without them OV3600 is not able to communicate with the AP via SCP. The line "`aaa authorization exec default local`" must be in the APs configuration file and the AP must have the SCP server enabled. These three settings correspond to the following lines in the AP's configuration file:

- `username Cisco privilege 15 password 7 0802455D0A16`
- `aaa authorization exec default local`
- `ip scp server enable`

The `username` line is a guideline and will vary based on the username being set, in this case Cisco, and the password and encoding type, in this case 0802455D0A16 and 7 respectively.

These values can be set on a group wide level using Templates and TFTP. Once these lines are set, SCP can be enabled on the **Groups > Basic** configuration page without problems.

Supporting Multiple Radio Types via a Single IOS Template

Some lines in an IOS configuration file should only apply to 802.11g vs. 802.11b. For instance, lines related to speed rates that mention rates above 11.0Mb/s do not work for 802.11b radios that cannot support these data rates.Use the "`%IF variable=value% … %ENDIF%`" construct to allow a single IOS configuration template to configure APs with different radio types within the same Group as illustrated below:

```
interface Dot11Radio0
…
%IF radio_type=g%
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
%ENDIF%
%IF radio_type=b%
speed basic-1.0 2.0 5.5 11.0
%ENDIF%
%IF radio_type=g%
power local cck %CCK_POWER%
power local ofdm %OFDM_POWER%
%ENDIF%
…
```

Configuring Single and Dual-Radio APs via a Single IOS Template

To configure single and dual-radio APs using the same IOS config template, you can use the interface variable within the %IF…% construct. The below example illustrates this usage:

```
%IF interface=Dot11Radio1%
interface Dot11Radio1
 bridge-group 1
 bridge-group 1 block-unknown-source
 bridge-group 1 spanning-disabled
 bridge-group 1 subscriber-loop-control
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 no ip address
 no ip route-cache
 rts threshold 2312
 speed basic-6.0 basic-9.0 basic-12.0 basic-18.0 basic-24.0 36.0 48.0 54.0
 ssid decibel-ios-a
   authentication open
   guest-mode
   station-role root
      %ENDIF%
```

Configuring Cisco Catalyst Switch Templates

Cisco Catalyst Switch templates are configured much like Cisco IOS templates with the addition of the *`interfaces`* and *`switch_command`* (for stacked switches) variables. Interfaces can be configured on the Device Interface pages, as shown in "Configuring Device Interfaces for Cisco Catalyst Switches" on page 138. You can import interface information as described in this section or by fetching a template from that device, as described in "Configuring General Templates" on page 152.

NOTE

Just one template is used for any type of Cisco IOS device, and another is used for any type of Catalyst Switch regardless of individual model.

Configuring Symbol Controller / HP WESM Templates

This section describes the configuration of templates for Symbol controllers and HP WESM devices.

Symbol switches (RFS x000, 5100 and 2000) can be configured in OV3600 using templates. OV3600 supports Symbol thin AP firmware upgrades from the controller's manage page.

A sample running-configuration file template is provided in this topic for reference. A template can be fetched from a model device using the Cisco IOS device procedure described in "Configuring Cisco IOS Templates" on page 156. Cisco IOS template directives such as `ignore_and_do_not_push` can also be applied to Symbol templates.

Certain parameters such as `hostname` and `location` are turned into variables with the `%` tags so that device-specific values can be read from the individual manage pages and inserted into the template. They are listed in Available Variable boxes on the right-hand side of the template fields.

Certain settings have integrated variables, including `ap-license` and `adoption-preference-id`. The radio preamble has been template-integrated as well. An option on the **Group > Templates** page reboots the device after pushing a configuration to it.

A sample Symbol controller partial template is included below for reference.

```
!
! configuration of RFS4000 version 4.2.1.0-005R
!
version 1.4
!
!
aaa authentication login default local none
service prompt crash-info
!
network-element-id RFS4000
!
username admin password 1 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
access-list 100 permit ip 192.168.0.0/24 any rule-precedence 10
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst configuration
 name My Name
!
ip dns-server-forward
wwan auth-type chap
no bridge multiple-spanning-tree enable bridge-forward
country-code us
aap-ipfilter-list no port 3333 plz
aap-ipfilter-list no port 3333 tcp plz
 deny tcp src-start-ip 0.0.0.0 src-end-ip 255.255.255.255 dst-start-ip 0.0.0.0 dst-end-ip
255.255.255.255 dst-start-port 3333 dst-end-port 3334 rule 1
%redundancy_config%
logging buffered 4
logging console 4
snmp-server engineid netsnmp 6b8b45674b30f176
snmp-server location %location%
snmp-server contact %contact%
snmp-server sysname %hostname%
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5 0x1aa491f4ca7c55df0f57801bece9044c
snmp-server user snmpmanager v3 encrypted auth md5 0x1aa491f4ca7c55df0f57801bece9044c
snmp-server user snmpoperator v3 encrypted auth md5 0xb03b1ebfa0e3d02f50e2b1c092ab7c9f
```

A sample Symbol Smart RF template is provided below for reference:

```
radio %radio_index% radio-mac %radio_mac%
%if radio_type=11a%
  radio %radio_index% coverage-rate  18
%endif%
%if radio_type=11an%
  radio %radio_index% coverage-rate  18
%endif%
%if radio_type=11b%
  radio %radio_index% coverage-rate  5p5
%endif%
%if radio_type=11bg%
  radio %radio_index% coverage-rate  6
%endif%
%if radio_type=11bgn%
  radio %radio_index% coverage-rate  18
%endif%
```

A sample Symbol thin AP template is provided below for reference and for the formatting of **`if`** statements.

```
radio add %radio_index% %lan_mac% %radio_type% %ap_type%
 radio %radio_index% radio-number %radio_number%
 radio %radio_index% description %description%
 %if radio_type=11a%
 radio %radio_index% speed  basic6 9 basic12 18 basic24 36 48 54
 radio %radio_index% antenna-mode primary
 radio %radio_index% self-heal-offset 1
 radio %radio_index% beacon-interval 99
 radio %radio_index% rts-threshold 2345
 radio %radio_index% max-mobile-units 25
 radio %radio_index% admission-control voice max-perc 76
 radio %radio_index% admission-control voice res-roam-perc 11
 radio %radio_index% admission-control voice max-mus 101
 radio %radio_index% admission-control voice max-roamed-mus 11
 %endif%
 %if radio_type=11an%
 radio %radio_index% speed  basic11a 9 18 36 48 54 mcs
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
 %endif%
 %if radio_type=11b%
 radio %radio_index% speed  basic1 basic2 basic5p5 basic11
 %endif%
 %if radio_type=11bg%
 radio %radio_index% speed  basic1 basic2 basic5p5 6 9 basic11 12 18 24 36 48 54
 radio %radio_index% on-channel-scan
 radio %radio_index% adoption-pref-id 7
 radio %radio_index% enhanced-beacon-table
 radio %radio_index% enhanced-probe-table
 %endif%
 %if radio_type=11bgn%
 radio %radio_index% speed  basic11b2 6 9 12 18 24 36 48 54 mcs
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
 %endif%
 radio %radio_index% channel-power indoor %channel% %transmit_power% %channel_attribute%
 %detector%
%adoption_pref_id%
 radio %radio_index% enhanced-beacon-table
 radio %radio_index% on-channel-scan
%ap_include_4%
```

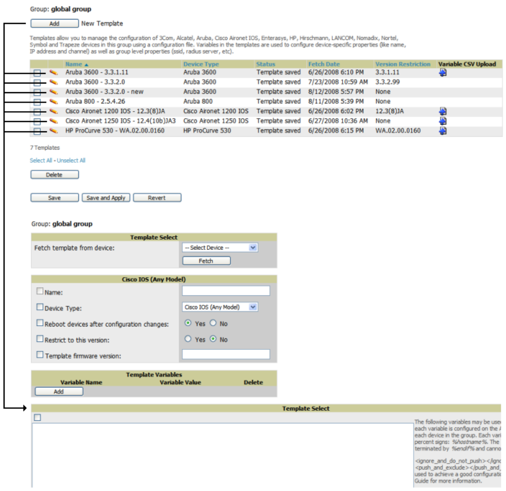
Configuring a Global Template

Global templates allow OV3600 users to define a single template in a global group that can be used to manage APs in subscriber groups. They turn settings like group RADIUS servers and encryption keys into variables that can be configured on a per-group basis.

Perform the following steps to create a global template, or to view or edit an existing global template:

1. Go to the **Group > Templates** configuration page for the global group that owns it.
2. Select **Add** to add a new template, or select the pencil icon next to an existing template to edit it.
3. Examine the configurations illustrated in Figure 112.

Figure 112 ***Group > Templates > Add** Page Illustration*



Group: **global group**

Add New Template

Templates allow you to manage the configuration of 3Com, Alcatel, Aruba, Cisco Aironet IOS, Enterasys, HP, Hirschmann, LANCOM, Nomadix, Nortel, Symbol and Trapeze devices in this group using a configuration file. Variables in the templates are used to configure device-specific properties (like name, IP address and channel) as well as group level properties (ssid, radius server, etc).

		Name ▲	Device Type	Status	Fetch Date	Version Restriction	Variable CSV Upload
□	✎	Aruba 3600 - 3.3.1.11	Aruba 3600	Template saved	6/26/2008 6:10 PM	3.3.1.11	⇪
□	✎	Aruba 3600 - 3.3.2.0	Aruba 3600	Template saved	7/23/2008 10:59 AM	3.3.2.99	
□	✎	Aruba 3600 - 3.3.2.0 - new	Aruba 3600	Template saved	8/12/2008 5:57 PM	None	
□	✎	Aruba 800 - 2.5.4.26	Aruba 800	Template saved	8/11/2008 5:39 PM	None	
□	✎	Cisco Aironet 1200 IOS - 12.3(8)JA	Cisco Aironet 1200 IOS	Template saved	6/26/2008 6:02 PM	12.3(8)JA	⇪
□	✎	Cisco Aironet 1250 IOS - 12.4(10b)JA3	Cisco Aironet 1250 IOS	Template saved	6/27/2008 10:36 AM	None	⇪
□	✎	HP ProCurve 530 - WA.02.00.0160	HP ProCurve 530	Template saved	6/26/2008 6:15 PM	WA.02.00.0160	⇪

7 Templates

Select All - Unselect All

Delete

Save | Save and Apply | Revert

Group: **global group**

Template Select	
Fetch template from device:	-- Select Device -- Fetch

Cisco IOS (Any Model)	
□ Name:	
□ Device Type:	Cisco IOS (Any Model)
□ Reboot devices after configuration changes:	● Yes ○ No
□ Restrict to this version:	○ Yes ● No
□ Template firmware version:	

Template Variables		
Variable Name	Variable Value	Delete
Add		

Template Select

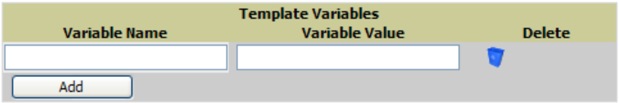
□

The following variables may be use
each variable is configured on the
each device in the group. Each vari
percent signs: *%hostname%*. The
terminated by *%endif%* and canno

<ignore_and_do_not_push></igno
<push_and_exclude></push_and_
used to achieve a good configurati
Guide for more information.

4. Use the drop-down menu to select a device from which to build the global template and select **Fetch**. The menus are populated with all devices that are contained in any group that subscribes to the global group. The fetched configuration populates the template field. Global template variables can be configured with the **Add** button in the **Template Variables** box, illustrated in Figure 113.

Figure 113 ***Template Variables Illustration***



Template Variables		
Variable Name	Variable Value	Delete
		🗑
Add		

The variable name cannot have any spaces or non-alphanumeric characters. The initial variable value entered is the default value, but can be changed on a per-group basis later. You can also populate global template variables by uploading a CSV file (see below).

5. Once you have configured your global template, select **Add**. You are taken to a confirmation configuration page where you can review your changes.
6. If you want to add the global template, select **Apply Changes Now**. If you do not want to add the template, select **Cancel and Discard Changes**. Canceling from the confirmation configuration page causes the template and all of the template variables to be lost.
7. Once you have added a new global template, you can use a CSV upload option to configure global template variables. Go to the **Groups > Templates** configuration page and select the **CSV** upload icon for the template. The CSV file must contain columns for **Group Name** and **Variable Name**. All fields must be completed.
   - **Group Name**—the name of the subscriber group that you wish to update.
   - **Variable Name**—the name of the group template variable you wish to update.

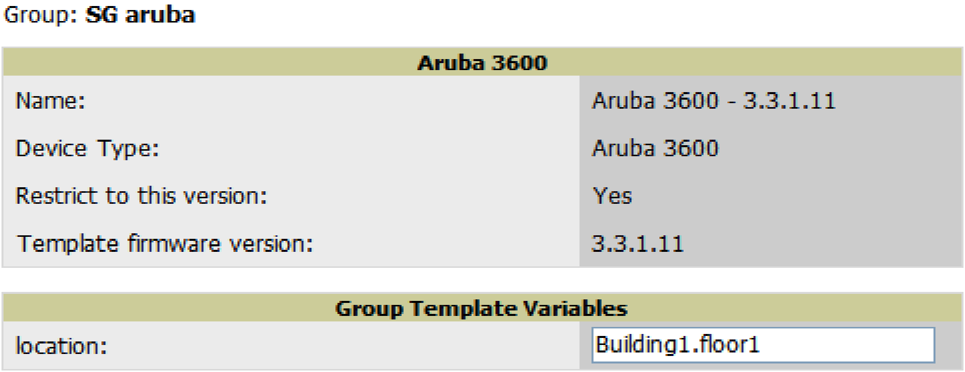
- **Variable Value**—the value to set.

For example, for a global template with a variable called "ssid_1", the CSV file might resemble what follows:

```
Group Name, ssid_1
Subscriber 1, Value 0
```

8. Once you have defined and saved a global template, it is available for use by any local group that subscribes to the global group. Go to the **Groups > Template** configuration page for the local group and select the pencil icon next to the global template in the list. Figure 114 illustrates this page.

Figure 114 ***Groups > Templates Edit**, Upper Portion*



Group: **SG aruba**

Aruba 3600	
Name:	Aruba 3600 - 3.3.1.11
Device Type:	Aruba 3600
Restrict to this version:	Yes
Template firmware version:	3.3.1.11

Group Template Variables	
location:	Building1.floor1

9. To make template changes, go to the **Groups > Template** configuration page for the global group and select the pencil icon next to the template you wish to edit. Note that you cannot edit the template itself from the subscriber group's **Groups > Templates** tab.

10. If group template variables have been defined, you are able to edit the value for the group on the **Groups > Templates, Add** configuration page in the **Group Template Variables** box. For Symbol devices, you are also able to define the template per group of APs.

For more information on using templates in OV3600, see the previous section of this chapter. It is also possible to create local templates in a subscriber group—using global groups does not mean that global templates are mandatory.

Chapter 7

Using RAPIDS and Rogue Classification

This chapter provides an overview to rogue device and IDS event detection, alerting, and analysis using RAPIDS, and contains the following sections:

Introduction to RAPIDS

Rogue device detection is a core component of wireless security. With RAPIDS rules engine and containment options, you can create a detailed definition of what constitutes a rogue device, and quickly act on a rogue AP for investigation, restrictive action, or both. Once rogue devices are discovered, RAPIDS alerts your security team of the possible threat and provides essential information needed to locate and manage the threat.

RAPIDS discovers unauthorized devices in your WLAN network in the following ways:

- Over the Air
  - Using your existing enterprise APs
  - Optional Alcatel-Lucent Management Client (AMC)
- On the Wire
  - Polling routers and switches to identify, classify, and locate unknown APs
  - Using HTTP and SNMP scanning

NOTE

To set up a scan, refer to "Discovering and Adding Devices" on page 107.

  - Using the controller's wired discovery information

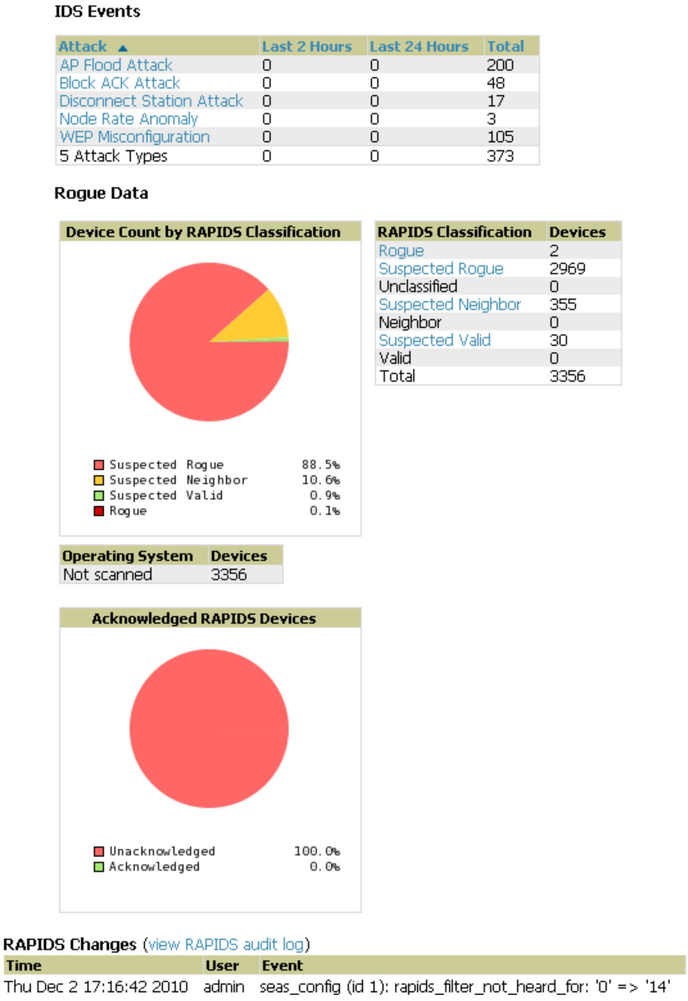
Furthermore, RAPIDS integrates with external intrusion detection systems (IDS), as follows:

- **Alcatel-Lucent WIP**—Alcatel-Lucent, Inc.'s Wireless Intrusion Protection (WIP) module integrates wireless intrusion protection into the mobile edge infrastructure. The WIP module provides wired and wireless AP detection, classification and containment; detects DoS and impersonation attacks; and prevents client and network intrusions.
- **Cisco WLSE** (1100 and 1200 IOS)—OV3600 fetches rogue information from the HTTP interface and gets new AP information from SOAP API. This system provides wireless discovery information rather than rogue detection information.
- **AirMagnet Enterprise**—Retrieves a list of managed APs from OV3600.
- **AirDefense**—Uses the OV3600 XML API to keep its list of managed devices up to date.
- **WildPackets OmniPeek**—Retrieves a list of managed APs from OV3600.

Viewing Overall Network Health on the RAPIDS > Overview Page

The **RAPIDS > Overview** page displays a page of RAPIDS summary information (see Figure 115). Table 92 defines the summary information that appears on the page.

Figure 115 ***RAPIDS > Overview** Page Illustration*



IDS Events

Attack ▲	Last 2 Hours	Last 24 Hours	Total
AP Flood Attack	0	0	200
Block ACK Attack	0	0	48
Disconnect Station Attack	0	0	17
Node Rate Anomaly	0	0	3
WEP Misconfiguration	0	0	105
5 Attack Types	0	0	373

Rogue Data

Device Count by RAPIDS Classification

🟥 Suspected Rogue	88.5%
🟨 Suspected Neighbor	10.6%
🟩 Suspected Valid	0.9%
🟥 Rogue	0.1%

RAPIDS Classification	Devices
Rogue	2
Suspected Rogue	2969
Unclassified	0
Suspected Neighbor	355
Neighbor	0
Suspected Valid	30
Valid	0
Total	3356

Operating System	Devices
Not scanned	3356

Acknowledged RAPIDS Devices

🟥 Unacknowledged	100.0%
🟩 Acknowledged	0.0%

RAPIDS Changes (view RAPIDS audit log)

Time	User	Event
Thu Dec 2 17:16:42 2010	admin	seas_config (id 1): rapids_filter_not_heard_for: '0' => '14'

Table 92 ***Overview** Fields*

Summary	Description
IDS Events	Displays a list of IDS events for the designated folder and subfolders. Field displays events from the past two hours, the past 24 hours, and total IDS events. Names of attacks link to summary pages with more details. **Note:** OV3600 should be configured as the SNMP trap receiver on the controllers to receive IDS traps. See the *Alcatel-Lucent Best Practices Guide* for details.
Rogue Data	A pie chart of rogue device percentages by RAPIDS classification. Select a classification from the **RAPIDS Classification** table to be taken to a **RAPIDS > List** page, filtered by that classification.
Operating System	Detected operating systems represented in both a color coded pie chart and a summary listing. OS scans can be run manually or enabled to run automatically on the **RAPIDS > Setup** page.
Acknowledged RAPIDS Devices	A color coded pie chart comparing the number of acknowledged devices to the unacknowledged devices.
RAPIDS Changes	Tracks every change made to RAPIDS including changes to rules, manual classification, and components on the **RAPIDS > Setup** page.

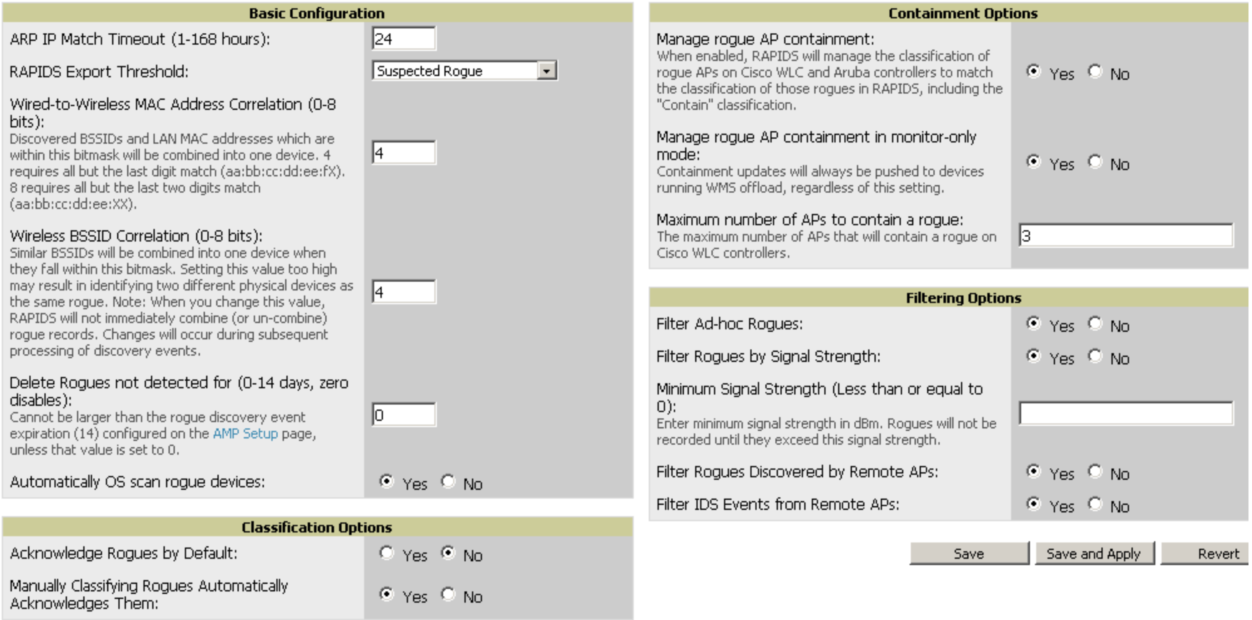
Setting Up RAPIDS

The **RAPIDS > Setup** page allows you to configure your OV3600 server for RAPIDS. Complete the settings on this page as desired, and select **Save**. Most of the settings are internal to how OV3600 will process rogues.

Basic Configuration

On the **RAPIDS > Setup** page, the **Basic Configuration** section allows you to define RAPIDS behavior settings. Figure 116 illustrates this page.

Figure 116 ***RAPIDS* > *Setup*** *Page Illustration*



Basic Configuration

ARP IP Match Timeout (1-168 hours):	24
RAPIDS Export Threshold:	Suspected Rogue
Wired-to-Wireless MAC Address Correlation (0-8 bits): Discovered BSSIDs and LAN MAC addresses which are within this bitmask will be combined into one device. 4 requires all but the last digit match (aa:bb:cc:dd:ee:fX). 8 requires all but the last two digits match (aa:bb:cc:dd:ee:XX).	4
Wireless BSSID Correlation (0-8 bits): Similar BSSIDs will be combined into one device when they fall within this bitmask. Setting this value too high may result in identifying two different physical devices as the same rogue. Note: When you change this value, RAPIDS will not immediately combine (or un-combine) rogue records. Changes will occur during subsequent processing of discovery events.	4
Delete Rogues not detected for (0-14 days, zero disables): Cannot be larger than the rogue discovery event expiration (14) configured on the AMP Setup page, unless that value is set to 0.	0
Automatically OS scan rogue devices:	● Yes ○ No

Classification Options

Acknowledge Rogues by Default:	○ Yes ● No
Manually Classifying Rogues Automatically Acknowledges Them:	● Yes ○ No

Containment Options

Manage rogue AP containment: When enabled, RAPIDS will manage the classification of rogue APs on Cisco WLC and Aruba controllers to match the classification of those rogues in RAPIDS, including the "Contain" classification.	● Yes ○ No
Manage rogue AP containment in monitor-only mode: Containment updates will always be pushed to devices running WMS offload, regardless of this setting.	● Yes ○ No
Maximum number of APs to contain a rogue: The maximum number of APs that will contain a rogue on Cisco WLC controllers.	3

Filtering Options

Filter Ad-hoc Rogues:	● Yes ○ No
Filter Rogues by Signal Strength:	● Yes ○ No
Minimum Signal Strength (Less than or equal to 0): Enter minimum signal strength in dBm. Rogues will not be recorded until they exceed this signal strength.	
Filter Rogues Discovered by Remote APs:	● Yes ○ No
Filter IDS Events from Remote APs:	● Yes ○ No

Table 93 ***RAPIDS* > *Setup* > *Basic Configuration*** *Fields*

Field	Default	Description
ARP IP Match Timeout	24	If you have routers and switches on the OV3600, and it's scanning them for ARP tables, this can assign a rogue IP address information. This timeout specifies how recent that information needs to be for the IP address to be considered valid. Note that the default ARP poll period is long (several hours).
RAPIDS Export Threshold	Suspected Rogue	Exported rogues will be sent to VisualRF for location calculation.
Wired-to-Wireless MAC Address Correlation	4	Discovered BSSIDs and LAN MAC addresses which are within this bitmask will be combined into one device. 4 requires all but the last digit match (aa:bb:cc:dd:ee:fX). 8 requires all but the last two digits match (aa:bb:cc:dd:ee:XX).
Wireless BSSID Correlation	4	Similar BSSIDs will be combined into one device when they fall within this bitmask. Setting this value too high may result in identifying two different physical devices as the same rogue. **Note:** When you change this value, RAPIDS will not immediately combine (or un-combine) rogue records. Changes will occur during subsequent processing of discovery events.
Delete Rogues not detected for (0-14 days, zero disables):	0	This value cannot be larger than the rogue discovery event expiration (14) configured on the **OV3600 Setup** page, unless that value is set to **0**.

Field	Default	Description
Automatically OS scan rogue devices	No	Whether to scan the operating system of rogues. Enabling this feature will cause RAPIDS to perform an OS scan when it gets in IP address for a rogue device. The OS scan will be run when a rogue gets an IP address for the first time or if the IP address changes.

Table 94 ***RAPIDS* > *Setup* > *Classification Options*** *Fields*

Field	Default	Description
Acknowledge Rogues by Default	No	Sets RAPIDS to acknowledge rogue devices upon initial detection, prior to their classification.
Manually Classifying Rogues Automatically Acknowledges them	Yes	Defines whether acknowledgement happens automatically whenever a rogue device receives a manual classification.

Filtered rogues are dropped from the system before they are processed through the rules engine. This can speed up overall performance but will eliminate all visibility into these types of devices.

Table 95 ***RAPIDS* > *Setup* > *Filtering*** *Options*

Field	Default	Description
Filter Ad-hoc rogues	No	Filters rogues according to ad-hoc status.
Filter Rogues by Signal Strength	No	Filters rogues according to signal strength. Since anything below the established threshold will be ignored and possibly dangerous, we do not recommend enabling this setting. Instead, we recommend you incorporate signal strength into the classification rules on the **RAPIDS > Rules** page.
Filter Rogues Discovered by Remote APs	No	Filters rogues according to the remote AP that discovers them. Enabling this option causes OV3600 to drop all rogue discovery information coming from remote APs.
Filter IDS Events from Remote APs	No	Filters IDS Events discovered by remote APs.

Rogue Containment Options

Using RAPIDS, OV3600 can shield rogue devices from associating to Cisco WLC controllers (versions 4.2.114 and later), and Alcatel-Lucent switches (running AOS-W versions 3.x and later). OV3600 will alert you to the appearance of the rogue device and identify any mismatch between switch configuration and the desired configuration.

NOTE

WMS Offload is not required to manage containment in OV3600.

Table 96 shows the Containment Options section of the **RAPIDS > Setup** page.

Table 96 ***RAPIDS* > *Setup* > *Containment Options*** *Fields and Default Values*

Field	Default	Description
Manage rogue AP Containment	Yes	Rogue APs on Cisco WLC and Alcatel-Lucent controllers as defined by the Rules engine will be classified as a Contained Rogue. OV3600 pushes the containment status of a rogue device to the controller and the controller takes the appropriate action. For the rogue device to be contained, you may need to configure containment on the controller.

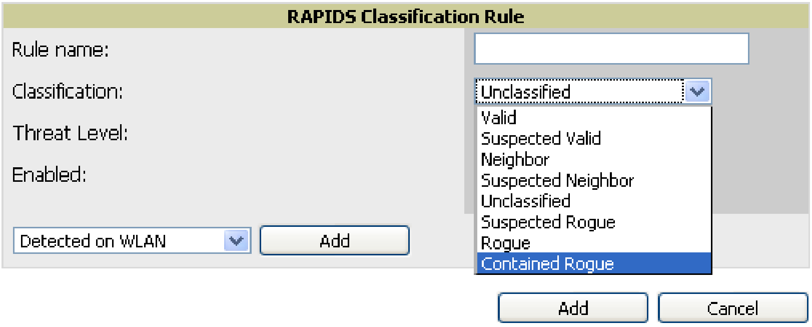
Table 96 ***RAPIDS > Setup > Containment Options*** *Fields and Default Values*

Field	Default	Description
Manage rogue AP containment in monitor-only mode	No	If disabled, OV3600 will display the desired containment settings but will not push them to devices. This may result in mismatches in device classifications. This can be useful for administrators that want to see what RAPIDS would push to the controller without making any changes to their network. If enabled, OV3600 will push the desired containment settings to the controllers in Monitor-Only mode, as well as the devices in **Managed** mode.
Maximum number of APs to contain a rogue	3	Sets the maximum number of APs that will contain a rogue on Cisco WLC controllers.

1. Navigate to the **RAPIDS > Setup** page.
2. From the **Containment Options** section, select **Yes** to manage rogue AP containment. Once this is done, the Contained Rogue classification will appear as an option in the classification drop down menu as shown in Figure 117.

   Additionally, once this option been enabled, the option to manage contained APs in **Monitor-Only** mode becomes available. Containment in Monitor-Only mode means configuration changes will still be pushed to the controller, even though it is in monitor-only mode.

Figure 117 ***RAPIDS > Classification Rule*** *Menu with Containment*



RAPIDS Classification Rule

Rule name:

Classification: Unclassified

Threat Level:

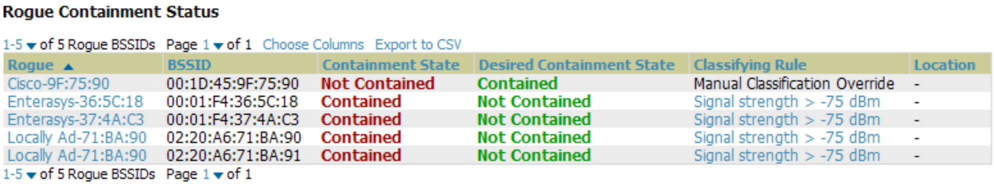
Enabled:

From the **APs/Devices > Rogues Contained** page, you can see the containment status information, as shown in Figure 118.

NOTE

The Rogue Containment device tab is only present for devices that support containment.

Figure 118 *Rogue Containment Status Page*



Rogue Containment Status

1-5 ▾ of 5 Rogue BSSIDs Page 1 ▾ of 1 Choose Columns Export to CSV

Rogue ▲	BSSID	Containment State	Desired Containment State	Classifying Rule	Location
Cisco-9F:75:90	00:1D:45:9F:75:90	Not Contained	Contained	Manual Classification Override	-
Enterasys-36:5C:18	00:01:F4:36:5C:18	Contained	Not Contained	Signal strength > -75 dBm	-
Enterasys-37:4A:C3	00:01:F4:37:4A:C3	Contained	Not Contained	Signal strength > -75 dBm	-
Locally Ad-71:BA:90	02:20:A6:71:BA:90	Contained	Not Contained	Signal strength > -75 dBm	-
Locally Ad-71:BA:90	02:20:A6:71:BA:91	Contained	Not Contained	Signal strength > -75 dBm	-

1-5 ▾ of 5 Rogue BSSIDs Page 1 ▾ of 1

Additional Settings

Additional RAPIDS settings such as role filtering and performance tuning are available in the following locations:

- Use the **OV3600 Setup > Roles > Add/Edit Role Page** to define the ability to use RAPIDS by user role. Refer to "Creating OV3600 User Roles" on page 44.
- Use the **OV3600 Setup > General > Performance Tuning** page to define the processing priority of RAPIDS in relation to OV3600 as a whole (see Table 16 on page 40).

Defining RAPIDS Rules

The **RAPIDS > Rules** page is one of the core components of RAPIDS. This feature allows you to define rules by which any detected device on the network is classified.

This section describes how to define, use, and monitor RAPIDS rules, provides examples of such rules, and demonstrates how they are helpful.

This section contains the following topics:

Switch Classification with WMS Offload

This classification method is supported only when WMS offload is enabled on Alcatel-Lucent WLAN switches. Switch classification of this type remains distinct from RAPIDS classification. WLAN switches feed wireless device information to OV3600, which OV3600 then processes. OV3600 then pushes the WMS classification to all of the AOS-W switches that are WMS offload enabled.

WMS Offload ensures that a particular BSSID has the same classification on all of the switches. WMS Offload removes some load from master switches and feeds 'connected-to-lan' information to the RAPIDS classification engine. RAPIDS classifications and switch classifications are separate and often are not synchronized.

NOTE

RAPIDS classification is not pushed to the devices.

The following table compares how default classification may differ between OV3600 and AOS-W for scenarios involving WMS Offload.

Table 97 *Rogue Device Classification Matrix*

OV3600	AOS-W (ARM)
Unclassified (default state)	Unknown
Rogue	Rogue
Suspected Neighbor	Interfering
Neighbor	Known Interfering
Valid	Valid
Contained Rogue	DOS

For additional information about WMS Offload, refer to the *Alcatel-Lucent and AirWave Best Practices Guide*.

Device OUI Score

The Organizationally Unique Identifier (OUI) score is based on the LAN MAC address of a device. RAPIDS can be configured to poll your routers and switches for the bridge forwarding tables. RAPIDS then takes the MAC addresses from those tables and runs them through a proprietary database to derive the OUI score.

The OUI score of each device is viewable from each rogue's detail page. Table 98 provides list the OUI scores definitions.

Table 98 *Device OUI Scores*

Score	Description
Score of 1	Indicates any device on the network; this is the lowest threat level on the network.
Score of 2	Indicates any device in which the OUI belongs to a manufacturer that produces wireless (802.11) equipment.
Score of 3	Indicates that the OUI matches a block that contains APs from vendors in the Enterprise and small office/ small home market.
Score of 4	Indicates that the OUI matches a block that belonged to a manufacturer that produces small office/ small home access points.

Rogue Device Threat Level

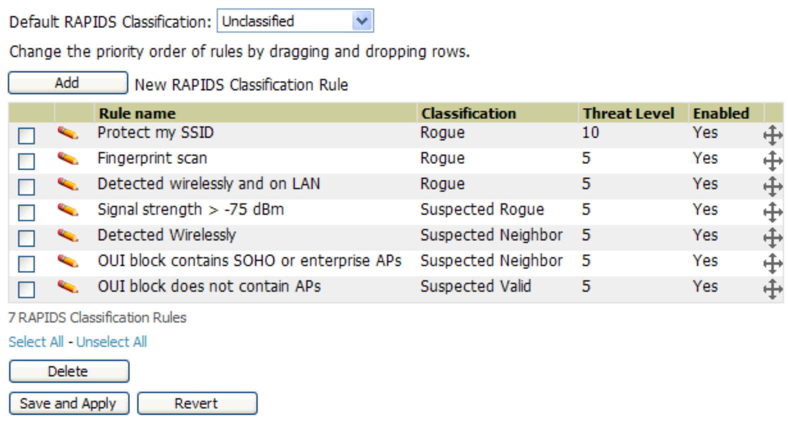
The threat level classification adds granularity for each general RAPIDS classification. Devices of the same classification can have differing threat scores based on the classifying rule, ranging from 1 to 10 with a default value of **5**. This classification process can help identify the greater threat. Alerts can be defined and sorted by threat level.

Threat level and classification are both assigned to a device when a device matches a rule. Once classified, a device's classification and threat level change only if it is classified by a new rule or is manually changed. Threats levels can be manually defined on the **RAPIDS > Detail** page when the RAPIDS classification is manually overridden or you can edit the rule to have a higher threat level.

Viewing and Configuring RAPIDS Rules

To view the RAPIDS rules that are currently configured on OV3600, navigate to the **RAPIDS > Rules** page (Figure 119).

Figure 119 ***RAPIDS** > **Rules** Page Illustration*



Default RAPIDS Classification: Unclassified

Change the priority order of rules by dragging and dropping rows.

Add New RAPIDS Classification Rule

		Rule name	Classification	Threat Level	Enabled	
□	✎	Protect my SSID	Rogue	10	Yes	✥
□	✎	Fingerprint scan	Rogue	5	Yes	✥
□	✎	Detected wirelessly and on LAN	Rogue	5	Yes	✥
□	✎	Signal strength > -75 dBm	Suspected Rogue	5	Yes	✥
□	✎	Detected Wirelessly	Suspected Neighbor	5	Yes	✥
□	✎	OUI block contains SOHO or enterprise APs	Suspected Neighbor	5	Yes	✥
□	✎	OUI block does not contain APs	Suspected Valid	5	Yes	✥

7 RAPIDS Classification Rules

Select All - Unselect All

Table 99 defines the fields in the **RAPIDS > Rules** page.

Table 99 ***RAPIDS** > **Rules** Page*

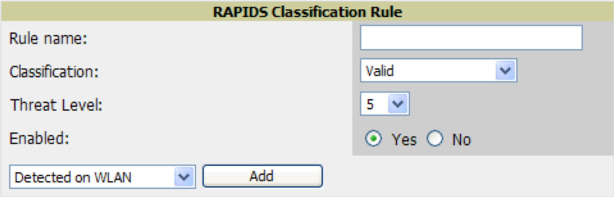
Field	Description
Default Classification	Sets the classification that a rogue device receives when it does not match any rules.
Add New RAPIDS Classification Rule	Select this button to create a RAPIDS classification rule.
Rule Name	Displays the name of any rule that has been configured. Rule names should be descriptive and should convey the core purpose for which it was created.

Table 99 ***RAPIDS*** **>** ***Rules*** *Page*

Field	Description
Classification	Displays the classification that devices receive if they meeting the rule criteria.
Threat Level	Displays the numeric threat level for the rogue device that pertains to the rule. Refer to “Rogue Device Threat Level” on page 169 for additional information.
Enabled	Displays the status of the rule, whether enabled or disabled.
Reorder Drag and Drop Icon ✥	Changes the sequence of rules in relation to each other. Select, then drag and drop, the icon for any rule to move it up or down in relation to other rules. A revised sequence of rules must be saved before rogues are classified in the revised sequence. **NOTE:** The sequence of rules is very important for proper rogue classification. A device gets classified by the first rule to which it complies, even if it conforms to additional rules later in the sequence.

To create a new rule, select the **Add** button next to **New RAPIDS Classification Rule** to launch the **RAPIDS Classification Rule** page (see Figure 120).

Figure 120 ***Classification Rule*** *Page*



RAPIDS Classification Rule

Rule name:

Classification: Valid

Threat Level: 5

Enabled: ● Yes ○ No

Detected on WLAN

Fill in the settings described in Table 99 then select an option from the drop down menu.

Table 100 defines the drop down menu options that are at the bottom left of the RAPIDS Classification Rule dialog box (see Figure 120). Once all rule settings are defined, select **Add**. The new rule automatically appears in the **RAPIDS > Rules** page.

Table 100 ***Properties*** *Drop Down Menu*

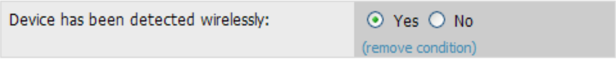
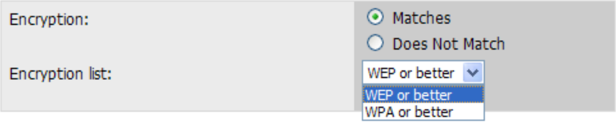
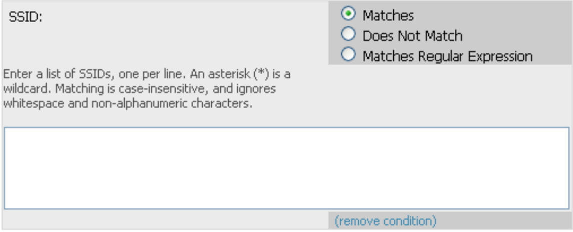
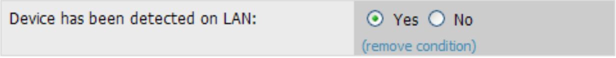
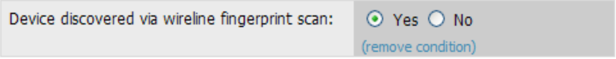
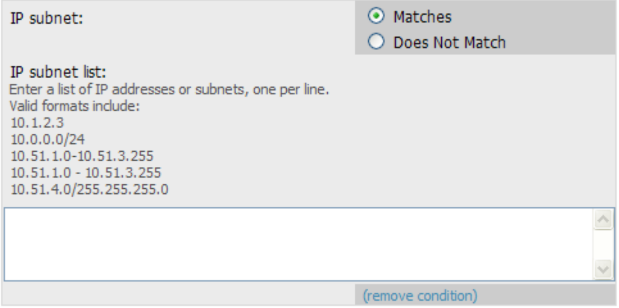
Option	Description
Wireless Properties	
Detected on WLAN	Classifies based on how the rogue is detected on the wireless LAN.  Device has been detected wirelessly: ● Yes ○ No
Detecting AP Count	Classifies based on the number of managed devices that can hear the rogue. Enter a numeric value and select **At Least** or **At Most**.
Encryption	Classifies based on the rogue matching a specified encryption method. Note that you can select for 'no encryption' with a rule that says "Encryption does not match WEP or better".  Encryption: ● Matches ○ Does Not Match Encryption list: WEP or better
Network type	Rogue is running on the selected network type, either **Ad-hoc** or **Infrastructure.**
Signal Strength	Rogue matches signal strength parameters. Specify a minimum and maximum value in dBm.

Table 100 ***Properties*** *Drop Down Menu*

Option	Description
SSID	Classifies the rogue when it matches or does not match the specified string for the SSID or a specified regular expression.  SSID: ● Matches ○ Does Not Match ○ Matches Regular Expression Enter a list of SSIDs, one per line. An asterisk (*) is a wildcard. Matching is case-insensitive, and ignores whitespace and non-alphanumeric characters. (remove condition) **NOTE:** For SSID matching functions, OV3600 processes only alpha-numeric characters and the asterisk wildcard character (*). OV3600 ignores all other non-alpha-numeric characters. For example, the string of `ethersphere-*` matches the SSID of `ethersphere-wpa2` but also the SSID of `ethersphere_this_is_an_example` (without any dashes).
Wireline Properties	
Detected on LAN	Rogue is detected on the wired network. Select **Yes** or **No**.  Device has been detected on LAN: ● Yes ○ No (remove condition)
Fingerprint Scan	Rogue matches fingerprint parameters.  Device discovered via wireline fingerprint scan: ● Yes ○ No (remove condition)
IP Address	Rogue matches a specified IP address or subnet. Enter IP address or subnet information as explained by the fields.  IP subnet: ● Matches ○ Does Not Match IP subnet list: Enter a list of IP addresses or subnets, one per line. Valid formats include: 10.1.2.3 10.0.0.0/24 10.51.1.0-10.51.3.255 10.51.1.0 - 10.51.3.255 10.51.4.0/255.255.255.0 (remove condition)
OUI Score	Rogue matches manufacturer OUI criteria. You can specify minimum and maximum OUI score settings from two drop-down lists. Select **remove** to remove one or both criteria, as desired.
Operating System	Rogue matches OS criteria. Specify matching or non-matching OS criteria as prompted by the fields.
Wireless/Wireline Properties	
Manufacturer	Rogue matches the manufacturer information of the rogue device. Specify matching or non-matching manufacturer criteria.
MAC Address	Rogue matches the MAC address. Specify matching or non-matching address criteria, or use a wildcard (*) for partial matches.
Alcatel-Lucent Controller Properties	
Controller Classification	Rogue matches the specified controller classification.
Confidence	Rogue falls within a specified minimum and maximum confidence level, ranging from 1 to 100.

After creating a new rule, select **Add** to return to the **RAPIDS > Rules** page. Select **Save and Apply** to have the new rule take effect.

Deleting or Editing a Rule

To delete a rule from the RAPIDS rules list, go to the **RAPIDS > Rules** page. Select the check box next to the rule you want to delete, and select **Delete**. The rule is automatically deleted from **RAPIDS > Rules**.

To edit any existing rule, select its pencil icon to launch the **RAPIDS Classification Rule** page (see Figure 120). Edit or revise the fields as necessary, then select **Save**.

To change the sequence in which rules apply to any rogue device, drag and drop the rule to a new position in the rules sequence.

Recommended RAPIDS Rules

- **If Any Device Has Your SSID, Then Classify as Rogue**

  The only devices broadcasting your corporate SSID should be devices that you are aware of and are managed by OV3600. Rogue devices often broadcast your official SSID in an attempt to get access to your users, or to trick your users into providing their authentication credentials. Devices with your SSID generally pose a severe threat. This rule helps to discover, flag, and emphasize such a device for prompt response on your part.
- **If Any Device Has Your SSID and is Not an Ad-Hoc Network Type, Then Classify as Rogue**

  This rule classifies a device as a rogue when the SSID for a given device is your SSID and is not an Ad-Hoc device. Windows XP automatically tries to create an Ad-hoc network if it can not find the SSID for which it is searching. This means that user's laptops on your network may appear as Ad-Hoc devices that are broadcasting your SSID. If this happens too frequently, you can restrict the rule to apply to non-ad-hoc devices.
- **If More Than Four APs Have Discovered a Device, Then Classify as Rogue**

  By default, OV3600 tries to use Signal Strength to determine if a device is on your premises. Hearing device count is another metric that can be used.

  The important concept in this scenario is that legitimate neighboring devices are only heard by a few APs on the edge of your network. Devices that are heard by a large number of your APs are likely to be in the heart of your campus. This rule works best for scenarios in large campuses or that occupy an entire building. For additional rules that may help you in your specific network scenario, contact Alcatel support.

Using RAPIDS Rules with Additional OV3600 Functions

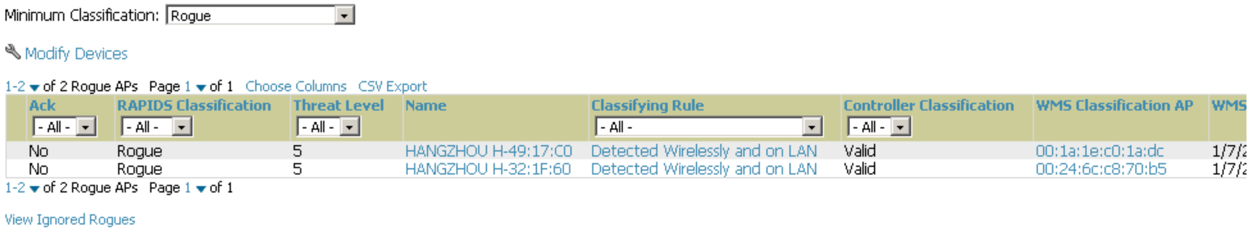
Rules that you configure on the **RAPIDS > Rules** page establish an important way of processing rogue devices on your network, and flagging them for attention as required. Such devices appear on the following pages in OV3600, with additional information:

- **RAPIDS > List**—Lists rogue devices as classified by rules.
- **RAPIDS > Rules**—Displays the rules that classify rogue devices.
- **RAPIDS > Overview**—Displays general rogue device count and statistical information.
- **System > Triggers**—Displays triggers that are currently configured, including any triggers that have been defined for rogue events.
- **Reports > Definitions**—Allows you to run New Rogue Devices Report with custom settings.
- **VisualRF**—Displays physical location information for rogue devices.

Viewing Rogues on the RAPIDS > List Page

To view a rogue AP, select the **RAPIDS > List** tab and select a rogue device type from the **Minimum Classification** drop-down menu (see Figure 121). You can sort the table columns (up/down) by selecting the column head or filter data using the column head drop down menus. The active links on this page launch additional pages for RAPIDS configuration or device processing.

Figure 121 ***RAPIDS > List Page*** *Illustration (partial view)*



Minimum Classification: Rogue

Modify Devices

1-2 of 2 Rogue APs Page 1 of 1 Choose Columns CSV Export

Ack	RAPIDS Classification	Threat Level	Name	Classifying Rule	Controller Classification	WMS Classification AP	WMS
- All -	- All -	- All -		- All -	- All -		
No	Rogue	5	HANGZHOU H-49:17:C0	Detected Wirelessly and on LAN	Valid	00:1a:1e:c0:1a:dc	1/7/2
No	Rogue	5	HANGZHOU H-32:1F:60	Detected Wirelessly and on LAN	Valid	00:24:6c:c8:70:b5	1/7/2

1-2 of 2 Rogue APs Page 1 of 1

View Ignored Rogues

Table 101 details the column information displayed in Figure 121. For additional information about RAPIDS rules, refer to “Defining RAPIDS Rules” on page 168.

Table 101 ***RAPIDS > List*** *Column Definitions*

Column	Description
Ack	Displays whether or not the rogue device has been acknowledged. Devices can be acknowledged manually or you can configure RAPIDS so that manually classifying rogues will automatically acknowledges them. Additionally, devices can be acknowledged by using Modify Devices of the **List** page. Rogues should be acknowledged when the OV3600 user has investigated them and determined that they are not a threat (see “Basic Configuration” on page 165).
RAPIDS Classification	Displays the current RAPIDS classification. This classification is determined by the rules defined on the **RAPIDS > Rules** page.
Threat Level	This field displays the numeric threat level of the device, in a range from 1 to 10. The definition of threat level is configurable, as described in “Rogue Device Threat Level” on page 169. The threat level is also supported with Triggers (see “Monitoring and Supporting OV3600 with the System Pages” on page 204).
Name	Displays the alpha-numeric name of the rogue device, as known. By default, OV3600 assigns each rogue device a name derived from the OUI vendor and the final six digits of the MAC address.
Classifying Rule	Displays the RAPIDS Rule that classified the rogue device (see“Viewing and Configuring RAPIDS Rules” on page 169).
Controller Classification	Displays the classification of the device based on the controller’s hard-coded rules. **NOTE:** This column is hidden unless **Offload WMS Database** is enabled by at least one group on the **Groups > Basic** page.
WMS Classification AP	The AP that provided the information used to classify the device.
WMS Classification Date	The date that WMS decided the classification
Confidence	The confidence level of the suspected rogue. How confidence is calculated varies based on the version of AOS-W. When an AOS-W switch sees evidence that a device might be on the wire it will up the confidence level. If AOS-W is completely sure that it is on the wire, it gets classified as a rogue.
Wired	Displays whether the rogue device has been discovered on one of your wired networks by polling routers/switches, your SNMP/HTTP scans, or Alcatel-Lucent WIP information. This column displays **Yes** or is blank if wired information was not detected.
Detecting APs	Displays the number of AP devices that have wirelessly detected the rogue device. A designation of heard implies the device was heard over the air.
Location	As with most **List** pages in OV3600, the **RAPIDS > List** page includes the **Location** column. If the rogue has been placed in VisualRF, this column will display the name of the floor plan the rogue is on. RAPIDS and VisualRF must be licensed on the OV3600 for this functionality to be supported.
SSID	Displays the most recent SSID that was heard from the rogue device.
Signal	Displays the strongest signal strength detected for the rogue device.

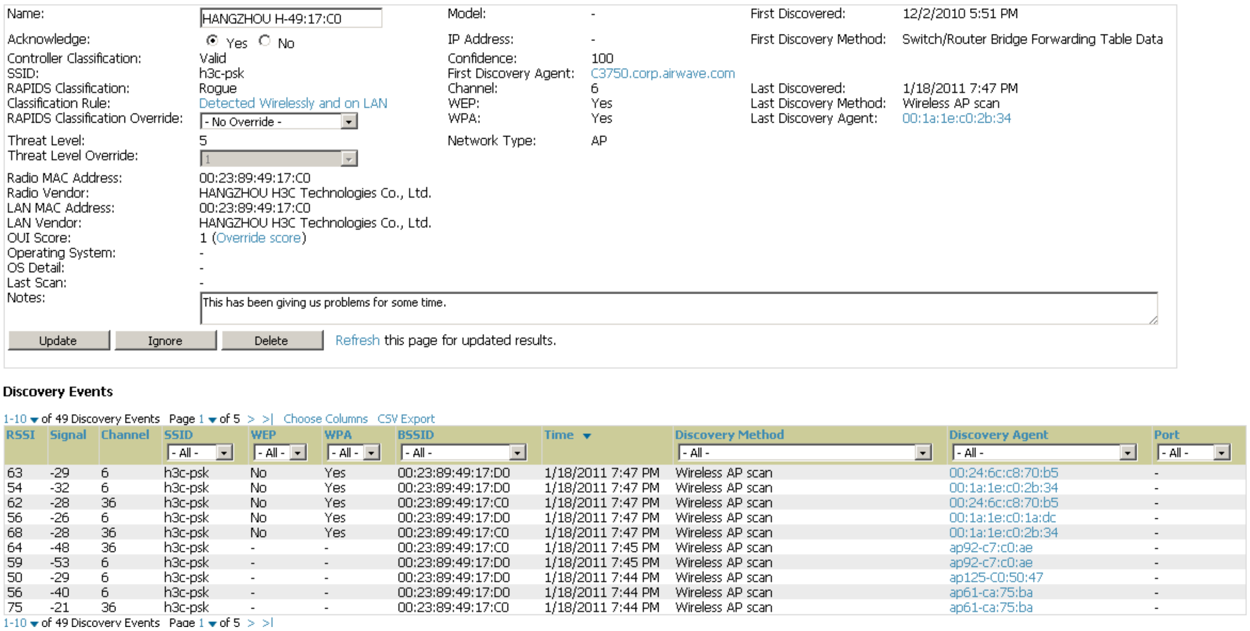
Table 101 ***RAPIDS** > **List*** *Column Definitions*

Column	Description
RSSI	Displays Received Signal Strength Indication (RSSI) designation, a measure of the power present in a received radio signal.
Network Type	Displays the type of network in which the rogue is present, for example: ● **Ad-hoc**—This type of network usually indicates that the rogue is a laptop that attempts to create a network with neighboring laptops, and is less likely to be a threat. ● **AP**—This type of network usually indicates an infrastructure network, for example. This may be more of a threat. ● **Unknown**—The network type is not known.
Encryption Type	Displays the encryption that is used by the device. Possible contents of this field include the following encryption types: ● **Open**—No encryption ● **WEP**—Wired Equivalent Privacy ● **WPA**—Wi-Fi Protected Access Generally, this field alone does not provide enough information to determine if a device is a rogue, but it is a useful attribute. If a rogue is not running any encryption method, you have a wider security hole than with an AP that is using encryption.
Ch	Indicates the most recent RF channel on which the rogue was detected. **Note:** it may be detected on more than one channel if it contains more than one radio.
LAN MAC Address	The LAN MAC address of the rogue device.
LAN Vendor	Indicates the LAN vendor of the rogue device, when known.
Radio Vendor	Indicates the radio vendor of the rogue device, when known.
OS	This field displays the OS of the device, as known. OS is the result of a running an OS port scan on a device. An IP addresses is required to run an OS scan. The OS reported here is based on the results of the scan.
Model	Displays the model of rogue device, if known. This is determined with a fingerprint scan, and this information may not always be available.
IP Address	Displays the IP address of the rogue device. The IP address data comes from fingerprint scans or ARP polling of routers and switches.
Last Discovering AP	Displays the most recent AP to discover the rogue device. The device name in this column is taken from the device name in OV3600.
Switch/Router	Displays the switch or router where the device's LAN MAC address was last seen.
Port	Indicates the physical port of the switch or router where the rogue was last seen.
Last Seen	Indicates the date and time the rogue device was last seen.

Overview of the RAPIDS > Detail Page

Select a device **Name** in the **RAPIDS > List** page to view the **Detail** page (Figure 122).

Figure 122 ***RAPIDS** > **Detail*** *Page Illustration*



Name: HANGZHOU H-49:17:C0
Acknowledge: ● Yes ○ No
Controller Classification: Valid
SSID: h3c-psk
RAPIDS Classification: Rogue
Classification Rule: Detected Wirelessly and on LAN
RAPIDS Classification Override: - No Override -
Threat Level: 5
Threat Level Override: 1
Radio MAC Address: 00:23:89:49:17:C0
Radio Vendor: HANGZHOU H3C Technologies Co., Ltd.
LAN MAC Address: 00:23:89:49:17:C0
LAN Vendor: HANGZHOU H3C Technologies Co., Ltd.
OUI Score: 1 (Override score)
Operating System: -
OS Detail: -
Last Scan: -
Notes: This has been giving us problems for some time.

Model: -
IP Address: -
Confidence: 100
First Discovery Agent: C3750.corp.airwave.com
Channel: 6
WEP: Yes
WPA: Yes
Network Type: AP

First Discovered: 12/2/2010 5:51 PM
First Discovery Method: Switch/Router Bridge Forwarding Table Data
Last Discovered: 1/18/2011 7:47 PM
Last Discovery Method: Wireless AP scan
Last Discovery Agent: 00:1a:1e:c0:2b:34

Refresh this page for updated results.

Discovery Events

1-10 of 49 Discovery Events Page 1 of 5 > >| Choose Columns CSV Export

RSSI	Signal	Channel	SSID	WEP	WPA	BSSID	Time	Discovery Method	Discovery Agent	Port
			- All -	- All -	- All -	- All -		- All -	- All -	- All -
63	-29	6	h3c-psk	No	Yes	00:23:89:49:17:D0	1/18/2011 7:47 PM	Wireless AP scan	00:24:6c:c8:70:b5	-
54	-32	6	h3c-psk	No	Yes	00:23:89:49:17:D0	1/18/2011 7:47 PM	Wireless AP scan	00:1a:1e:c0:2b:34	-
62	-28	36	h3c-psk	No	Yes	00:23:89:49:17:C0	1/18/2011 7:47 PM	Wireless AP scan	00:24:6c:c8:70:b5	-
56	-26	6	h3c-psk	No	Yes	00:23:89:49:17:D0	1/18/2011 7:47 PM	Wireless AP scan	00:1a:1e:c0:1a:dc	-
68	-28	36	h3c-psk	No	Yes	00:23:89:49:17:C0	1/18/2011 7:47 PM	Wireless AP scan	00:1a:1e:c0:2b:34	-
64	-48	36	h3c-psk	-	-	00:23:89:49:17:C0	1/18/2011 7:45 PM	Wireless AP scan	ap92-c7:c0:ae	-
59	-53	6	h3c-psk	-	-	00:23:89:49:17:D0	1/18/2011 7:45 PM	Wireless AP scan	ap92-c7:c0:ae	-
50	-29	6	h3c-psk	-	-	00:23:89:49:17:D0	1/18/2011 7:44 PM	Wireless AP scan	ap125-C0:50:47	-
56	-40	6	h3c-psk	-	-	00:23:89:49:17:D0	1/18/2011 7:44 PM	Wireless AP scan	ap61-ca:75:ba	-
75	-21	36	h3c-psk	-	-	00:23:89:49:17:C0	1/18/2011 7:44 PM	Wireless AP scan	ap61-ca:75:ba	-

1-10 of 49 Discovery Events Page 1 of 5 > >|

Important things to remember regarding the information in the device detail page are:

- Users with the role of **Admin** can see all rogue AP devices.
- Users with roles limited by folder can *see* a rogue AP if there is at least one discovering device that they can see.
- The discovery events displayed are from APs that you can see on the network. There may be additional discovery events that remain hidden to certain user roles.
- Each rogue device frequently has multiple discovery methods, all of which are listed.
- As you work through the rogue devices, use the **Name** and **Notes** fields to identify the AP and document its location.
- You can use the global filtering options on the **RAPIDS > Setup** page to filter rogue devices according to signal strength, ad-hoc status, and discovered by remote APs.
- VisualRF uses the heard signal information to calculate the physical location of the device.
- If the device is seen on the wire, RAPIDS reports the switch and port for easy isolation.
- If you find that the rogue belongs to a neighboring business, for example, you can override the classification to a neighbor and acknowledge the device. Otherwise, Alcatel-Lucent strongly recommends that you extract the device from your building and delete the rogue device from your system. If you delete a rogue, you will be notified the next time it is discovered.

To update a rogue device:

1. Select the **Identify OS for Suspected Rogues** option if an IP address is available to obtain operating system information using an nmap scan. Note that if you are running wireline security software on your network, it may identify your OV3600 as a threat, which you can ignore.
2. Select the **Ignore** button if the rogue device is to be ignored. Ignored devices will not trigger alerts if they are rediscovered or reclassified.
3. Select the **Delete** button if the rogue device is to be removed from OV3600 processing.

Viewing Ignored Rogue Devices

The **RAPIDS > List** page allows you to view ignored rogues—devices that have been removed from the rogue count displayed by OV3600. Such devices do not trigger alerts and do not display on lists of rogue devices. To display ignored rogue devices, perform the following steps., select **View Ignored Rogues (**at the bottom left of the page).

Once a classification that has rogue devices is chosen from the drop-down menu, a detailed table displays all known information.

Using RAPIDS Workflow to Process Rogue Devices

One suggested workflow for using RAPIDS is as follows:

- Start from the **RAPIDS > List** page. Sort the devices on this page based on classification type. Begin with Rogue APs, working your way through the devices listed.
- Select **Modify Devices**, then select all devices that have an IP address and select **Identify OS**. OV3600 performs a port scan on the device and attempts to determine the operating system (see "Setting Up RAPIDS" on page 165)

  You should investigate devices running an embedded Linux OS installation. The OS scan can help identify false positives and isolate some devices that should receive the most attention.
- Find the port and switch at which the device is located and shut down the port or follow wiring to the device.
- To manage the rogue, remove it from the network and acknowledge the rogue record. If you want to allow it on the network, classify the device as valid and update with notes that describe it.

NOTE

Not all rogue discovery methods will have all information required for resolution. For example, the switch/router information, port, or IP address are found only through switch or router polling. Furthermore, RSSI, signal, channel, SSID, WEP, or network type information only appear through wireless scanning. Such information can vary according to the device type that performs the scan.

Score Override

On **RAPIDS > Score Override** page you can change the OUI scores that are given to MAC addresses detected during scans of bridge forwarding tables on routers or switches. Figure 123, Figure 124, and Table 102 illustrate and describe RAPIDS Score Override. Perform these steps to create a score override.

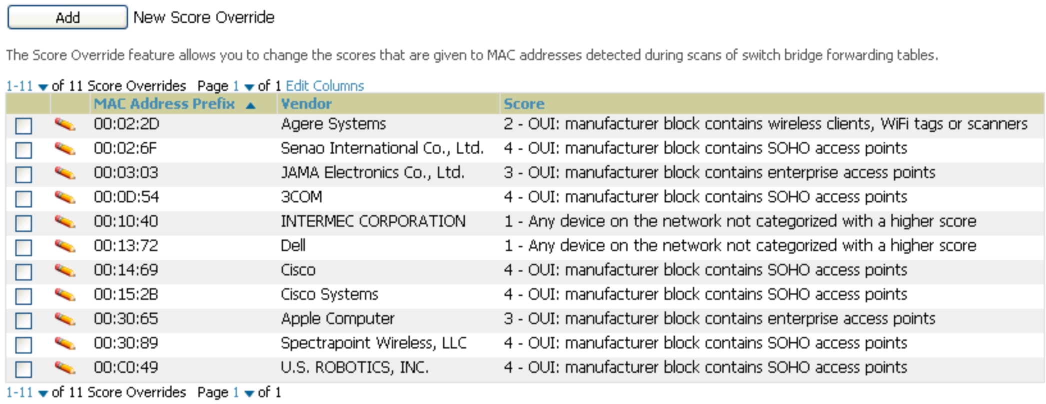
Once a new score is assigned, all devices with the specified MAC address prefix receive the new score.

NOTE

Note that rescoring a MAC Address Prefix poses a security risk. The block has received its score for a reason. Any devices that fall within this block receive the new score.

1. Navigate to the **RAPIDS > Score Override** page. This page lists all existing overrides if they have been created.

Figure 123 *RAPIDS > Score Override* Page



Add New Score Override

The Score Override feature allows you to change the scores that are given to MAC addresses detected during scans of switch bridge forwarding tables.

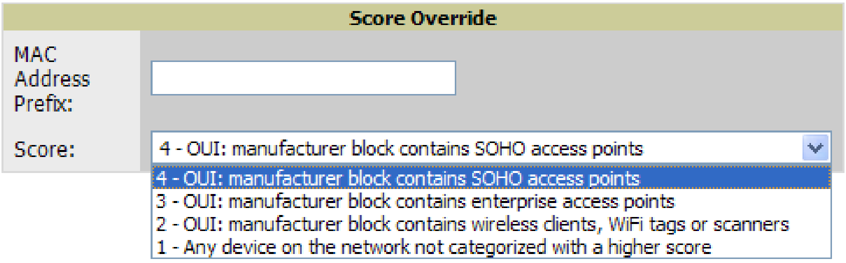
1-11 ▾ of 11 Score Overrides Page 1 ▾ of 1 Edit Columns

		MAC Address Prefix ▲	Vendor	Score
□	✎	00:02:2D	Agere Systems	2 - OUI: manufacturer block contains wireless clients, WiFi tags or scanners
□	✎	00:02:6F	Senao International Co., Ltd.	4 - OUI: manufacturer block contains SOHO access points
□	✎	00:03:03	JAMA Electronics Co., Ltd.	3 - OUI: manufacturer block contains enterprise access points
□	✎	00:0D:54	3COM	4 - OUI: manufacturer block contains SOHO access points
□	✎	00:10:40	INTERMEC CORPORATION	1 - Any device on the network not categorized with a higher score
□	✎	00:13:72	Dell	1 - Any device on the network not categorized with a higher score
□	✎	00:14:69	Cisco	4 - OUI: manufacturer block contains SOHO access points
□	✎	00:15:2B	Cisco Systems	4 - OUI: manufacturer block contains SOHO access points
□	✎	00:30:65	Apple Computer	3 - OUI: manufacturer block contains enterprise access points
□	✎	00:30:89	Spectrapoint Wireless, LLC	4 - OUI: manufacturer block contains SOHO access points
□	✎	00:C0:49	U.S. ROBOTICS, INC.	4 - OUI: manufacturer block contains SOHO access points

1-11 ▾ of 11 Score Overrides Page 1 ▾ of 1

2. Select **Add** to create a new override or select the pencil icon next to an existing override to edit that override. The **Score Override** add or edit page appears (Figure 124).

Figure 124 *Add/Edit Score Override* Page



Score Override

MAC Address Prefix:

Score: 4 - OUI: manufacturer block contains SOHO access points

4 - OUI: manufacturer block contains SOHO access points
3 - OUI: manufacturer block contains enterprise access points
2 - OUI: manufacturer block contains wireless clients, WiFi tags or scanners
1 - Any device on the network not categorized with a higher score

Table 102 *RAPIDS > Add/Edit Score Override* Page Fields

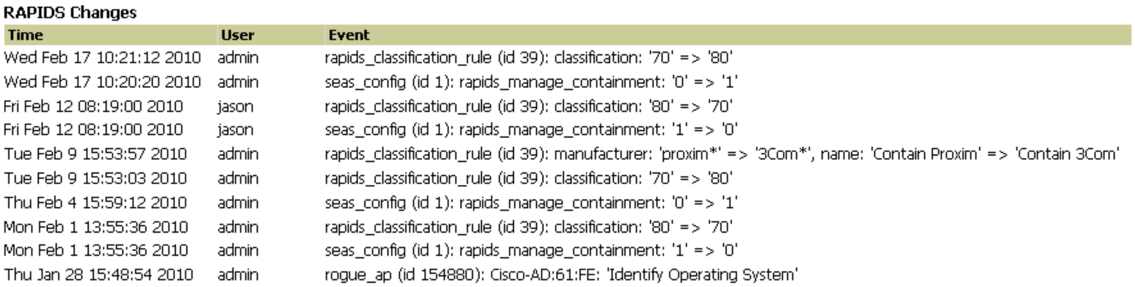
Field	Description
MAC Address Prefix	Use this field to define the OUI prefix to be re-scored.
Score	Use this field to set the score that a device, with the specified MAC address prefix, will receive.

3. Enter in the six-digit MAC prefix for which to define a score, and select the desired score. Once the new score has been saved, all detected devices with that prefix receive the new score.
4. Select **Add** to create the new override, or select **Save** to retain changes to an existing override. The new or revised override appears on the **RAPIDS > Score Override** page.
5. To remove any override, select that override in the checkbox and select **Delete**.

Audit Log

The Audit Log is a record of any changes made to the RAPIDS rules, setup page, and manual changes to specific rogues. This allows you to see how something is changes, when it changed, and who made the alteration. The Audit Log can be found at **RAPIDS > Audit Log**. See Figure 125 for more information.

Figure 125 *Audit Log*



RAPIDS Changes

Time	User	Event
Wed Feb 17 10:21:12 2010	admin	rapids_classification_rule (id 39): classification: '70' => '80'
Wed Feb 17 10:20:20 2010	admin	seas_config (id 1): rapids_manage_containment: '0' => '1'
Fri Feb 12 08:19:00 2010	jason	rapids_classification_rule (id 39): classification: '80' => '70'
Fri Feb 12 08:19:00 2010	jason	seas_config (id 1): rapids_manage_containment: '1' => '0'
Tue Feb 9 15:53:57 2010	admin	rapids_classification_rule (id 39): manufacturer: 'proxim*' => '3Com*', name: 'Contain Proxim' => 'Contain 3Com'
Tue Feb 9 15:53:03 2010	admin	rapids_classification_rule (id 39): classification: '70' => '80'
Thu Feb 4 15:59:12 2010	admin	seas_config (id 1): rapids_manage_containment: '0' => '1'
Mon Feb 1 13:55:36 2010	admin	rapids_classification_rule (id 39): classification: '80' => '70'
Mon Feb 1 13:55:36 2010	admin	seas_config (id 1): rapids_manage_containment: '1' => '0'
Thu Jan 28 15:48:54 2010	admin	rogue_ap (id 154880): Cisco-AD:61:FE: 'Identify Operating System'

Additional Security Resources

The following OV3600 tools support RAPIDS:

- **System Triggers and Alerts**—Triggers and Alerts that are associated with rogue devices follow the classification-based system described in this chapter. For additional information about triggers that support rogue device detection, see to “Monitoring and Supporting OV3600 with the System Pages” on page 204.
- **Reports**—The **Rogue Devices Report** displays summary and detail information about all rogues first discovered in a given time period. For more information, see “Defining Reports” on page 241.

For additional security-related features and functions, see the following topics in this guide.

- “Configuring Group Security Settings” on page 80
- “Configuring Security Parameters and Functions” on page 96
- “Configuring Group SSIDs and VLANs” on page 83
- “Monitoring and Supporting OV3600 with the System Pages” on page 204
- Appendix B, “Third-Party Security Integration for OV3600” on page 257

Chapter 8

Performing Daily Administration in OV3600

Daily WLAN administration often entails network monitoring, supporting WLAN and OV3600 users, and monitoring OV3600 system operations.

This chapter contains the following administration procedures:

- "Overview of Triggers and Alerts" on page 179
- "Monitoring and Supporting WLAN Users" on page 187
- "Evaluating and Diagnosing User Status and Issues" on page 192
- "Managing Mobile Devices with SOTI MobiControl and OV3600" on page 195
- "Upgrading OV3600" on page 215
- "Backing Up OV3600" on page 214
- "Monitoring and Supporting OV3600 with the System Pages" on page 204
- "Backing Up OV3600" on page 215

Overview of Triggers and Alerts

This section describes triggers and alerts and contain the following topics:

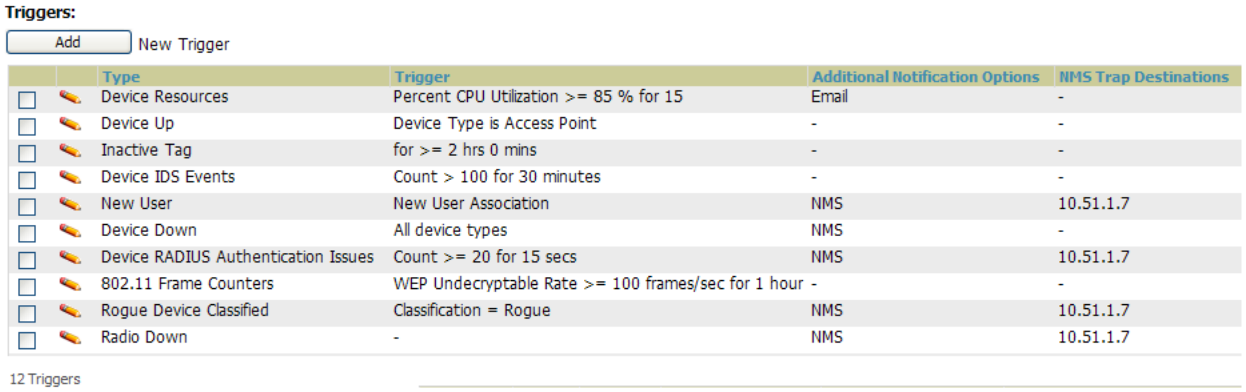
- Viewing Triggers
- Creating New Triggers
- Delivering Triggered Alerts
- Viewing Alerts
- Responding to Alerts

OV3600 monitors key aspects of wireless LAN performance. When certain parameters or conditions arise that are outside normal bounds, OV3600 generates (or triggers) alerts that enable you to address problems, frequently before users have a chance to report them.

Viewing Triggers

To view defined system triggers, navigate to the **System > Triggers** page. Figure 126 illustrates this page.

Figure 126 ***System > Triggers*** *Page Illustration (partial view)*



		Type	Trigger	Additional Notification Options	NMS Trap Destinations
□	✎	Device Resources	Percent CPU Utilization >= 85 % for 15	Email	-
□	✎	Device Up	Device Type is Access Point	-	-
□	✎	Inactive Tag	for >= 2 hrs 0 mins	-	-
□	✎	Device IDS Events	Count > 100 for 30 minutes	-	-
□	✎	New User	New User Association	NMS	10.51.1.7
□	✎	Device Down	All device types	NMS	-
□	✎	Device RADIUS Authentication Issues	Count >= 20 for 15 secs	NMS	10.51.1.7
□	✎	802.11 Frame Counters	WEP Undecryptable Rate >= 100 frames/sec for 1 hour	-	-
□	✎	Rogue Device Classified	Classification = Rogue	NMS	10.51.1.7
□	✎	Radio Down	-	NMS	10.51.1.7

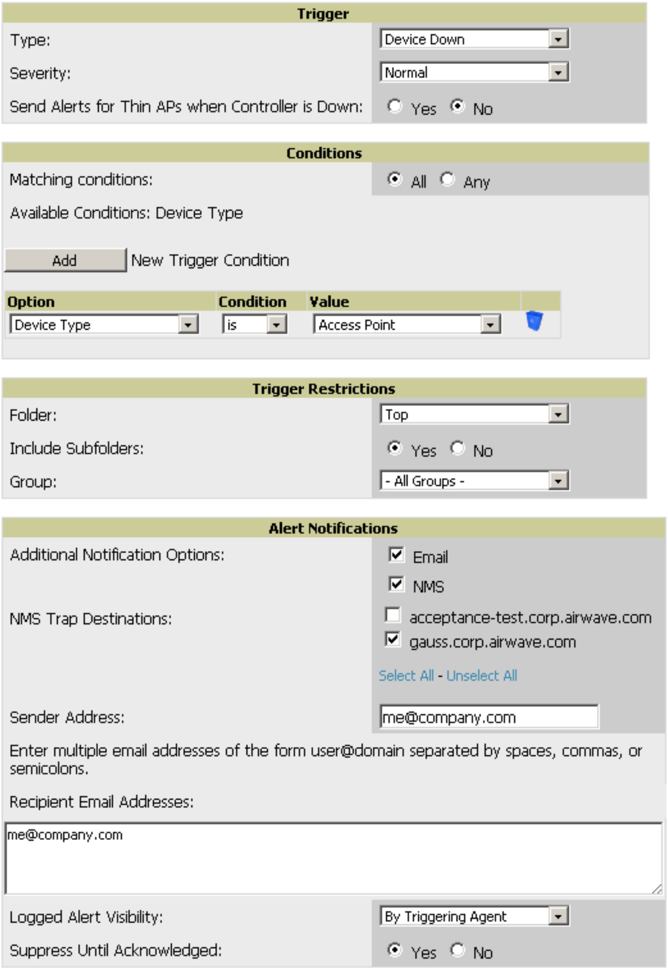
12 Triggers

Creating New Triggers

Perform the following steps to create and configure one or more new triggers. These steps define settings that are required for any type of trigger.

1. To create a new trigger, select the **Add New Trigger** button from the **System > Triggers** page. The page that appears is illustrated in Figure 127.

Figure 127 ***Add New Trigger*** *Page Illustration*



Trigger

Type: Device Down

Severity: Normal

Send Alerts for Thin APs when Controller is Down: ○ Yes ● No

Conditions

Matching conditions: ● All ○ Any

Available Conditions: Device Type

Add | New Trigger Condition

Option	Condition	Value
Device Type	is	Access Point

Trigger Restrictions

Folder: Top

Include Subfolders: ● Yes ○ No

Group: - All Groups -

Alert Notifications

Additional Notification Options: ☑ Email ☑ NMS

NMS Trap Destinations: ☐ acceptance-test.corp.airwave.com ☑ gauss.corp.airwave.com

Select All - Unselect All

Sender Address: me@company.com

Enter multiple email addresses of the form user@domain separated by spaces, commas, or semicolons.

Recipient Email Addresses:

me@company.com

Logged Alert Visibility: By Triggering Agent

Suppress Until Acknowledged: ● Yes ○ No

2. Configure the **Trigger Restrictions** and **Alert Notifications**. This configuration is consistent regardless of the trigger type to be defined.

   a. The **Trigger Restrictions** settings establishes how widely or how narrowly the trigger applies. Define the folder, subfolder, and Group covered by this trigger. Table 103 describes the options for trigger restrictions.

Table 103 ***System > Trigger Details*** *Fields and Default Values*

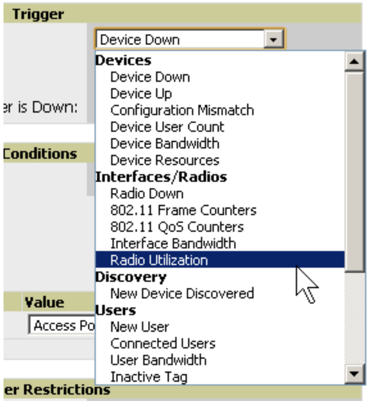
Notification Option	Description
Folder	Sets the trigger to apply only to APs/Devices in the specified folder or subfolders depending on the **Include Subfolders** option. **NOTE:** If the trigger is restricted by folder and group, it only applies to the intersection of the two—it only applies to APs in the group and in the folder.
Include Subfolders	Sets the trigger to apply to all devices in the specified folder and all of the devices in folders under the specified folder.
Group	Sets the trigger to apply only to APs/Devices in the specified group. **NOTE:** If the trigger is restricted by folder and group, it only applies to the intersection of the two—it only applies to APs in the group and in the folder.

b. In addition to appearing on the **System > Alerts** page, the **Alert Notifications** settings can be configured to distribute to email or to a network management system (NMS), or to both.

  - If you select **Email**, you are prompted to set the sender's email address and recipient email addresses.
  - If you select **NMS**, you are prompted to choose one or more of the pre-defined trap destinations, which are configured on the **OV3600 Setup > NMS** page.
  - Define the **Logged Alert Visibility**, in which you can choose how this trigger is distributed. The trigger can distribute according to how is it generated (**triggering agent**), or by the **role** with which it is associated.
  - The **Suppress Until Acknowledged** setting defines whether the trigger requires manual and administrative acknowledgement to gain visibility. If **No** is selected, a new alert will be created every time the trigger criteria are met. If **Yes**, an alert will only be received the first time the criteria is met. A new alert for the device is not created until the initial one is acknowledged.

3. In the **Trigger** section, choose the desired trigger **Type** and **Severity**. Figure 128 illustrates some of the supported trigger types. Severity levels are indicated in the email alerts. The alert summary information at the top of the OV3600 screen can be configured to separately display severe alerts. Please see the **Home > User Info** section for more details.

Figure 128 ***System > Triggers > Add Trigger Type*** *Drop-down Menu*



Once you have selected a trigger type, the **Add Trigger** page changes. In many cases, you must configure at least one **Condition** setting. Conditions, settings, and default values vary according to trigger type. Triggers with conditions can be configured to fire if any criteria match as well as if all criteria match.

- Some trigger types share common settings, such as **Duration** (which can be expressed in hours, minutes, seconds, or a combination of these) and **Severity** (from Normal to Critical).
- After you select **Save**, the trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.
- You can edit or delete any trigger as desired from the **System > Triggers** page.
  - To edit an existing trigger, select the pencil icon next to the respective trigger and edit settings in the **Trigger Detail** page described in Table 104.
  - To delete a trigger, check the box next to the trigger to remove, and select **Delete**.

Repeat this procedure for as many triggers and conditions as desired.

Complete the creation of your trigger type using one of the following procedures for each trigger:

- "Setting Triggers for Devices" on page 182
- "Setting Triggers for Radios" on page 182
- "Setting Triggers for Discovery" on page 183
- "Setting Triggers for Users" on page 183
- "Setting Triggers for RADIUS Authentication Issues" on page 184

- "Setting Triggers for IDS Events" on page 184
- "Setting Triggers for OV3600 Health" on page 185

Setting Triggers for Devices

Perform the following steps to complete the configuration of device-related triggers.

a. Choose a device type from the **Devices** listed in the **Type** drop-down menu. See Figure 128. Table 104 itemizes and describes device trigger options and condition settings.

Table 104 *Device Trigger Types*

Option	Description
Device Down	This is the default type whenever configuring a new trigger. This type of trigger activates when an authorized, monitored AP has failed to respond to SNMP queries from OV3600. To set the conditions for this trigger type, select **Add** in the **Conditions** section. Complete the conditions with the **Option**, **Condition**, and **Value** drop-down menus. The conditions establish the device type. Multiple conditions can apply to this type of trigger. The Device Down trigger can be configured to send alerts for thin APs when the controller is down; this behavior is turned off by default.
Device Up	This trigger type activates when an authorized, previously down AP is now responding to SNMP queries. To set the conditions for this trigger type, select **Add** in the **Conditions** section.
Configuration Mismatch	This trigger type activates when the actual configuration on the AP does not match the defined **Group** configuration policy. To set the conditions for this trigger type, select **Add** in the **Conditions** section.
Device User Count	Activates when a device reaches a user-count threshold for more than a specified period (such as more than 10 users associated for more than 60 seconds).
Device Bandwidth	Activates when the total bandwidth through the device has exceeded a predefined threshold for more than a specified period (such as more than 1500kbps for more than 120 seconds). You can also select bandwidth direction and page/radio. Selecting this type displays the following new fields in the **Type** section. Define these settings. ● **Alert if Device Bandwidth >= (kbps)**—This threshold establishes a device-specific bandwidth policy, not a bandwidth policy on the network as a whole. ● **Bandwidth Direction**—Choose **In**, **Out**, or **Combined**. This bandwidth is monitored on the device itself, not on the network as a whole.
Device Resources	This type of trigger indicates that the CPU or memory utilization for a device (including router or switch) has exceeded a defined percentage for a specified period of time.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 180 to create a new trigger.

Setting Triggers for Radios

Perform the following steps to complete the configuration of radio-related triggers.

a. Choose a trigger type from the **Radios** category, listed in the **Type** drop-down menu. Table 105 itemizes and describes the radio trigger types and condition settings.

Table 105 *Radio-Related Trigger Types*

Radio Trigger Options	Description
Radio Down	Indicates that a device's radio is down on the network. Once you choose this trigger type, select **Add New Trigger Condition** to create at least one condition. This type requires that a radio capability be set as a condition. The **Value** drop-down menu supports several condition options.

Table 105 *Radio-Related Trigger Types (Continued)*

Radio Trigger Options	Description
802.11 Frame Counters	Enables monitoring of traffic levels. There are multiple rate-related parameters for which you define conditions including ACK Failures, Retry Rate, and Rx Fragment Rate. See the **Option** drop-down menu in the **Conditions** section of the trigger page for a complete list of parameters. Select **Add New Trigger Condition** to access these settings. Define at least one condition for this trigger type.
802.11 QoS Counters	Enables monitoring of Quality of Service (QoS) parameters on the network, according to traffic type. The rate of different parameters includes ACK Failures, Duplicated Frames and Transmitted Fragments. See the drop-down field menu in the conditions section of the trigger page for a complete list of parameters. Select **Add New Trigger Condition** to access these settings. Define at least one condition for this trigger type.
Interface Bandwidth	Interface labels defined on the trigger page will be used to set up triggers on one or more interfaces and/or radios. Available conditions are **Device Type**, **Interface Description**, **Interface Label**, **Interface Mode**, **Interface Speed In (Mbps)**, **Interface Speed Out (Mbps)**, **Interface Type**, and **Radio Type**.
Radio Utilization	Indicates that channel utilization has crossed particular thresholds. Available conditions are **Interference (%)**, **Radio Type**, **Time Busy (%)**, **Time Receiving (%)**, and **Time Transmitting (%)**.

Setting Triggers for Discovery

Perform the following steps to complete the configuration of triggers related to device discovery.

a. If you have not already done so, choose a trigger type from the **Discovery** category, listed in the **Type** drop-down menu. See Figure 128. Table 106 itemizes and describes the Discovery-related trigger types, and condition settings for each discovery trigger type.

Table 106 *Discovery Trigger Types and Condition Settings*

Discovery Trigger Options	Description
New Devices Discovered	This trigger type flags the discovery of a new AP, router or switch connected to the network (a device that OV3600 can monitor and configure). Once you choose this trigger type, select **Add New Trigger Condition** to specify a device type.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 180 to create a new trigger.

Setting Triggers for Users

Perform the following steps to complete the configuration of user-related triggers.

a. If you have not already done so, choose a trigger type from the **Users** category, listed in the **Type** drop-down menu. See Figure 128. Table 107 itemizes and describes the User-related trigger types, and condition settings for each discovery trigger type.

Table 107 *User Trigger Types and Condition Settings*

User Trigger Option	Description
New User	This trigger type indicates when a new user has associated to a device within a defined set of groups or folders. Note that the **New User** trigger type does not require the configuration of any condition settings, so the **Condition** section disappears.
Connected Users	This trigger type indicates when a device (based on an input list of MAC addresses) has associated to the wireless network. It is required to define one or more MAC addresses with the field that appears.

Table 107 *User Trigger Types and Condition Settings (Continued)*

User Trigger Option	Description
User Bandwidth	This trigger type indicates that the sustained rate of bandwidth used by an individual user has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 1500kbps for more than 120 seconds). Once you choose this trigger type, select **Add New Trigger Condition** to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger. The **Value** field requires that you input a numerical figure for kilobits per second (kbps).
Inactive Tag	This tags flags events when an RFID tag has not been reported back to OV3600 by a controller for more than a certain number of hours. This trigger can be used to help identify inventory that might be lost or stolen. Set the time duration for this trigger type if not already completed.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 180 to create a new trigger.

Setting Triggers for RADIUS Authentication Issues

Perform the following steps to complete the configuration of RADIUS-related triggers.

a. If you have not already done so, choose a trigger type from the **RADIUS...** list in the drop-down **Type** menu. Table 108 itemizes and describes the condition settings for each **RADIUS Authentication** trigger type.

Table 108 *RADIUS Authentication Trigger Types and Condition Settings*

Option	Description
User RADIUS Authentication Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a user. Select **Add New Trigger Condition** to specify the count characteristics that trigger an alert. The **Option**, **Condition**, and **Value** fields allow you to define the numeric value of user issues.
Device RADIUS Authentication Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a device. The **Option**, **Condition**, and **Value** fields allow you to define the numeric value of user issues.
Total RADIUS Authentication Issues	This trigger sets the threshold for the maximum number of failures before an alert is issued for both users and devices.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 180 to create a new trigger.

Setting Triggers for IDS Events

Perform the following steps to complete the configuration of Intrusion Detection System (IDS)-related triggers.

a. If you have not already done so, choose the **Device IDS Events** trigger type from the drop-down **Type** menu. See Figure 128. Table 109 describes condition settings for this trigger type.

Table 109 *Device IDS Events Authentication Trigger Types and Condition Settings*

IDS Trigger Options	Description
Device IDS Events	This trigger type is based on the number of IDS events has exceeded the threshold specified as Count in the Condition within the period of time specified in seconds in Duration. Alerts can also be generated for traps based on name, category or severity. Select **Add New Trigger Condition** to specify the count characteristics that trigger an IDS alert.

Table 109 *Device IDS Events Authentication Trigger Types and Condition Settings*

IDS Trigger Options	Description
Rogue Device Classified	This trigger type indicates that a device has been discovered with the specified Rogue Score. Ad-hoc devices can be excluded automatically from this trigger by selecting **Yes**. See "Using RAPIDS and Rogue Classification" on page 163 for more information on score definitions and discovery methods. Select **Add New Trigger Condition** to create one or more conditions. A condition for this trigger enables you to specify the nature of the rogue device in multiple ways.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 180 to create a new trigger.

Setting Triggers for OV3600 Health

Perform the following steps to complete the configuration of IDS-related triggers.

a. If you have not already done so, choose the **Disk Usage** trigger type from the drop-down **Type** menu. See Figure 128 for trigger types. Table 110 describes the condition settings for this trigger type.

Table 110 *Disk Usage Trigger and Condition Settings*

OV3600 Health Trigger	Description
Disk Usage	This trigger type is based on the disk usage of OV3600. This type of trigger indicates that disk usage for the OV3600 server has met or surpassed a defined threshold. Select **Add New Trigger Condition** to specify the disk usage characteristics that trigger an alert. Alcatel-Lucent recommends setting one of these triggers at **90%** so you receive a warning before OV3600 suffers performance degradation due to lack of disk space.

b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 180 to create a new trigger.

Delivering Triggered Alerts

OV3600 uses Postfix to deliver alerts and reports via email because it provides a high level of security and queues email locally until delivery. If OV3600 is located behind a firewall, preventing it from sending email directly to a specified recipient, use the following procedures to forward email to a smarthost.

1. Add the following line to /etc/postfix/main.cf:

   ```
   relayhost = [mail.example.com]
   where mail.example.com is the IP address or hostname of your smarthost
   ```

2. Run `service postfix restart`.
3. Send a test message to an email address:

   ```
   Mail -v user@example.com
   Subject: test mail
   .
   CC:
   ```

4. Press **Enter**.
5. Check the mail log to ensure mail was sent:

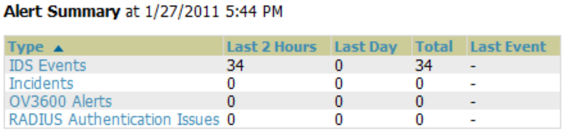
   ```
   tail -f /var/log/maillog
   ```

Viewing Alerts

OV3600 displays alerts and provides additional alert details in two ways, as follows:

1. The **Alerts Summary** table is one way to monitor and process OV3600 alerts. The **Alert Summary** table is available on the following OV3600 pages, and is illustrated in Figure 129:
   - **APs/Devices > List**
   - **Groups > Monitor**
   - **Home > Overview**
   - **Users > Connected** or **User Detail**

Figure 129 ***Alert Summary*** *Table Illustration*



Alert Summary at 1/27/2011 5:44 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
IDS Events	34	0	34	-
Incidents	0	0	0	-
OV3600 Alerts	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

This table displays alerts as follows; select the alert **Type** to display alert details:

- **OV3600 Alerts**—Displays details for all device alerts.
- **IDS Events**—Displays details of all Intrusion Detection System (IDS) events and attacks under the RAPIDS tab. You must have a RAPIDS license and be enabled as a RAPIDS user to see this page.
- **Incidents**—Displays recent helpdesk incidents in which the incidents are open and associated to an AP. For a complete listing of incidents, navigate to the **Helpdesk > Incidents** page.

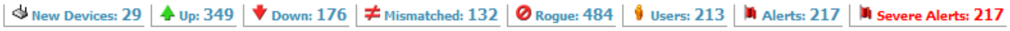
NOTE

The **Incidents** portion of this **Alert Summary** table only increments the counter for incidents that are open and associated to a Device, Group, or Folder. Unassociated incidents are not are not counted in this **Alert Summary**. To view all incidents, including those not associated to an AP, navigate to the **Helpdesk > Incidents** page.

- **RADIUS Authentication Issues**—Displays RADIUS-related alerts for devices in the top viewable folder available to the OV3600 user. The detailed list displays the MAC address, username, AP, radio, controller, RADIUS server, and time of each event. Alerts can be sorted by any column.

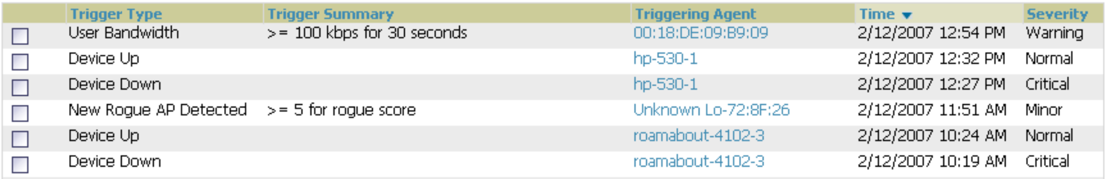
2. The second way to display and process alerts is to use the **Alerts** and **Severe Alerts** counters in the **Status** bar at the top of all OV3600 pages, illustrated in Figure 130. The Severe Alert Threshold can be configured on the **Home > User Info** page.

Figure 130 *Alerts in the OV3600 Status Bar*



Select the **Alerts** or the **Severe Alerts** counter or navigate to the **System > Alerts** page. Figure 131 illustrates this page.

Figure 131 ***System > Alerts*** *Page Illustration*



	Trigger Type	Trigger Summary	Triggering Agent	Time ▼	Severity
□	User Bandwidth	>= 100 kbps for 30 seconds	00:18:DE:09:B9:09	2/12/2007 12:54 PM	Warning
□	Device Up		hp-530-1	2/12/2007 12:32 PM	Normal
□	Device Down		hp-530-1	2/12/2007 12:27 PM	Critical
□	New Rogue AP Detected	>= 5 for rogue score	Unknown Lo-72:8F:26	2/12/2007 11:51 AM	Minor
□	Device Up		roamabout-4102-3	2/12/2007 10:24 AM	Normal
□	Device Down		roamabout-4102-3	2/12/2007 10:19 AM	Critical

For each new alert, the **System > Alerts** page displays the items listed in Table 111.

Table 111 ***System > Alerts*** *Fields and Default Settings*

Field	Description
Trigger Type	Displays and sorts triggers by the type of trigger.
Trigger Summary	Provides an additional summary information related to the trigger.
Triggering Agent	Lists the name of the AP that generated the trigger. Select the name to display its **APs/ Devices > Manage** page.
Time	Displays the date and time the trigger was generated.

Table 111 ***System > Alerts*** *Fields and Default Settings*

Field	Description
Severity	Displays the severity code associated with that trigger.

Responding to Alerts

Once you have viewed an alert, you may take one of the following courses of action:

- Leave it in active status if it is unresolved. The alert remains on the **New Alerts** list until you acknowledge or delete it. If an alert already exists, the trigger for that AP or user does not create another alert until the existing alert has been acknowledged or deleted.
- Move the alert to the Alert Log by selecting it and selecting **Acknowledge**.
- You may see all logged alerts by selecting the **View logged alerts** link at the top of the **System > Alerts** page. Select the **New Alerts** link to return to the list of new alerts.
- Delete the alert by selecting it from the list and selecting **Delete**.

Monitoring and Supporting WLAN Users

The OV3600 **Users** pages support WLAN users in OV3600. This section describes the **Users** pages as follows:

- Overview of the Users Pages
- Monitoring WLAN Users with the Users > Connected and Users > All Pages
- Supporting Guest WLAN Users With the Users > Guest Users Page
- Supporting RFID Tags With the Users > Tags Page
- See also Evaluating and Diagnosing User Status and Issues.

For information about creating OV3600 users and OV3600 user roles, refer to:

- Creating OV3600 Users
- Creating OV3600 User Roles

If you need to create an OV3600 user account for frontline personnel who are to support Guest WLAN users, refer to "Supporting Guest WLAN Users With the Users > Guest Users Page" on page 189.

Overview of the Users Pages

The **Users** pages display multiple types of user data for existing WLAN users. The data comes from a number of locations, including data tables on the access points, information from RADIUS accounting servers, and OV3600-generated data. OV3600 supports the following **Users** pages:

- **Users > Connected**—Displays active users that are currently connected to the WLAN. Refer to "Monitoring WLAN Users with the Users > Connected and Users > All Pages" on page 188.
- **Users > All**—Displays all users of which OV3600 is aware, with related information. Non-active users are listed in gray text. For a description of the information supported on this page, refer to "Monitoring WLAN Users with the Users > Connected and Users > All Pages" on page 188.
- **Users > Guest Users**—Displays all guest users in OV3600 and allows you to create, edit, or delete guest users. See "Supporting Guest WLAN Users With the Users > Guest Users Page" on page 189.
- **Users > User Detail**—Displays client device information, alerts, signal quality, bandwidth, and association history. This page appears when you select a user's MAC address from:
  - **Users > Connected**
  - **Users > All**
  - **Home > Search** page results or **Search** field results that display the user MAC address

  See "Evaluating and Diagnosing User Status and Issues" on page 192.

- **Users > Diagnostics**—Displays possible client device issues, diagnostic summary data, user counts, AP information, 802.11 counters summary, and additional information. This page appears when you select a user's MAC address from one of the following pages:
  - **Users > Connected**
  - **Users > All**
  - **Home > Search** page results or **Search** field results that display the user MAC address

  See "Evaluating and Diagnosing User Status and Issues" on page 192.
- **Users > Tags**—Displays a list of wireless tags, such as Aeroscout, PanGo and Newbury, that are heard by thin APs, and reported back to a controller that is monitored by OV3600. "Supporting RFID Tags With the Users > Tags Page" on page 191.

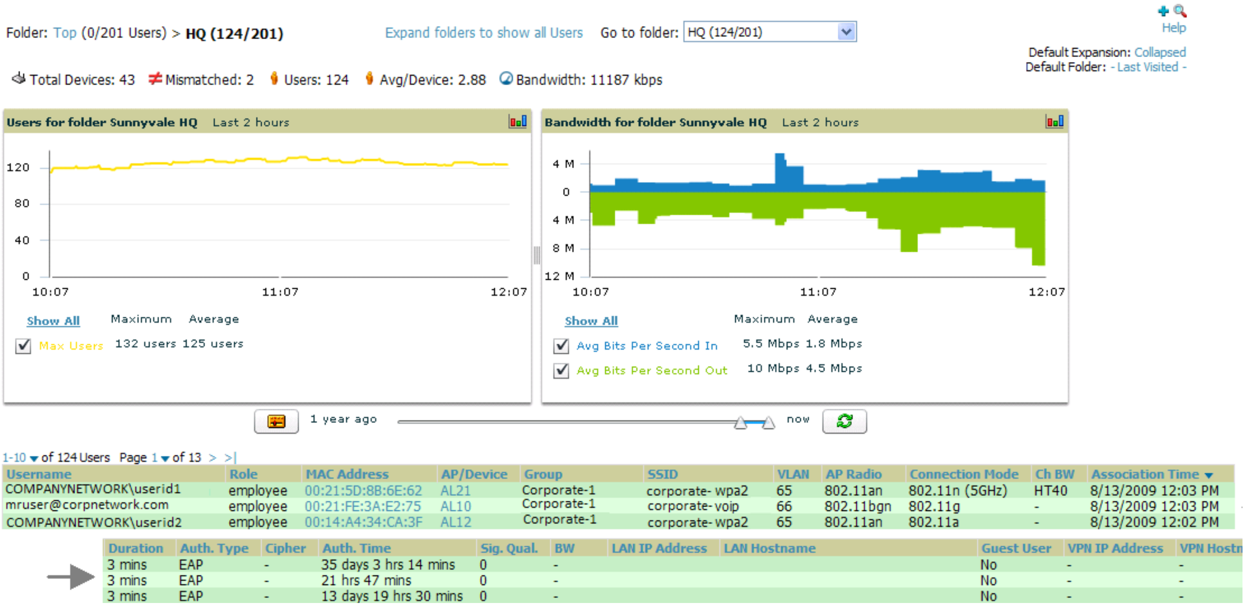
Monitoring WLAN Users with the Users > Connected and Users > All Pages

The **Users > Connected** page displays all users currently connected in OV3600, and is illustrated in Figure 132 and described in Table 112. The information on this page can be adjusted in the following ways:

- Drag the slider to pick the time range on the interactive graphs, and select **Show All** to select other options to display.
- The **Alerts** section displays custom configured alerts that were defined in the **System > Alerts** page.

In more recent versions of OV3600, the **Users > Connected** page includes SSID information for users, and can display wired users using remote Access Point (RAP) devices in tunnel and split-tunnel mode.

Figure 132 ***Users > Connected*** *Page Illustration*



Folder: Top (0/201 Users) > HQ (124/201)   Expand folders to show all Users   Go to folder: HQ (124/201)

Default Expansion: Collapsed
Default Folder: - Last Visited -

Total Devices: 43   Mismatched: 2   Users: 124   Avg/Device: 2.88   Bandwidth: 11187 kbps

Help
Users for folder Sunnyvale HQ   Last 2 hours
120
80
40
0
10:07
11:07
12:07
Show All
Maximum
Average
☑ Max Users   132 users   125 users
Bandwidth for folder Sunnyvale HQ   Last 2 hours
4 M
0
4 M
8 M
12 M
10:07
11:07
12:07
Show All
Maximum
Average
☑ Avg Bits Per Second In   5.5 Mbps   1.8 Mbps
☑ Avg Bits Per Second Out   10 Mbps   4.5 Mbps
1 year ago
now

1-10 of 124 Users Page 1 of 13 > >|

Username	Role	MAC Address	AP/Device	Group	SSID	VLAN	AP Radio	Connection Mode	Ch BW	Association Time
COMPANYNETWORK\userid1	employee	00:21:5D:8B:6E:62	AL21	Corporate-1	corporate- wpa2	65	802.11an	802.11n (5GHz)	HT40	8/13/2009 12:03 PM
mruser@corpnetwork.com	employee	00:21:FE:3A:E2:75	AL10	Corporate-1	corporate- voip	66	802.11bgn	802.11g	-	8/13/2009 12:03 PM
COMPANYNETWORK\userid2	employee	00:14:A4:34:CA:3F	AL12	Corporate-1	corporate- wpa2	65	802.11an	802.11a	-	8/13/2009 12:02 PM

Duration	Auth. Type	Cipher	Auth. Time	Sig. Qual.	BW	LAN IP Address	LAN Hostname	Guest User	VPN IP Address	VPN Hostn
3 mins	EAP	-	35 days 3 hrs 14 mins	0	-			No	-	-
3 mins	EAP	-	21 hrs 47 mins	0	-			No	-	-
3 mins	EAP	-	13 days 19 hrs 30 mins	0	-			No	-	-

Table 112 ***Users > Connected*** *Table Columns and Links*

Field	Description
Username	Displays the name of the user associated to the AP. OV3600 gathers this data from device traps, SNMP polling, or RADIUS accounting. Usernames appear in italics when a username for that MAC address has been stored in the database from a previous association, but OV3600 is not getting a username for the current association. This may indicate that the user has not yet been authenticated for this session or OV3600 may not be getting a username from an external source like a RADIUS server for this association.
Role	Specifies the role by which the user is connected.
MAC Address	Displays the MAC address of the user associated to APs. Also displays a link that redirects to the **Users > User Detail** page.

Table 112 ***Users*** **>** ***Connected*** *Table Columns and Links (Continued)*

Field	Description
AP/Device	Displays the name of the AP to which the MAC address is associated. Also displays a link that takes you to this AP's **AP Monitoring** page.
Group	Displays the group containing the AP that the user is associated with.
SSID	Displays the SSID with which the user is associated.
VLAN	Displays the VLAN assigned to the user, if available.
AP Radio	Displays the radio type of the radio that the user is associated with.
Connection Mode	Displays the 802.11 mode by which the user is connected.
Ch BW	Displays the channel bandwidth that currently supports 802.11n users.
Connection Mode	Displays the Radio mode used by the user to associate to the AP for 802.11n clients.
Association Time	Displays the first time OV3600 recorded the user for this association.
Duration	Displays the length of time the MAC address has been associated.
Auth. Type	Displays the type of authentication employed by the user: ● WPA2 (EAP-PEAP) is the standard setting. ● EAP is reported by Alcatel-Lucent devices and Cisco VxWorks via SNMP traps. ● RADIUS accounting servers integrated with OV3600 will provide the RADIUS Accounting Auth type. ● Web (PAP) - Captive Portal. ● All others are considered to be not authenticated.
Cipher	Displays WEP with keys. This data is also displayed in the **User Session** report in the **Session Data By User** section.
Auth. Time	Displays the how long ago the user authenticated. **NOTE:** This value displays as a negative number for unauthenticated users.
Sig. Qual.	Displays the average signal quality the user enjoyed.
BW	Displays the average bandwidth consumed by the MAC address.
Location	Displays the VisualRF QuickView box including heatmap for a device and user location history.
LAN IP Address	Displays the IP assigned to the user MAC. OV3600 gathers it from the association table of APs.
LAN Hostname	Displays the LAN hostname of the user MAC.
Guest User	Specifies whether the user is a guest.
VPN IP Address	Displays the VPN IP of the user MAC. This information can be obtained from VPN servers that send RADIUS accounting packets to OV3600.
VPN Hostname	Displays the VPN hostname of the user MAC.

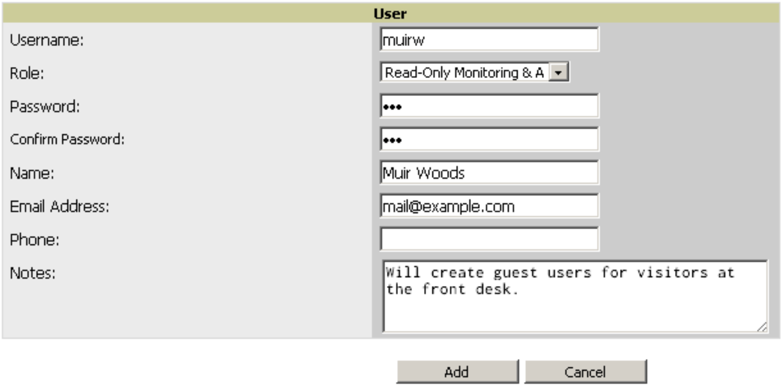
Supporting Guest WLAN Users With the Users > Guest Users Page

OV3600 supports guest user provisioning for Dell PowerConnect W, Alcatel-Lucent, Inc. and Cisco WLC devices. This allows frontline staff such as receptionists or help desk technicians to grant wireless access to WLAN visitors or other temporary personnel.

Perform the following steps in the pages described to configure these settings.

1. Navigate to the **OV3600 Setup > Roles** page and select the **Read-Only Monitoring & Auditing** role type. Under **Guest User Preferences**, enable **Allow creation of Guest Users**.
2. Next, navigate to the **OV3600 Setup > Users** page and create a new user with the role that was just created. Figure 133 illustrates this page.

Figure 133 ***OV3600 Setup > Users*** *Page Illustration*



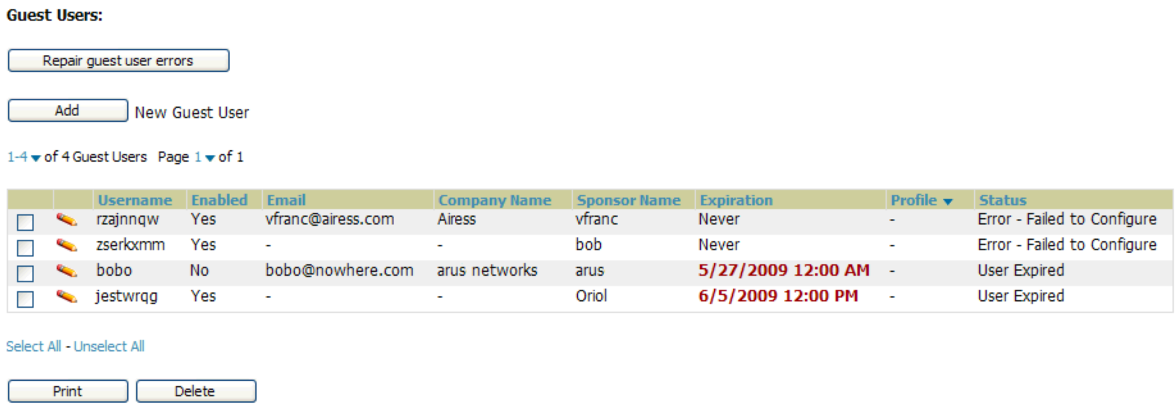
User

Username:	muirw
Role:	Read-Only Monitoring & A
Password:	•••
Confirm Password:	•••
Name:	Muir Woods
Email Address:	mail@example.com
Phone:	
Notes:	Will create guest users for visitors at the front desk.

3. The newly created login information should be provided to the person or people who will be responsible for creating guest access users.
4. The next step in creating a guest access user is to navigate to the **Users > Guest Users** tab. From this tab, you can add new guest users, you can edit existing users, and you can repair guest user errors.

   This page displays a list of guest users and data, to include the expiration date, the SSID (for Cisco WLC) and other information. Figure 134 illustrates this page and Table 113 describes the information.

Figure 134 ***Users > Guest Users*** *Page Illustration*



Guest Users:

1-4 of 4 Guest Users Page 1 of 1

		Username	Enabled	Email	Company Name	Sponsor Name	Expiration	Profile	Status
□		rzajnnqw	Yes	vfranc@airess.com	Airess	vfranc	Never	-	Error - Failed to Configure
□		zserkxmm	Yes	-	-	bob	Never	-	Error - Failed to Configure
□		bobo	No	bobo@nowhere.com	arus networks	arus	5/27/2009 12:00 AM	-	User Expired
□		jestwrqg	Yes	-	-	Oriol	6/5/2009 12:00 PM	-	User Expired

Table 113 ***Users > Guest Users*** *Fields*

Field	Description
Repair Guest User Errors	Sets OV3600 to attempt to push the guest user again in an attempt to repair any errors in the **Status** column.
Add New Guest User	Adds a new guest user to a controller via OV3600.
Username	Randomly generates a user name for privacy protection. This name appears on the **Guest User** detail page.
Enabled	Enables or disables the user status. Set the status of the guest user as active (enabled) or expired (disabled).
Email	Displays the optional email address of the user.
Company Name	Displays the optional company name for the user.

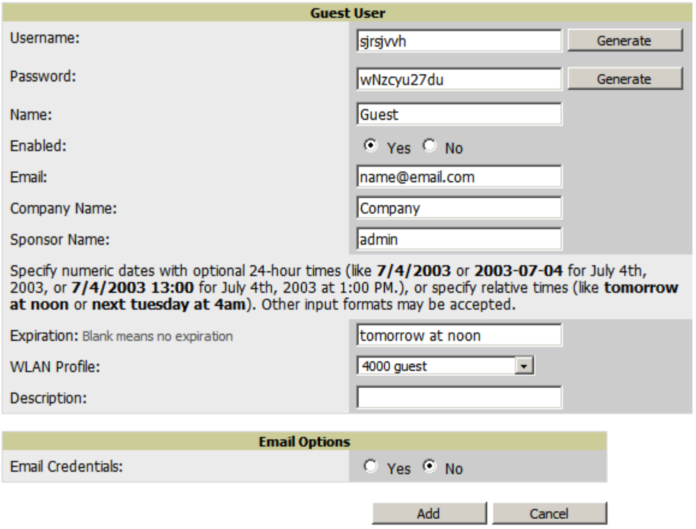
Table 113 ***Users > Guest Users*** *Fields (Continued)*

Field	Description
Sponsor Name	Displays the name of the sponsor for the guest user. This setting is optional.
Expiration	Displays the date the guest user's access is to expire.
WLAN Profile	Sets the SSID that the guest user can access. This setting applies to Cisco WLC only.
Status	Reports current status by the controller. If error messages appear in this column, select the user with the checkbox at left, and select the **Repair guest user errors** button.

Guest users associated to the wireless network appear on the same list as other wireless users, but are identified as guest users in the **Guest User** column. The **User Detail** page for a guest user also contains a box with the same guest information that appears for each user on the **Users > Guest Users** list.

5. To add a new guest user, select **Add**, and complete the fields illustrated in Figure 135. Table 113 above describes most fields. The first three fields are required, and the remaining fields are optional.

Figure 135 ***Users > Guest Users > Add New Guest User*** *Page Illustration*



Guest User

Username:	sjrsjvvh
Password:	wNzcyu27du
Name:	Guest
Enabled:	● Yes ○ No
Email:	name@email.com
Company Name:	Company
Sponsor Name:	admin

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

Expiration: Blank means no expiration	tomorrow at noon
WLAN Profile:	4000 guest
Description:	

Email Options

Email Credentials:	○ Yes ● No

To make the Username or Password anonymous and to increase security, complete these fields, then select **Generate**. The anonymous and secure **Username** and **Password** appear in the respective fields.

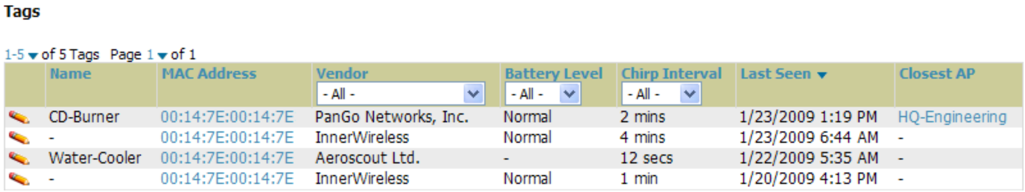
6. Select **Add** to complete the new guest user, or select **Cancel** to back out of new user creation. The **Users > Guest Users** page appears and displays results, as applicable.

Supporting RFID Tags With the Users > Tags Page

Radio Frequency Identification (RFID) is an industry-standard method that supports identifying and tracking wireless devices with radio waves. RFID uses radio wave tags for these and additional functions. Active tags have a battery and transmit signals autonomously, and passive tags have no battery. RFID tags often support additional and proprietary innovations that improve network integration, battery life, and other functions.

The **Users > Tags** page displays a list of wireless tags, such as Aeroscout, PanGo and Newbury, that are heard by thin APs, and reported back to a controller that OV3600 monitors. OV3600 displays the information it receives from the controller in a table on this page. Figure 136 illustrates this page, and Table 114 describes fields and information displayed.

Figure 136 ***Users > Tags*** *Page Illustration*



Tags

1-5 ▾ of 5 Tags Page 1 ▾ of 1

	Name	MAC Address	Vendor - All -	Battery Level - All -	Chirp Interval - All -	Last Seen ▾	Closest AP
✎	CD-Burner	00:14:7E:00:14:7E	PanGo Networks, Inc.	Normal	2 mins	1/23/2009 1:19 PM	HQ-Engineering
✎	-	00:14:7E:00:14:7E	InnerWireless	Normal	4 mins	1/23/2009 6:44 AM	-
✎	Water-Cooler	00:14:7E:00:14:7E	Aeroscout Ltd.	-	12 secs	1/22/2009 5:35 AM	-
✎	-	00:14:7E:00:14:7E	InnerWireless	Normal	1 min	1/20/2009 4:13 PM	-

Table 114 ***Users > Tags*** *Fields and Descriptions*

Field	Description
Name	Displays the user-editable name associated with the tag.
MAC Address	Displays the MAC address of the AP that reported the tag.
Vendor	Displays the vendor of the tag (Aeroscout, PanGo and Newbury)—display all or filter by type.
Battery Level	Displays battery information—filterable in drop-down menu at the top of the column; is not displayed for Aeroscout tags.
Chirp Interval	Displays the tag chirp frequency or interval, filterable from the drop-down menu at the top of the column. Note that the chirp interval from the RFID tag influences the battery life of active tags as well as search times. If a tag chirps with very long chirp interval, it may take longer time for the location engine to accurately measure x and y coordinates.
Last Seen	Date and time the tag was last reported to OV3600.
Closest AP	The AP that last reported the tag to the controller (linked to the AP monitoring page in OV3600).

- To edit the name of the tag, or to add notes to the tag's record, select the pencil icon next to the entry in the list. You can then add or change the name and add notes like "maternity ward inventory" or "Chicago warehouse," as two examples.
- There is also a **Tag Not Heard** trigger, which can be used to generate an alert if a tag is not reported to OV3600 after a certain interval. This can help to identify lost or stolen inventory. For more information about enabling this trigger, refer to the section "Monitoring and Supporting OV3600 with the System Pages" on page 204.

Evaluating and Diagnosing User Status and Issues

If a WLAN user reports difficulty with the wireless network, the administration or Helpdesk personnel can view and process related user information from the **User Detail** and **Diagnostic** pages. This section describes these two pages as follows:

- Evaluating User Status with the Users > User Detail Page
- Evaluating User Status with the Users > Diagnostics Page

Evaluating User Status with the Users > User Detail Page

The **Users > User Detail** page is a focused subtab that becomes visible when you select a specific user. Access the **Users > User Detail** page by selecting the MAC Address for a specific user from one of the following pages:

- **Users > Connected**
- **Users > All**

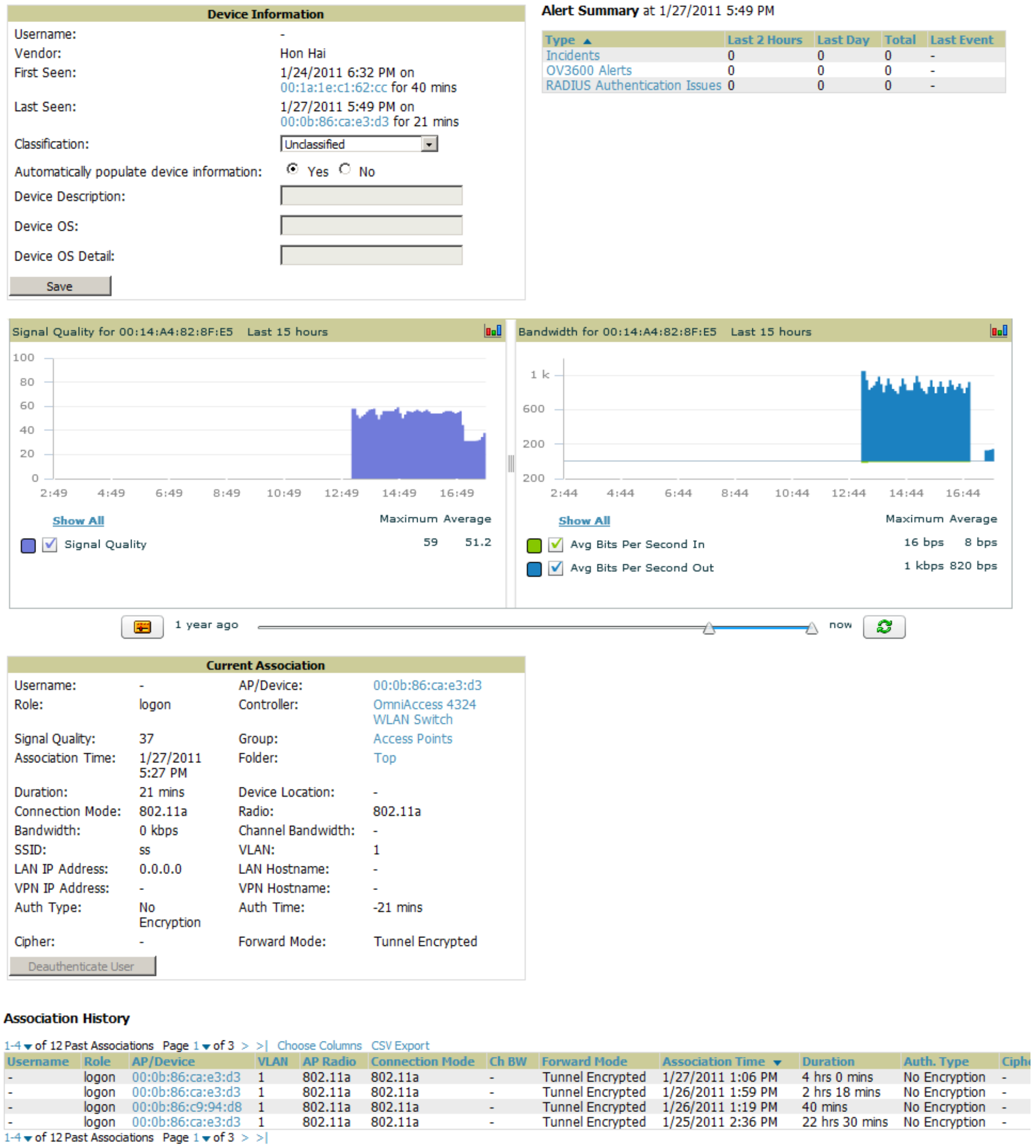
This page provides information for the wireless device, signal quality, and bandwidth consumption. This page also provides an AP association history and current association status. Finally, when VisualRF is licensed and enabled, this page provides a graphical map of the user location and facility information.

If you have deployed Alcatel-Lucent switches and have WMS Offload enabled on the network, the **Users > User Detail** page allows you to classify the device in the **Device Information** section, and to push this configuration to the Alcatel-Lucent switches that govern the devices. The classifications are as follows:

- **Unclassified**—Devices are unclassified by default.
- **Valid**—If the **Protect Valid Stations** option is enabled, this setting designates the device as a legitimate network device. Once this **Valid** setting is pushed, this setting prevents valid stations from connecting to a non-valid AP.
- **Contained**—When this status is pushed to the device, Alcatel-Lucent switches will attempt to keep it contained from the network.

You can classify the user regardless of whether WMS Offload is enabled. If WMS Offload is enabled, the classification will get pushed up to the switch. Figure 137 illustrates the **Users > User Details** page.

Figure 137 ***Users > User Detail** Page Illustration*



Device Information

Username:	-
Vendor:	Hon Hai
First Seen:	1/24/2011 6:32 PM on 00:1a:1e:c1:62:cc for 40 mins
Last Seen:	1/27/2011 5:49 PM on 00:0b:86:ca:e3:d3 for 21 mins
Classification:	Unclassified ▾
Automatically populate device information:	● Yes ○ No
Device Description:	
Device OS:	
Device OS Detail:	

Save

Alert Summary at 1/27/2011 5:49 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
Incidents	0	0	0	-
OV3600 Alerts	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Current Association

Username:	-	AP/Device:	00:0b:86:ca:e3:d3
Role:	logon	Controller:	OmniAccess 4324 WLAN Switch
Signal Quality:	37	Group:	Access Points
Association Time:	1/27/2011 5:27 PM	Folder:	Top
Duration:	21 mins	Device Location:	-
Connection Mode:	802.11a	Radio:	802.11a
Bandwidth:	0 kbps	Channel Bandwidth:	-
SSID:	ss	VLAN:	1
LAN IP Address:	0.0.0.0	LAN Hostname:	-
VPN IP Address:	-	VPN Hostname:	-
Auth Type:	No Encryption	Auth Time:	-21 mins
Cipher:	-	Forward Mode:	Tunnel Encrypted

Deauthenticate User

Association History

1-4 ▾ of 12 Past Associations Page 1 ▾ of 3 > >| Choose Columns CSV Export

Username	Role	AP/Device	VLAN	AP Radio	Connection Mode	Ch BW	Forward Mode	Association Time ▾	Duration	Auth. Type	Ciphe
-	logon	00:0b:86:ca:e3:d3	1	802.11a	802.11a	-	Tunnel Encrypted	1/27/2011 1:06 PM	4 hrs 0 mins	No Encryption	-
-	logon	00:0b:86:ca:e3:d3	1	802.11a	802.11a	-	Tunnel Encrypted	1/26/2011 1:59 PM	2 hrs 18 mins	No Encryption	-
-	logon	00:0b:86:c9:94:d8	1	802.11a	802.11a	-	Tunnel Encrypted	1/26/2011 1:19 PM	40 mins	No Encryption	-
-	logon	00:0b:86:ca:e3:d3	1	802.11a	802.11a	-	Tunnel Encrypted	1/25/2011 2:36 PM	22 hrs 30 mins	No Encryption	-

1-4 ▾ of 12 Past Associations Page 1 ▾ of 3 > >|

Using the Deauthenticate User Feature

Some displays of the **User > User Detail** page include the **Deauthenticate User** feature in the **Current Association** section, illustrated in Figure 137 above. Specifically, those displays are for devices which support this operation, namely Alcatel-Lucent and Cisco WLC with firmware version v4.0.0.0 or later.

Select the **Deauthenticate User** button to use this feature.

Evaluating User Status with the Users > Diagnostics Page

The **Users > Diagnostics** page is accessible from the User Detail page. You can also search for a user and select the associated MAC address from the search results.

This page provides an overview of a user's general status and connectivity on the network.

Each section of the **Users > Diagnostics** page displays information by which to evaluate possible user issues. Refer to Table 115 for explanation and illustration of page components.

Table 115 ***Users > Diagnostics*** *Page Sections*

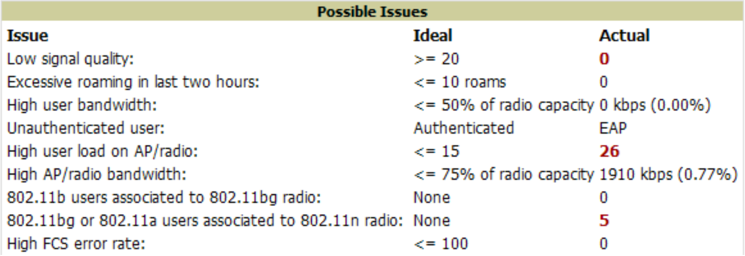
<table>
<tr><th>Section</th><th>Description</th></tr>
<tr><td><b>Possible Issues</b></td><td>
<p>This section summarizes the most likely items to create issues for a user on the network. Figure 138 illustrates this section.</p>
<p><b>NOTE</b>: Items in red are the values considered "out of spec."</p>
<p><b>Figure 138</b> <b><i>Groups > Diagnostics > Possible Issues</i></b> <i>Illustration</i></p>

<p><b>Possible Issues</b></p>
<table>
<tr><th>Issue</th><th>Ideal</th><th>Actual</th></tr>
<tr><td>Low signal quality:</td><td>>= 20</td><td>0</td></tr>
<tr><td>Excessive roaming in last two hours:</td><td><= 10 roams</td><td>0</td></tr>
<tr><td>High user bandwidth:</td><td><= 50% of radio capacity</td><td>0 kbps (0.00%)</td></tr>
<tr><td>Unauthenticated user:</td><td>Authenticated</td><td>EAP</td></tr>
<tr><td>High user load on AP/radio:</td><td><= 15</td><td>26</td></tr>
<tr><td>High AP/radio bandwidth:</td><td><= 75% of radio capacity</td><td>1910 kbps (0.77%)</td></tr>
<tr><td>802.11b users associated to 802.11bg radio:</td><td>None</td><td>0</td></tr>
<tr><td>802.11bg or 802.11a users associated to 802.11n radio:</td><td>None</td><td>5</td></tr>
<tr><td>High FCS error rate:</td><td><= 100</td><td>0</td></tr>
</table>
<ul>
<li><b>Low signal quality</b>—If signal quality falls outside of ideal range, then possible resolution might be moving the client, adjusting client antennae, installing more or better antennas on the APs, adding APs, increasing the transmit power of the APs, investigating intermittent RF interference (such as the startup schedule of a nearby air conditioning unit), or evaluating the client settings.</li>
<li><b>Excessive roaming in last two hours</b>—Excessive roaming means that a user's connection moves from one AP to another 10 or more roaming instances in the past two hours. If there is excessive roaming but the user has been stationary, then the user might be located where there is weak coverage from two overlapping APs. Adjusting the signal strength for one of those APs may resolve the issue.</li>
<li><b>High User Bandwidth</b>—Network performance issues might mean excessive bandwidth consumption. Investigate user bandwidth consumption for all users on a given AP, not strictly the user who reports a problem.</li>
<li><b>Unauthenticated User</b>—This section conveys the user's current authentication status and the actual authentication type. If a network deploys RADIUS, then the RADIUS server could be experiencing issues even if a user attempts to log in with valid credentials but shows as <b>Unauthenticated</b> on this page.</li>
</ul>
</td></tr>
<tr><td><b>Possible Issues (Cont'd)</b></td><td>
<ul>
<li><b>High user load on AP/radio</b>—This field indicates whether the number of users on a given AP has exceeded that AP's functional capacity. Excessive users on an AP could degrade performance for all users on that AP. Consider adding another AP in that area. Refer to the <b>Current User Counts</b> section on this page for more details.</li>
<li><b>High AP radio bandwidth</b>—This figure derives from how groups of users share radio bandwidth on a shared AP. You may not need to add an additional AP to resolve this issue, but you would need to determine why neighboring APs are not functioning properly.</li>
<li><b>802.11 radio parameters</b>—These two sections indicate the likelihood that a user's issues are derived from mismatched 802.11 deployment. That is, an 802.11ab or g user who is connected through an 802.11n radio might not benefit from full 802.11n functionality. These two fields indicate the likelihood of such an issue impacting a user's experience on the network, as well as a reduction of available bandwidth for other users.</li>
<li><b>High FCS error rates</b>—Frame Check Sequence (FCS) errors are checksum errors in the 802.11 protocol and may indicate interference and congestion. One response is to assign a different channel to the AP manually or by using Adaptive Radio Management (ARM).</li>
</ul>
</td></tr>
</table>

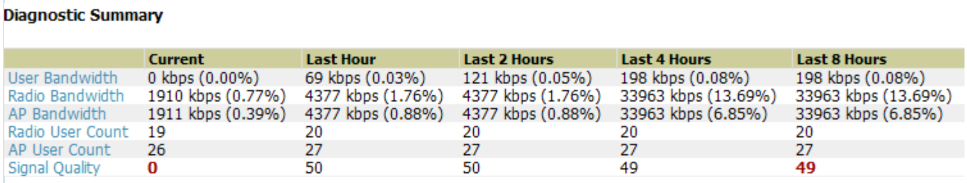
Table 115 ***Users > Diagnostics*** *Page Sections*

<table>
<tr><th>Section</th><th>Description</th></tr>
<tr><td>**Diagnostics Summary**</td><td>

This section summarizes bandwidth, user count, and signal quality parameters for specific windows of time. This section is useful when diagnosis or troubleshooting follows issues that had been observed a few or several hours prior. Figure 139 illustrates this section.

NOTE: Large negative changes in value are displayed in red.

Figure 139 ***Diagnostics Summary*** *Illustration (Partial Display)*



Diagnostic Summary

<table>
<tr><th></th><th>Current</th><th>Last Hour</th><th>Last 2 Hours</th><th>Last 4 Hours</th><th>Last 8 Hours</th></tr>
<tr><td>User Bandwidth</td><td>0 kbps (0.00%)</td><td>69 kbps (0.03%)</td><td>121 kbps (0.05%)</td><td>198 kbps (0.08%)</td><td>198 kbps (0.08%)</td></tr>
<tr><td>Radio Bandwidth</td><td>1910 kbps (0.77%)</td><td>4377 kbps (1.76%)</td><td>4377 kbps (1.76%)</td><td>33963 kbps (13.69%)</td><td>33963 kbps (13.69%)</td></tr>
<tr><td>AP Bandwidth</td><td>1911 kbps (0.39%)</td><td>4377 kbps (0.88%)</td><td>4377 kbps (0.88%)</td><td>33963 kbps (6.85%)</td><td>33963 kbps (6.85%)</td></tr>
<tr><td>Radio User Count</td><td>19</td><td>20</td><td>20</td><td>20</td><td>20</td></tr>
<tr><td>AP User Count</td><td>26</td><td>27</td><td>27</td><td>27</td><td>27</td></tr>
<tr><td>Signal Quality</td><td>0</td><td>50</td><td>50</td><td>49</td><td>49</td></tr>
</table>

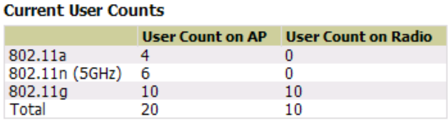
The following categories link to additional details pages:

- **User Bandwidth**—select this link to display flash graphs for user bandwidth metrics.
- **Radio Bandwidth**—select this link to display flash graphs for radio bandwidth consumption.
- **AP Bandwidth**—select this link to display flash graphs for AP bandwidth consumption.
- **Radio User Count**—select this link to display flash graphs for user count metrics.
- **AP User Count**—select this link to display flash graphs for user count metrics.
- **Signal Quality**—select this link to display flash graphs for signal quality.

</td></tr>
<tr><td>**Current User Counts**</td><td>

The **Current User Counts** section displays user counts for APs and radios, and includes additional summary information for APs. Figure 140 illustrates this section:

Figure 140 ***Users > Diagnostics > Current User Counts*** *Illustration*



Current User Counts

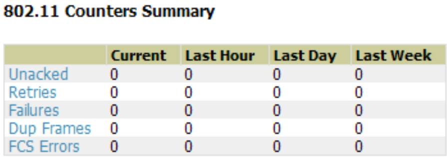
<table>
<tr><th></th><th>User Count on AP</th><th>User Count on Radio</th></tr>
<tr><td>802.11a</td><td>4</td><td>0</td></tr>
<tr><td>802.11n (5GHz)</td><td>6</td><td>0</td></tr>
<tr><td>802.11g</td><td>10</td><td>10</td></tr>
<tr><td>Total</td><td>20</td><td>10</td></tr>
</table>

Use this section in combination with the **Possible Issues** section.

</td></tr>
<tr><td>**802.11 Counters Summary**</td><td>

The **802.11 Counters Summary** section conveys the same information that is available from the **Statistics** link from the **APs/Devices > Monitor** page. Figure 141 illustrates this section.

Figure 141 ***Users > Diagnostics > 802.11 Counters Summary*** *Illustration*



802.11 Counters Summary

<table>
<tr><th></th><th>Current</th><th>Last Hour</th><th>Last Day</th><th>Last Week</th></tr>
<tr><td>Unacked</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>Retries</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>Failures</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>Dup Frames</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>FCS Errors</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
</table>

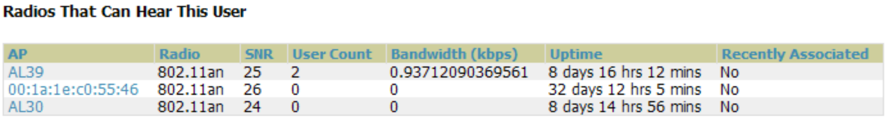
NOTE: This section is supported for Cisco and Alcatel-Lucent devices.

For additional information, select the link to the device on this page.

</td></tr>
<tr><td>**Radios That Can Hear This User**</td><td>

The **Radios That Can Hear This User** section shows the radios that reported the signal from this client, and displays statistics. Figure 142 illustrates this section.

Figure 142 ***Users > Diagnostics*** > ***Radios That Can Hear This User*** *Illustration*



Radios That Can Hear This User

<table>
<tr><th>AP</th><th>Radio</th><th>SNR</th><th>User Count</th><th>Bandwidth (kbps)</th><th>Uptime</th><th>Recently Associated</th></tr>
<tr><td>AL39</td><td>802.11an</td><td>25</td><td>2</td><td>0.93712090369561</td><td>8 days 16 hrs 12 mins</td><td>No</td></tr>
<tr><td>00:1a:1e:c0:55:46</td><td>802.11an</td><td>26</td><td>0</td><td>0</td><td>32 days 12 hrs 5 mins</td><td>No</td></tr>
<tr><td>AL30</td><td>802.11an</td><td>24</td><td>0</td><td>0</td><td>8 days 14 hrs 56 mins</td><td>No</td></tr>
</table>

</td></tr>
</table>

Managing Mobile Devices with SOTI MobiControl and OV3600

Overview of SOTI MobiControl

SOTI MobiControl, the mobile device management platform for Windows Mobile, Blackberry, Apple, and Android devices, has been integrated into OV3600 to provide direct access to the MobiControl Console.

MobiControl runs on your Mobile Device Manager (MDM) server. This server provisions mobile devices via HTTP to configure connectivity settings, enforce security policies, restore lost data, and other administrative services. Information gathered from mobile devices can include policy breaches, data consumption, and existing configuration settings.

Prerequisites for Using MobiControl with OV3600

In order to use the MobiControl integration in OV3600, the following is required:

- Your OV3600 must be running version 7.2
- An MDM server with SOTI MobiControl Console 8.50 Build 3989, Web Version 8.50 Build 5066
- A client device that is:
  - associated with WLAN infrastructure managed by the OV3600 server running 7.2
  - being actively managed by the SOTI MobiControl server running with proper build numbers

For more information about setting up MobiControl, please see http://www.soti.net/mc/help/.

In order to use SOTI MobiControl from within OV3600, you must first add your MDM server and designate it as a MobiControl.

Adding a Mobile Device Management Server for MobiControl

1. To add an MDM server to OV3600, navigate to **OV3600 Setup > MDM Server** and select **Add**. Complete the fields on this page. Table 116 describes the settings and default values:

Table 116 ***OV3600 Setup > MDM Server > Add*** *Fields and Descriptions*

Field	Description
Hostname/IP Address	The address or DNS hostname configured for your MDM server.
Protocol	Whether HTTP or HTTPS is to be used when polling the MDM server. The port on which to connect to the MDM server is inferred from the protocol: with HTTP, OV3600 will connect to port 80 of the SOTI server; with HTTPS, OV3600 will connect to port 443.
URL Context	The URL context appended to the server URL to build the URL when connecting with the SOTI server. Enter **MobiControl** in this space for SOTI support.
Enabled	Whether this server can be polled by OV3600. Make sure it is set to **Yes**.
Username/ Password	The login credentials for this MDM server.
Polling Period	The frequency in which OV3600 polls the MDM server to gather information. The default is 5 minutes.

2. When finished, select **Add.**

The list page for the MDM server also displays:

- **Last Contacted –** The last time OV3600 was able to contact the MDM server.
- **Errors** – Issues, if any, encountered during the last contact.

During each polling period, OV3600 will to obtain a list of all device IDs and their WLAN MAC addresses. The information about Device Type, OS, and OS version are retrieved from MobiControl and populated to the **Users > User Detail** page for supported mobile devices. A **View device in SOTI MobiControl** link provides direct access to the MobiControl Web Console for additional details about the device. MobiControl information overrides data obtained by AOS-W 6.0 switches.

Accessing MobiControl from the Users > User Detail Page

In order to access the MobiControl web console for a SOTI-managed mobile device from within OV3600, follow these steps:

1. Navigate to a page that lists clients. This can include:
   - **Users > Connected** or **Users > All**
   - Search results that display user MAC address
2. Select the MAC address in the **Users** list table. The **Users > User Detail** page displays.
3. Under the Classification field, select the **View device in SOTI MobiControl** link. A new window will display the MobiControl Web Console for this device.

Monitoring and Supporting OV3600 with the Home Pages

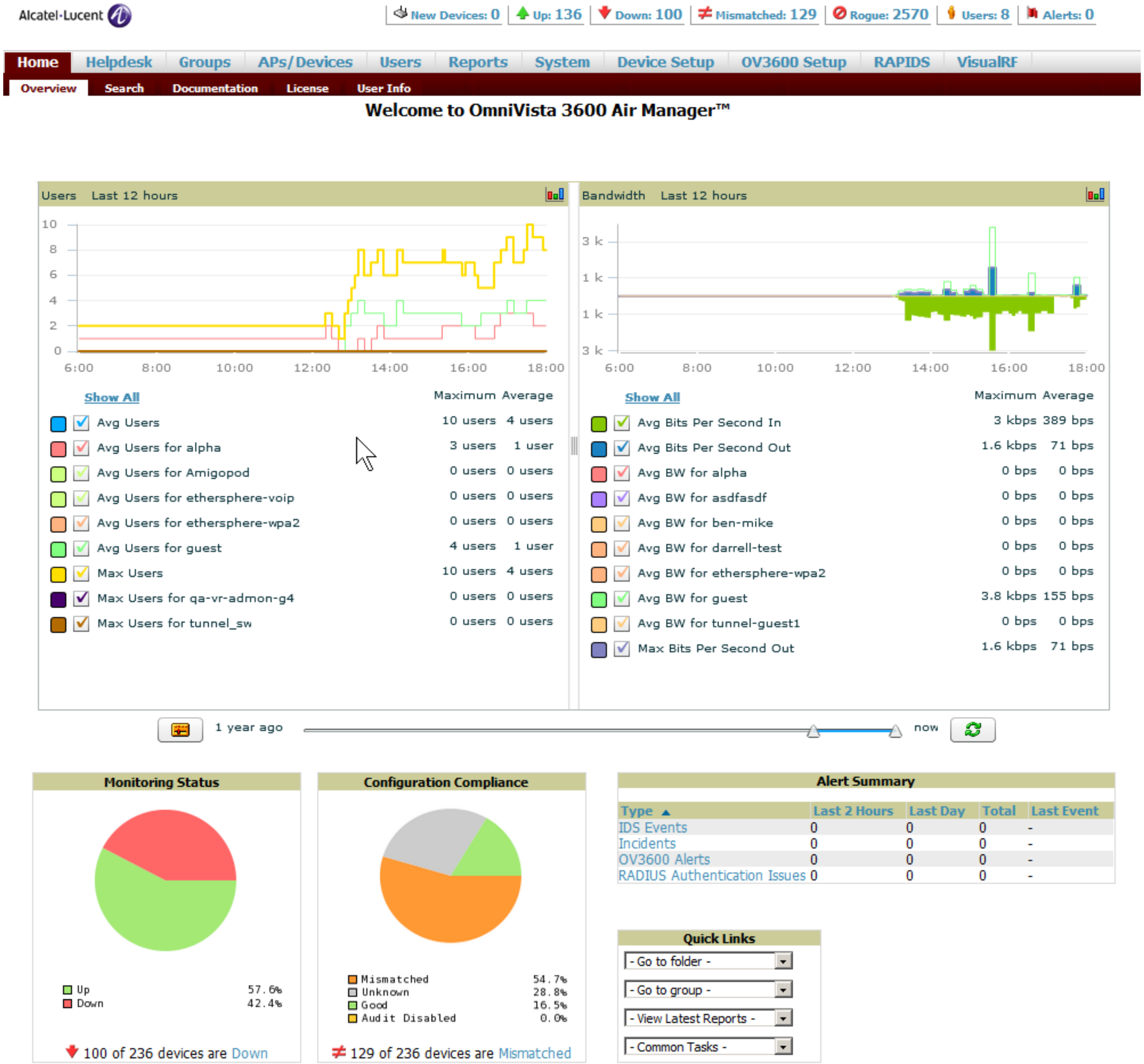
The **Home** tab of OV3600 provides the most frequent starting point for monitoring network status and establishing primary OV3600 functions, once OV3600 configuration is complete. Access the following pages:

- The **Home > Overview** page condenses a large amount of information about your OV3600. You can view the health and usage of your network and use shortcuts to view system information. Refer to Monitoring OV3600 with the Home > Overview Page below.
- The **Home > Search** page provides a simple way to find users. managed devices, groups, and rogues. Refer to "Searching OV3600 with the Home > Search Page" on page 200.
- The **Home > Documentation** page contains all relevant OV3600 documentation. See "Accessing OV3600 Documentation" on page 201.
- The **Home > License** page provides product licensing information. See "Viewing and Updating License Information" on page 199.
- The **Home > User Info** page displays information about the users logged in to OV3600, including the role, authentication type, and access level. See "Configuring Your Own User Information with the Home > User Info Page" on page 202.
- The **Customize** link on the upper-right side of the page allows you to customize the widgets on the **Home > Overview** page. See "Customizing the Overview Subtab Display" on page 32.

Monitoring OV3600 with the Home > Overview Page

To view your overall network health at a glance, navigate to **Home > Overview** page. Figure 143 illustrates this page, and Table 117 describes the contents. The information that displays will vary depending on your role.

Figure 143 ***Home*** **>** ***Overview*** *Page Illustration*



Welcome to OmniVista 3600 Air Manager™

Show All	Maximum	Average
☑ Avg Users	10 users	4 users
☑ Avg Users for alpha	3 users	1 user
☑ Avg Users for Amigopod	0 users	0 users
☑ Avg Users for ethersphere-voip	0 users	0 users
☑ Avg Users for ethersphere-wpa2	0 users	0 users
☑ Avg Users for guest	4 users	1 user
☑ Max Users	10 users	4 users
☑ Max Users for qa-vr-admon-g4	0 users	0 users
☑ Max Users for tunnel_sw	0 users	0 users

Show All	Maximum	Average
☑ Avg Bits Per Second In	3 kbps	389 bps
☑ Avg Bits Per Second Out	1.6 kbps	71 bps
☑ Avg BW for alpha	0 bps	0 bps
☑ Avg BW for asdfasdf	0 bps	0 bps
☑ Avg BW for ben-mike	0 bps	0 bps
☑ Avg BW for darrell-test	0 bps	0 bps
☑ Avg BW for ethersphere-wpa2	0 bps	0 bps
☑ Avg BW for guest	3.8 kbps	155 bps
☑ Avg BW for tunnel-guest1	0 bps	0 bps
☑ Max Bits Per Second Out	1.6 kbps	71 bps

Up	57.6%
Down	42.4%

100 of 236 devices are Down

Mismatched	54.7%
Unknown	28.8%
Good	16.5%
Audit Disabled	0.0%

129 of 236 devices are Mismatched

Alert Summary

Type ▲	Last 2 Hours	Last Day	Total	Last Event
IDS Events	0	0	0	-
Incidents	0	0	0	-
OV3600 Alerts	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Table 117 ***Home*** **>** ***Overview*** *Sections and Charts*

Section	Description
Users	This chart is a graphical summary of the number of users on the network during a period of time. The time can be adjusted. Select **Show All** to display a list of data series that this graph can display, such as the user count by SSID. Clear the **Max Users** or **Avg Users** checkbox to change the display of the graph. The graph displays the maximum number of users by default. To view historical graphs in a new window, select the three-bar icon on the upper right of the chart.
Bandwidth	This adjustable chart displays bandwidth data over time. To remove bandwidth in or out from the graphical display, clear the check box for **Avg Bits Per Second In** or **Out**. To display details for specific devices, select **Show All** and select the devices to be included in the graphical bandwidth summary chart. To view historical graphs in a new window, select the three-bar icon on the upper right of the chart.
Monitoring Status	This pie chart shows the percentage of all devices that are up and down on the network. To review devices that are down, select **Down** in the legend or the chart, and the **APs/Devices > Down** page displays.
Configuration Compliance	The pie chart displays all known device configuration status on the network. Devices are classified as **Good**, **Unknown**, **Mismatched,** or **Audit Disabled**. Select the **Mismatched** link to see the **APs/Devices > Mismatched** page.

Table 117 ***Home*** **>** ***Overview*** *Sections and Charts*

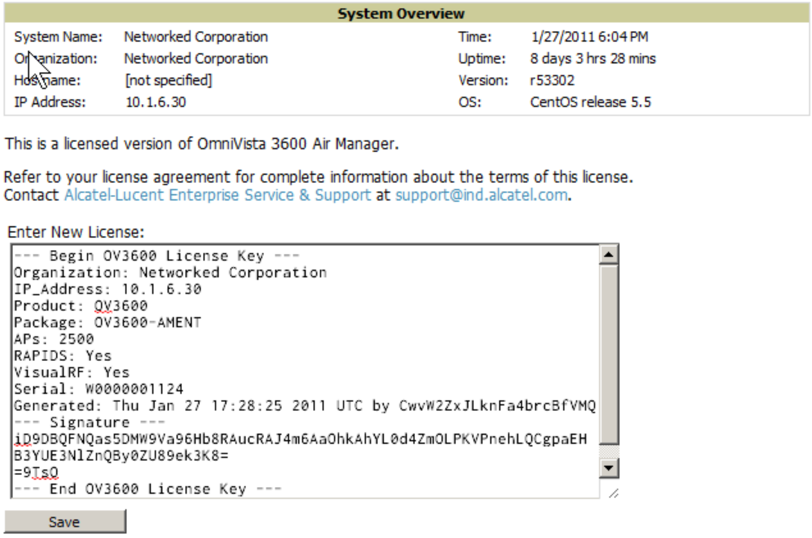
Section	Description
Alert Summary	This section displays all known and current alerts configured and enabled in the **System > Alerts** page. Alerts can be sorted using the column headers (**Type**, **Last 2 Hours**, **Last Day**, **Total**, or **Last Event**). The **Alert Summary** field displays four types of alerts, as follows: ● **OV3600 Alerts** ● **IDS Events** ● **Incidents** ● **RADIUS Authentication Issues** Select any alert type for more information. **NOTE:** The **Incidents** portion of this summary table only increments the counter for incidents that are open and associated to an AP. This is also the case if you select **Incidents** and view incident details. To view all incidents, including those not associated to an AP, navigate to the **Helpdesk > Incidents** page.
Quick Links	The **Quick Links** section provides drop-down menus that enable you to move to the most common and frequently used pages in OV3600, as follows: ● **Go to folder**—This menu lists all folders defined in OV3600 from the **APs/Devices List** page. See "Using Device Folders (Optional)" on page 131. ● **Go to group**—This menu lists all groups defined in OV3600, and enables you to display information for any or all of them. Use the **Groups** pages to edit, add, or delete groups that appear in this section. See "Configuring and Using Device Groups in OV3600" on page 69. ● **View latest reports**—OV3600 supports creating custom reports or viewing the latest daily version of any report. Select any report type to display the daily version. See "Creating, Running, and Emailing Reports" on page 219. ● **Common Tasks**—This menu lists quick links to the most heavily used task-oriented pages in OV3600, to include the following: ■ **Configure Alert Thresholds**—This link takes you to the **System > Triggers** page. See "Overview of Triggers and Alerts" on page 179. ■ **Configure Default Credentials**—This link takes you to the **Device Setup > Communication** page. See "Configuring Communication Settings for Discovered Devices" on page 47. ■ **Discover New Devices on Your Network**—This link takes you to the **Device Setup > Discover** page. See "Discovering, Adding, and Managing Devices" on page 107. ■ **Supported Devices and Features**—This link displays a PDF that summarizes all supported devices and features in chart format for OV3600. ■ **Upload Device Firmware**—This link displays the **Device Setup > Firmware & Files Upload** page. See "Overview of the Device Setup > Upload Firmware & Files Page" on page 49. ■ **View Event Log**—This link displays the **System > Event Log** page. See "Using the System > Event Log Page" on page 206.

Viewing and Updating License Information

Navigate to the **Home > License** page using the standard OV3600 menu. Figure 144 illustrates this page, and Table 118 describes the contents.

Please be aware that you cannot enter multiple licenses. To combine multiple license entitlements into one new license, contact Alcatel support.

Figure 144 ***Home* > *License*** *Page Illustration*



System Overview

System Name:	Networked Corporation	Time:	1/27/2011 6:04 PM
Organization:	Networked Corporation	Uptime:	8 days 3 hrs 28 mins
Hostname:	[not specified]	Version:	r53302
IP Address:	10.1.6.30	OS:	CentOS release 5.5

This is a licensed version of OmniVista 3600 Air Manager.

Refer to your license agreement for complete information about the terms of this license.
Contact Alcatel-Lucent Enterprise Service & Support at support@ind.alcatel.com.

Enter New License:

```
--- Begin OV3600 License Key ---
Organization: Networked Corporation
IP_Address: 10.1.6.30
Product: OV3600
Package: OV3600-AMENT
APs: 2500
RAPIDS: Yes
VisualRF: Yes
Serial: W0000001124
Generated: Thu Jan 27 17:28:25 2011 UTC by CwvW2ZxJLknFa4brcBfVMQ
--- Signature ---
iD9DBQFNQas5DMW9Va96Hb8RAucRAJ4m6AaOhkAhYL0d4ZmOLPKVPnehLQCgpaEH
B3YUE3NlZnQBy0ZU89ek3K8=
=9TsO
--- End OV3600 License Key ---
```

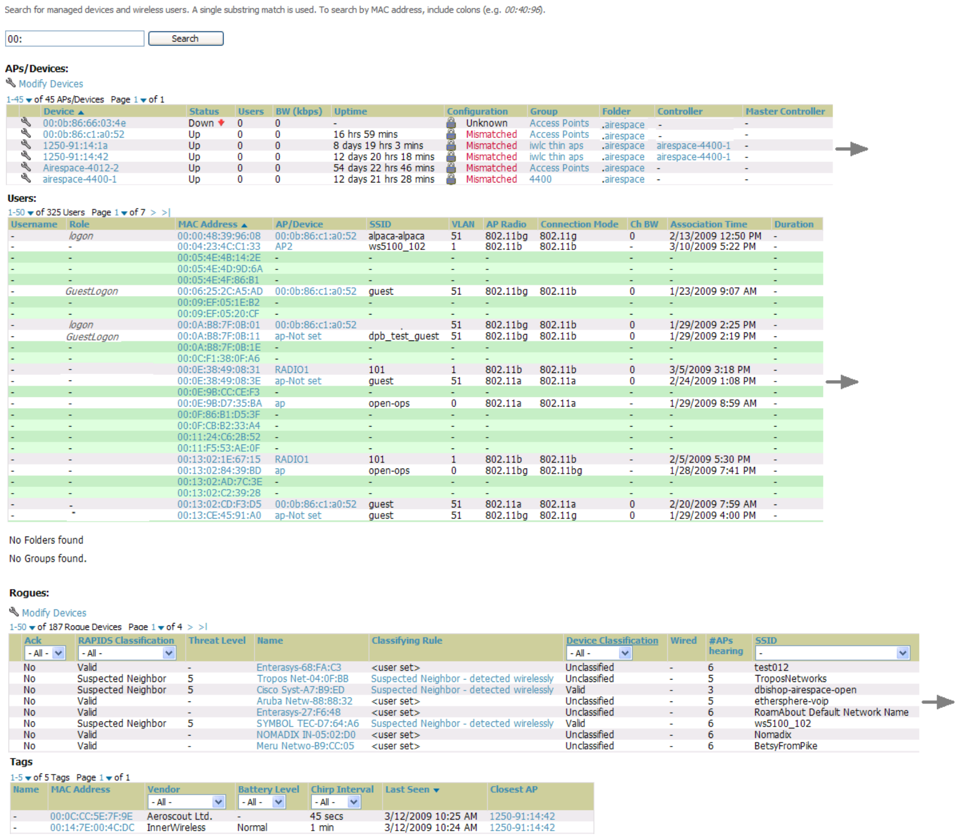
Table 118 ***Home* > *License*** *Fields*

Field	Description
System Name	Displays a user-definable name for OV3600. The System Name can be configured from the **OV3600 Setup > General** page.
Organization	Displays the organization listed on your license key.
Hostname	Displays the DNS name assigned to OV3600.
IP Address	Displays the static IP address assigned to OV3600. The IP Address can be configured from the **OV3600 Setup > Network** page.
Time	Displays the current date and time set on OV3600.
Uptime	Displays the amount of time since the operating system was last booted.
Version	Displays the version number of OV3600 code currently running.
OS	Displays the version of Linux installed on the server.

Searching OV3600 with the Home > Search Page

The **Home > Search** page provides a simple way to find connected and historical users, managed devices, rogue devices, groups, folders, and more. Search performs partial string searches on a large number of fields including the notes, version, secondary version, radio serial number, device serial number, LAN MAC, radio MAC and apparent IP address of all the APs, as well as the client MAC, VPN user, User, LAN IP and VPN IP fields. Figure 145 illustrates this page.

Figure 145 ***Home > Search*** *Page Illustration with Sample Hits on "00:"*



Search for managed devices and wireless users. A single substring match is used. To search by MAC address, include colons (e.g. *00:40:96*).

APs/Devices:

Modify Devices

1-45 ▾ of 45 APs/Devices Page 1 ▾ of 1

Device ▲	Status	Users	BW (kbps)	Uptime	Configuration	Group	Folder	Controller	Master Controller
00:0b:86:66:03:4e	Down	0	0	-	Unknown	Access Points	.airespace	-	-
00:0b:86:c1:a0:52	Up	0	0	16 hrs 59 mins	Mismatched	Access Points	.airespace	-	-
1250-91:14:1a	Up	0	0	8 days 19 hrs 3 mins	Mismatched	iwlc thin aps	.airespace	airespace-4400-1	-
1250-91:14:42	Up	0	0	12 days 20 hrs 18 mins	Mismatched	iwlc thin aps	.airespace	airespace-4400-1	-
Airespace-4012-2	Up	0	0	54 days 22 hrs 46 mins	Mismatched	Access Points	.airespace	-	-
airespace-4400-1	Up	0	0	12 days 21 hrs 28 mins	Mismatched	4400	.airespace	-	-

Users:

1-50 ▾ of 325 Users Page 1 ▾ of 7 > >|

Username	Role	MAC Address ▲	AP/Device	SSID	VLAN	AP Radio	Connection Mode	Ch BW	Association Time	Duration
-	*logon*	00:00:48:39:96:08	00:0b:86:c1:a0:52	alpaca-alpaca	51	802.11bg	802.11g	0	2/13/2009 12:50 PM	-
-	-	00:04:23:4C:C1:33	AP2	ws5100_102	1	802.11b	802.11b	-	3/10/2009 5:22 PM	-
-	-	00:05:4E:4B:14:2E	-	-	-	-		-	-	-
-	-	00:05:4E:4D:9D:6A	-	-	-	-		-	-	-
-	-	00:05:4E:4F:86:B1	-	-	-	-		-	-	-
-	*GuestLogon*	00:06:25:2C:A5:AD	00:0b:86:c1:a0:52	guest	51	802.11bg	802.11b	0	1/23/2009 9:07 AM	-
-	-	00:09:EF:05:1E:B2	-	-	-	-		-	-	-
-	-	00:09:EF:05:20:CF	-	-	-	-		-	-	-
-	*logon*	00:0A:B8:7F:0B:01	00:0b:86:c1:a0:52		51	802.11bg	802.11b	0	1/29/2009 2:25 PM	-
-	*GuestLogon*	00:0A:B8:7F:0B:11	ap-Not set	dpb_test_guest	51	802.11bg	802.11b	0	1/29/2009 2:19 PM	-
-	-	00:0A:B8:7F:0B:1E	-	-	-	-		-	-	-
-	-	00:0C:F1:38:0F:A6	-	-	-	-		-	-	-
-	-	00:0E:38:49:08:31	RADIO1	101	1	802.11b	802.11b	0	3/5/2009 3:18 PM	-
-	-	00:0E:38:49:08:3E	ap-Not set	guest	51	802.11a	802.11a	0	2/24/2009 1:08 PM	-
-	-	00:0E:9B:CC:CE:F3	-	-	-	-		-	-	-
-	-	00:0E:9B:D7:35:BA	ap	open-ops	0	802.11a	802.11a	-	1/29/2009 8:59 AM	-
-	-	00:0F:86:B1:D5:3F	-	-	-	-		-	-	-
-	-	00:0F:CB:B2:33:A4	-	-	-	-		-	-	-
-	-	00:11:24:C6:2B:52	-	-	-	-		-	-	-
-	-	00:11:F5:53:AE:0F	-	-	-	-		-	-	-
-	-	00:13:02:1E:67:15	RADIO1	101	1	802.11b	802.11b	-	2/5/2009 5:30 PM	-
-	-	00:13:02:84:39:BD	ap	open-ops	0	802.11bg	802.11bg	-	1/28/2009 7:41 PM	-
-	-	00:13:02:AD:7C:3E	-	-	-	-		-	-	-
-	-	00:13:02:C2:39:28	-	-	-	-		-	-	-
-	-	00:13:02:CD:F3:D5	00:0b:86:c1:a0:52	guest	51	802.11a	802.11a	0	2/20/2009 7:59 AM	-
-	-	00:13:CE:45:91:A0	ap-Not set	guest	51	802.11bg	802.11g	0	1/29/2009 4:00 PM	-

No Folders found

No Groups found.

Rogues:

Modify Devices

1-50 ▾ of 187 Rogue Devices Page 1 ▾ of 4 > >|

Ack	RAPIDS Classification	Threat Level	Name	Classifying Rule	Device Classification	Wired	#APs hearing	SSID
- All -	- All -				- All -			-
No	Valid	-	Enterasys-68:FA:C3	<user set>	Unclassified	-	6	test012
No	Suspected Neighbor	5	Tropos Net-04:0F:BB	Suspected Neighbor - detected wirelessly	Unclassified	-	5	TroposNetworks
No	Suspected Neighbor	5	Cisco Syst-A7:B9:ED	Suspected Neighbor - detected wirelessly	Valid	-	3	dbishop-airespace-open
No	Valid	-	Aruba Netw-88:88:32	<user set>	Unclassified	-	5	ethersphere-voip
No	Valid	-	Enterasys-27:F6:48	<user set>	Unclassified	-	6	RoamAbout Default Network Name
No	Suspected Neighbor	5	SYMBOL TEC-D7:64:A6	Suspected Neighbor - detected wirelessly	Valid	-	6	ws5100_102
No	Valid	-	NOMADIX IN-05:02:D0	<user set>	Unclassified	-	6	Nomadix
No	Valid	-	Meru Netwo-B9:CC:05	<user set>	Unclassified	-	6	BetsyFromPike

Tags

1-5 ▾ of 5 Tags Page 1 ▾ of 1

Name	MAC Address	Vendor	Battery Level	Chirp Interval	Last Seen ▾	Closest AP
		- All -	- All -	- All -		
-	00:0C:CC:5E:7F:9E	Aeroscout Ltd.	-	45 secs	3/12/2009 10:25 AM	1250-91:14:42
-	00:14:7E:00:4C:DC	InnerWireless	Normal	1 min	3/12/2009 10:24 AM	1250-91:14:42

1. Enter the keyword or text with which to search. If searching for a MAC address, enter it in colon-delimited format.

NOTE

The OV3600 Search utility is case-insensitive.

2. Select **Search**, and the results display after a short moment. Results support several hypertext links to additional pages, and drop-down menus allow for additional filtering of search returns.

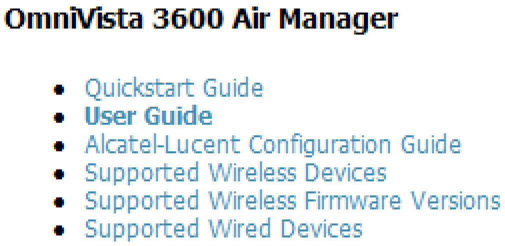
   Search results are categorized in the following sequence. Categories of search results can be customized on the **Home > User Info** page to limit the scope of information returned. Not all categories below may offer returns for a given search:

   - **Devices**
   - **Users**
   - **Rogues**
   - **Tags**
   - **Folders and Groups**

Accessing OV3600 Documentation

The **Home > Documentation** page provides easy access to all relevant OV3600 documentation. All of the documents on the **Home > Documentation** page are hosted locally by OV3600 and can be viewed by any PDF viewer. Figure 146 illustrates this page.

Figure 146 ***Home > Documentation** Page Illustration*



OmniVista 3600 Air Manager

- Quickstart Guide
- User Guide
- Alcatel-Lucent Configuration Guide
- Supported Wireless Devices
- Supported Wireless Firmware Versions
- Supported Wired Devices

If you have any questions that are not answered by the documentation, please contact Alcatel support.

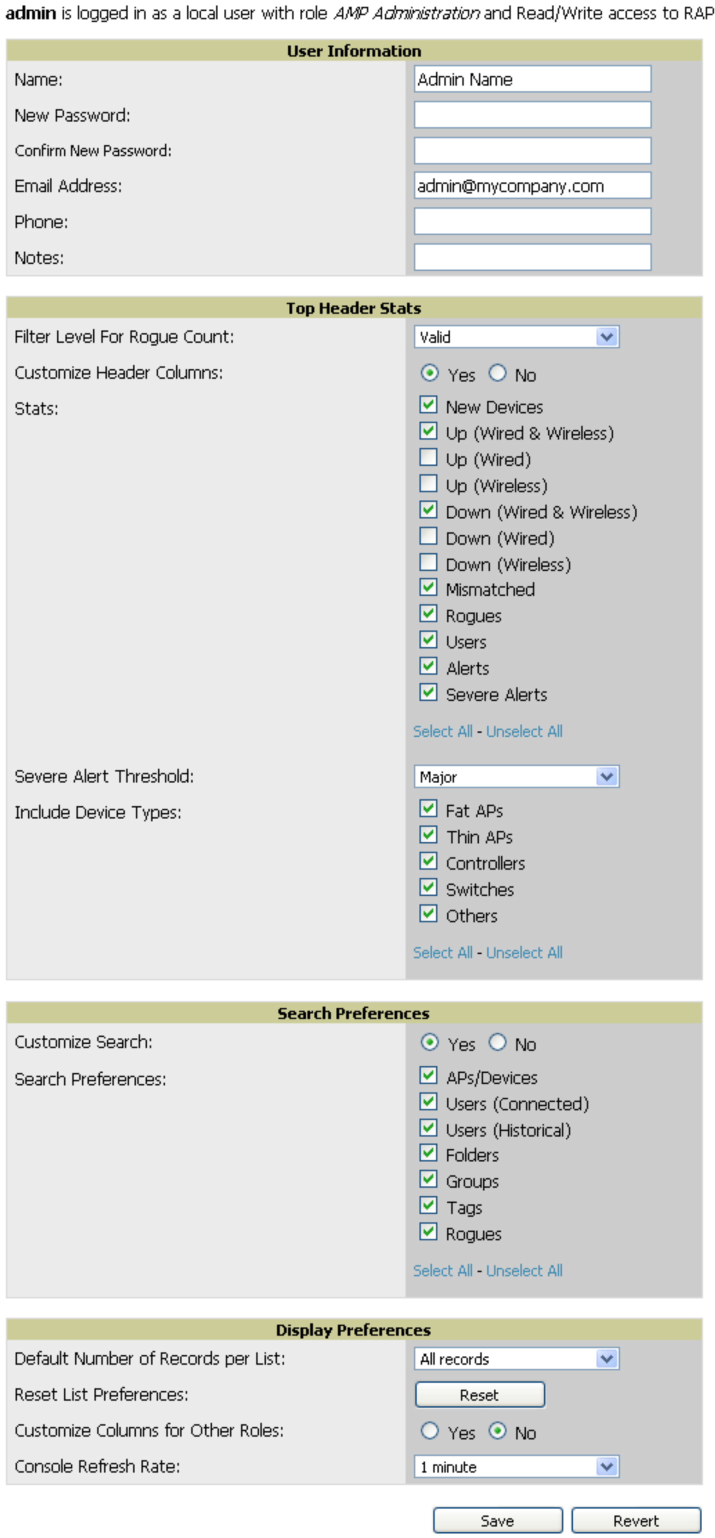
Configuring Your Own User Information with the Home > User Info Page

The **Home > User Info** page displays information about the user that is logged into OV3600. This page includes the authentication type (local user, RADIUS, or TACACS+) and access level. This page enables customization some of the information displayed in OV3600, and is the place to change your password.

To create new users, navigate to the **OV3600 Setup > Users** page, and refer to "Creating OV3600 Users" on page 43. Users can customize the information displayed in the OV3600 header.

Figure 147 illustrates the **Home > User Info** page, and Table 119 lists the fields.

Figure 147 ***Home* > *User Info*** *Page Illustration*



admin is logged in as a local user with role *AMP Administration* and Read/Write access to RAPIDS.

User Information

Name:	Admin Name
New Password:	
Confirm New Password:	
Email Address:	admin@mycompany.com
Phone:	
Notes:	

Top Header Stats

Filter Level For Rogue Count:	Valid
Customize Header Columns:	● Yes ○ No
Stats:	☑ New Devices ☑ Up (Wired & Wireless) □ Up (Wired) □ Up (Wireless) ☑ Down (Wired & Wireless) □ Down (Wired) □ Down (Wireless) ☑ Mismatched ☑ Rogues ☑ Users ☑ Alerts ☑ Severe Alerts Select All - Unselect All
Severe Alert Threshold:	Major
Include Device Types:	☑ Fat APs ☑ Thin APs ☑ Controllers ☑ Switches ☑ Others Select All - Unselect All

Search Preferences

Customize Search:	● Yes ○ No
Search Preferences:	☑ APs/Devices ☑ Users (Connected) ☑ Users (Historical) ☑ Folders ☑ Groups ☑ Tags ☑ Rogues Select All - Unselect All

Display Preferences

Default Number of Records per List:	All records
Reset List Preferences:	Reset
Customize Columns for Other Roles:	○ Yes ● No
Console Refresh Rate:	1 minute

Table 119 ***Home* > *User Info*** *Fields*

Field	Description
Filter Level For Rogue Count	Specifies the minimum classification that will cause a device to be included in the rogue count header information.
Customize Header Columns	Enables/disables the ability to control which statistics hyperlinks are displayed at the top of every OV3600 screen.

Table 119 *Home > User Info* Fields *(Continued)*

Field	Description
Stats	Select the specific data you would like to see in the header. **Note**: This field only appears if you selected **Yes** in the previous field.
Severe Alert Threshold	Configures the minimum severity of an alert to be included in the Severe Alerts count. Note: The severe alerts count header info will only be displayed if 'Severe Alerts' is selected in the Stats section above. **Note**: This field only appears if you selected **Yes** in the **Customize Header Columns** field.
Include Device Types	Configures the types of devices that should be included in the header stats. If a device type is not selected then it will not be included in the header stats. **Note**: This field only appears if you selected **Yes** in the **Customize Header Columns** field.
Customize Search/Search Preferences	Set to **No** by default; when set to **Yes**, you can select which search categories to display when search results are returned.
Default Number of Records per List	Defines the number of rows to appear in any list by default. If a row count is manually set, it will override the default setting.
Reset List Preferences	Reset all list preferences including number of records per list, column order and hidden column information.
Customize Columns for Other Roles	Allows admin users to determine the columns that should be displayed and the order they should be displayed for specific user roles. To customize lists for other users, navigate to that list and select the **Choose Columns for roles** link above the list. Make the desired column changes; select the roles to update and select **Save**.
Console Refresh Rate	The frequency in which lists and charts automatically refresh on a page.

Perform the following steps to configure your own user account with the **Home > User Info** page:

1. In the **User Information** section, enter the following information:
   - **Name**—Enter the ID by which you log into and operate in OV3600.
   - **Email Address**—Enter the email address to be used for alerts, triggers, and additional OV3600 functions that support an email address.
   - **Phone**—Enter the area code and phone number, if desired.
   - **Notes**—Enter any additional text-based information that helps other OV3600 users or administrators to understand the functions, roles, or other rights of the user being created.

Monitoring and Supporting OV3600 with the System Pages

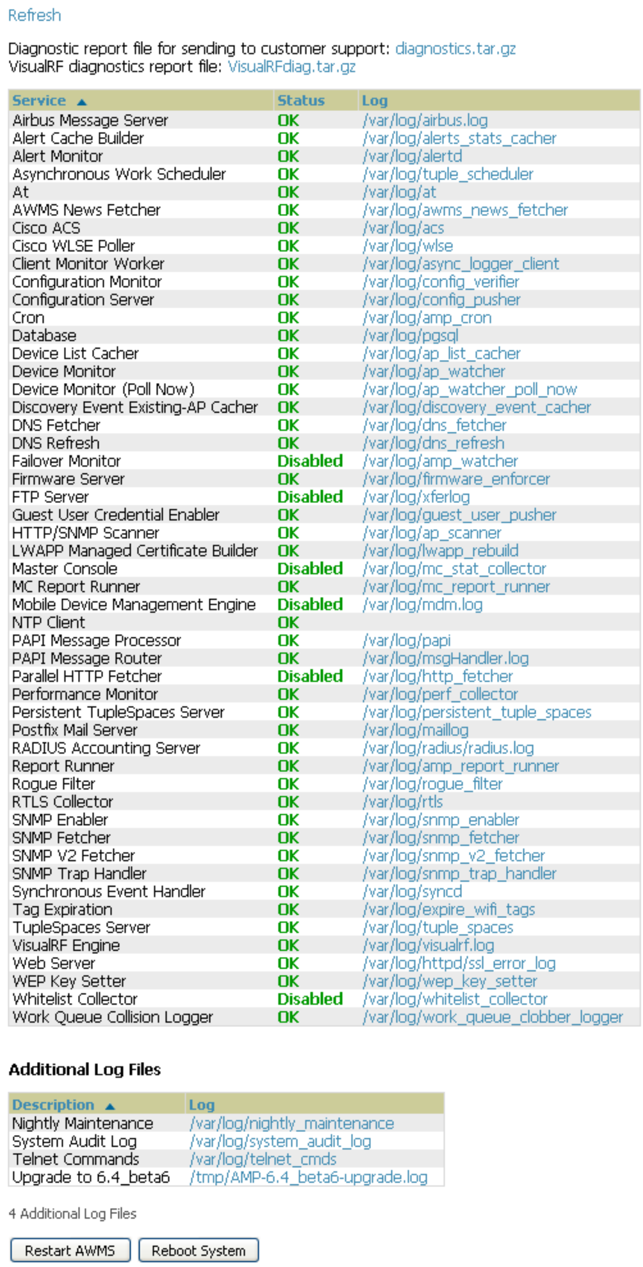
The **System** pages provide a centralized location for system-wide OV3600 data and settings. Apart from **Triggers**, **Alerts**, and **Backups** pages that are described elsewhere in this chapter, the remaining pages of the **System** section are as follows:

- **System > Status**—Displays status of all OV3600 services. Refer to "Using the System > Status Page" on page 205.
- **System > Event Log**—This useful debugging tool keeps a list of recent OV3600 events, including APs coming up and down, services restarting, and most OV3600-related errors as well as the user that initiated the action. Refer to "Using the System > Event Log Page" on page 206.
- **System > Configuration Change Jobs**—Manages configuration changes in OV3600. Refer to "Using the System > Configuration Change Jobs Page" on page 206.
- **System > Firmware Upgrade Jobs**—Displays information about current and scheduled firmware upgrades. Refer to "Loading Firmware Files to OV3600" on page 50.
- **System > Performance**—Displays basic OV3600 hardware information as well as resource usage over time. Refer to "Using the System > Performance Page" on page 207.

Using the System > Status Page

The **System > Status** page displays the status of all of OV3600 services. Services will either be **OK**, **Disabled**, or **Down**. If any service is **Down** (displayed in red) please contact Alcatel-Lucent support. The **Reboot System** button provides a graceful way to power cycle your OV3600 remotely when it is needed. The **Restart OV3600** button will restart the OV3600 services without power cycling the server or reloading the OS. Figure 148 illustrates this page.

Figure 148 ***System* > *Status* *Page Illustration***



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

Service ▲	Status	Log
Airbus Message Server	OK	/var/log/airbus.log
Alert Cache Builder	OK	/var/log/alerts_stats_cacher
Alert Monitor	OK	/var/log/alertd
Asynchronous Work Scheduler	OK	/var/log/tuple_scheduler
At	OK	/var/log/at
AWMS News Fetcher	OK	/var/log/awms_news_fetcher
Cisco ACS	OK	/var/log/acs
Cisco WLSE Poller	OK	/var/log/wlse
Client Monitor Worker	OK	/var/log/async_logger_client
Configuration Monitor	OK	/var/log/config_verifier
Configuration Server	OK	/var/log/config_pusher
Cron	OK	/var/log/amp_cron
Database	OK	/var/log/pgsql
Device List Cacher	OK	/var/log/ap_list_cacher
Device Monitor	OK	/var/log/ap_watcher
Device Monitor (Poll Now)	OK	/var/log/ap_watcher_poll_now
Discovery Event Existing-AP Cacher	OK	/var/log/discovery_event_cacher
DNS Fetcher	OK	/var/log/dns_fetcher
DNS Refresh	OK	/var/log/dns_refresh
Failover Monitor	Disabled	/var/log/amp_watcher
Firmware Server	OK	/var/log/firmware_enforcer
FTP Server	Disabled	/var/log/xferlog
Guest User Credential Enabler	OK	/var/log/guest_user_pusher
HTTP/SNMP Scanner	OK	/var/log/ap_scanner
LWAPP Managed Certificate Builder	OK	/var/log/lwapp_rebuild
Master Console	Disabled	/var/log/mc_stat_collector
MC Report Runner	OK	/var/log/mc_report_runner
Mobile Device Management Engine	Disabled	/var/log/mdm.log
NTP Client	OK	
PAPI Message Processor	OK	/var/log/papi
PAPI Message Router	OK	/var/log/msgHandler.log
Parallel HTTP Fetcher	Disabled	/var/log/http_fetcher
Performance Monitor	OK	/var/log/perf_collector
Persistent TupleSpaces Server	OK	/var/log/persistent_tuple_spaces
Postfix Mail Server	OK	/var/log/maillog
RADIUS Accounting Server	OK	/var/log/radius/radius.log
Report Runner	OK	/var/log/amp_report_runner
Rogue Filter	OK	/var/log/rogue_filter
RTLS Collector	OK	/var/log/rtls
SNMP Enabler	OK	/var/log/snmp_enabler
SNMP Fetcher	OK	/var/log/snmp_fetcher
SNMP V2 Fetcher	OK	/var/log/snmp_v2_fetcher
SNMP Trap Handler	OK	/var/log/snmp_trap_handler
Synchronous Event Handler	OK	/var/log/syncd
Tag Expiration	OK	/var/log/expire_wifi_tags
TupleSpaces Server	OK	/var/log/tuple_spaces
VisualRF Engine	OK	/var/log/visualrf.log
Web Server	OK	/var/log/httpd/ssl_error_log
WEP Key Setter	OK	/var/log/wep_key_setter
Whitelist Collector	Disabled	/var/log/whitelist_collector
Work Queue Collision Logger	OK	/var/log/work_queue_clobber_logger

Additional Log Files

Description ▲	Log
Nightly Maintenance	/var/log/nightly_maintenance
System Audit Log	/var/log/system_audit_log
Telnet Commands	/var/log/telnet_cmds
Upgrade to 6.4_beta6	/tmp/AMP-6.4_beta6-upgrade.log

4 Additional Log Files

- The link **diagnostics.tar.gz** contains reports and logs that are helpful to Alcatel-Lucent support in troubleshooting and solving problems. Your Alcatel-Lucent support representative may ask for this file along with other logs that are linked on this page.
- Similarly, the **VisualRFdiag.zip** link contains VisualRF diagnostic information that might be requested by Alcatel-Lucent support.
- A summary table lists logs that appear on the **System > Status** page. These are used to diagnose OV3600 problems. Additional logs are available via SSH access in the /var/log and /tmp directories;

Alcatel-Lucent support engineers may request these logs for help in troubleshooting problems and will provide detailed instructions on how to retrieve them. Table 120 describes some of the important logs:

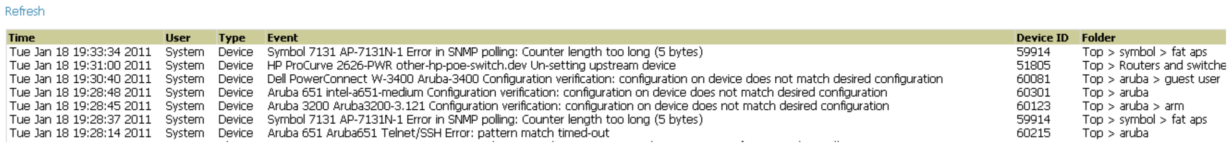
Table 120 *A Sample of Important Status Log***s**

Log	Description
pgsql	Logs database activity.
ssl_error_log	Reports problems with the web server. Also linked from the internal server error page that displays on the web page; please send this log to Alcatel-Lucent support whenever reporting an internal server error.
maillog	Applies in cases where emailed reports or alerts do not arrive at the intended recipient's address.
radius	Displays error messages associated with RADIUS accounting.
async_logger	Tracks many device monitoring processes, including user-AP association.
async_logger_client	Logs device configuration checks.
config_pusher	Logs errors in pushing configuration to devices.
visualrf.log	Details errors and messages associated with the VisualRF application.

Using the System > Event Log Page

The **System > Event Log** page is a very useful debugging tool containing a list of recent OV3600 events including APs coming up and down, services restarting, and most OV3600-related errors as well as the user that initiated the action. Figure 149 illustrates this page, and Table 121 describes the page components.

Figure 149 ***System > Event Log*** *Page Illustration*



Time	User	Type	Event	Device ID	Folder
Tue Jan 18 19:33:34 2011	System	Device	Symbol 7131 AP-7131N-1 Error in SNMP polling: Counter length too long (5 bytes)	59914	Top > symbol > fat aps
Tue Jan 18 19:31:00 2011	System	Device	HP ProCurve 2626-PWR other-hp-poe-switch.dev Un-setting upstream device	51805	Top > Routers and switche
Tue Jan 18 19:30:40 2011	System	Device	Dell PowerConnect W-3400 Aruba-3400 Configuration verification: configuration on device does not match desired configuration	60081	Top > aruba > guest user
Tue Jan 18 19:28:48 2011	System	Device	Aruba 651 intel-a651-medium Configuration verification: configuration on device does not match desired configuration	60301	Top > aruba
Tue Jan 18 19:28:45 2011	System	Device	Aruba 3200 Aruba3200-3.121 Configuration verification: configuration on device does not match desired configuration	60123	Top > aruba > arm
Tue Jan 18 19:28:37 2011	System	Device	Symbol 7131 AP-7131N-1 Error in SNMP polling: Counter length too long (5 bytes)	59914	Top > symbol > fat aps
Tue Jan 18 19:28:14 2011	System	Device	Aruba 651 Aruba651 Telnet/SSH Error: pattern match timed-out	60215	Top > aruba

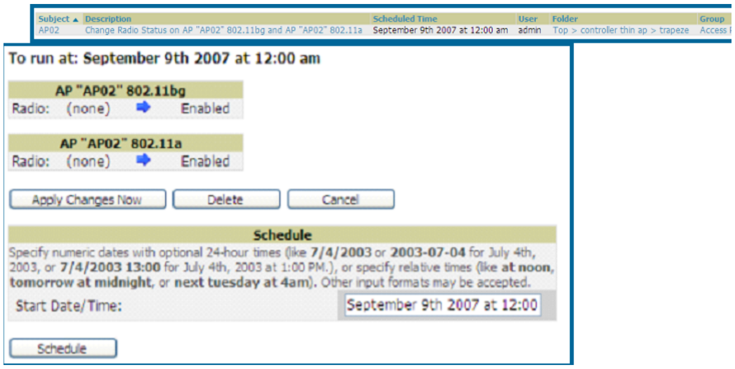
Table 121 ***Event Log*** *Fields*

Column	Description
Time	Date and time of the event.
User	The OV3600 user that triggered the event. When OV3600 itself is responsible, **System** is displayed.
Type	Displays the Type of event recorded, which is one of four types, as follows: ● **Device**—An event localized to one specific device. ● **Group**—A group-wide event. ● **System**—A system-wide event. ● **Alert**—If a trigger is configured to report to the log, an **Alert** type event will be logged here.
Event	The event OV3600 observed; useful for debugging, user tracking, and change tracking.

Using the System > Configuration Change Jobs Page

Schedule configuration change jobs are summarized on the **System > Configuration Change Jobs** page. Perform the following steps to use this page, illustrated in Figure 150.

Figure 150 ***System > Configuration Change Jobs*** *Page Illustration*



Subject ▲	Description	Scheduled Time	User	Folder	Group
AP02	Change Radio Status on AP "AP02" 802.11bg and AP "AP02" 802.11a	September 9th 2007 at 12:00 am	admin	Top > controller thin ap > trapeze	Access

To run at: **September 9th 2007 at 12:00 am**

AP "AP02" 802.11bg			
Radio:	(none)	➡	Enabled

AP "AP02" 802.11a			
Radio:	(none)	➡	Enabled

Schedule

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

Start Date/Time: September 9th 2007 at 12:00

1. To edit an existing configuration change job select on the linked description name. On the subsequent edit page you can choose to run the job immediately by selecting **Apply Changes Now**, reschedule the job by selecting **Schedule**, **Delete** the job, or **Cancel** the job edit.
2. Select the linked AP or group name under the **Subject** column to go to its monitoring page.
3. Select the linked group and folder names under **Folder** or **Group** to go to the AP's folder or group page.
4. Scheduled configuration change jobs will also appear on the **Manage** page for an AP or the **Monitoring** page for a group.

Using the System > Performance Page

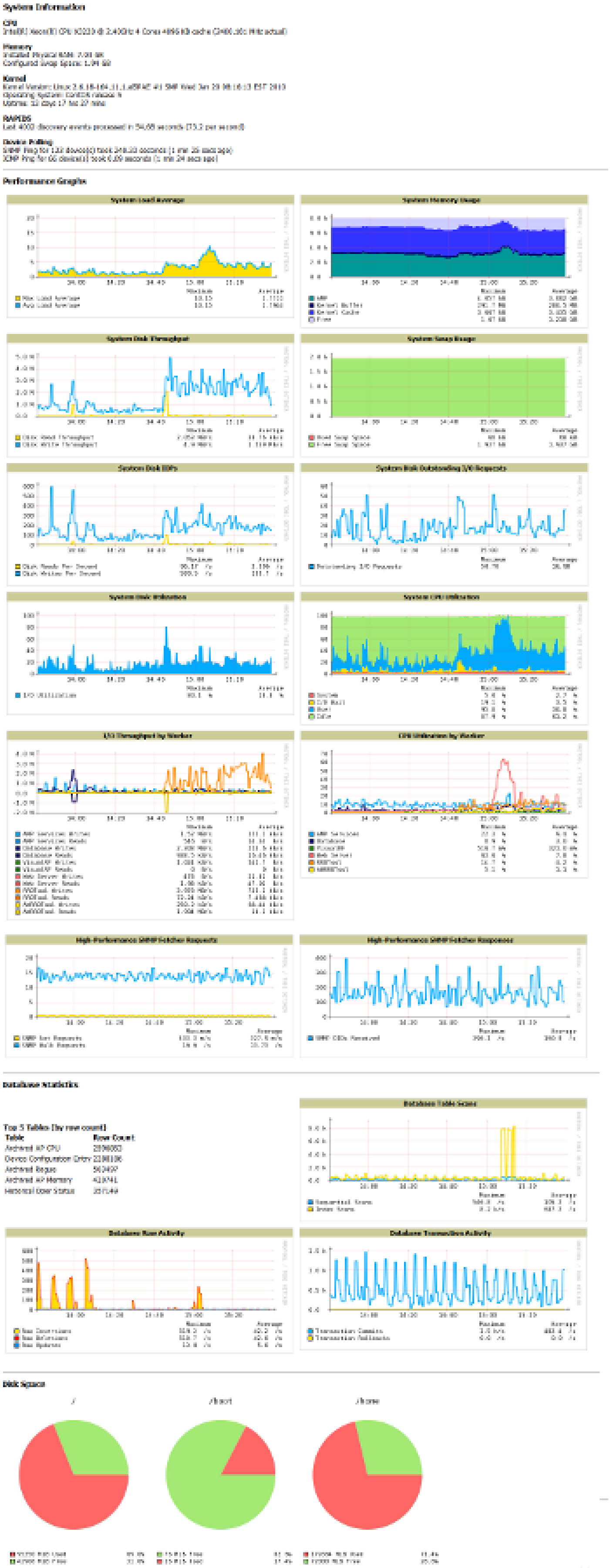
The **System > Performance** page displays basic OV3600 hardware information as well as resource usage over time. OV3600 logs performance statistics such as load average, memory and swap data every minute. The historical logging can be used to help determine the best usable polling period and track the health of OV3600 over time.

The page is divided into four sections:

- System Information
- Performance Graphs
- Database Statistics
- Disk Usage

Figure 151 illustrates this page and Table 122 describes fields and information displayed.

Figure 151 *System > Performance* Page Illustration (Partial Screen)



System Information

CPU
Intel(R) Xeon(R) CPU X3220 @ 2.40GHz 4 Cores 4096 KB cache (2400.360 MHz actual)

Memory
Installed Physical RAM: 7.93 GB
Configured Swap Space: 1.94 GB

Kernel
Kernel Version: Linux 2.6.18-164.11.1.el5PAE #1 SMP Wed Jan 20 08:16:13 EST 2010
Operating System: CentOS release 5
Uptime: 33 days 17 hrs 37 mins

RAPIDS
Last 4000 discovery events processed in 54.65 seconds (73.2 per second)

Device Polling
SNMP Ping for 122 device(s) took 248.20 seconds (1 min 26 secs ago)
ICMP Ping for 66 device(s) took 6.09 seconds (1 min 24 secs ago)

Performance Graphs

Database Statistics

Top 5 Tables (by row count)

Table	Row Count
Archived AP CPU	2896083
Device Configuration Entry	2288106
Archived Rogue	563497
Archived AP Memory	419741
Historical User Status	357149

Disk Space

Table 122 ***System > Performance*** *Page Fields and Graphs*

Field	Description
System Information	
CPU(s)	Basic CPU information as reported by the operating system.
Memory	The amount of physical RAM and Swap space seen by the operating system. Refer to the *OV3600 Server Hardware Guide* for hardware requirements.
Kernel	The version of the Linux kernel running on the box.
Device Polling	Displays some AP/Device polling statistics.
Performance Graphs	
System Load Average	The number of jobs currently waiting to be processed. Load is a rough metric that will tell you how busy a server is. A typical OV3600 load is around 2-3 times the number of CPU cores you have in your system. A constant load of 4x to 5x is cause for concern. A load above 6x is a serious issue and will probably result in OV3600 becoming unusable. To lower the average, increase a few polling periods in **Groups > Basic**.
System Memory Usage	The amount of RAM that is currently used broken down by usage. It is normal for OV3600 to have very little free RAM. Linux automatically allocates all free RAM as cache and buffer. If the kernel needs additional RAM for process it will dynamically take it from the cache and buffer.
System Disk Utilization	The amount of data read from the disk and written to the disk.
System Disk IOPs	The number of disk reads and writes per second.
System Disk Throughput	The rate of reading and writing from and to the disk in bytes per second.
System Disk Outstanding I/O Requests	The average number of outstanding I/O requests (queue depth). If it's high, it means that I/O requests (disk reads/writes) aren't being serviced as fast.
System Swap Usage	The amount of Swap memory used by OV3600. Swap is used when there is no more free physical RAM. A large performance penalty is paid when swap is used. If an OV3600 consistently uses swap, you should consider installing additional RAM.
System CPU Utilization	The percentage of CPU that has been used by the user and the system as well as the amount that was idle.
I/O Throughput by Worker/by Service	Displays reads and writes for workers (OV3600 services, database, VisualRF, web server, RRD tool and AWRRD tool) and for services (OV3600, VisualRF and web server).
CPU Utilization by Worker/by Service	Displays reads and writes for workers (OV3600 services, database, VisualRF, web server, RRD tool and AWRRD tool) and for services (OV3600, VisualRF and web server).
System Network Bandwidth	All traffic in and out measured in bits per second of your primary network interface (Eth0 being the most common).
Bandwidth by Protocol	Displays the amount of traffic used by Telnet, HTTPS and SNMP used by your primary network interface (Eth0 being the most common).
Legacy SNMP Fetcher Requests	The number of SNMP get and walk requests per second performed by the legacy (v1 and v3) SNMP fetcher.
Legacy SNMP Fetcher Responses	The number of SNMP OIDs received per second performed by the legacy (v1 and v3) SNMP fetcher.
High Performance SNMP Fetcher Requests	The number of SNMP get and walk requests per second performed by the high performance SNMP (v2c) fetcher.
High Performance SNMP Fetcher Responses	The number of SNMP OIDs received per second performed by the high performance SNMP (v2c) fetcher.

Table 122 ***System* > *Performance*** *Page Fields and Graphs (Continued)*

Field	Description
Database Statistics	
Top 5 Tables (by row count)	The five largest tables in OV3600. Degraded performance has been noticed for in some cases for tables over 200,000 rows. Alcatel-Lucent recommends decreasing the length of time client data is stored on the OV3600 page if a user/client table exceeds 250,000 rows.
Database Table Scans	The number of Database table scans performed by the database.
Database Row Activity	The number of insertions, deletions and updates performed to the database.
Database Transaction Activity	The number of commits and rollbacks performed by the database.
Disk Space	
Disk Space	Pie charts that display the amount of used and free hard drive space for each partition. If a drive reaches over 80% full, lower the **Historical Data Retention** settings on the **OV3600 Setup > General** page or consider additional hard drive space.

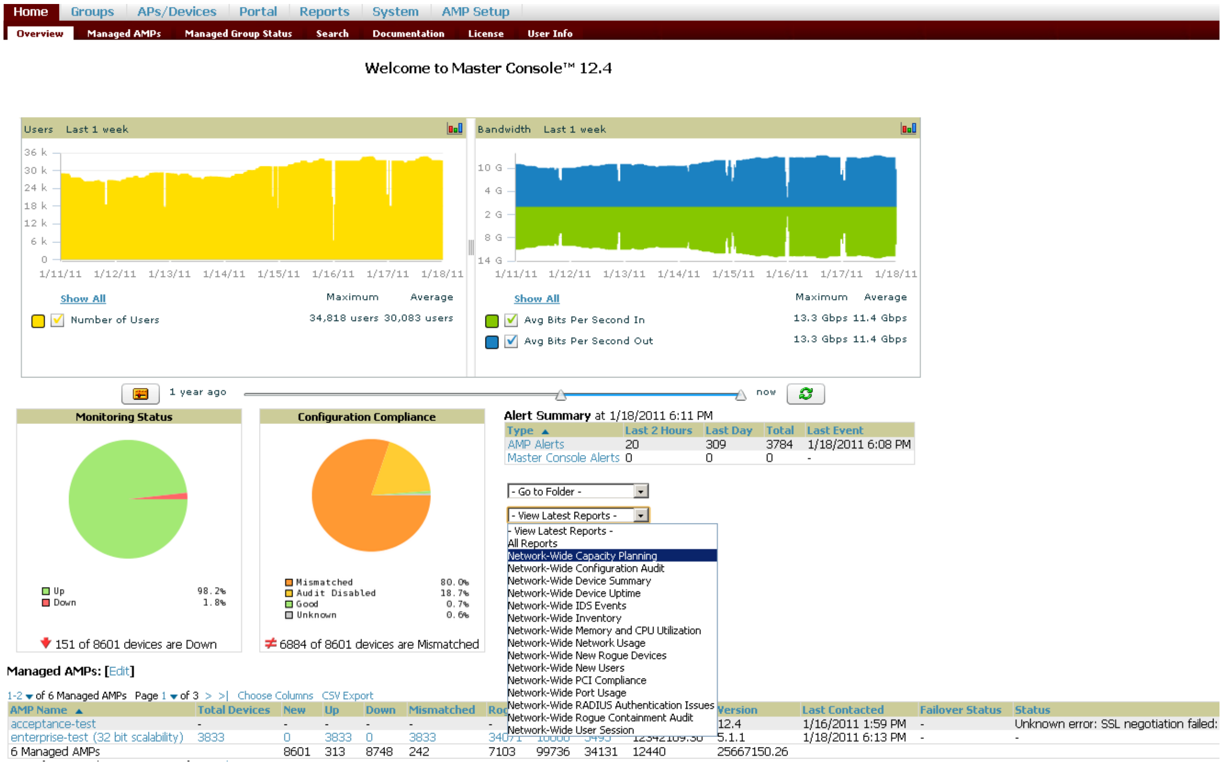
There are several initial steps that you can take to troubleshoot OV3600 performance problems, including slow page loads and timeout errors. Initial troubleshooting steps would include the following:

- Increasing the polling period settings on the **Groups > Basic** page.
- Increasing the polling period time for groups with routers and switches.
- Adding additional memory to the server. Please consult the sizing information in the latest edition of the *OV3600 Sizing Guide* or contact Alcatel support for the latest recommendations

Supporting OV3600 Servers with the Master Console

The **Master Console** (MC) is used to monitor multiple OV3600 stations from one central location. The Master Console is designed for customers running multiple OV3600 servers. Once an OV3600 station has been added to the MC, it will be polled for basic OV3600 information. Much like the normal **Home > Overview** page, the **Master Console Home > Overview** page provides summary statistics for the entire network at a glance. Figure 152 illustrates the Overview page:

Figure 152 *Master Console* ***Home > Overview*** *Page Illustration*



Welcome to Master Console™ 12.4

	Maximum	Average
☑ Number of Users	34,818 users	30,083 users

	Maximum	Average
☑ Avg Bits Per Second In	13.3 Gbps	11.4 Gbps
☑ Avg Bits Per Second Out	13.3 Gbps	11.4 Gbps

Monitoring Status	
Up	98.2%
Down	1.8%

151 of 8601 devices are Down

Configuration Compliance	
Mismatched	80.0%
Audit Disabled	18.7%
Good	0.7%
Unknown	0.6%

6884 of 8601 devices are Mismatched

Alert Summary at 1/18/2011 6:11 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	20	309	3784	1/18/2011 6:08 PM
Master Console Alerts	0	0	0	-

- View Latest Reports -
All Reports
Network-Wide Capacity Planning
Network-Wide Configuration Audit
Network-Wide Device Summary
Network-Wide Device Uptime
Network-Wide IDS Events
Network-Wide Inventory
Network-Wide Memory and CPU Utilization
Network-Wide Network Usage
Network-Wide New Rogue Devices
Network-Wide New Users
Network-Wide PCI Compliance
Network-Wide Port Usage
Network-Wide RADIUS Authentication Issues
Network-Wide Rogue Containment Audit
Network-Wide User Session

Managed AMPs: [Edit]

1-2 ▾ of 6 Managed AMPs Page 1 ▾ of 3 > >| Choose Columns CSV Export

AMP Name ▲	Total Devices	New	Up	Down	Mismatched	Rog				Version	Last Contacted	Failover Status	Status
acceptance-test	-	-	-	-	-	-				12.4	1/16/2011 1:59 PM	-	Unknown error: SSL negotiation failed:
enterprise-test (32 bit scalability)	3833	0	3833	0	3833	34071	10000	3493	12342109.30	5.1.1	1/18/2011 6:13 PM	-	-
6 Managed AMPs		8601	313	8748	242	7103	99736	34131	12440	25667150.26			

- Reports can be run from the **Master Console t**o display information from multiple OV3600 stations; because such reports can be extremely large, reports can also be run as **summary only** so that they generate more quickly and finish as a manageable file size.
- The Master Console can also be used to populate group-level configuration on managed OV3600 installations using the **Global Groups** feature.
- The Master Console offers a display of devices that are in a **Down** or **Error** state anywhere on the network. This information is supported on Master Console pages that display device lists such as **Home > Overview** and **APs Devices > List**.
- The Master Console and Failover servers can be configured with a **Managed OV3600 Down** trigger that generates an alert if communication is lost to a managed or watched OV3600 station. The Master Console or Failover server can also send email or NMS notifications about the event. See "Overview of Triggers and Alerts" on page 179.

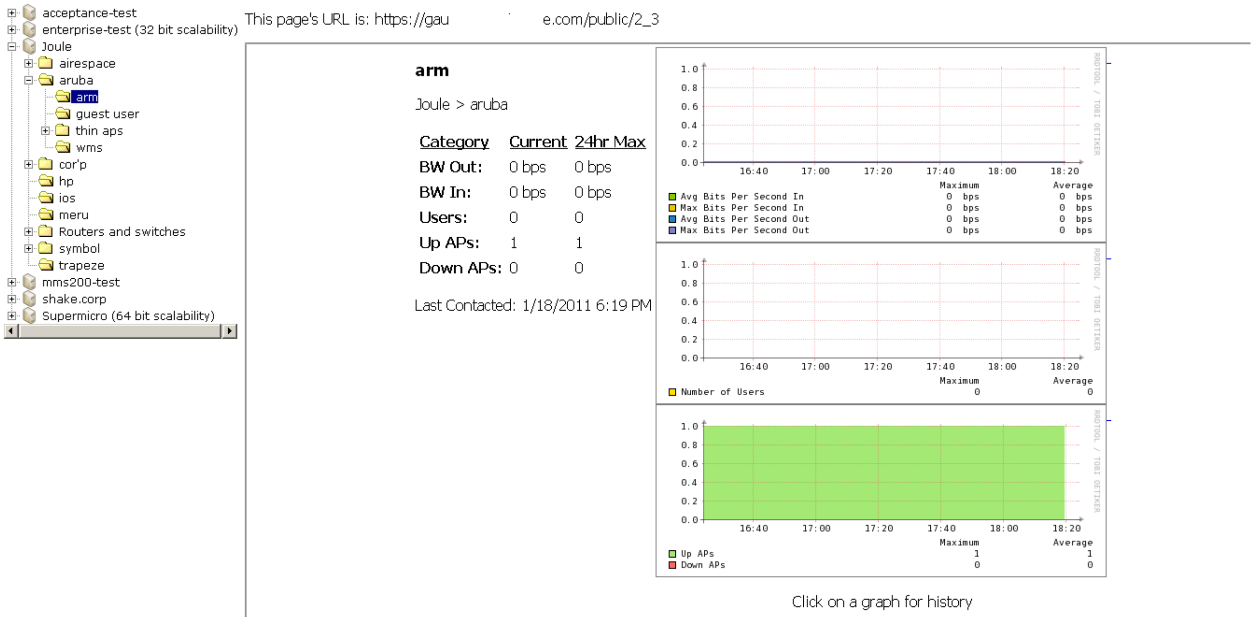
NOTE

The license key determines if the server will behave as a Master Console or as a standard OV3600 server.

Using the Public Portal on Master Console

The Master Console also contains an optional Public Portal which allows any user to view basic group-level data for each managed OV3600. This feature is disabled by default for security reasons; no OV3600 or Master Console login is required to view the public portal. The Public Portal can be enabled in **OV3600 Setup > General** in the **Master Console** section. Once enabled, a new **Portal** tab will appear to the right of the **Groups** tab (refer to the navigation section in Figure 152 in the previous page). The URL of the public portal will be https://your.OV3600.name/public. When you upgrade to the latest version of OV3600, the public portal is disabled by default, regardless of the type of license.

Figure 153 *Public Portal Page Illustration*



- acceptance-test
- enterprise-test (32 bit scalability)
- Joule
  - airespace
  - aruba
    - arm
    - guest user
    - thin aps
    - wms
  - cor'p
  - hp
  - ios
  - meru
  - Routers and switches
  - symbol
  - trapeze
- mms200-test
- shake.corp
- Supermicro (64 bit scalability)

This page's URL is: https://gau e.com/public/2_3

arm

Joule > aruba

Category	Current	24hr Max
BW Out:	0 bps	0 bps
BW In:	0 bps	0 bps
Users:	0	0
Up APs:	1	1
Down APs:	0	0

Last Contacted: 1/18/2011 6:19 PM

	Maximum	Average
🟩 Avg Bits Per Second In	0 bps	0 bps
🟨 Max Bits Per Second In	0 bps	0 bps
🟦 Avg Bits Per Second Out	0 bps	0 bps
🟪 Max Bits Per Second Out	0 bps	0 bps

	Maximum	Average
🟨 Number of Users	0	0

	Maximum	Average
🟩 Up APs	1	1
🟥 Down APs	0	0

Click on a graph for history

The **Public Portal** supports configuration of the iPhone interface. This can be configured using the Master Console OV3600 page. See "Defining General OV3600 Server Settings" on page 35.

Adding a Managed OV3600 with the Master Console

Perform the following steps to add a managed OV3600 console.

1. Navigate to the **Home > Managed OV3600s** page.
2. Select the pencil icon to edit or reconfigure an existing OV3600 console, or select **Add New Managed OV3600** to create a new OV3600 console. The **Managed** OV3600 page appears. Complete the settings on this page as described in Table 123.

Table 123 ***Managed OV3600*** *Fields and Default Values*

Field	Default	Description
Hostname / IP Address	N/A	Enter the IP address or Hostname of the managed OV3600 server.
Polling Enabled	Yes	Enables or disables the Master Console polling of managed OV3600.
Polling Period	5 minutes	Determines how frequently the Master Console polls the managed OV3600.
Username	N/A	The username used by the Master Console to login to the managed OV3600 server. The user needs to be an AP/Device Manager or OV3600 Administrator.
Password (Confirm Password)	N/A	The password used by the Master Console OV3600 to login to the managed OV3600.
HTTP Timeout (5-1000 sec)	60	Defines the timeout period used when polling the managed OV3600 server.
Manage Group Configuration	No	Defines whether the Master Console can manage device groups on the managed OV3600 server.

3. When finished, select **Add** to be returned to the **Managed OV3600s** list page.

Using Global Groups with Master Console

To push configurations to managed groups using the OV3600 Global Groups feature, follow these steps:

1. Navigate to the Master Console's **Groups > List** page.
2. Select **Add** to add a new group, or select the name of the group to edit settings for an existing group.
3. Select the **Duplicate** icon to create a new group with identical configuration to an existing group. Groups created on the Master Console will act as Global Groups, or groups with master configurations that can be pushed out to subscriber groups on managed OV3600s. Global groups are visible to all users, so they cannot contain APs (which can be restricted based on user role).
4. Selecting the name of an existing group on the Master Console loads the subtabs for **Basic, Security, SSIDs, AAA Servers, Templates, Radio, Cisco WLC, Proxim Mesh,** and **MAC ACL** pages, if such pages and configurations are active for the devices in that group.

   These subtabs contain the same fields as the group subtabs on a monitored OV3600, but each field also has a checkbox. The Master Console can also configure global templates that can be used in subscriber groups. The process is the same as described in the Chapter 6, “Creating and Using Templates” , except that there is no process by which templates can be fetched from devices in the subscriber group on managed OV3600s. Instead, the template must be pasted into the Master Console Global Group.

When a Global Group is pushed from the Master Console to subscriber groups on managed OV3600s, all settings will be static except for settings with the checkbox selected; for fields with checkboxes selected, the value or setting can be changed on the corresponding tab for each managed group. For list pages, override options are available only on the **Add** page for each list. It will take several minutes for changes to Global Groups on the Master Console to be pushed to the managed OV3600s; make sure that the **Manage Group Configuration** option is enabled for each managed OV3600.

Once Global Groups have been configured on the Master Console, groups must be created or configured on the managed OV3600s to subscribe to a particular Global Group. To configure subscriber groups, enable **Use Global Groups** on the **Group > Basic** page of a group on a managed OV3600. Select the name of the Global Group from the drop-down menu, and then select **Save and Apply**. Note that the MC doesn't push anything when you create new subscriber groups; the copy of the Global Group already on the managed OV3600 provides the information.

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

The Global Groups feature can also be used without the Master Console. For more information about how this feature works, refer to “Configuring and Using Device Groups in OV3600” on page 69.

Upgrading OV3600

The OV3600 upgrade process may change. Please contact support and consult the latest OV3600 release announcement for detailed instructions and changes. The following is sample instructions from the 6.4:

Upgrade Instructions

To upgrade your OV3600:

1. Log in to the OV3600 server as the root user.
2. Run the following command (where x.x.x is equal to the latest OV3600 version)

```
# start_amp_upgrade -v x.x.x
```

Upgrading Without Internet Access

If your OV3600 cannot get to the Internet:

1. Download the latest OV3600 version from our download page: www.alcatel-lucent.com/enterprise
2. Copy the file to OV3600 /root directory using WinSCP.
3. On the OV3600, run the following command:

```
# start_amp_upgrade -v x.x.x
```

The `start_amp_upgrade` script will check the `/root` directory for the latest update. If the update is not found, the script will attempt to download it from the AirWave support page. The script will then extract the version specific upgrade script. The version specific script will deploy all needed files, update the database, perform any data migrations and restart the OV3600 services.

Backing Up OV3600

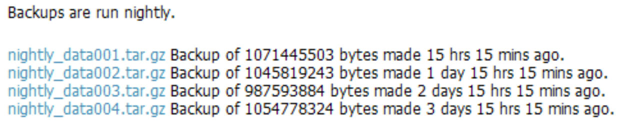
OV3600 creates nightly archives of all relational data, statistical data, and log files. This occurs by default at 4:15 AM, but is configurable on **OV3600 Setup > General** under the **Nightly Maintenance Time** setting.

Although OV3600 only keeps the last four sets of archives, the archives can be downloaded manually or automatically off-site for more extensive backup strategies. OV3600 creates one data backup file each night. The data backup file contains all of the device and group information as well as historical data and system files, including IP address, NTP information, mail relay hosts, and other OV3600 settings.

Viewing and Downloading Backups

To view current OV3600 backup files, go to the **System > Backups** page. Figure 154 illustrates this page.

Figure 154 ***System > Backups*** *Page Illustration*



Backups are run nightly.

nightly_data001.tar.gz Backup of 1071445503 bytes made 15 hrs 15 mins ago.
nightly_data002.tar.gz Backup of 1045819243 bytes made 1 day 15 hrs 15 mins ago.
nightly_data003.tar.gz Backup of 987593884 bytes made 2 days 15 hrs 15 mins ago.
nightly_data004.tar.gz Backup of 1054778324 bytes made 3 days 15 hrs 15 mins ago.

To download a backup file, select the filename URL and the **File Download** popup page appears.

Regularly save the data backup file to another machine or media. This process can be automated easily with a nightly script.

NOTE

Nightly maintenance and amp_backup scripts back up the full OV3600 data and save the file as nightly_data00[1-4].tar.gz. In previous OV3600 versions, the scripts created both config backup and data backup files. In order to restore the OV3600 data, it is only necessary to have most recent data backup file, and OV3600 no longer uses or supports the config backup file, effective as of OV3600 6.3.2 and later OV3600 versions.

Running Backup on Demand

To create an immediate backup:

1. Log into the OV3600 system as **root**.
2. Run the backup script by typing **`amp_backup`**.

This creates a backup of the system located in `/alternative/databackup.tar.gz.`

Restoring from a Backup

To restore a backup file on a new machine:

1. Use your OV3600 Installation CD to build a new machine. The new machine must be running the same version as the OV3600 that created the backup file.
2. Copy the nightly_data00[1-4].tar.gz file to the `/tmp` directory in the new OV3600.

   A file transfer Windows client that supports SFTP/SCP is WinSCP: http://winscp.sourceforge.net/eng/.

   WinSCP allows you to transfer the nightly00[1-4].tar.gz file from your local PC to the new OV3600 using the secure copy protocol (SCP).
3. Log onto the new server as **root**.
4. Change to the scripts directory by typing **`scripts`**.
5. Run the restore script by typing **`./amp_restore -d /tmp/nightly_data00[1-4].tar.gz`**.

NOTE

Network administrators can now use the nightly backup from a 32-bit OV3600 to restore OV3600 on a 64-bit installation, rather than having to create a special backup file or use the special restore script.

Upgrading OV3600

The OV3600 upgrade process may change. Please consult support of the latest OV3600 release announcement for detailed instructions. The following is sample instructions from the 6.4 email:

Upgrade Instructions

To upgrade your OV3600:

1. Login to the OV3600 server as the root user.
2. Run the following command

```
# start_ov3600_upgrade -v 6.4.0
```

Upgrading Without Internet Access

If your OV3600 cannot get to the Internet:

1. Download OV3600 6.4.0 from our download page: http://service.esd.alcatel-lucent.com
2. Copy the file to OV3600 /root directory using WinSCP.
3. On the OV3600, run the following command:

```
# start_ov3600_upgrade -v 6.4.0
```

The `start_ov3600_upgrade` script will check the /root directory for the latest update. If the update is not found, the script will attempt to download it from the Alcatel-Lucent support page. The script will then extract the version specific upgrade script. The version specific script will deploy all needed files, update the database, perform any data migrations and restart the OV3600 services.

Backing Up OV3600

Overview of Backups

OV3600 creates nightly archives of all relational data, statistical data, and log files. This occurs by default at 4:15 AM, but is configurable on the **OV3600 Setup > General** page under the **Nightly Maintenance Time** setting.

Although OV3600 only keeps the last four sets of archives, the archives can be downloaded manually or automatically off-site for more extensive backup strategies. OV3600 creates one data backup file each night. The data backup file contains all of the device and group information as well as historical data and system files, including IP address, NTP information, mail relay hosts, and other OV3600 settings.

Viewing and Downloading Backups

To view current OV3600 backup files, go to the **System > Backups** page. Figure 154 illustrates this page.

To download a backup file, click the filename URL and the **File Download** popup page appears. Proceed as prompted.

Alcatel-Lucent recommends regularly saving the data backup file to another machine or media. This process can be automated easily with a nightly script.

NOTE

Nightly maintenance and ov3600_backup scripts back up the full OV3600 data and save the file as nightly_data001.tar.gz. In previous OV3600 versions, the scripts created both config backup and data backup files. In order to restore the OV3600 data, it is only necessary to have most recent data backup file, and OV3600 no longer uses or supports the config backup file, effective with OV3600 6.3.2 and later OV3600 versions.

Running Backup on Demand

To create an immediate backup, use the following procedure:

1. Log into the OV3600 system as root.
2. Run the backup script by typing **ov3600_backup**

This creates a backup of the system located in /alternative/databackup.tar.gz.

Restoring from a Backup

To restore a backup file on a new machine use the following procedure:

1. Use your OV3600 Installation CD to build a new machine. The new machine must be running the same version as the OV3600 that created the backup file.
2. Copy the nightly_data00[1-4].tar.gz file to the new OV3600. The /tmp directory is a good destination.

   A good open source Windows file transfer client that supports SFTP and SCP for is WinSCP, available from http://winscp.sourceforge.net/eng/.
3. Log onto the new server as **root**.
4. Run the restore script by typing **ov3600_restore -d /tmp/nightly_data00[1-4].tar.gz**.

Using OV3600 Failover for Backup

The failover version of OV3600 provides a “many to one” hot backup server. The Failover OV3600 polls the watched OV3600s to verify that each is up and running. If the watched OV3600 is unreachable for the specified number of polls, the Failover OV3600 automatically restores the most recent saved backup from the watched OV3600 and begins polling its APs.

Navigation Section of OV3600 Failover

The **Navigation** section displays tabs to all main GUI pages within OV3600 Failover. The top navigation bar containing tabs for the main components of OV3600, while the lower bar is context-sensitive and displays the subtabs for the highlighted tab. Table 124 describes the contents of this page.

Table 124 *Contents of the Navigation Section of Failover*

Main Tab	Description	Subtabs
Home	The **Home** page provides basic OV3600 Failover information including system name, hostname, IP address, current time, running time, software version, and watched OV3600 information.	● **Overview** ● **User Info** ● **Watched OV3600s** ● **License**

Table 124 *Contents of the Navigation Section of Failover*

Main Tab	Description	Subtabs
System	The **System** page provides information related to OV3600 operation and administration including overall system status, performance monitoring, and backups.	- **Status** - **Triggers** - **Alerts** - **Event Log** - **Backups** - **Performance**
OV3600 Setup	The **Setup** page provides all information relating to the configuration of OV3600 itself and its connection to your network.	- **General** - **Network** - **Users** - **TACACS+**

Adding Watched OV3600 Stations

Navigate to the **Home > Watched OV3600s** page to begin backing up and monitoring OV3600 stations. Once an OV3600 installation has been added to the Watched OV3600 list, the Failover OV3600 will download the most recent backup and begin polling. The Failover OV3600 and the Watched OV3600 must be on the same version or else the watched OV3600 will be unable to restore properly. If any of the watched OV3600s are not on the same version of OV3600, you will need to upgrade. The Failover OV3600 will need HTTPS access (port 443) to the watched OV3600 to verify that the web page is active and to fetch downloads.

Once the Failover OV3600 determines that the Watched OV3600 is not up (based on the user-defined missed poll threshold) it will restore the data backup of the Watched OV3600 and begin monitoring the watched OV3600 APs and devices. There are many variables that affect how long this will take including how long client historical data is being retained, but for an OV3600 with 1,000 APs it might take up to 10 minutes. For an OV3600 with 2,500 APs, it might take as long as 20 minutes. The Failover OV3600 retains its original IP.

In summary, the Failover OV3600 could take over for the Watched OV3600 in as little as five minutes; it might take up to an additional 10-20 minutes to unpack the watched OV3600 data and begin monitoring APs. The most important factors are the missed poll threshold, which is defined by the user, and the size of the watched OV3600 backup, which is affected by the total number of APs and by the amount of data being saved, especially client historical data.

To restore the Watched OV3600, run the backup script from the command line and copy the current data file and the old Watched OV3600 configuration file to the Watched OV3600. Then run the restore script. More information about backups and restores can be found in "Backing Up OV3600" on page 215.

Table 125 ***Home*** **>** ***Watched*** *Page Fields and Default Values*

Setting	Default	Description
IP/Hostname	None	The IP address or Hostname of the watched OV3600. The Failover OV3600 needs HTTPS access to the watched OV3600s.
Username	None	A username with management rights on the watched OV3600.
Password	None	The password for the username with management rights specified above.
HTTP Timeout (5-1000 Sec)	60	The amount of time before OV3600 considers a polling attempt failed.
Polling Enabled	Yes	Enables or disables polling of the Watched OV3600. **NOTE:** You do not need to disable polling of the watched OV3600 system if it is set to be down during nightly maintenance or is being upgraded.
Polling Period	5 minutes	The amount of time between polls of the Watched OV3600.
Missed Poll Threshold	None	The number of polls that can be missed before the failover OV3600 will begin actively monitoring the Watched OV3600 APs.

Chapter 9

Creating, Running, and Emailing Reports

This chapter describes OV3600 reports, including access, creation, scheduling, and distribution.

This chapter includes the following sections:

OV3600 ships with several reports enabled by default. Default reports may run nightly or weekly, depending on the OV3600 release. Review the list of defined and scheduled reports with the **Reports > Generated** and **Reports > Definition** pages to determine if default reports are desired. If not, you can delete, disable, or reschedule any of them.

OV3600 supports additional specialized reports as follows:

- **System > Status** page supports the diagnostic report file for sending to customer support: diagnostics.tar.gz.
- **System > Status** page supports the VisualRF diagnostics report file: VisualRFdiag.tar.gz.
- **VisualRF > Network View** supports the Bill of Materials (BOM) report. Refer to the *VisualRF User Guide*.

Overview of OV3600 Reports

Reports are powerful tools in network analysis, user configuration, device optimization, and network monitoring on multiple levels. Among their benefits, reports provide an interface for multiple configurations.

OV3600 reports have the following general parameters:

- OV3600 runs daily versions of all reports during predefined windows of time. All reports can be scheduled to run in the background.
- The daily version of any report is available instantly in the **Reports > Generated** page.
- The **Inventory** and the **Configuration Audit** reports are the only reports that don't span a period of time. Instead, these two reports provide a snapshot of the current state of the network.
- Users can create all other reports over a custom time period on the **Reports > Definitions** page. All reports can be emailed or exported to XML format for easy data manipulation using a spreadsheet.

Reports > Definitions Page Overview

The **Reports > Definitions** page allows you to define new reports and see the reports already defined.

The **Definitions** page includes these sections:

- **Report definitions** section—The **Add** button allows you to define a custom report using the **Custom Options** drag and drop interface, or from any of the report types in the dropdown menu. The **Report Definitions** table has a complete list of all saved report definitions with an option to return to each definition's table to further customize your report.
  - **Add and Run** allows you to create a report definition and run that report immediately.

- **Run Now** (visible from the expanded **Report Definitions** menu) allows immediate running of a custom report as soon as you set the parameters. You must save its definition separately, if you want to remember the parameters.

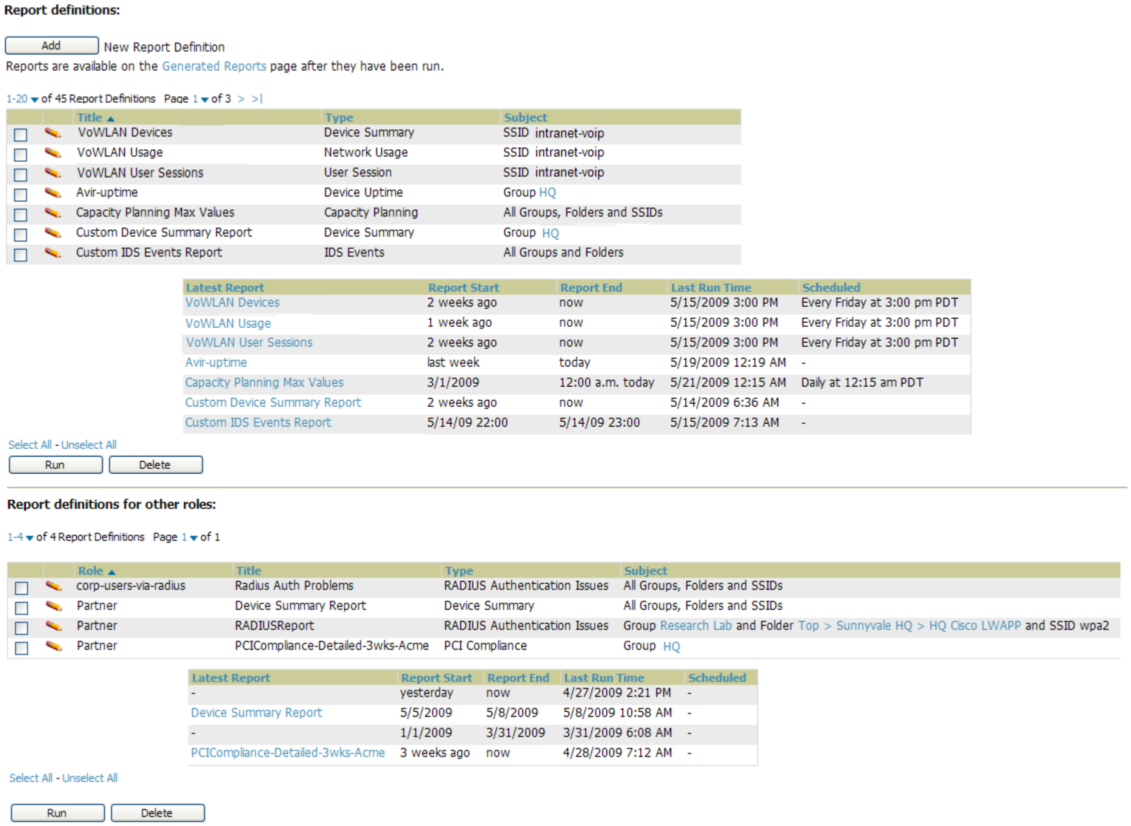
- **Report definitions for other roles** section—This section, supported for **admin** users, displays additional reports that have been scheduled for other roles. This section of the page adds the **Role** column, and other columns are the same.

Each pane includes a **Latest Report** column with the most recently run reports for each definition and role created. **Run** and **Delete** buttons allow you to select a report from the definitions table to run or delete. Once you define a report from the **Definition** page, it appears on the **Generated** page. The **Reports > Definition** page is shown in Figure 155, and Table 126 describes the fields available when you select a specific report definition.

Table 126 ***Reports > Definition*** *Page Fields and Descriptions*

Field	Description
Report Definition	Displays a field for entering report title and dropdown menu, shown in Figure 156, displaying all possible report types.
Report Restrictions	Displays dynamic fields that include spaces for selecting attributes and entering data relevant to your selected report type scope such as groups, folders, SSID, Device Search filter, report start and end times.
Scheduling Options	Reveals options for one time or regularly scheduled reporting by selecting **Yes**. Options include report frequency, start time, and current system time.
Report Visibility	Allows you to determine a report's visibility according to user role.
Email Options	Reveals email address preferences for sending reports by selecting **Yes**.
Add and Run	Allows you to create a report definition and run that report right then.
Run Now	Allows you to run any report that has been defined on the spot without saving settings or creating a new report definition.
Add	Saves report definition you just created.

Figure 155 ***Reports > Definitions*** *Page Illustration (Split View)*



Report definitions:

Add New Report Definition

Reports are available on the Generated Reports page after they have been run.

1-20 ▾ of 45 Report Definitions Page 1 ▾ of 3 > >|

		Title ▲	Type	Subject
□	✎	VoWLAN Devices	Device Summary	SSID intranet-voip
□	✎	VoWLAN Usage	Network Usage	SSID intranet-voip
□	✎	VoWLAN User Sessions	User Session	SSID intranet-voip
□	✎	Avir-uptime	Device Uptime	Group HQ
□	✎	Capacity Planning Max Values	Capacity Planning	All Groups, Folders and SSIDs
□	✎	Custom Device Summary Report	Device Summary	Group HQ
□	✎	Custom IDS Events Report	IDS Events	All Groups and Folders

Latest Report	Report Start	Report End	Last Run Time	Scheduled
VoWLAN Devices	2 weeks ago	now	5/15/2009 3:00 PM	Every Friday at 3:00 pm PDT
VoWLAN Usage	1 week ago	now	5/15/2009 3:00 PM	Every Friday at 3:00 pm PDT
VoWLAN User Sessions	2 weeks ago	now	5/15/2009 3:00 PM	Every Friday at 3:00 pm PDT
Avir-uptime	last week	today	5/19/2009 12:19 AM	-
Capacity Planning Max Values	3/1/2009	12:00 a.m. today	5/21/2009 12:15 AM	Daily at 12:15 am PDT
Custom Device Summary Report	2 weeks ago	now	5/14/2009 6:36 AM	-
Custom IDS Events Report	5/14/09 22:00	5/14/09 23:00	5/15/2009 7:13 AM	-

Select All - Unselect All

Run Delete

Report definitions for other roles:

1-4 ▾ of 4 Report Definitions Page 1 ▾ of 1

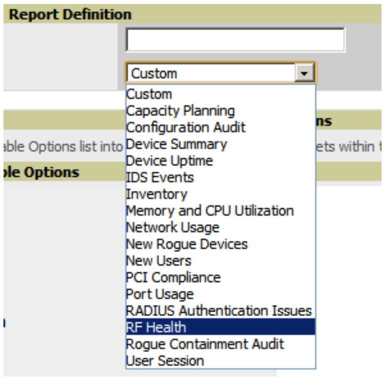
		Role ▲	Title	Type	Subject
□	✎	corp-users-via-radius	Radius Auth Problems	RADIUS Authentication Issues	All Groups, Folders and SSIDs
□	✎	Partner	Device Summary Report	Device Summary	All Groups, Folders and SSIDs
□	✎	Partner	RADIUSReport	RADIUS Authentication Issues	Group Research Lab and Folder Top > Sunnyvale HQ > HQ Cisco LWAPP and SSID wpa2
□	✎	Partner	PCICompliance-Detailed-3wks-Acme	PCI Compliance	Group HQ

Latest Report	Report Start	Report End	Last Run Time	Scheduled
-	yesterday	now	4/27/2009 2:21 PM	-
Device Summary Report	5/5/2009	5/8/2009	5/8/2009 10:58 AM	-
-	1/1/2009	3/31/2009	3/31/2009 6:08 AM	-
PCICompliance-Detailed-3wks-Acme	3 weeks ago	now	4/28/2009 7:12 AM	-

Select All - Unselect All

Run Delete

Figure 156 ***Report Type*** *Drop-down Menu in* ***Reports > Definitions*** *Illustration*



Report Definition

Custom ▾

NOTE

Only **admin** users have complete access to all report information. The OV3600 reports and online displays of information can vary with configuration, User Roles, and Folders.

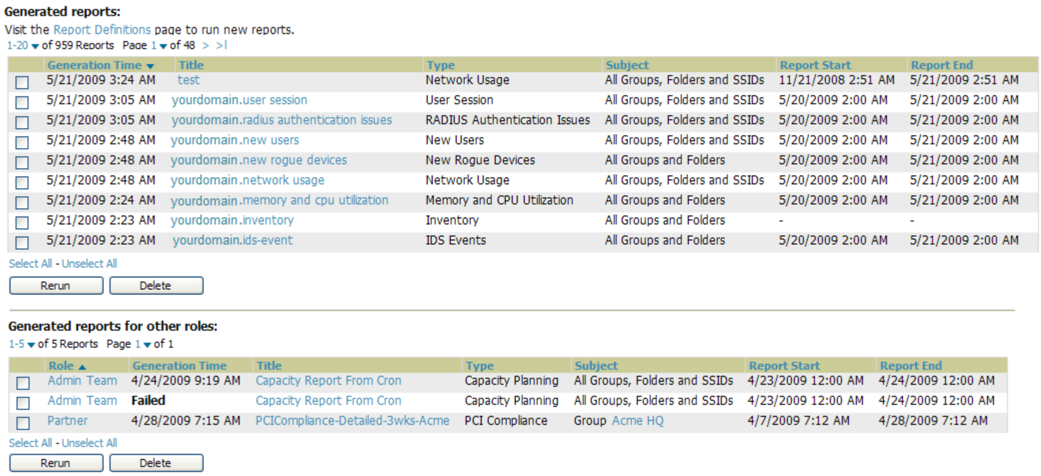
Reports > Generated Page Overview

The **Reports > Generated** page displays reports that have been run, as well as the most recent daily version of any report. An **Admin** user can see and edit all report definitions in OV3600. Users with **Monitor Only** roles can see reports and definitions only if they have access to all devices in the reports.

The **Reports > Generated** page contains three primary sections, as follows:

- Generated reports configured for the current role and for additional roles
- Generated reports for other roles
- The latest daily reports for immediate online viewing

Figure 157 ***Reports > Generated** Page Example*



Generated reports:

Visit the Report Definitions page to run new reports.

1-20 ▾ of 959 Reports Page 1 ▾ of 48 > >|

	Generation Time ▾	Title	Type	Subject	Report Start	Report End
□	5/21/2009 3:24 AM	test	Network Usage	All Groups, Folders and SSIDs	11/21/2008 2:51 AM	5/21/2009 2:51 AM
□	5/21/2009 3:05 AM	yourdomain.user session	User Session	All Groups, Folders and SSIDs	5/20/2009 2:00 AM	5/21/2009 2:00 AM
□	5/21/2009 3:05 AM	yourdomain.radius authentication issues	RADIUS Authentication Issues	All Groups, Folders and SSIDs	5/20/2009 2:00 AM	5/21/2009 2:00 AM
□	5/21/2009 2:48 AM	yourdomain.new users	New Users	All Groups, Folders and SSIDs	5/20/2009 2:00 AM	5/21/2009 2:00 AM
□	5/21/2009 2:48 AM	yourdomain.new rogue devices	New Rogue Devices	All Groups and Folders	5/20/2009 2:00 AM	5/21/2009 2:00 AM
□	5/21/2009 2:48 AM	yourdomain.network usage	Network Usage	All Groups, Folders and SSIDs	5/20/2009 2:00 AM	5/21/2009 2:00 AM
□	5/21/2009 2:24 AM	yourdomain.memory and cpu utilization	Memory and CPU Utilization	All Groups and Folders	5/20/2009 2:00 AM	5/21/2009 2:00 AM
□	5/21/2009 2:23 AM	yourdomain.inventory	Inventory	All Groups and Folders	-	-
□	5/21/2009 2:23 AM	yourdomain.ids-event	IDS Events	All Groups and Folders	5/20/2009 2:00 AM	5/21/2009 2:00 AM

Select All - Unselect All

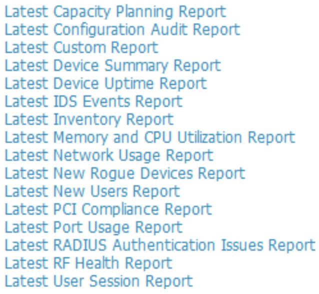
Generated reports for other roles:

1-5 ▾ of 5 Reports Page 1 ▾ of 1

	Role ▴	Generation Time	Title	Type	Subject	Report Start	Report End
□	Admin Team	4/24/2009 9:19 AM	Capacity Report From Cron	Capacity Planning	All Groups, Folders and SSIDs	4/23/2009 12:00 AM	4/24/2009 12:00 AM
□	Admin Team	**Failed**	Capacity Report From Cron	Capacity Planning	All Groups, Folders and SSIDs	4/23/2009 12:00 AM	4/24/2009 12:00 AM
□	Partner	4/28/2009 7:15 AM	PCICompliance-Detailed-3wks-Acme	PCI Compliance	Group Acme HQ	4/7/2009 7:12 AM	4/28/2009 7:12 AM

Select All - Unselect All

Figure 158 ***Reports > Generated** Page with Single-click Report Viewing Options*



Latest Capacity Planning Report
Latest Configuration Audit Report
Latest Custom Report
Latest Device Summary Report
Latest Device Uptime Report
Latest IDS Events Report
Latest Inventory Report
Latest Memory and CPU Utilization Report
Latest Network Usage Report
Latest New Rogue Devices Report
Latest New Users Report
Latest PCI Compliance Report
Latest Port Usage Report
Latest RADIUS Authentication Issues Report
Latest RF Health Report
Latest User Session Report

Using Daily Reports

This section describes the default and custom-scheduled reports supported in OV3600. These reports can be accessed from the **Reports > Generated** page.

Viewing Generated Reports

The **Reports > Generated** page supports the following general viewing options:

- By default, the reports on the **Reports > Generated** page are sorted by **Generation Time**. You can sort reports by any other column header in sequential or reverse sequential order. You can also choose columns, export the Generated Reports list in CSV, and modify the pagination of this list.
- The **Reports > Detail** page launches when you select any report title from this page.

The **Generated Reports** page contains fewer columns and information than the **Definitions** page. Table 127 describes each column for the **Reports > Generated** page.

Table 127 ***Reports > Generated** Page Fields and Descriptions*

Field	Description
Generated Time	Displays the date and time of the last time the report was run, or when the latest report is available. Selecting the link in this field displays the latest version of a given report. When the latest version of a given report is not available, this field is blank. In this case, a report can be run by selecting the report title and selecting **Run**.
Title	Displays title of the report. This is a user-configured field when creating the report.
Type	Displays the type of the report.
Subject	Displays the scope of the report, to include groups, folders, SSIDs, or any combination of these that are included in the report.
Report Start	Displays the beginning of the time period covered in the report.

Table 127 ***Reports > Generated*** *Page Fields and Descriptions*

Field	Description
Report End	Displays the end of the time period covered in the report.
Role	In the **Reports definitions for other roles** section, this column indicates the roles for which additional reports are defined.

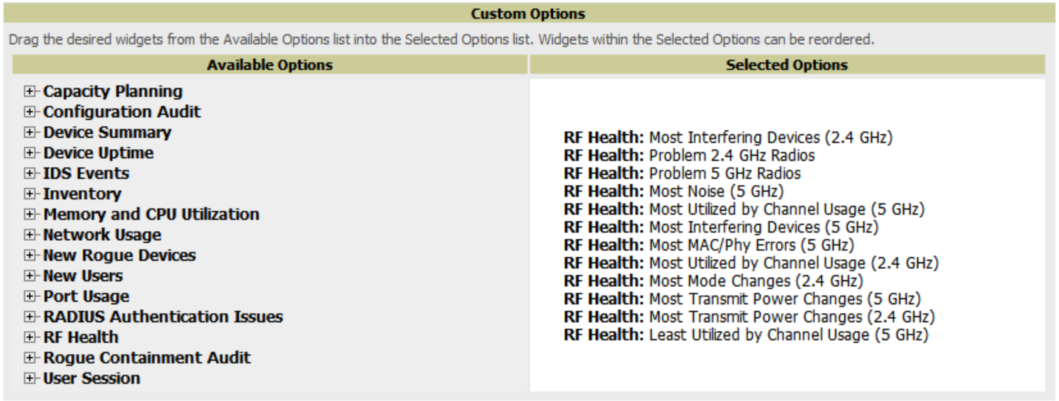
Using Custom Reports

Custom reports allow users to specify the data that should be included in a report.

Perform these steps to create a Custom Report.

1. Navigate to the **Reports > Definitions** page.
2. Select **Add**.
3. By default, the Custom option will be selected in the Type drop-down menu, and the **Custom Options** section appears below as shown in Figure 159.

Figure 159 ***OV3600 Custom Options*** *Page Illustration*



Custom Options

Drag the desired widgets from the Available Options list into the Selected Options list. Widgets within the Selected Options can be reordered.

Available Options

- ⊞ Capacity Planning
- ⊞ Configuration Audit
- ⊞ Device Summary
- ⊞ Device Uptime
- ⊞ IDS Events
- ⊞ Inventory
- ⊞ Memory and CPU Utilization
- ⊞ Network Usage
- ⊞ New Rogue Devices
- ⊞ New Users
- ⊞ Port Usage
- ⊞ RADIUS Authentication Issues
- ⊞ RF Health
- ⊞ Rogue Containment Audit
- ⊞ User Session

Selected Options

RF Health: Most Interfering Devices (2.4 GHz)
RF Health: Problem 2.4 GHz Radios
RF Health: Problem 5 GHz Radios
RF Health: Most Noise (5 GHz)
RF Health: Most Utilized by Channel Usage (5 GHz)
RF Health: Most Interfering Devices (5 GHz)
RF Health: Most MAC/Phy Errors (5 GHz)
RF Health: Most Utilized by Channel Usage (2.4 GHz)
RF Health: Most Mode Changes (2.4 GHz)
RF Health: Most Transmit Power Changes (5 GHz)
RF Health: Most Transmit Power Changes (2.4 GHz)
RF Health: Least Utilized by Channel Usage (5 GHz)

The left pane of the **Custom Options** section lists all available data that can be included in the report. For example, if the data you want to include is in the RF Health report, select **RF Health** to view a list of all available radio frequency information. Then, simply drag the desired data from the **Available Options** list on the left to the **Selected Options** pane on the right. The order of the data in the **Selected Options** section is the order that it will appear in the report. The data can be reordered by dragging an item up or down the list.

4. Below the Custom Options panes are the **Report Restrictions**, **Scheduling Options**, **Report Visibility**, and **Email Options** sections. Choose the parameters as needed for your report, especially a **Report Start** and **Report End**.
5. When finished, select **Add and Run** to add the report to your list and run it immediately, **Run Now** to run without being added to the list, **Add** to add but not run the report, and **Cancel** to exit this page.

Using the Capacity Planning Report

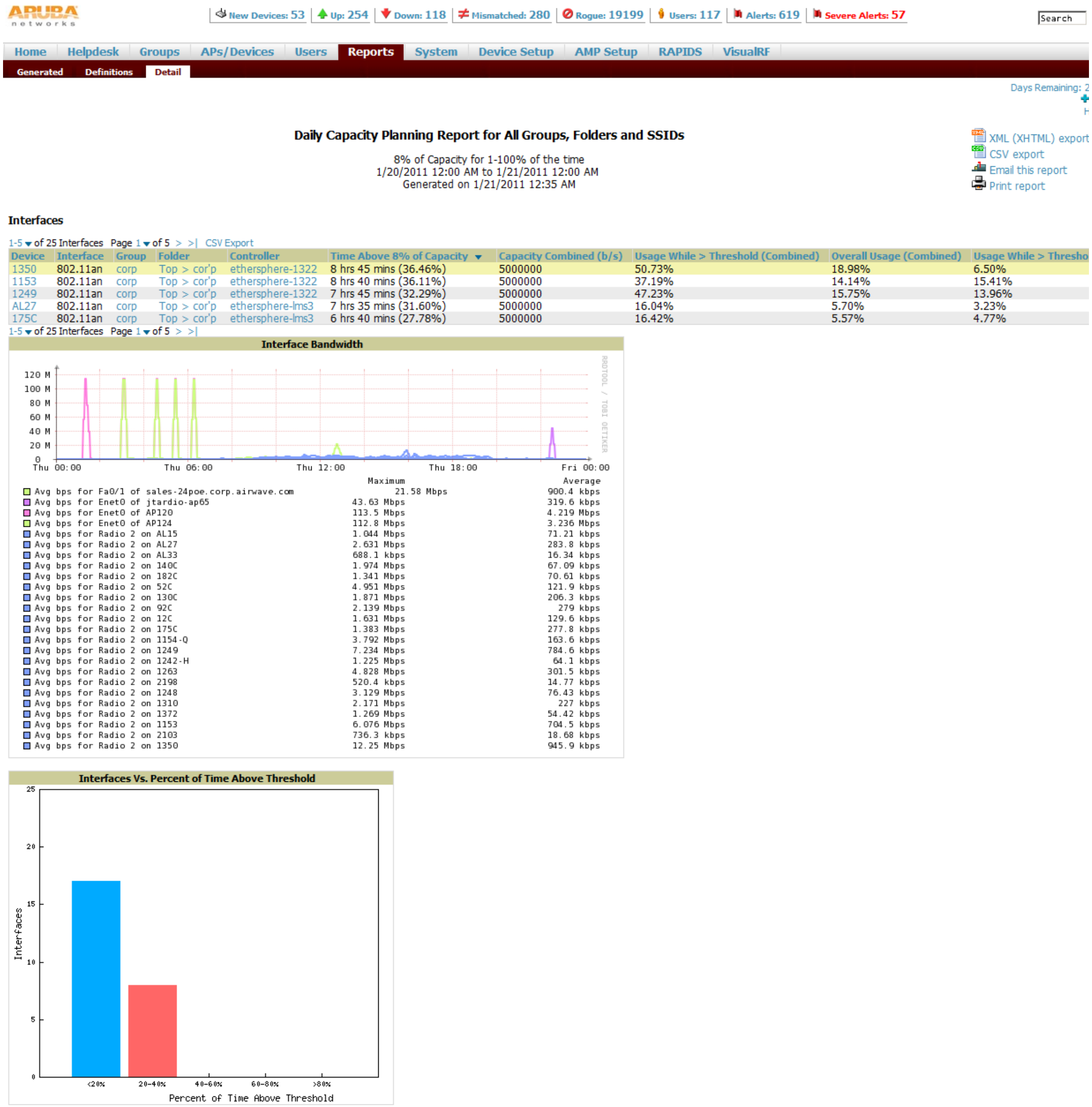
The **Capacity Planning Report** tracks device bandwidth capacity and throughput in device groups, folders, and SSIDs. This report assists in analyzing device capacity and performance on the network, and such analysis can help to achieve network efficiency and improved experience for users.

This report is based on interface-level activity. The information in this report can be sorted by any column header in sequential or reverse-sequential order by selecting the column heading.

Refer also to the "Using the Network Usage Report" on page 231 for additional bandwidth information.

The following figures and Table 128 illustrate and describe the contents of the **Capacity Planning Report**.

Figure 160 ***Capacity Planning Report*** *Detail Page*



Daily Capacity Planning Report for All Groups, Folders and SSIDs

8% of Capacity for 1-100% of the time
1/20/2011 12:00 AM to 1/21/2011 12:00 AM
Generated on 1/21/2011 12:35 AM

Interfaces

1-5 ▾ of 25 Interfaces Page 1 ▾ of 5 > >| CSV Export

Device	Interface	Group	Folder	Controller	Time Above 8% of Capacity ▾	Capacity Combined (b/s)	Usage While > Threshold (Combined)	Overall Usage (Combined)	Usage While > Thresho
1350	802.11an	corp	Top > cor'p	ethersphere-1322	8 hrs 45 mins (36.46%)	5000000	50.73%	18.98%	6.50%
1153	802.11an	corp	Top > cor'p	ethersphere-1322	8 hrs 40 mins (36.11%)	5000000	37.19%	14.14%	15.41%
1249	802.11an	corp	Top > cor'p	ethersphere-1322	7 hrs 45 mins (32.29%)	5000000	47.23%	15.75%	13.96%
AL27	802.11an	corp	Top > cor'p	ethersphere-lms3	7 hrs 35 mins (31.60%)	5000000	16.04%	5.70%	3.23%
175C	802.11an	corp	Top > cor'p	ethersphere-lms3	6 hrs 40 mins (27.78%)	5000000	16.42%	5.57%	4.77%

1-5 ▾ of 25 Interfaces Page 1 ▾ of 5 > >|

Interface Bandwidth

	Maximum	Average
🟩 Avg bps for Fa0/1 of sales-24poe.corp.airwave.com	21.58 Mbps	900.4 kbps
🟪 Avg bps for Enet0 of jtardio-ap65	43.63 Mbps	319.6 kbps
🟪 Avg bps for Enet0 of AP120	113.5 Mbps	4.219 Mbps
🟩 Avg bps for Enet0 of AP124	112.8 Mbps	3.236 Mbps
🟦 Avg bps for Radio 2 on AL15	1.044 Mbps	71.21 kbps
🟦 Avg bps for Radio 2 on AL27	2.631 Mbps	283.8 kbps
🟦 Avg bps for Radio 2 on AL33	688.1 kbps	16.34 kbps
🟦 Avg bps for Radio 2 on 140C	1.974 Mbps	67.09 kbps
🟦 Avg bps for Radio 2 on 182C	1.341 Mbps	70.61 kbps
🟦 Avg bps for Radio 2 on 52C	4.951 Mbps	121.9 kbps
🟦 Avg bps for Radio 2 on 130C	1.871 Mbps	206.3 kbps
🟦 Avg bps for Radio 2 on 92C	2.139 Mbps	279 kbps
🟦 Avg bps for Radio 2 on 12C	1.631 Mbps	129.6 kbps
🟦 Avg bps for Radio 2 on 175C	1.383 Mbps	277.8 kbps
🟦 Avg bps for Radio 2 on 1154-Q	3.792 Mbps	163.6 kbps
🟦 Avg bps for Radio 2 on 1249	7.234 Mbps	784.6 kbps
🟦 Avg bps for Radio 2 on 1242-H	1.225 Mbps	64.1 kbps
🟦 Avg bps for Radio 2 on 1263	4.828 Mbps	301.5 kbps
🟦 Avg bps for Radio 2 on 2198	520.4 kbps	14.77 kbps
🟦 Avg bps for Radio 2 on 1248	3.129 Mbps	76.43 kbps
🟦 Avg bps for Radio 2 on 1310	2.171 Mbps	227 kbps
🟦 Avg bps for Radio 2 on 1372	1.269 Mbps	54.42 kbps
🟦 Avg bps for Radio 2 on 1153	6.076 Mbps	704.5 kbps
🟦 Avg bps for Radio 2 on 2103	736.3 kbps	18.68 kbps
🟦 Avg bps for Radio 2 on 1350	12.25 Mbps	945.9 kbps

Interfaces Vs. Percent of Time Above Threshold

Table 128 ***Capacity Planning Report*** *Fields and Contents, Top Portion*

Field	Description
Device	Displays the device type or name.
Interface	Displays the type of 802.11 wireless service supported by the device.
Group	Displays the device group with which the device is associated.
Folder	Displays the folder with which the device is associated.
Controller	Displays the controller with which a device operates.
Time Above 1% of Capacity	Displays the time duration in which the device has functioned above 0% of capacity. A low percentage of use in this field may indicate that a device is under-used or poorly configured in relation to its capacity, or in relation to user needs.
Capacity Combined (b/s)	Displays the combined capacity in and out of the device, in bits-per-second.

Table 128 ***Capacity Planning Report** Fields and Contents, Top Portion (Continued)*

Field	Description
Usage While > Threshold (Combined)	Displays the time in which a device has functioned above defined threshold capacity, both in and out.
Overall Usage (Combined)	Displays the overall usage of the device, both combined in and out traffic.
Usage While > Threshold (in)	Displays device usage that exceeds the defined and incoming threshold capacity.
Overall Usage (In)	Displays overall device usage for incoming data.
Usage While > Threshold (Out)	Displays device usage for outgoing data that exceeds defined thresholds.
Overall Usage (Out)	Displays device usage for outgoing data.

Using the Configuration Audit Report

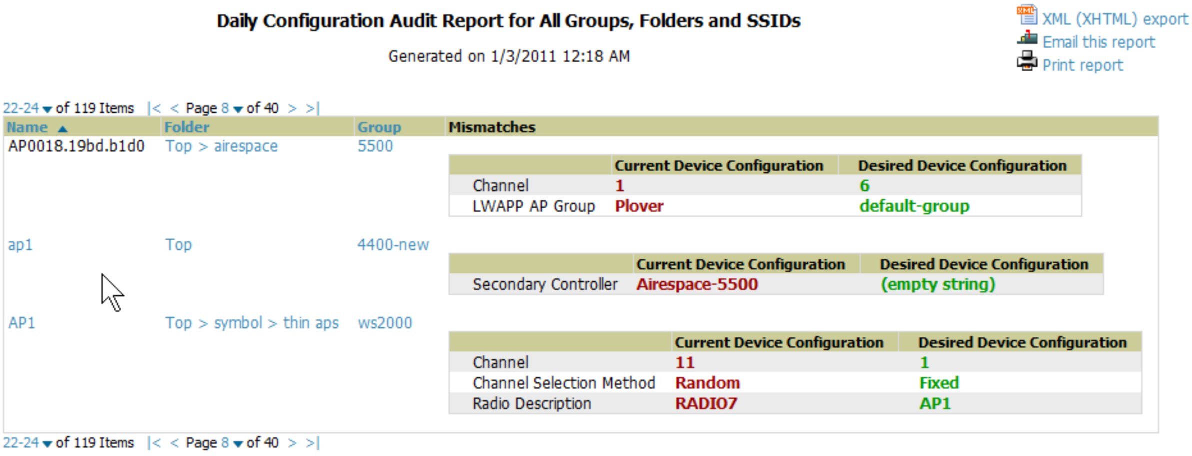
The **Configuration Audit Report** provides an inventory of device configurations on the network, enabling you to display information one device at a time, one folder at a time, or one device group at a time. This report links to additional configuration pages.

Perform these steps to view the most recent version of the report, then to configure a given device using this report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and select **Latest Configuration Audit Report** to display **Detail** device configuration information for all devices. The ensuing **Detail** report can be very large in size, and provides multiple links to additional device configuration or information display pages.
3. You can display device-specific configuration to reduce report size and to focus on a specific device. When viewing configured devices on the **Detail** page, select a device in the **Name** column. The device-specific configuration appears.
4. You can create or assign a template for a given device from the **Detail** page. Select **Add a Template** when viewing device-specific configuration information.
5. You can audit the current device configuration from the **Detail** page. Select **Audit** when viewing device-specific information.
6. You can display archived configuration about a given device from the **Detail** page. Select **Show Archived Device Configuration**.

Figure 161 and Table 129 illustrate and describe the general **Configuration Audit** report and related contents.

Figure 161 ***Reports > Generated > Daily Configuration Audit** Report Page, abbreviated example*



Daily Configuration Audit Report for All Groups, Folders and SSIDs

Generated on 1/3/2011 12:18 AM

Name ▲	Folder	Group	Mismatches	Current Device Configuration	Desired Device Configuration
AP0018.19bd.b1d0	Top > airespace	5500	Channel	1	6
			LWAPP AP Group	Plover	default-group
ap1	Top	4400-new	Secondary Controller	Airespace-5500	(empty string)
AP1	Top > symbol > thin aps	ws2000	Channel	11	1
			Channel Selection Method	Random	Fixed
			Radio Description	RADIO7	AP1

Table 129 *I Daily Configuration Audit Report*

Field	Description
Name	Displays the device name for every device on the network. Selecting a given device name in this column allows you to display device-specific configuration.
Folder	Displays the folder in which the device is configured in OV3600. Selecting the folder name in this report displays the **APs/Devices > List** page for additional device, folder and configuration options.
Group	Displays the group with which any given device associates. Selecting the group for a given device takes you to the **Groups > Monitor** page for that specific group, to display graphical group information, modification options, alerts, and an audit log for the related group.
Mismatches	This field displays configuration mismatch information. When a device configuration does not match ideal configuration, this field displays the ideal device settings compared to current settings.

Using the Device Summary Report

The **Device Summary Report** identifies devices that are the most or least used devices, and a comprehensive list of all devices. One potential use of this report is to establish more equal bandwidth distribution across multiple devices. This report contains the following five lists of devices.

- **Most Utilized by Maximum Number of Simultaneous Users**—By default, this list displays the 10 devices that support the highest numbers of users. This list provides links to additional information or configuration pages for each device to make adjustments, as desired.
- **Most Utilized by Bandwidth**—By default, this list displays the 10 devices that consistently have the highest bandwidth consumption during the time period defined for the report. This list provides links to additional information or configuration pages for each device.
- **Least Utilized by Maximum Number of Simultaneous Users**—By default, this list displays the 10 devices that are the least used, according to the number of users.
- **Least Utilized by Bandwidth**—By default, this list displays the 10 devices that are the least used, according to the bandwidth throughput.
- **Devices**—This list displays all devices in OV3600. By default it is sorted alphabetically by device name.

NOTE

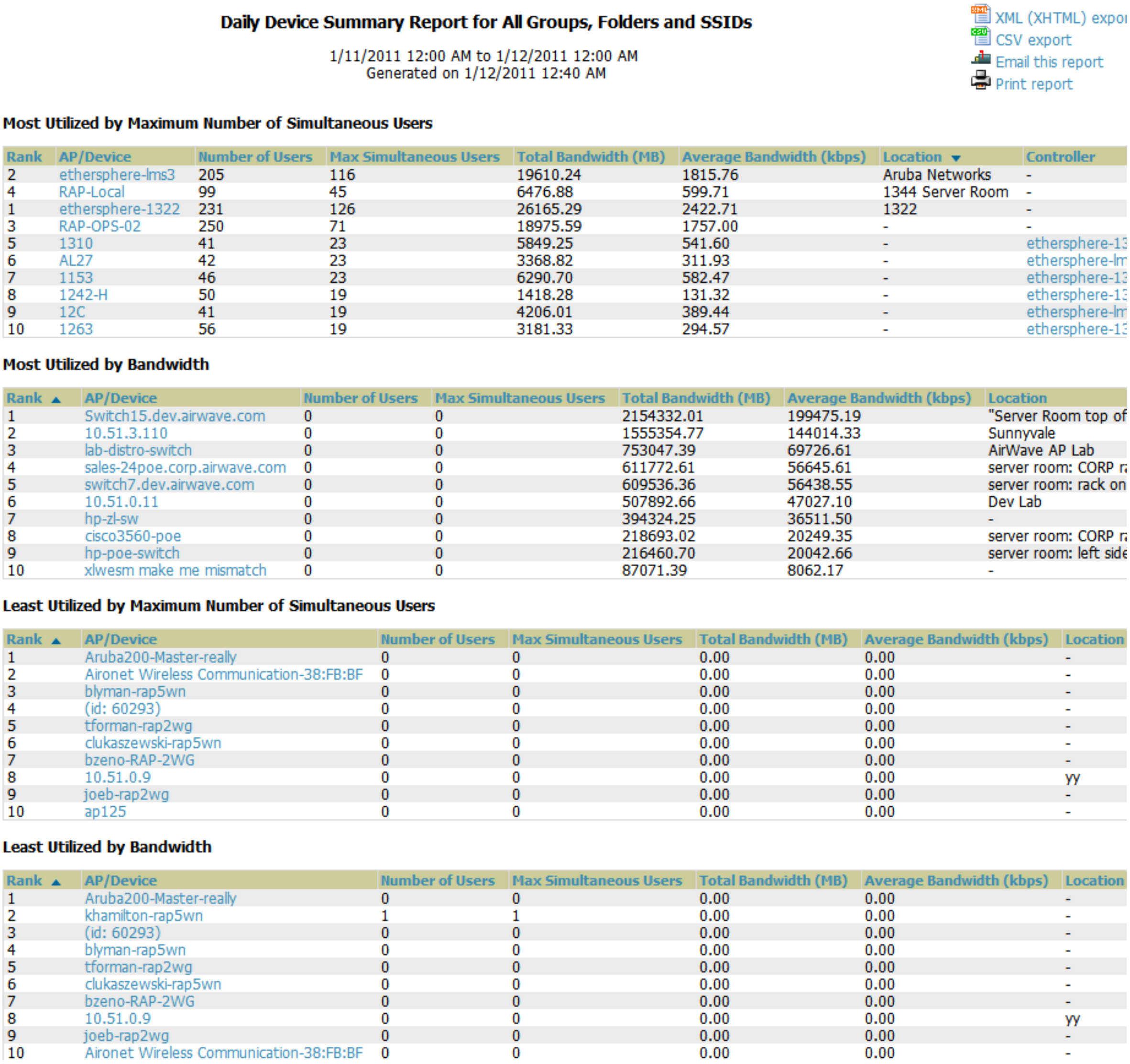
You can specify the number of devices that appear in each of the first four categories in the **Reports > Definitions > Add** page.

Any section of this report can be sorted by any of the columns. For example, you can specify a location and then sort the **Devices** list by the **Location** column to see details by location, or you can see all of the APs associated with a particular controller by sorting on the **Controller** column. If the AP name contains information about the location of the AP, you can sort by AP name.

If sorting the **Devices** list does not provide you with sufficient detail, you can specify a **Group** or **Folder** in the report **Definition** of a custom report. If you create a separate Group or Folder for each set of master and local controllers, you can generate a separate report for each Group or Folder. With this method, the summary sections of each report contain only devices from that Group or Folder.

Figure 162 and Table 130 illustrate and describe the **Reports > Generated > Device Summary Detail** page.

Figure 162 ***Reports > Generated > Daily Device Summary*** *Report Illustration (partial view)*



Daily Device Summary Report for All Groups, Folders and SSIDs

1/11/2011 12:00 AM to 1/12/2011 12:00 AM
Generated on 1/12/2011 12:40 AM

Most Utilized by Maximum Number of Simultaneous Users

Rank	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location ▼	Controller
2	ethersphere-lms3	205	116	19610.24	1815.76	Aruba Networks	-
4	RAP-Local	99	45	6476.88	599.71	1344 Server Room	-
1	ethersphere-1322	231	126	26165.29	2422.71	1322	-
3	RAP-OPS-02	250	71	18975.59	1757.00	-	-
5	1310	41	23	5849.25	541.60	-	ethersphere-13
6	AL27	42	23	3368.82	311.93	-	ethersphere-lm
7	1153	46	23	6290.70	582.47	-	ethersphere-13
8	1242-H	50	19	1418.28	131.32	-	ethersphere-13
9	12C	41	19	4206.01	389.44	-	ethersphere-lm
10	1263	56	19	3181.33	294.57	-	ethersphere-13

Most Utilized by Bandwidth

Rank ▲	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location
1	Switch15.dev.airwave.com	0	0	2154332.01	199475.19	"Server Room top of
2	10.51.3.110	0	0	1555354.77	144014.33	Sunnyvale
3	lab-distro-switch	0	0	753047.39	69726.61	AirWave AP Lab
4	sales-24poe.corp.airwave.com	0	0	611772.61	56645.61	server room: CORP r
5	switch7.dev.airwave.com	0	0	609536.36	56438.55	server room: rack on
6	10.51.0.11	0	0	507892.66	47027.10	Dev Lab
7	hp-zl-sw	0	0	394324.25	36511.50	-
8	cisco3560-poe	0	0	218693.02	20249.35	server room: CORP r
9	hp-poe-switch	0	0	216460.70	20042.66	server room: left side
10	xlwesm make me mismatch	0	0	87071.39	8062.17	-

Least Utilized by Maximum Number of Simultaneous Users

Rank ▲	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location
1	Aruba200-Master-really	0	0	0.00	0.00	-
2	Aironet Wireless Communication-38:FB:BF	0	0	0.00	0.00	-
3	blyman-rap5wn	0	0	0.00	0.00	-
4	(id: 60293)	0	0	0.00	0.00	-
5	tforman-rap2wg	0	0	0.00	0.00	-
6	clukaszewski-rap5wn	0	0	0.00	0.00	-
7	bzeno-RAP-2WG	0	0	0.00	0.00	-
8	10.51.0.9	0	0	0.00	0.00	yy
9	joeb-rap2wg	0	0	0.00	0.00	-
10	ap125	0	0	0.00	0.00	-

Least Utilized by Bandwidth

Rank ▲	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location
1	Aruba200-Master-really	0	0	0.00	0.00	-
2	khamilton-rap5wn	1	1	0.00	0.00	-
3	(id: 60293)	0	0	0.00	0.00	-
4	blyman-rap5wn	0	0	0.00	0.00	-
5	tforman-rap2wg	0	0	0.00	0.00	-
6	clukaszewski-rap5wn	0	0	0.00	0.00	-
7	bzeno-RAP-2WG	0	0	0.00	0.00	-
8	10.51.0.9	0	0	0.00	0.00	yy
9	joeb-rap2wg	0	0	0.00	0.00	-
10	Aironet Wireless Communication-38:FB:BF	0	0	0.00	0.00	-

Table 130 ***Reports > Generated > Daily Device Summary Report*** *Unique Fields and Descriptions*

Field	Description
Max Simultaneous Users	Displays the maximum number of users that were active on the associated device during the period of time that the report covers.
Total Bandwidth (MB)	Displays the bandwidth in megabytes that the device supported during the period of time covered by the report.
Average Bandwidth (kbps)	Displays the average bandwidth throughput for the device during the period of time covered by the report.

Using the Device Uptime Report

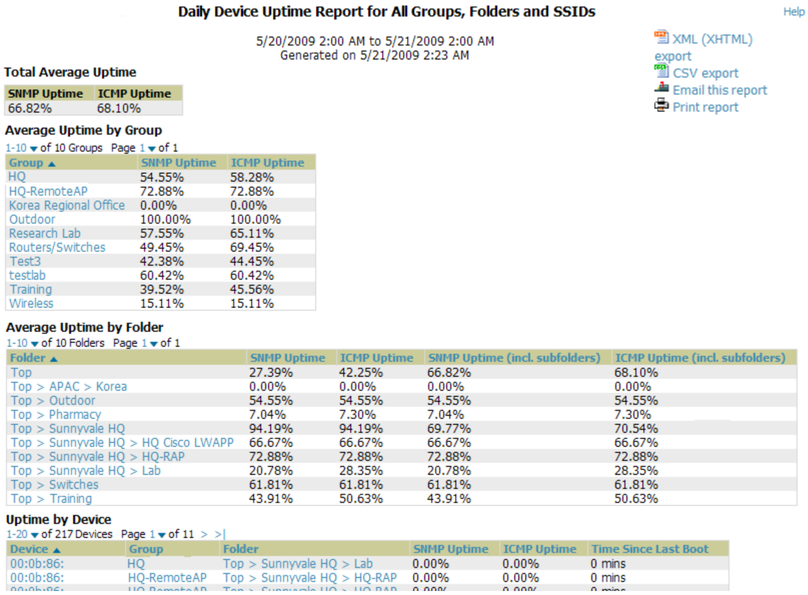
The **Device Uptime Report** monitors device performance and availability on the network, tracking uptime by multiple criteria to include the following:

- Total average uptime by SNMP and ICMP
- Average uptime by device group
- Average uptime by device folder

You can use this report as the central starting point to improve uptime by multiple criteria. This report covers protocol-oriented, device-oriented, or SSID-oriented information. This report can help to monitor and optimize the network in multiple ways. This report can demonstrate service parameters, can establish locations that have superior or problematic uptime availability, and can help with additional analysis in multiple ways. Locations, device groups, or other groupings within a network can be identified as needing attention or can be proven to have superior performance when using this report.

Figure 163 and Table 130 illustrate and describe the **Reports > Generated > Device Uptime Detail** report.

Figure 163 ***Device Uptime Report** Illustration*



Daily Device Uptime Report for All Groups, Folders and SSIDs

5/20/2009 2:00 AM to 5/21/2009 2:00 AM
Generated on 5/21/2009 2:23 AM

Total Average Uptime

SNMP Uptime	ICMP Uptime
66.82%	68.10%

Average Uptime by Group

1-10 ▾ of 10 Groups Page 1 ▾ of 1

Group ▲	SNMP Uptime	ICMP Uptime
HQ	54.55%	58.28%
HQ-RemoteAP	72.88%	72.88%
Korea Regional Office	0.00%	0.00%
Outdoor	100.00%	100.00%
Research Lab	57.55%	65.11%
Routers/Switches	49.45%	69.45%
Test3	42.38%	44.45%
testlab	60.42%	60.42%
Training	39.52%	45.56%
Wireless	15.11%	15.11%

Average Uptime by Folder

1-10 ▾ of 10 Folders Page 1 ▾ of 1

Folder ▲	SNMP Uptime	ICMP Uptime	SNMP Uptime (incl. subfolders)	ICMP Uptime (incl. subfolders)
Top	27.39%	42.25%	66.82%	68.10%
Top > APAC > Korea	0.00%	0.00%	0.00%	0.00%
Top > Outdoor	54.55%	54.55%	54.55%	54.55%
Top > Pharmacy	7.04%	7.30%	7.04%	7.30%
Top > Sunnyvale HQ	94.19%	94.19%	69.77%	70.54%
Top > Sunnyvale HQ > HQ Cisco LWAPP	66.67%	66.67%	66.67%	66.67%
Top > Sunnyvale HQ > HQ-RAP	72.88%	72.88%	72.88%	72.88%
Top > Sunnyvale HQ > Lab	20.78%	28.35%	20.78%	28.35%
Top > Switches	61.81%	61.81%	61.81%	61.81%
Top > Training	43.91%	50.63%	43.91%	50.63%

Uptime by Device

1-20 ▾ of 217 Devices Page 1 ▾ of 11 > >|

Device ▲	Group	Folder	SNMP Uptime	ICMP Uptime	Time Since Last Boot
00:0b:86:	HQ	Top > Sunnyvale HQ > Lab	0.00%	0.00%	0 mins
00:0b:86:	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	0.00%	0.00%	0 mins
00:0b:86:	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	0.00%	0.00%	0 mins

Table 131 ***Reports > Generated > Device Uptime Report** Unique Fields and Descriptions*

Field	Description
SNMP Uptime	Displays the percentage of time the device was reachable via ICMP. OV3600 polls the device via SNMP at the rate specified on the **Groups > Basic** page.
ICMP Uptime	Displays the percentage of time the device was reachable via ICMP. If the device is reachable via SNMP it is assumed to be reachable via ICMP. OV3600 only pings the device if SNMP fails and then it pings at the SNMP polling interval rate.
Time Since Last Boot	The uptime as reported by the device at the end of the time period covered by the report.

Using the IDS Events Report

The **IDS Events Report** lists and tracks IDS events on the network involving APs or controller devices. This report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours, and provides links to support additional analysis or configuration in response.

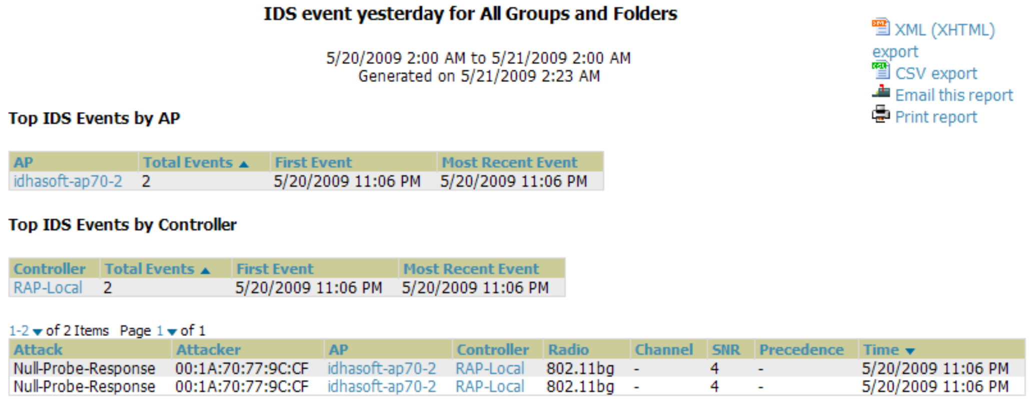
Your OV3600 must have a RAPIDS license, and your role must be enabled to view RAPIDS, to see this report.

The **Home > License** page also cites IDS events, and triggers can be configured for IDS events. Refer to "Setting Triggers for IDS Events" on page 184 for additional information.

Selecting the AP device or controller name takes you to the **APs/Devices > List** page.

Figure 164 and Table 132 illustrate and describe the **Reports > Generated > IDS Events Detail** page.

Figure 164 *Reports > Generated > IDS Events Report Illustration*



IDS event yesterday for All Groups and Folders

5/20/2009 2:00 AM to 5/21/2009 2:00 AM
Generated on 5/21/2009 2:23 AM

Top IDS Events by AP

AP	Total Events ▲	First Event	Most Recent Event
idhasoft-ap70-2	2	5/20/2009 11:06 PM	5/20/2009 11:06 PM

Top IDS Events by Controller

Controller	Total Events ▲	First Event	Most Recent Event
RAP-Local	2	5/20/2009 11:06 PM	5/20/2009 11:06 PM

1-2 ▾ of 2 Items Page 1 ▾ of 1

Attack	Attacker	AP	Controller	Radio	Channel	SNR	Precedence	Time ▾
Null-Probe-Response	00:1A:70:77:9C:CF	idhasoft-ap70-2	RAP-Local	802.11bg	-	4	-	5/20/2009 11:06 PM
Null-Probe-Response	00:1A:70:77:9C:CF	idhasoft-ap70-2	RAP-Local	802.11bg	-	4	-	5/20/2009 11:06 PM

Table 132 *Reports > Generated > IDS Events Detail Unique Fields and Descriptions*

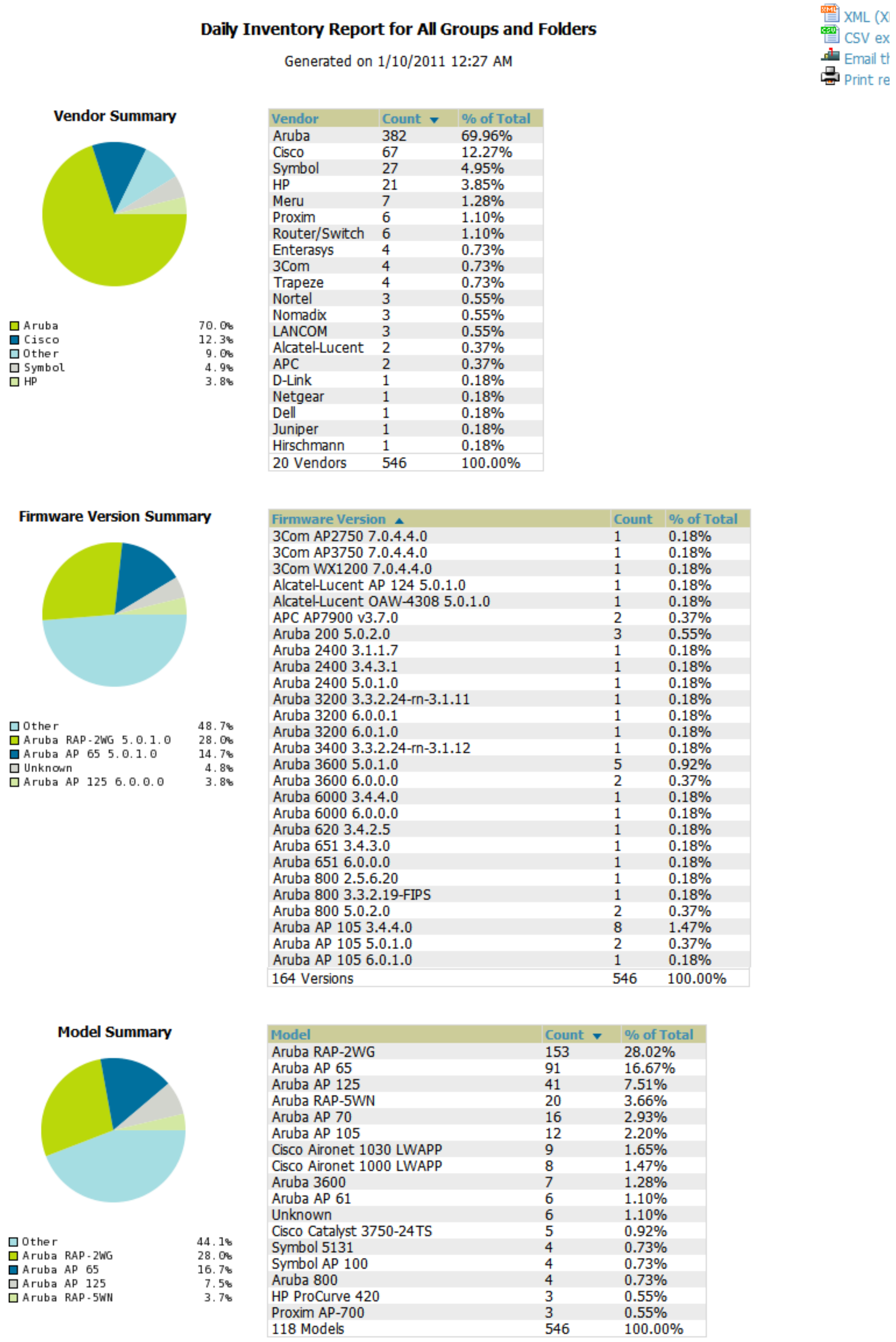
Field	Description
Attack	Displays the name or label for the IDS event.
Controllers	This column lists the controllers for which IDS events have occurred in the prior 24 hours, and provides a link to the **APs/Devices > Monitor** page for each.
Attacker	Displays the MAC address of the device that generated the IDS event.
Radio	Displays the 802.11 radio type associated with the IDS event.
Channel	Displays the 802.11 radio channel associated with the IDS event, when known.
SNR	Displays the signal-to-noise (SNR) radio associated with the IDS event.
Precedence	Displays precedence information associated with the IDS event, when known.
Time	Displays the time of the IDS event.

Using the Inventory Report

The **Inventory Report** itemizes all devices and firmware versions on the network, to include vendor information and graphical pie-chart summaries. The primary sections of this report are as follows:

- Vendor Summary—Lists the vendors for all devices or firmware on the network.
- Firmware Version Summary—Lists the firmware version for all firmware used on the network.
- Model Summary—Lists the model numbers for all devices or firmware on the network.

Figure 165 ***Reports* > *Generated* > *Inventory*** *Report Illustration (Edited View)*



XML (X
CSV ex
Email tl
Print re

Daily Inventory Report for All Groups and Folders

Generated on 1/10/2011 12:27 AM

Vendor Summary

🟩 Aruba	70.0%
🟦 Cisco	12.3%
□ Other	9.0%
□ Symbol	4.9%
□ HP	3.8%

Vendor	Count ▼	% of Total
Aruba	382	69.96%
Cisco	67	12.27%
Symbol	27	4.95%
HP	21	3.85%
Meru	7	1.28%
Proxim	6	1.10%
Router/Switch	6	1.10%
Enterasys	4	0.73%
3Com	4	0.73%
Trapeze	4	0.73%
Nortel	3	0.55%
Nomadix	3	0.55%
LANCOM	3	0.55%
Alcatel-Lucent	2	0.37%
APC	2	0.37%
D-Link	1	0.18%
Netgear	1	0.18%
Dell	1	0.18%
Juniper	1	0.18%
Hirschmann	1	0.18%
20 Vendors	546	100.00%

Firmware Version Summary

□ Other	48.7%
🟩 Aruba RAP-2WG 5.0.1.0	28.0%
🟦 Aruba AP 65 5.0.1.0	14.7%
□ Unknown	4.8%
□ Aruba AP 125 6.0.0.0	3.8%

Firmware Version ▲	Count	% of Total
3Com AP2750 7.0.4.4.0	1	0.18%
3Com AP3750 7.0.4.4.0	1	0.18%
3Com WX1200 7.0.4.4.0	1	0.18%
Alcatel-Lucent AP 124 5.0.1.0	1	0.18%
Alcatel-Lucent OAW-4308 5.0.1.0	1	0.18%
APC AP7900 v3.7.0	2	0.37%
Aruba 200 5.0.2.0	3	0.55%
Aruba 2400 3.1.1.7	1	0.18%
Aruba 2400 3.4.3.1	1	0.18%
Aruba 2400 5.0.1.0	1	0.18%
Aruba 3200 3.3.2.24-rn-3.1.11	1	0.18%
Aruba 3200 6.0.0.1	1	0.18%
Aruba 3200 6.0.1.0	1	0.18%
Aruba 3400 3.3.2.24-rn-3.1.12	1	0.18%
Aruba 3600 5.0.1.0	5	0.92%
Aruba 3600 6.0.0.0	2	0.37%
Aruba 6000 3.4.4.0	1	0.18%
Aruba 6000 6.0.0.0	1	0.18%
Aruba 620 3.4.2.5	1	0.18%
Aruba 651 3.4.3.0	1	0.18%
Aruba 651 6.0.0.0	1	0.18%
Aruba 800 2.5.6.20	1	0.18%
Aruba 800 3.3.2.19-FIPS	1	0.18%
Aruba 800 5.0.2.0	2	0.37%
Aruba AP 105 3.4.4.0	8	1.47%
Aruba AP 105 5.0.1.0	2	0.37%
Aruba AP 105 6.0.1.0	1	0.18%
164 Versions	546	100.00%

Model Summary

□ Other	44.1%
🟩 Aruba RAP-2WG	28.0%
🟦 Aruba AP 65	16.7%
□ Aruba AP 125	7.5%
□ Aruba RAP-5WN	3.7%

Model	Count ▼	% of Total
Aruba RAP-2WG	153	28.02%
Aruba AP 65	91	16.67%
Aruba AP 125	41	7.51%
Aruba RAP-5WN	20	3.66%
Aruba AP 70	16	2.93%
Aruba AP 105	12	2.20%
Cisco Aironet 1030 LWAPP	9	1.65%
Cisco Aironet 1000 LWAPP	8	1.47%
Aruba 3600	7	1.28%
Aruba AP 61	6	1.10%
Unknown	6	1.10%
Cisco Catalyst 3750-24TS	5	0.92%
Symbol 5131	4	0.73%
Symbol AP 100	4	0.73%
Aruba 800	4	0.73%
HP ProCurve 420	3	0.55%
Proxim AP-700	3	0.55%
118 Models	546	100.00%

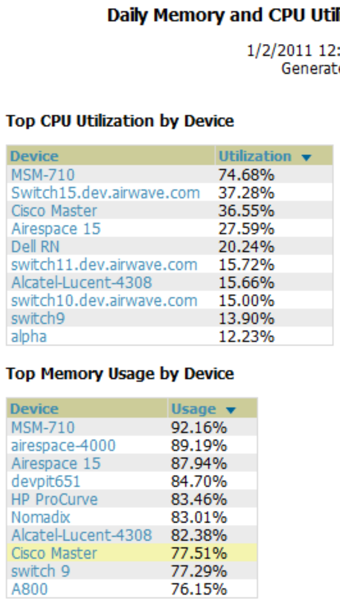
Using the Memory and CPU Utilization Report

The **Memory and CPU Utilization Report** displays the top memory usage by device, and CPU usage on the network by device. Both are by percentage.

To create a scheduled and generated report of this type, refer to “Using Daily Reports” on page 222.

Figure 166 illustrates the **Reports > Detail** page for this report.

Figure 166 ***Reports > Generated > Daily Memory and CPU Usage** Report Illustration (Rearranged for Space)*



Daily Memory and CPU Utilization Report for All Groups and Folders

1/2/2011 12:00 AM to 1/3/2011 12:00 AM
Generated on 1/3/2011 12:21 AM

Top CPU Utilization by Device

Device	Utilization ▼
MSM-710	74.68%
Switch15.dev.airwave.com	37.28%
Cisco Master	36.55%
Airespace 15	27.59%
Dell RN	20.24%
switch11.dev.airwave.com	15.72%
Alcatel-Lucent-4308	15.66%
switch10.dev.airwave.com	15.00%
switch9	13.90%
alpha	12.23%

Top Memory Usage by Device

Device	Usage ▼
MSM-710	92.16%
airespace-4000	89.19%
Airespace 15	87.94%
devpit651	84.70%
HP ProCurve	83.46%
Nomadix	83.01%
Alcatel-Lucent-4308	82.38%
Cisco Master	77.51%
switch 9	77.29%
A800	76.15%

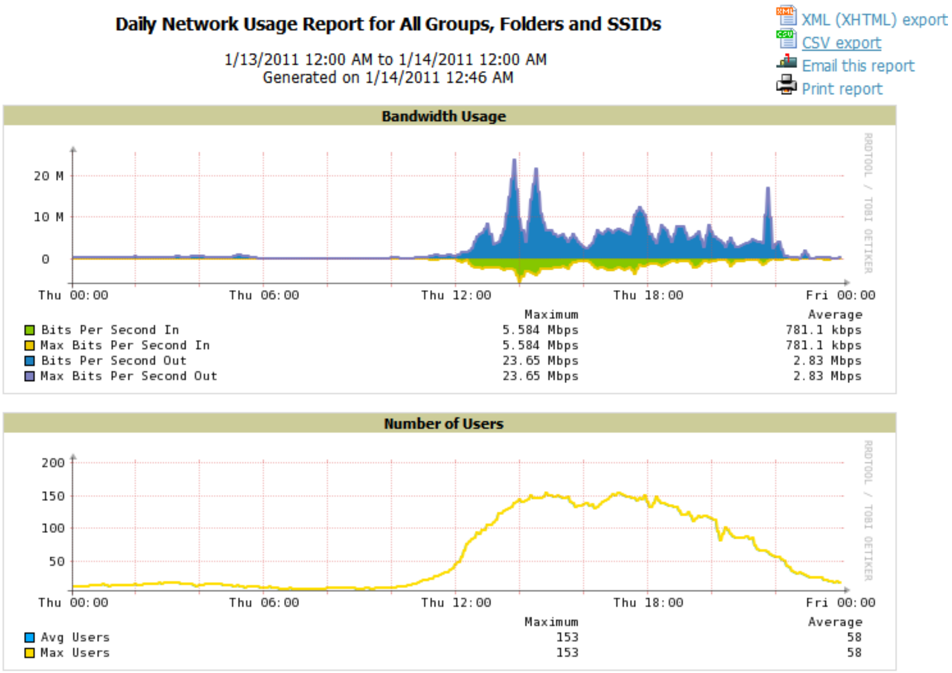
Using the Network Usage Report

The **Network Usage Report** contains network-wide information in two categories:

- **Bandwidth usage by device**—maximum and average bandwidth in kbps
- **Number of users by time period**—average bandwidth in and out

Figure 167 illustrates the **Reports > Detail** page for the Daily Network Usage.

Figure 167 ***Reports > Generated > Network Usage** Report Illustration*



Daily Network Usage Report for All Groups, Folders and SSIDs

1/13/2011 12:00 AM to 1/14/2011 12:00 AM
Generated on 1/14/2011 12:46 AM

```
                                 Maximum        Average
🟩 Bits Per Second In            5.584 Mbps     781.1 kbps
🟨 Max Bits Per Second In        5.584 Mbps     781.1 kbps
🟦 Bits Per Second Out           23.65 Mbps     2.83 Mbps
🟪 Max Bits Per Second Out       23.65 Mbps     2.83 Mbps
```

```
                   Maximum   Average
🟦 Avg Users       153       58
🟨 Max Users       153       58
```

Using the New Rogue Devices Report

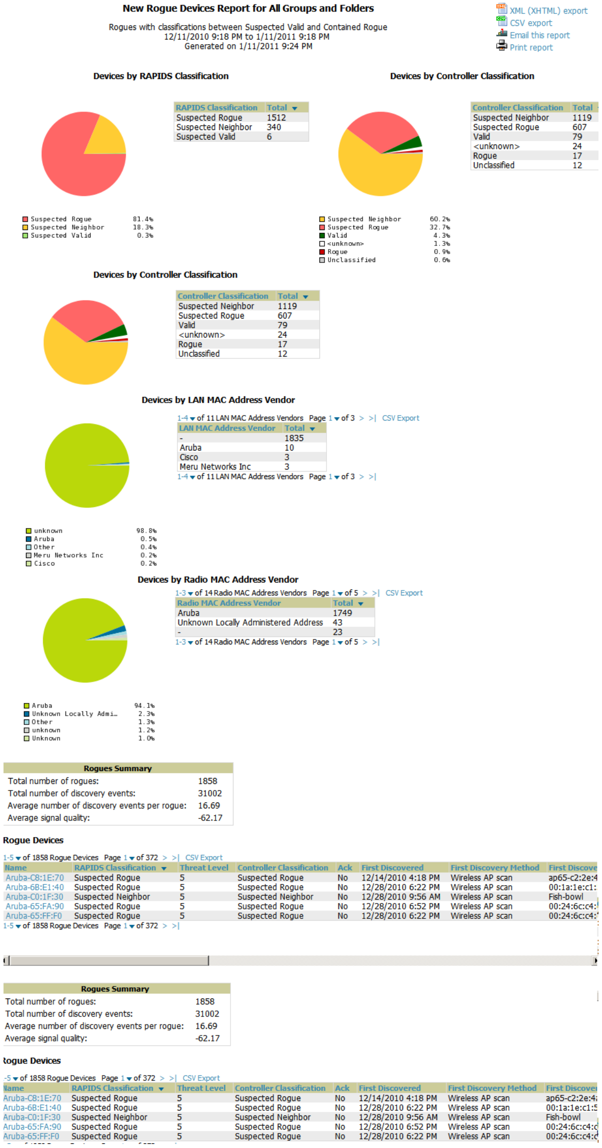
The **New Rogue Devices Report** summarizes rogue device information including the following categories of information:

- Rogue devices by RAPIDS classification—described in "Using RAPIDS and Rogue Classification" on page 163
- Top rogue devices by number of discovering APs
- Top rogue devices by signal strength
- Graphical summary of rogue devices by LAN MAC address vendor
- Graphical summary of rogue devices by radio MAC address vendor
- Text-based table summary of rogue device counts
- Detailed and text-based table of rogue devices discovered only wirelessly with extensive device parameters and hyperlink interoperability to additional OV3600 pages
- Detailed and text-based table of all rogue devices supporting all discovery methods with extensive device parameters and hyperlink interoperability to additional OV3600 pages
- Detailed and text-based table of discovery events pertaining to the discovery of rogue devices with extensive parameters and hyperlink interoperability to additional OV3600 pages

This report is not run by default, but is available after you define it.

Refer to Figure 168 for a sample illustration of this report.

Figure 168 ***Reports > Generated > New Rogue Devices*** *Report Illustration*



New Rogue Devices Report for All Groups and Folders

Rogues with classifications between Suspected Valid and Contained Rogue
12/11/2010 9:18 PM to 1/11/2011 9:18 PM
Generated on 1/11/2011 9:24 PM

Devices by RAPIDS Classification

RAPIDS Classification	Total ▼
Suspected Rogue	1512
Suspected Neighbor	340
Suspected Valid	6

🟥 Suspected Rogue	81.4%
🟨 Suspected Neighbor	18.3%
🟩 Suspected Valid	0.3%

Devices by Controller Classification

Controller Classification	Total
Suspected Neighbor	1119
Suspected Rogue	607
Valid	79
<unknown>	24
Rogue	17
Unclassified	12

🟨 Suspected Neighbor	60.2%
🟥 Suspected Rogue	32.7%
🟩 Valid	4.3%
□ <unknown>	1.3%
🟥 Rogue	0.9%
□ Unclassified	0.6%

Devices by Controller Classification

Controller Classification	Total ▼
Suspected Neighbor	1119
Suspected Rogue	607
Valid	79
<unknown>	24
Rogue	17
Unclassified	12

Devices by LAN MAC Address Vendor

1-4 ▼ of 11 LAN MAC Address Vendors Page 1 ▼ of 3 > >| CSV Export

LAN MAC Address Vendor	Total ▼
-	1835
Aruba	10
Cisco	3
Meru Networks Inc	3

1-4 ▼ of 11 LAN MAC Address Vendors Page 1 ▼ of 3 > >|

🟩 unknown	98.8%
🟦 Aruba	0.5%
□ Other	0.4%
□ Meru Networks Inc	0.2%
□ Cisco	0.2%

Devices by Radio MAC Address Vendor

1-3 ▼ of 14 Radio MAC Address Vendors Page 1 ▼ of 5 > >| CSV Export

Radio MAC Address Vendor	Total ▼
Aruba	1749
Unknown Locally Administered Address	43
-	23

1-3 ▼ of 14 Radio MAC Address Vendors Page 1 ▼ of 5 > >|

🟩 Aruba	94.1%
🟦 Unknown Locally Admi…	2.3%
□ Other	1.3%
□ unknown	1.2%
□ Unknown	1.0%

Rogues Summary	
Total number of rogues:	1858
Total number of discovery events:	31002
Average number of discovery events per rogue:	16.69
Average signal quality:	-62.17

Rogue Devices

1-5 ▼ of 1858 Rogue Devices Page 1 ▼ of 372 > >| CSV Export

Name	RAPIDS Classification ▼	Threat Level	Controller Classification	Ack	First Discovered	First Discovery Method	First Discove
Aruba-C8:1E:70	Suspected Rogue	5	Suspected Rogue	No	12/14/2010 4:18 PM	Wireless AP scan	ap65-c2:2e:4
Aruba-6B:E1:40	Suspected Rogue	5	Suspected Rogue	No	12/28/2010 6:22 PM	Wireless AP scan	00:1a:1e:c1:
Aruba-C0:1F:30	Suspected Neighbor	5	Suspected Neighbor	No	12/28/2010 9:56 AM	Wireless AP scan	Fish-bowl
Aruba-65:FA:90	Suspected Rogue	5	Suspected Rogue	No	12/28/2010 6:52 PM	Wireless AP scan	00:24:6c:c4:
Aruba-65:FF:F0	Suspected Rogue	5	Suspected Rogue	No	12/28/2010 6:22 PM	Wireless AP scan	00:24:6c:c4:

1-5 ▼ of 1858 Rogue Devices Page 1 ▼ of 372 > >|

Rogues Summary	
Total number of rogues:	1858
Total number of discovery events:	31002
Average number of discovery events per rogue:	16.69
Average signal quality:	-62.17

ogue Devices

-5 ▼ of 1858 Rogue Devices Page 1 ▼ of 372 > >| CSV Export

Name	RAPIDS Classification ▼	Threat Level	Controller Classification	Ack	First Discovered	First Discovery Method	First Discover
Aruba-C8:1E:70	Suspected Rogue	5	Suspected Rogue	No	12/14/2010 4:18 PM	Wireless AP scan	ap65-c2:2e:4
Aruba-6B:E1:40	Suspected Rogue	5	Suspected Rogue	No	12/28/2010 6:22 PM	Wireless AP scan	00:1a:1e:c1:5
Aruba-C0:1F:30	Suspected Neighbor	5	Suspected Neighbor	No	12/28/2010 9:56 AM	Wireless AP scan	Fish-bowl
Aruba-65:FA:90	Suspected Rogue	5	Suspected Rogue	No	12/28/2010 6:52 PM	Wireless AP scan	00:24:6c:c4:c
Aruba-65:FF:F0	Suspected Rogue	5	Suspected Rogue	No	12/28/2010 6:22 PM	Wireless AP scan	00:24:6c:c4:c

The rogue device inventories that comprise this report contain many fields, described in Table 133.

Table 133 *New Rogue Devices Report* Fields

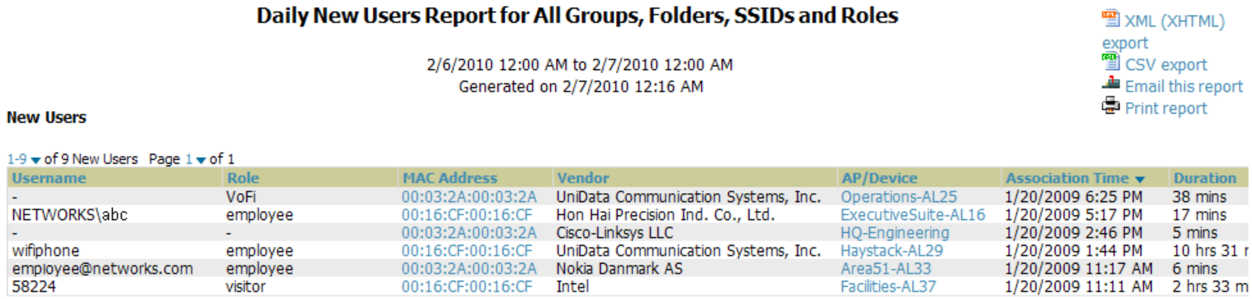
Field	Description
Name	Displays the device name, as able to be determined.
RAPIDS Classification	Displays the RAPIDS classification for the rogue device, as classified by rules defined on the **RAPIDS > Rules** page. Refer to "Using RAPIDS and Rogue Classification" on page 163 for additional information.
Threat Level	Displays the numeric threat level by which the device has been classified, according to rules defined on the **RAPIDS > Rules** page. Refer to "Using RAPIDS and Rogue Classification" on page 163 for additional information.
Ack	Displays whether the device has been acknowledged with the network.
First Discovered	Displays the date and time that the rogue device was first discovered on the network.
First Discovery Method	Displays the method by which the rogue device was discovered.
First Discovery Agent	Displays the network device that first discovered the rogue device.
Last Discovering AP	Displays the network device that most recently discovered the rogue device.
Model	Displays the rogue device type when known.
Operating System	Displays the operating system for the device type, when known.
IP Address	Displays the IP address of the rogue device when known.
SSID	Displays the SSID for the rogue device when known.
Network Type	Displays the network type on which the rogue was detected, when known.
Channel	Displays the wireless RF channel on which the rogue device was detected.
WEP	Displays WEP encryption usage when known.
RSSI	Displays Received Signal Strength (RSSI) information for radio signal strength when known.
Signal	Displays signal strength when known.
LAN MAC Address	Displays the MAC address for the associated LAN when known.
LAN Vendor	Displays LAN vendor information associated with the rogue device, when known.
Radio MAC Address	Displays the MAC address for the radio device, when known.
Radio Vendor	Displays the vendor information for the radio device when known.
Port	Displays the router or switch port associated with the rogue device when known.
Last Seen	Displays the last time in which the rogue device was seen on the network.
Total Discovering APs	Displays the total number of APs that detected the rogue device.
Total Discovery Events	Displays the total number of instances in which the rogue device was discovered.

Using the New Users Report

The **New Users Report** lists all new users that have appeared on the network during the time duration defined for the report. This report covers the user identifier, the associated role when known, device information and more. The report definition can filter on connection mode (wired, wireless or both).

Figure 169 illustrates the fields and information in the **New Users Report**.

Figure 169 ***Reports > Generated > New Users Repor**t Illustration*



Daily New Users Report for All Groups, Folders, SSIDs and Roles

2/6/2010 12:00 AM to 2/7/2010 12:00 AM
Generated on 2/7/2010 12:16 AM

New Users

1-9 ▾ of 9 New Users Page 1 ▾ of 1

Username	Role	MAC Address	Vendor	AP/Device	Association Time ▾	Duration
-	VoFi	00:03:2A:00:03:2A	UniData Communication Systems, Inc.	Operations-AL25	1/20/2009 6:25 PM	38 mins
NETWORKS\abc	employee	00:16:CF:00:16:CF	Hon Hai Precision Ind. Co., Ltd.	ExecutiveSuite-AL16	1/20/2009 5:17 PM	17 mins
-	-	00:03:2A:00:03:2A	Cisco-Linksys LLC	HQ-Engineering	1/20/2009 2:46 PM	5 mins
wifiphone	employee	00:16:CF:00:16:CF	UniData Communication Systems, Inc.	Haystack-AL29	1/20/2009 1:44 PM	10 hrs 31 r
employee@networks.com	employee	00:03:2A:00:03:2A	Nokia Danmark AS	Area51-AL33	1/20/2009 11:17 AM	6 mins
58224	visitor	00:16:CF:00:16:CF	Intel	Facilities-AL37	1/20/2009 11:11 AM	2 hrs 33 m

Using the PCI Compliance Report

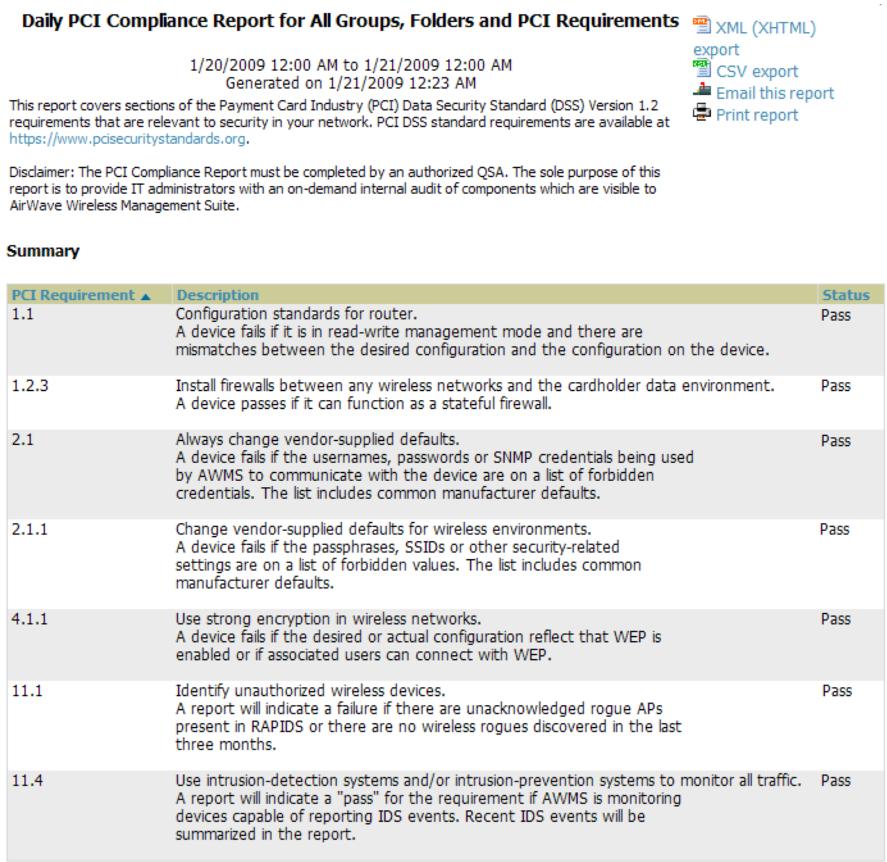
OV3600 supports PCI requirements in accordance with the Payment Card Industry (PCI) Data Security Standard (DSS). The **PCI Compliance Report** displays current PCI configurations and status as enabled on the network. Verify that OV3600 is enabled to monitor compliance with PCI requirements, as described in the "Enabling or Disabling PCI Auditing" on page 65.

In addition to citing simple pass or fail status with regard to each PCI requirement, OV3600 introduces very detailed diagnostic information to recommend the specific action or actions required to achieve Pass status, when sufficient information is available.

Refer to the "Auditing PCI Compliance on the Network" on page 63 for information about enabling PCI on the network. The configurations in that section enable or disable the contents of the PCI Compliance Report that is viewable on the **Reports > Generated** page.

Figure 170 illustrates the fields and information in the most recent **PCI Compliance Report**.

Figure 170 ***Reports > Generated > PCI Compliance Report** Illustration Example*



Daily PCI Compliance Report for All Groups, Folders and PCI Requirements

1/20/2009 12:00 AM to 1/21/2009 12:00 AM
Generated on 1/21/2009 12:23 AM

This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.2 requirements that are relevant to security in your network. PCI DSS standard requirements are available at https://www.pcisecuritystandards.org.

Disclaimer: The PCI Compliance Report must be completed by an authorized QSA. The sole purpose of this report is to provide IT administrators with an on-demand internal audit of components which are visible to AirWave Wireless Management Suite.

Summary

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

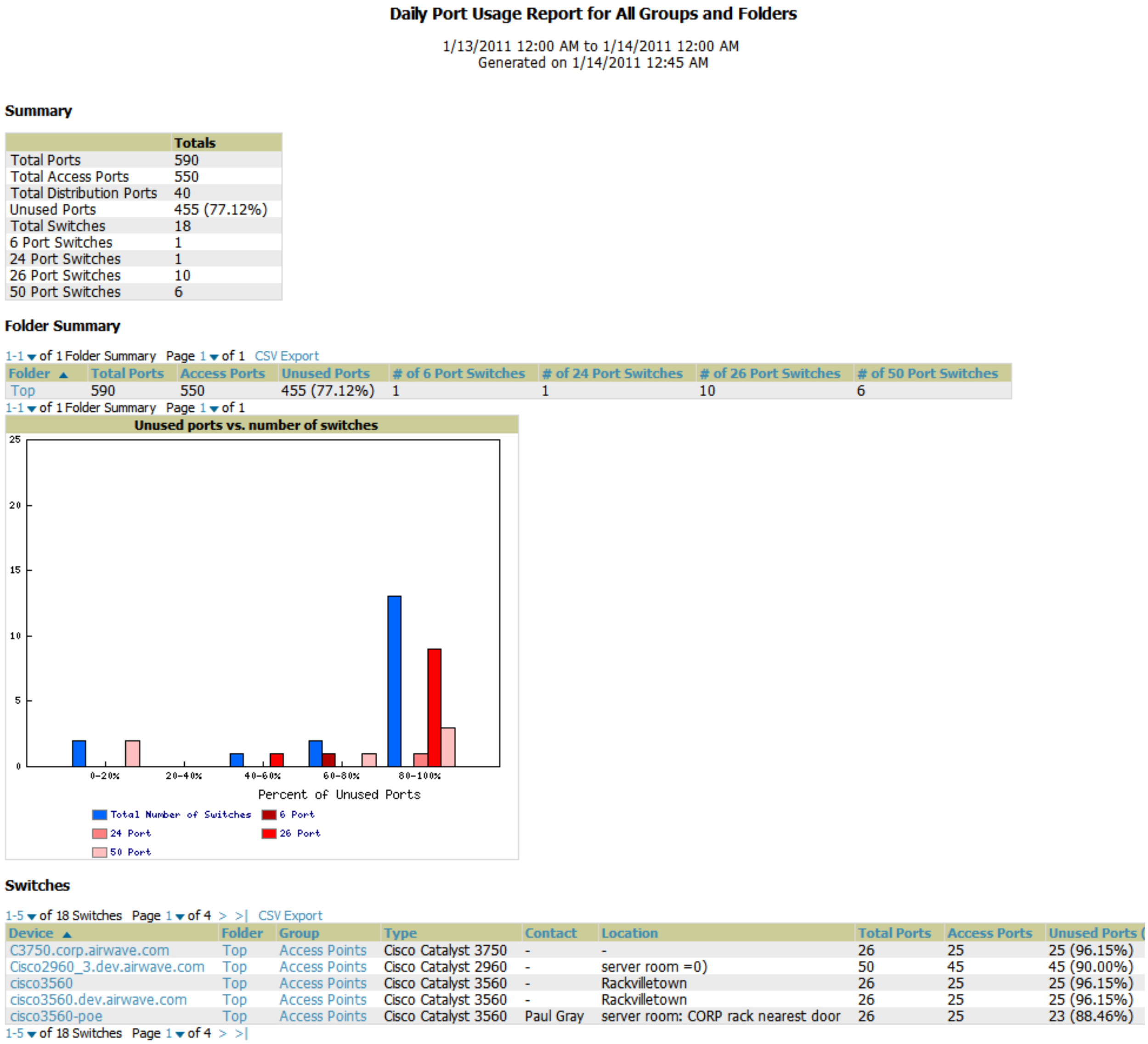
Using the Port Usage Report

You can generate a wide array of port usage statistics from the **Port Usage Report** including each of the following:

- List of all the switches and ports in your network by folder
- List of unused ports
- List of access and distribution ports
- Histogram displaying unused ports vs. unused switches by type (access or distribution)
- List of most used switches
- List of most used ports

A sample of the types of information you might choose to generate in a **Port Usage Report** appears in Figure 171.

Figure 171 ***Reports* > *Generated* > *Port Usage Report*** *Detail Page (partial view)*



Daily Port Usage Report for All Groups and Folders

1/13/2011 12:00 AM to 1/14/2011 12:00 AM
Generated on 1/14/2011 12:45 AM

Summary

	Totals
Total Ports	590
Total Access Ports	550
Total Distribution Ports	40
Unused Ports	455 (77.12%)
Total Switches	18
6 Port Switches	1
24 Port Switches	1
26 Port Switches	10
50 Port Switches	6

Folder Summary

1-1 ▾ of 1 Folder Summary Page 1 ▾ of 1 CSV Export

Folder ▲	Total Ports	Access Ports	Unused Ports	# of 6 Port Switches	# of 24 Port Switches	# of 26 Port Switches	# of 50 Port Switches
Top	590	550	455 (77.12%)	1	1	10	6

1-1 ▾ of 1 Folder Summary Page 1 ▾ of 1

Switches

1-5 ▾ of 18 Switches Page 1 ▾ of 4 > >| CSV Export

Device ▲	Folder	Group	Type	Contact	Location	Total Ports	Access Ports	Unused Ports (
C3750.corp.airwave.com	Top	Access Points	Cisco Catalyst 3750	-	-	26	25	25 (96.15%)
Cisco2960_3.dev.airwave.com	Top	Access Points	Cisco Catalyst 2960	-	server room =0)	50	45	45 (90.00%)
cisco3560	Top	Access Points	Cisco Catalyst 3560	-	Rackvilletown	26	25	25 (96.15%)
cisco3560.dev.airwave.com	Top	Access Points	Cisco Catalyst 3560	-	Rackvilletown	26	25	25 (96.15%)
cisco3560-poe	Top	Access Points	Cisco Catalyst 3560	Paul Gray	server room: CORP rack nearest door	26	25	23 (88.46%)

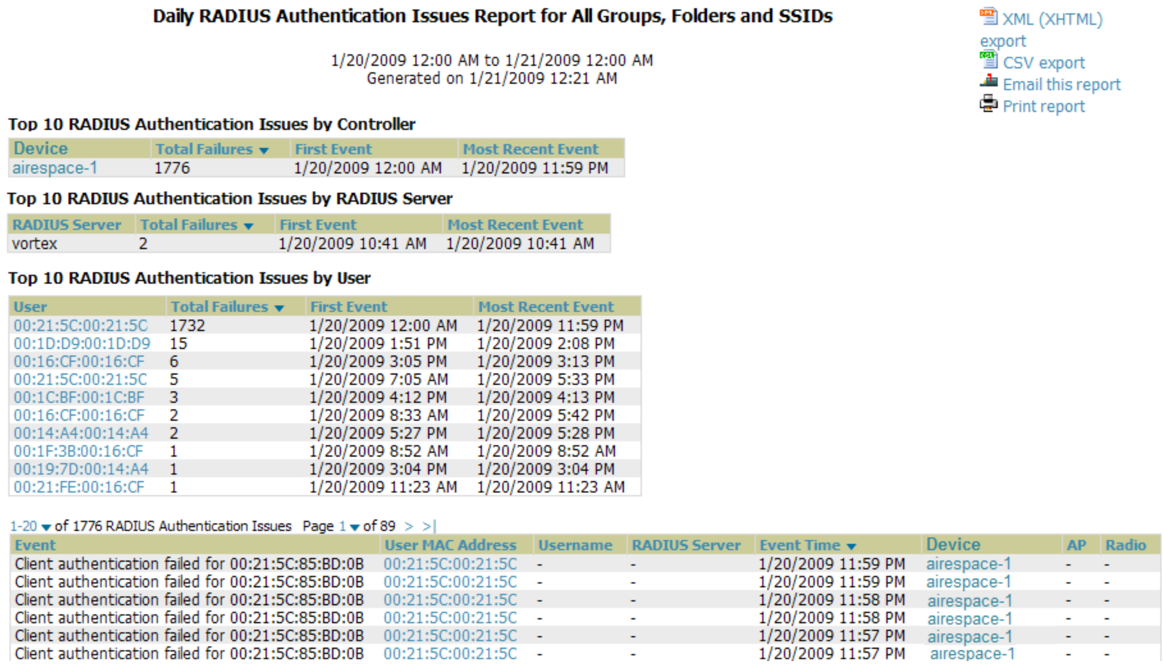
1-5 ▾ of 18 Switches Page 1 ▾ of 4 > >|

Using the RADIUS Authentication Issues Report

The **RADIUS Authentication Issues Report** contains issues that may appear with controllers, RADIUS servers, and users.

Figure 172 illustrates the fields and information in the **RADIUS Authentication Issues Report.**

Figure 172 ***Reports > Generated > RADIUS Authentication Issues*** *Detail Page Illustration*



Daily RADIUS Authentication Issues Report for All Groups, Folders and SSIDs

1/20/2009 12:00 AM to 1/21/2009 12:00 AM
Generated on 1/21/2009 12:21 AM

Top 10 RADIUS Authentication Issues by Controller

Device	Total Failures ▼	First Event	Most Recent Event
airespace-1	1776	1/20/2009 12:00 AM	1/20/2009 11:59 PM

Top 10 RADIUS Authentication Issues by RADIUS Server

RADIUS Server	Total Failures ▼	First Event	Most Recent Event
vortex	2	1/20/2009 10:41 AM	1/20/2009 10:41 AM

Top 10 RADIUS Authentication Issues by User

User	Total Failures ▼	First Event	Most Recent Event
00:21:5C:00:21:5C	1732	1/20/2009 12:00 AM	1/20/2009 11:59 PM
00:1D:D9:00:1D:D9	15	1/20/2009 1:51 PM	1/20/2009 2:08 PM
00:16:CF:00:16:CF	6	1/20/2009 3:05 PM	1/20/2009 3:13 PM
00:21:5C:00:21:5C	5	1/20/2009 7:05 AM	1/20/2009 5:33 PM
00:1C:BF:00:1C:BF	3	1/20/2009 4:12 PM	1/20/2009 4:13 PM
00:16:CF:00:16:CF	2	1/20/2009 8:33 AM	1/20/2009 5:42 PM
00:14:A4:00:14:A4	2	1/20/2009 5:27 PM	1/20/2009 5:28 PM
00:1F:3B:00:16:CF	1	1/20/2009 8:52 AM	1/20/2009 8:52 AM
00:19:7D:00:14:A4	1	1/20/2009 3:04 PM	1/20/2009 3:04 PM
00:21:FE:00:16:CF	1	1/20/2009 11:23 AM	1/20/2009 11:23 AM

1-20 ▼ of 1776 RADIUS Authentication Issues Page 1 ▼ of 89 > >|

Event	User MAC Address	Username	RADIUS Server	Event Time ▼	Device	AP	Radio
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:59 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:59 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:58 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:58 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:57 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:57 PM	airespace-1	-	-

Using the RF Health Report

The RF Health Report tracks the top AP radio issues by noise, MAC/Phy errors, channel changes, transmit power changes, mode changes, and interfering devices (the last two apply only if there are ARM events). This report assists in pinpointing the most problematic devices on your network, and lists the top 10 devices by problem type.

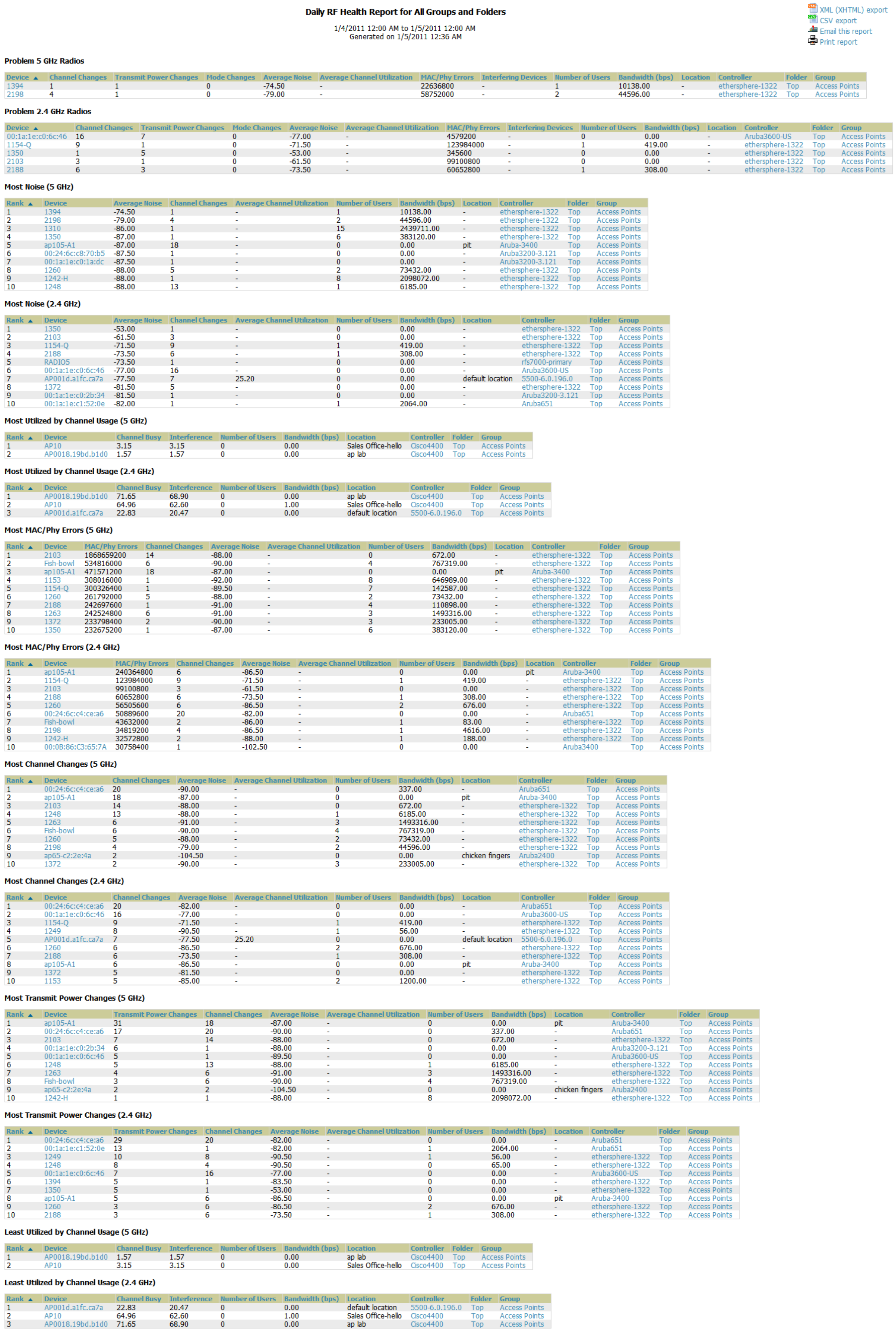
Problematic APs are displayed in two separate lists Problem Radios lists, grouped by radio frequency. A device will make it into the list if it violates two or more thresholds. (For more on the thresholds that indicate problems, refer to "Evaluating Radio Statistics for an AP" on page 123.)

Other lists grouped by radio frequency include Most Noise, Most/Least Utilized by Channel Usage, Most MAC/Phy Errors, Most Channel Changes, Most Transmit Power Changes.

If an RF Health Report has not been generated before, you can create it by following the instructions on the Defining Reports section of this chapter.

Figure 173 illustrates a sample RF Health Report.

Figure 173 *Reports > Detail > Daily RF Health Report*



Daily RF Health Report for All Groups and Folders

1/4/2011 12:00 AM to 1/5/2011 12:00 AM
Generated on 1/5/2011 12:36 AM

Problem 5 GHz Radios

Device ▲	Channel Changes	Transmit Power Changes	Mode Changes	Average Noise	Average Channel Utilization	MAC/Phy Errors	Interfering Devices	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1394	1	1	0	-74.50	-	22636800	-	1	10138.00	-	ethersphere-1322	Top	Access Points
2198	4	1	0	-79.00	-	58752000	-	2	44596.00	-	ethersphere-1322	Top	Access Points

Problem 2.4 GHz Radios

Device ▲	Channel Changes	Transmit Power Changes	Mode Changes	Average Noise	Average Channel Utilization	MAC/Phy Errors	Interfering Devices	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
00:1a:1e:c0:6c:46	16	7	0	-77.00	-	4579200	-	0	0.00	-	Aruba3600-US	Top	Access Points
1154-Q	9	1	0	-71.50	-	123984000	-	1	419.00	-	ethersphere-1322	Top	Access Points
1350	1	5	0	-53.00	-	345600	-	0	0.00	-	ethersphere-1322	Top	Access Points
2103	3	1	0	-61.50	-	99100800	-	0	0.00	-	ethersphere-1322	Top	Access Points
2188	6	3	0	-73.50	-	60652800	-	1	308.00	-	ethersphere-1322	Top	Access Points

Most Noise (5 GHz)

Rank ▲	Device	Average Noise	Channel Changes	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	1394	-74.50	1	-	1	10138.00	-	ethersphere-1322	Top	Access Points
2	2198	-79.00	4	-	2	44596.00	-	ethersphere-1322	Top	Access Points
3	1310	-86.00	1	-	15	2439711.00	-	ethersphere-1322	Top	Access Points
4	1350	-87.00	1	-	6	383120.00	-	ethersphere-1322	Top	Access Points
5	ap105-A1	-87.00	18	-	0	0.00	pit	Aruba-3400	Top	Access Points
6	00:24:6c:c8:70:b5	-87.50	1	-	0	0.00	-	Aruba3200-3.121	Top	Access Points
7	00:1a:1e:c0:1a:dc	-87.50	1	-	0	0.00	-	Aruba3200-3.121	Top	Access Points
8	1260	-88.00	5	-	2	73432.00	-	ethersphere-1322	Top	Access Points
9	1242-H	-88.00	1	-	8	2098072.00	-	ethersphere-1322	Top	Access Points
10	1248	-88.00	13	-	1	6185.00	-	ethersphere-1322	Top	Access Points

Most Noise (2.4 GHz)

Rank ▲	Device	Average Noise	Channel Changes	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	1350	-53.00	1	-	0	0.00	-	ethersphere-1322	Top	Access Points
2	2103	-61.50	3	-	0	0.00	-	ethersphere-1322	Top	Access Points
3	1154-Q	-71.50	9	-	1	419.00	-	ethersphere-1322	Top	Access Points
4	2188	-73.50	6	-	1	308.00	-	ethersphere-1322	Top	Access Points
5	RADIO5	-73.50	1	-	0	0.00	-	rfs7000-primary	Top	Access Points
6	00:1a:1e:c0:6c:46	-77.00	16	-	0	0.00	-	Aruba3600-US	Top	Access Points
7	AP001d.a1fc.ca7a	-77.50	7	25.20	0	0.00	default location	5500-6.0.196.0	Top	Access Points
8	1372	-81.50	5	-	0	0.00	-	ethersphere-1322	Top	Access Points
9	00:1a:1e:c0:2b:34	-81.50	1	-	0	0.00	-	Aruba3200-3.121	Top	Access Points
10	00:1a:1e:c1:52:0e	-82.00	1	-	1	2064.00	-	Aruba651	Top	Access Points

Most Utilized by Channel Usage (5 GHz)

Rank ▲	Device	Channel Busy	Interference	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	AP10	3.15	3.15	0	0.00	Sales Office-hello	Cisco4400	Top	Access Points
2	AP0018.19bd.b1d0	1.57	1.57	0	0.00	ap lab	Cisco4400	Top	Access Points

Most Utilized by Channel Usage (2.4 GHz)

Rank ▲	Device	Channel Busy	Interference	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	AP0018.19bd.b1d0	71.65	68.90	0	0.00	ap lab	Cisco4400	Top	Access Points
2	AP10	64.96	62.60	0	1.00	Sales Office-hello	Cisco4400	Top	Access Points
3	AP001d.a1fc.ca7a	22.83	20.47	0	0.00	default location	5500-6.0.196.0	Top	Access Points

Most MAC/Phy Errors (5 GHz)

Rank ▲	Device	MAC/Phy Errors	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	2103	1868659200	14	-88.00	-	0	672.00	-	ethersphere-1322	Top	Access Points
2	Fish-bowl	534816000	6	-90.00	-	4	767319.00	-	ethersphere-1322	Top	Access Points
3	ap105-A1	471571200	18	-87.00	-	0	0.00	pit	Aruba-3400	Top	Access Points
4	1153	308016000	1	-92.00	-	8	646989.00	-	ethersphere-1322	Top	Access Points
5	1154-Q	300326400	1	-89.50	-	7	142587.00	-	ethersphere-1322	Top	Access Points
6	1260	261792000	5	-88.00	-	2	73432.00	-	ethersphere-1322	Top	Access Points
7	2188	242697600	1	-91.00	-	4	110898.00	-	ethersphere-1322	Top	Access Points
8	1263	242524800	6	-91.00	-	3	1493316.00	-	ethersphere-1322	Top	Access Points
9	1372	233798400	2	-90.00	-	3	233005.00	-	ethersphere-1322	Top	Access Points
10	1350	232675200	1	-87.00	-	6	383120.00	-	ethersphere-1322	Top	Access Points

Most MAC/Phy Errors (2.4 GHz)

Rank ▲	Device	MAC/Phy Errors	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	ap105-A1	240364800	6	-86.50	-	0	0.00	pit	Aruba-3400	Top	Access Points
2	1154-Q	123984000	9	-71.50	-	1	419.00	-	ethersphere-1322	Top	Access Points
3	2103	99100800	3	-61.50	-	0	0.00	-	ethersphere-1322	Top	Access Points
4	2188	60652800	6	-73.50	-	1	308.00	-	ethersphere-1322	Top	Access Points
5	1260	56505600	6	-86.50	-	2	676.00	-	ethersphere-1322	Top	Access Points
6	00:24:6c:c4:ce:a6	50889600	20	-82.00	-	0	0.00	-	Aruba651	Top	Access Points
7	Fish-bowl	43632000	2	-86.00	-	1	83.00	-	ethersphere-1322	Top	Access Points
8	2198	34819200	4	-86.50	-	1	4616.00	-	ethersphere-1322	Top	Access Points
9	1242-H	32572800	2	-88.00	-	1	188.00	-	ethersphere-1322	Top	Access Points
10	00:0B:86:C3:65:7A	30758400	1	-102.50	-	0	0.00	-	Aruba3400	Top	Access Points

Most Channel Changes (5 GHz)

Rank ▲	Device	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	00:24:6c:c4:ce:a6	20	-90.00	-	0	337.00	-	Aruba651	Top	Access Points
2	ap105-A1	18	-87.00	-	0	0.00	pit	Aruba-3400	Top	Access Points
3	2103	14	-88.00	-	0	672.00	-	ethersphere-1322	Top	Access Points
4	1248	13	-88.00	-	1	6185.00	-	ethersphere-1322	Top	Access Points
5	1263	6	-91.00	-	3	1493316.00	-	ethersphere-1322	Top	Access Points
6	Fish-bowl	6	-90.00	-	4	767319.00	-	ethersphere-1322	Top	Access Points
7	1260	5	-88.00	-	2	73432.00	-	ethersphere-1322	Top	Access Points
8	2198	4	-79.00	-	2	44596.00	-	ethersphere-1322	Top	Access Points
9	ap65-c2:2e:4a	2	-104.50	-	0	0.00	chicken fingers	Aruba2400	Top	Access Points
10	1372	2	-90.00	-	3	233005.00	-	ethersphere-1322	Top	Access Points

Most Channel Changes (2.4 GHz)

Rank ▲	Device	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	00:24:6c:c4:ce:a6	20	-82.00	-	0	0.00	-	Aruba651	Top	Access Points
2	00:1a:1e:c0:6c:46	16	-77.00	-	0	0.00	-	Aruba3600-US	Top	Access Points
3	1154-Q	9	-71.50	-	1	419.00	-	ethersphere-1322	Top	Access Points
4	1249	8	-90.50	-	1	56.00	-	ethersphere-1322	Top	Access Points
5	AP001d.a1fc.ca7a	7	-77.50	25.20	0	0.00	default location	5500-6.0.196.0	Top	Access Points
6	1260	6	-86.50	-	2	676.00	-	ethersphere-1322	Top	Access Points
7	2188	6	-73.50	-	1	308.00	-	ethersphere-1322	Top	Access Points
8	ap105-A1	6	-86.50	-	0	0.00	pit	Aruba-3400	Top	Access Points
9	1372	5	-81.50	-	0	0.00	-	ethersphere-1322	Top	Access Points
10	1153	5	-85.00	-	2	1200.00	-	ethersphere-1322	Top	Access Points

Most Transmit Power Changes (5 GHz)

Rank ▲	Device	Transmit Power Changes	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	ap105-A1	31	18	-87.00	-	0	0.00	pit	Aruba-3400	Top	Access Points
2	00:24:6c:c4:ce:a6	17	20	-90.00	-	0	337.00	-	Aruba651	Top	Access Points
3	2103	7	14	-88.00	-	0	672.00	-	ethersphere-1322	Top	Access Points
4	00:1a:1e:c0:2b:34	6	1	-88.00	-	0	0.00	-	Aruba3200-3.121	Top	Access Points
5	00:1a:1e:c0:6c:46	5	1	-89.50	-	0	0.00	-	Aruba3600-US	Top	Access Points
6	1248	5	13	-88.00	-	1	6185.00	-	ethersphere-1322	Top	Access Points
7	1263	4	6	-91.00	-	3	1493316.00	-	ethersphere-1322	Top	Access Points
8	Fish-bowl	3	6	-90.00	-	4	767319.00	-	ethersphere-1322	Top	Access Points
9	ap65-c2:2e:4a	2	2	-104.50	-	0	0.00	chicken fingers	Aruba2400	Top	Access Points
10	1242-H	1	1	-88.00	-	8	2098072.00	-	ethersphere-1322	Top	Access Points

Most Transmit Power Changes (2.4 GHz)

Rank ▲	Device	Transmit Power Changes	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	00:24:6c:c4:ce:a6	29	20	-82.00	-	0	0.00	-	Aruba651	Top	Access Points
2	00:1a:1e:c1:52:0e	13	1	-82.00	-	1	2064.00	-	Aruba651	Top	Access Points
3	1249	10	8	-90.50	-	1	56.00	-	ethersphere-1322	Top	Access Points
4	1248	8	4	-90.50	-	0	65.00	-	ethersphere-1322	Top	Access Points
5	00:1a:1e:c0:6c:46	7	16	-77.00	-	0	0.00	-	Aruba3600-US	Top	Access Points
6	1394	5	1	-83.50	-	0	0.00	-	ethersphere-1322	Top	Access Points
7	1350	5	1	-53.00	-	0	0.00	-	ethersphere-1322	Top	Access Points
8	ap105-A1	5	6	-86.50	-	0	0.00	pit	Aruba-3400	Top	Access Points
9	1260	3	6	-86.50	-	2	676.00	-	ethersphere-1322	Top	Access Points
10	2188	3	6	-73.50	-	1	308.00	-	ethersphere-1322	Top	Access Points

Least Utilized by Channel Usage (5 GHz)

Rank ▲	Device	Channel Busy	Interference	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	AP0018.19bd.b1d0	1.57	1.57	0	0.00	ap lab	Cisco4400	Top	Access Points
2	AP10	3.15	3.15	0	0.00	Sales Office-hello	Cisco4400	Top	Access Points

Least Utilized by Channel Usage (2.4 GHz)

Rank ▲	Device	Channel Busy	Interference	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	AP001d.a1fc.ca7a	22.83	20.47	0	0.00	default location	5500-6.0.196.0	Top	Access Points
2	AP10	64.96	62.60	0	1.00	Sales Office-hello	Cisco4400	Top	Access Points
3	AP0018.19bd.b1d0	71.65	68.90	0	0.00	ap lab	Cisco4400	Top	Access Points

All tables indicate the rank, device type, number of users, bandwidth, location, controller, folder, and group, and all are sorted according to rank. Selecting a value under the **Device** column in any table will take you to the **APs/Devices > Monitor > Radio Statistics** page for the band indicated in the table title (5 GHz or 2.4 GHz).

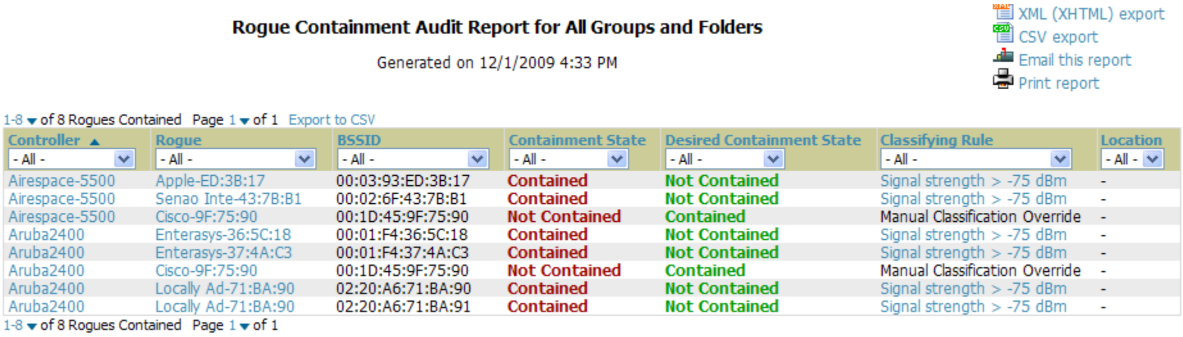
- Every list contains Rank, Device (name, not type), Channel Changes, Average Noise, Average Channel Utilization, Users, Bandwidth, Location, Controller name, Folder, and Group.
- The third column in the list (after Device) will be the column the list is sorted by.
- If that column would otherwise be in the list (Channel Changes), it does not show up in the list where it would otherwise.
- Note that sometimes the sorted column is not one of those common ones, such as the Interfering Devices section.

OV3600 limits data storage to 183 days (approximately six months) per radio. If you create an RF Health Report with a date range longer than 183 days, it will only include Channel Changes, Transmit Power Changes, Average Utilization, Mac/Phy Errors and Average Noise based on whatever part of the report intersects the last 183 days. This differs from most other reports, because other data (like bandwidth and users) maxes out at 425 days, and OV3600 validates reports so you can only run them over a 366 day duration.

Using the Rogue Containment Audit Report

The rogue containment audit report that lets you know if any containment is failing. Figure 174 illustrates the fields and information in this report type.

Figure 174 ***Reports > Detail > Rogue Containment Audit Report*** *Page Illustration*



Rogue Containment Audit Report for All Groups and Folders

Generated on 12/1/2009 4:33 PM

1-8 ▾ of 8 Rogues Contained Page 1 ▾ of 1 Export to CSV

Controller ▲	Rogue	BSSID	Containment State	Desired Containment State	Classifying Rule	Location
- All -	- All -	- All -	- All -	- All -	- All -	- All -
Airespace-5500	Apple-ED:3B:17	00:03:93:ED:3B:17	Contained	Not Contained	Signal strength > -75 dBm	-
Airespace-5500	Senao Inte-43:7B:B1	00:02:6F:43:7B:B1	Contained	Not Contained	Signal strength > -75 dBm	-
Airespace-5500	Cisco-9F:75:90	00:1D:45:9F:75:90	Not Contained	Contained	Manual Classification Override	-
Aruba2400	Enterasys-36:5C:18	00:01:F4:36:5C:18	Contained	Not Contained	Signal strength > -75 dBm	-
Aruba2400	Enterasys-37:4A:C3	00:01:F4:37:4A:C3	Contained	Not Contained	Signal strength > -75 dBm	-
Aruba2400	Cisco-9F:75:90	00:1D:45:9F:75:90	Not Contained	Contained	Manual Classification Override	-
Aruba2400	Locally Ad-71:BA:90	02:20:A6:71:BA:90	Contained	Not Contained	Signal strength > -75 dBm	-
Aruba2400	Locally Ad-71:BA:90	02:20:A6:71:BA:91	Contained	Not Contained	Signal strength > -75 dBm	-

1-8 ▾ of 8 Rogues Contained Page 1 ▾ of 1

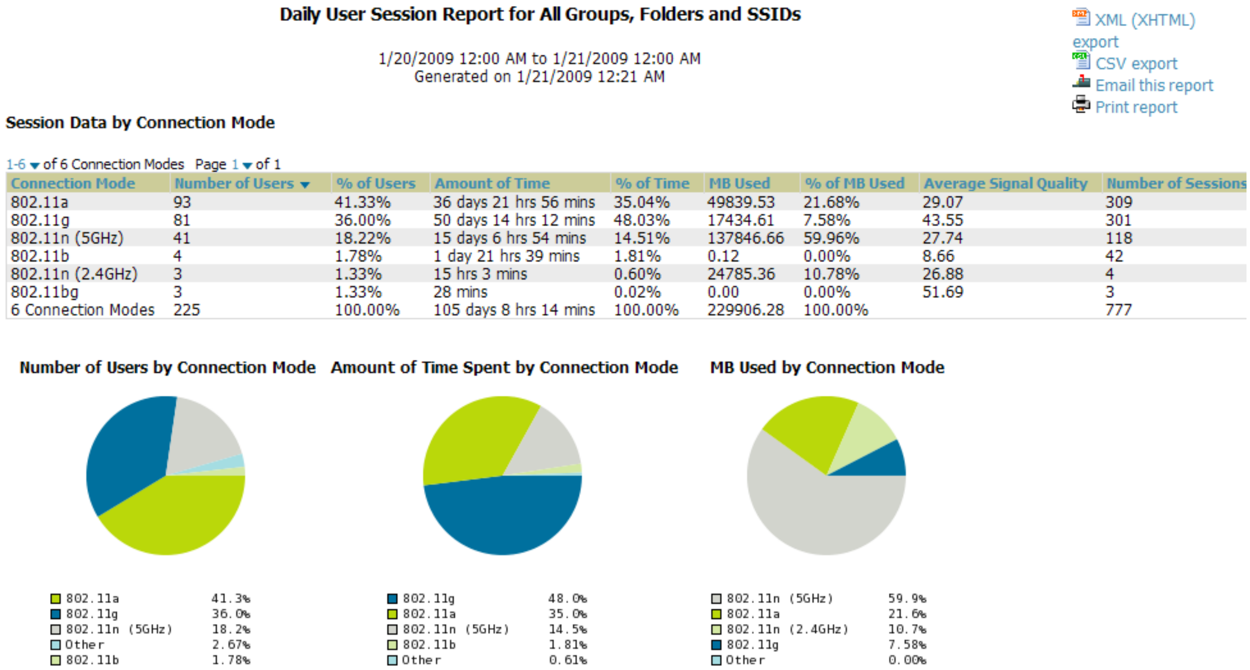
Using the User Session Report

The **User Session Report** extensively itemizes user-level activity by session. A session is any instance in which a user connects to the network. You can track and display in list and chart form session information that includes all of the following:

- Connection Mode (wired, wireless or both depending on how report definition is created)
- SSID
- Role
- VLAN
- Cipher
- Summary
- Sessions
- User

The figures that follow illustrate the fields and information in the **User Session Report.**

Figure 175 ***User Session Detail,*** *Connection Mode Information*



Daily User Session Report for All Groups, Folders and SSIDs

1/20/2009 12:00 AM to 1/21/2009 12:00 AM
Generated on 1/21/2009 12:21 AM

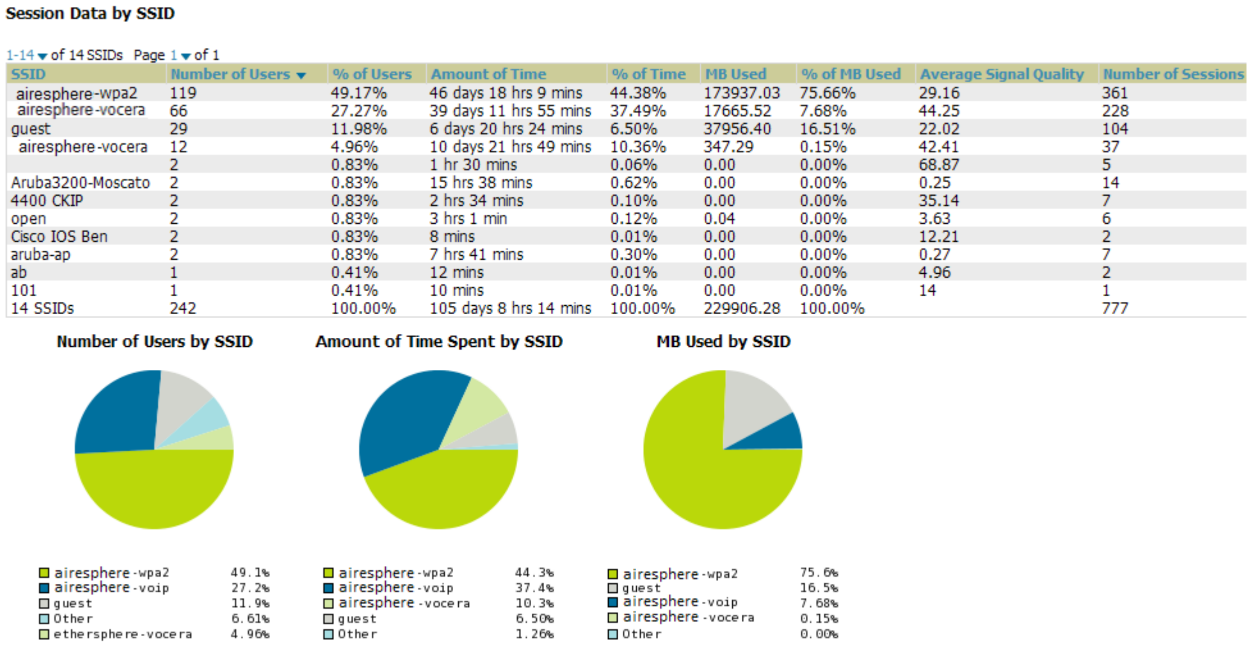
Session Data by Connection Mode

1-6 ▾ of 6 Connection Modes Page 1 ▾ of 1

Connection Mode	Number of Users ▾	% of Users	Amount of Time	% of Time	MB Used	% of MB Used	Average Signal Quality	Number of Sessions
802.11a	93	41.33%	36 days 21 hrs 56 mins	35.04%	49839.53	21.68%	29.07	309
802.11g	81	36.00%	50 days 14 hrs 12 mins	48.03%	17434.61	7.58%	43.55	301
802.11n (5GHz)	41	18.22%	15 days 6 hrs 54 mins	14.51%	137846.66	59.96%	27.74	118
802.11b	4	1.78%	1 day 21 hrs 39 mins	1.81%	0.12	0.00%	8.66	42
802.11n (2.4GHz)	3	1.33%	15 hrs 3 mins	0.60%	24785.36	10.78%	26.88	4
802.11bg	3	1.33%	28 mins	0.02%	0.00	0.00%	51.69	3
6 Connection Modes	225	100.00%	105 days 8 hrs 14 mins	100.00%	229906.28	100.00%		777

Number of Users by Connection Mode **Amount of Time Spent by Connection Mode** **MB Used by Connection Mode**

Figure 176 ***User Session Detail > SSID*** *Information*



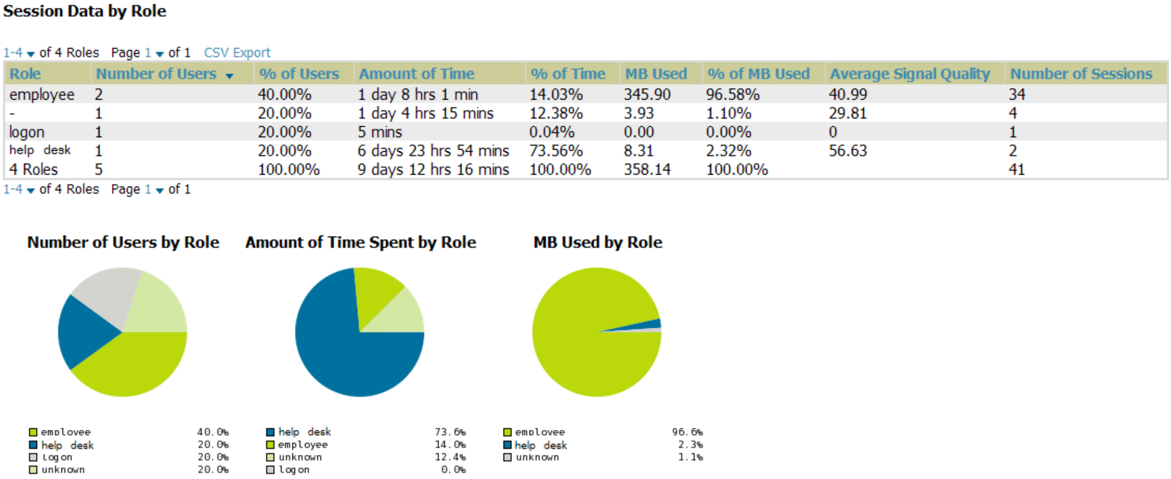
Session Data by SSID

1-14 ▾ of 14 SSIDs Page 1 ▾ of 1

SSID	Number of Users ▾	% of Users	Amount of Time	% of Time	MB Used	% of MB Used	Average Signal Quality	Number of Sessions
airesphere-wpa2	119	49.17%	46 days 18 hrs 9 mins	44.38%	173937.03	75.66%	29.16	361
airesphere-vocera	66	27.27%	39 days 11 hrs 55 mins	37.49%	17665.52	7.68%	44.25	228
guest	29	11.98%	6 days 20 hrs 24 mins	6.50%	37956.40	16.51%	22.02	104
airesphere-vocera	12	4.96%	10 days 21 hrs 49 mins	10.36%	347.29	0.15%	42.41	37
	2	0.83%	1 hr 30 mins	0.06%	0.00	0.00%	68.87	5
Aruba3200-Moscato	2	0.83%	15 hrs 38 mins	0.62%	0.00	0.00%	0.25	14
4400 CKIP	2	0.83%	2 hrs 34 mins	0.10%	0.00	0.00%	35.14	7
open	2	0.83%	3 hrs 1 min	0.12%	0.04	0.00%	3.63	6
Cisco IOS Ben	2	0.83%	8 mins	0.01%	0.00	0.00%	12.21	2
aruba-ap	2	0.83%	7 hrs 41 mins	0.30%	0.00	0.00%	0.27	7
ab	1	0.41%	12 mins	0.01%	0.00	0.00%	4.96	2
101	1	0.41%	10 mins	0.01%	0.00	0.00%	14	1
14 SSIDs	242	100.00%	105 days 8 hrs 14 mins	100.00%	229906.28	100.00%		777

Number of Users by SSID **Amount of Time Spent by SSID** **MB Used by SSID**

Figure 177 *User Session Detail* > *Role* Information



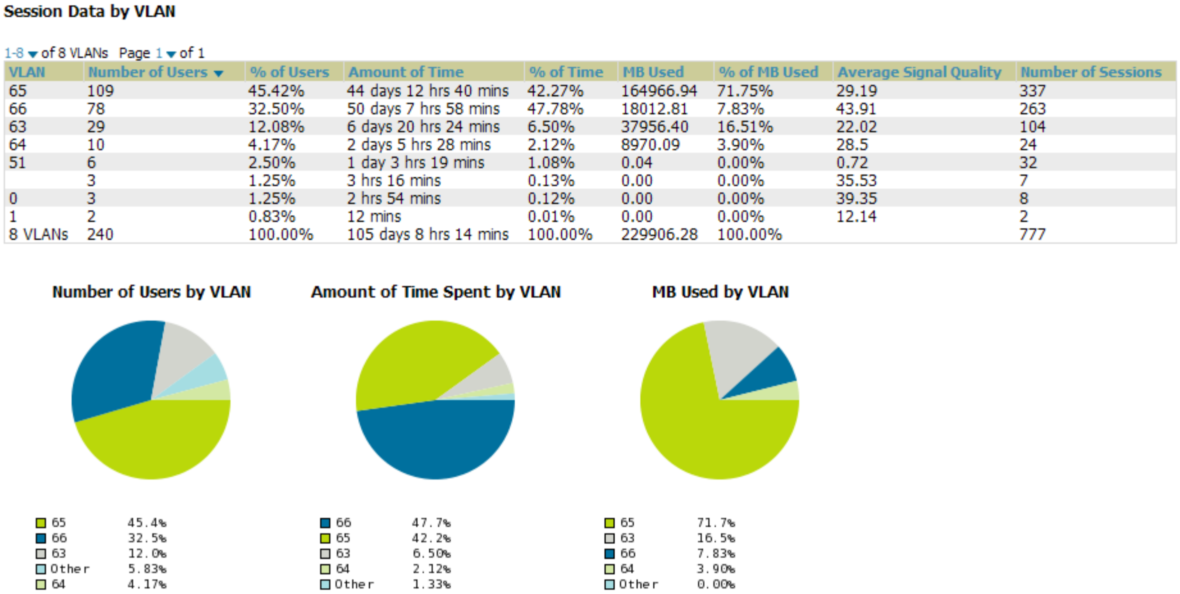
Session Data by Role

1-4 ▾ of 4 Roles   Page 1 ▾ of 1   CSV Export

Role	Number of Users ▾	% of Users	Amount of Time	% of Time	MB Used	% of MB Used	Average Signal Quality	Number of Sessions
employee	2	40.00%	1 day 8 hrs 1 min	14.03%	345.90	96.58%	40.99	34
-	1	20.00%	1 day 4 hrs 15 mins	12.38%	3.93	1.10%	29.81	4
logon	1	20.00%	5 mins	0.04%	0.00	0.00%	0	1
help desk	1	20.00%	6 days 23 hrs 54 mins	73.56%	8.31	2.32%	56.63	2
4 Roles	5	100.00%	9 days 12 hrs 16 mins	100.00%	358.14	100.00%		41

1-4 ▾ of 4 Roles   Page 1 ▾ of 1

Figure 178 *User Session Detail* > *VLAN* Information

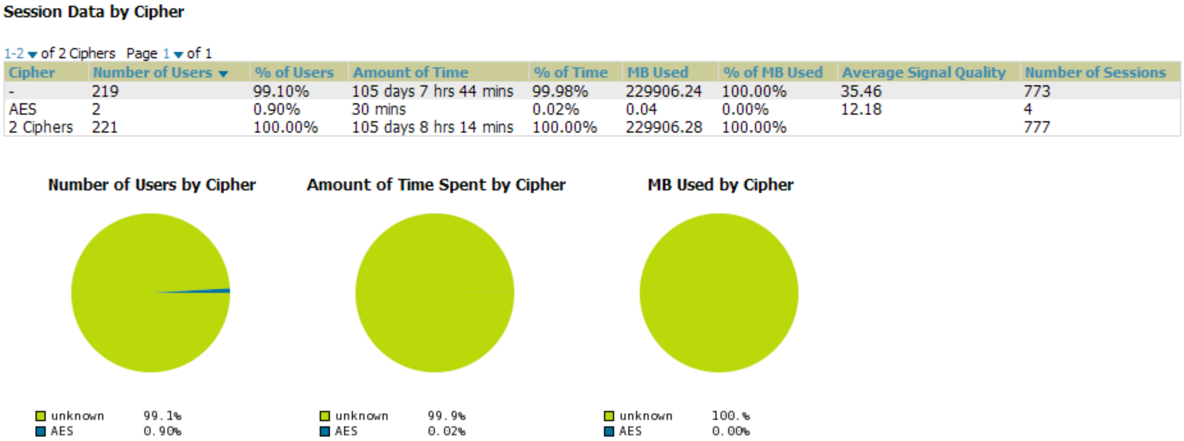


Session Data by VLAN

1-8 ▾ of 8 VLANs   Page 1 ▾ of 1

VLAN	Number of Users ▾	% of Users	Amount of Time	% of Time	MB Used	% of MB Used	Average Signal Quality	Number of Sessions
65	109	45.42%	44 days 12 hrs 40 mins	42.27%	164966.94	71.75%	29.19	337
66	78	32.50%	50 days 7 hrs 58 mins	47.78%	18012.81	7.83%	43.91	263
63	29	12.08%	6 days 20 hrs 24 mins	6.50%	37956.40	16.51%	22.02	104
64	10	4.17%	2 days 5 hrs 28 mins	2.12%	8970.09	3.90%	28.5	24
51	6	2.50%	1 day 3 hrs 19 mins	1.08%	0.04	0.00%	0.72	32
	3	1.25%	3 hrs 16 mins	0.13%	0.00	0.00%	35.53	7
0	3	1.25%	2 hrs 54 mins	0.12%	0.00	0.00%	39.35	8
1	2	0.83%	12 mins	0.01%	0.00	0.00%	12.14	2
8 VLANs	240	100.00%	105 days 8 hrs 14 mins	100.00%	229906.28	100.00%		777

Figure 179 *User Session Detail* > *Cipher* Information

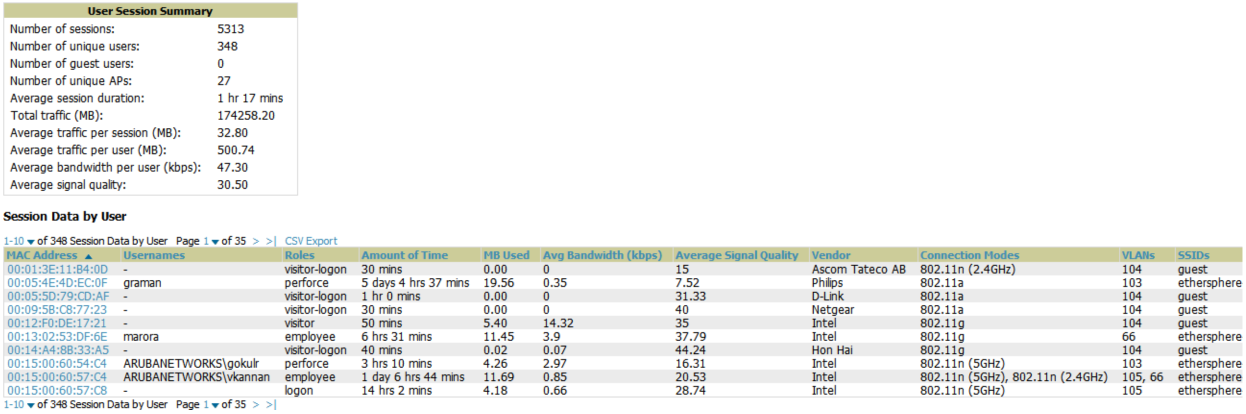


Session Data by Cipher

1-2 ▾ of 2 Ciphers   Page 1 ▾ of 1

Cipher	Number of Users ▾	% of Users	Amount of Time	% of Time	MB Used	% of MB Used	Average Signal Quality	Number of Sessions
-	219	99.10%	105 days 7 hrs 44 mins	99.98%	229906.24	100.00%	35.46	773
AES	2	0.90%	30 mins	0.02%	0.04	0.00%	12.18	4
2 Ciphers	221	100.00%	105 days 8 hrs 14 mins	100.00%	229906.28	100.00%		777

Figure 180 ***Summary and User*** *Information (partial view)*



User Session Summary	
Number of sessions:	5313
Number of unique users:	348
Number of guest users:	0
Number of unique APs:	27
Average session duration:	1 hr 17 mins
Total traffic (MB):	174258.20
Average traffic per session (MB):	32.80
Average traffic per user (MB):	500.74
Average bandwidth per user (kbps):	47.30
Average signal quality:	30.50

Session Data by User

1-10 ▾ of 348 Session Data by User Page 1 ▾ of 35 > >| CSV Export

MAC Address ▲	Usernames	Roles	Amount of Time	MB Used	Avg Bandwidth (kbps)	Average Signal Quality	Vendor	Connection Modes	VLANs	SSIDs
00:01:3E:11:B4:0D	-	visitor-logon	30 mins	0.00	0	15	Ascom Tateco AB	802.11n (2.4GHz)	104	guest
00:05:4E:4D:EC:0F	graman	perforce	5 days 4 hrs 37 mins	19.56	0.35	7.52	Philips	802.11a	103	ethersphere
00:05:5D:79:CD:AF	-	visitor-logon	1 hr 0 mins	0.00	0	31.33	D-Link	802.11a	104	guest
00:09:5B:C8:77:23	-	visitor-logon	30 mins	0.00	0	40	Netgear	802.11a	104	guest
00:12:F0:DE:17:21	-	visitor	50 mins	5.40	14.32	35	Intel	802.11g	104	guest
00:13:02:53:DF:6E	marora	employee	6 hrs 31 mins	11.45	3.9	37.79	Intel	802.11g	66	ethersphere
00:14:A4:8B:33:A5	-	visitor-logon	40 mins	0.02	0.07	44.24	Hon Hai	802.11g	104	guest
00:15:00:60:54:C4	ARUBANETWORKS\gokulr	perforce	3 hrs 10 mins	4.26	2.97	16.31	Intel	802.11n (5GHz)	103	ethersphere
00:15:00:60:57:C4	ARUBANETWORKS\vkannan	employee	1 day 6 hrs 44 mins	11.69	0.85	20.53	Intel	802.11n (5GHz), 802.11n (2.4GHz)	105, 66	ethersphere
00:15:00:60:57:C8	-	logon	14 hrs 2 mins	4.18	0.66	28.74	Intel	802.11n (5GHz)	105	ethersphere

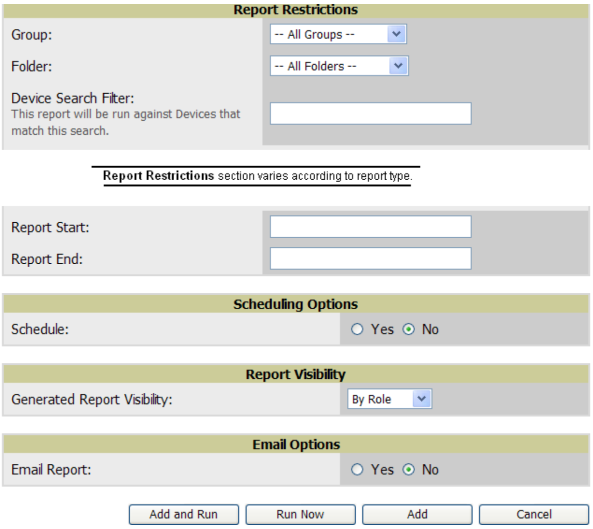
1-10 ▾ of 348 Session Data by User Page 1 ▾ of 35 > >|

Defining Reports

You can create reports in OV3600 for any time period you wish, to be run when you wish, and distributed to recipients that you define. Perform these steps to create and run custom reports. Reports created with the **Reports > Definition** page appear on this and on the **Reports > Generated** page once defined.

1. To create or edit a report, browse to the **Reports > Definition** page and select the **Add** button, or select the pencil icon to edit an existing report definition. Figure 181 illustrates one view of the **Reports > Definition** page.

Figure 181 *Defining a Report with* ***Reports*** *>* ***Definitions*** *>* ***Add*** *Button*



Report Restrictions

Group: -- All Groups --

Folder: -- All Folders --

Device Search Filter:
This report will be run against Devices that match this search.

Report Restrictions section varies according to report type.

Report Start:

Report End:

Scheduling Options

Schedule: ○ Yes ● No

Report Visibility

Generated Report Visibility: By Role

Email Options

Email Report: ○ Yes ● No

2. Complete the fields described in Table 134 and any additional **Report Restrictions**. The **Report Restrictions** section changes according to the report type you choose. Additional information about each report type is described in "Using Daily Reports" on page 222.

Table 134 ***Reports*** *>* ***Definitions*** *>* ***Add Page*** *Fields*

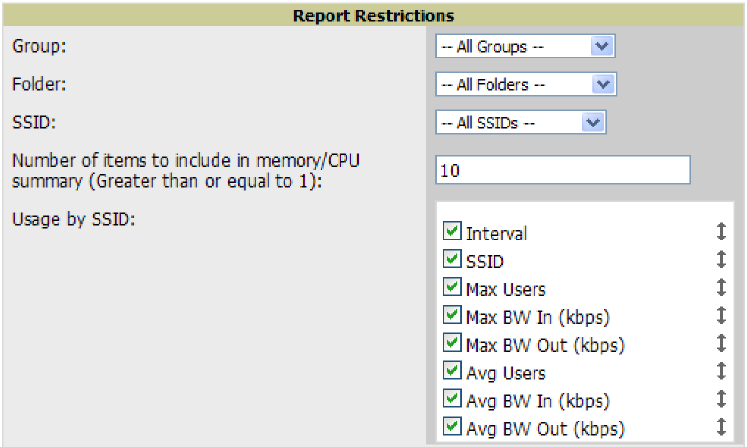
Field	Default	Description
Title	Empty	Enter a **Report Title**. Alcatel-Lucent recommends using a title that is a meaningful and descriptive, so it may be found easily on the lists of reports that appear on either **Generated** or **Definitions** pages.
Type	Capacity	Choose the type of report you wish to create in the Report Type drop-down menu.

Table 134 *Reports > Definitions > Add Page* Fields *(Continued)*

Field	Default	Description
Group	All Groups	Specify the groups and folders to be covered in the report by choosing **All Groups** (or **All Folders**) or specifying **Use selected groups** (or **Use selected folders**) in the drop-down menu. If **Use selected groups** is chosen, a menu with checkboxes appears, allowing you to choose the groups to include in the report.
Folder	All Folders	
Device Search Filter	Blank	Add a specific alpha numeric string for finding devices that match that which you entered. Note that once you enter a search string, new or deleted devices that match the search string will automatically be included or excluded in all future reports generated until you delete or change the search string. For certain reports, such as **New User** and **User Session**, will allow you to search devices associated with a specific user or device.
SSID	All SSIDs	This field displays for most report types. When this field appears, and when you select **Use Selected IDs**, a new list of SSIDs displays. Check (select) the specific SSIDs to be included in the report.
Report Start **Report End**	Blank	These fields establish the time period to be covered by the report. These fields are supported for most report types. When these fields do not appear, the report provides a snapshot of current status rather than information covering a period of time Times can be entered in relative or absolute form. A start date of 6 months 3 weeks 5 days 9 hours ago and an end time of 4 months 2 weeks 1 day ago is valid, as is a start date of 5/5/2008 13:00 and an end date of 6/6/2008 9:00. Absolute times must be entered in a 24-hour format. Other reports, like the Inventory Report, give a snapshot picture of the OV3600 at the present time.
Schedule	No	When you select **Yes**, new fields display that allow you to define a specific time for report creation. The report schedule setting is distinct from the **Report Start** and **Report End** fields, as these define the period of time to be covered by the report. These **Schedule** fields establish the time that a report runs, independent of report scope: • **Current Local Time**—Displays for reference the time of the OV3600 system. • **Desired Start Date/Time**—Sets the time the report runs, which may often be separate from the time period covered by the report. This allows you to run a report during less busy hours. • **Occurs**—Select whether the report is to be run one time, daily, weekly, monthly, or annually. Depending on the recurrence pattern selected, you get an additional drop-down menu. For example, if you select a recurrence of monthly, you get an additional drop-down menu that allows you to pick which day of the month (day 1, day 2, and so forth) the report should run.
Generated Report Visibility	By Role	This field allows you to display the report either by user role, with the report appearing in User Role lists on the **Reports > Generated** page. Alternatively, this field allows you to display reports by **Subject** on the **Reports > Generated** page.
Email Report	No	Select **Yes** to display sender and recipient fields. Enter the Sender Address where marked to indicate the address that appears in the **From** field of the emailed report. Enter recipient email addresses separated by commas when using multiple email addresses. **NOTE:** OV3600 will not attempt to email a report with an excessively large number of rows in the detail section.

In the report restrictions section you can customize any detailed information contained in a chosen report. Figure 182 shows a sample **Report Restrictions** page.

Figure 182 ***Report Restrictions** Illustration*



Report Restrictions

Group: -- All Groups --

Folder: -- All Folders --

SSID: -- All SSIDs --

Number of items to include in memory/CPU summary (Greater than or equal to 1): 10

Usage by SSID:

- ☑ Interval
- ☑ SSID
- ☑ Max Users
- ☑ Max BW In (kbps)
- ☑ Max BW Out (kbps)
- ☑ Avg Users
- ☑ Avg BW In (kbps)
- ☑ Avg BW Out (kbps)

By default all data will be included. Deselect the checkbox to hide specific information. The list can also be reordered by dragging and dropping the separate lines. The order displayed here will match the column order in the report.

3. Do one of the following:
   - Select **Add and Run** to generate the report immediately, in addition to saving report settings.
   - Select **Run Now** to generate the report immediately without creating a new report definition or saving the report settings.
   - Select **Add (**only) to complete the report creation, to be run at the time scheduled.
   - Select **Cancel** to exit from the **Add** page.

Table 135 describes the configurable settings for the custom report to be created. Select any of the report names to view additional information on that report type.

Table 135 *Report Types and Scheduling Options Supported for Custom Reports*

Report Type	Can by Run by Time Period	Can be Run by Group/Folder	Description
Using Custom Reports	Yes	Yes	Summarizes devices based on which have exceeded a defined percentage of their maximum bandwidth capacity. Pulls data for AP radios or interfaces of universal devices (ifSpeed value).
Using the Capacity Planning Report	Yes	Yes	Tracks bandwidth capacity and consumption according to thresholds for data throughput. This is a device-oriented report.
Using the Configuration Audit Report	**No**	Yes	Provides a snapshot of the configuration of all specified access points in OV3600, at report run time.
Using the Device Summary Report	Yes	Yes	Summarizes user and bandwidth statistics and lists devices in OV3600.
Using the Device Uptime Report	Yes	Yes	Summarizes device uptime within defined groups or folders.
Using the IDS Events Report	Yes	Yes	Summarizes IDS events; can be limited to a summary of a certain number of events.
Using the Inventory Report	**No**	Yes	Provides an audit of vendors, models and firmware versions of devices in OV3600.
Using the Memory and CPU Utilization Report	Yes	Yes	Summarizes usage for controllers for defined top number of devices; can be run with or without per-CPU details and details about device memory usage.

Table 135 *Report Types and Scheduling Options Supported for Custom Reports (Continued)*

Report Type	Can by Run by Time Period	Can be Run by Group/Folder	Description
Using the Network Usage Report	Yes	Yes	Summarizes bandwidth data and number of users.
Using the New Rogue Devices Report	Yes	**No**	Shows new rogue devices by score, discovering AP, and MAC address vendor.
Using the New Users Report	Yes	**No**	Provides a summary list of new users, including username, role, MAC address, discovering AP, and association time.
Using the PCI Compliance Report	Yes	Yes	Provides a summary of network compliance with PCI requirements, according to the PCI requirements enabled in OV3600 using the **OV3600 Setup > PCI Compliance** page.
Using the Port Usage Report	Yes	Yes	Summarizes switch and port information across the network. Generates information on the unused ports. Provides a detailed list of all available switches and ports in the network.
Using the RADIUS Authentication Issues Report	Yes	Yes	Summarizes RADIUS authentication issues by controller and by user, as well as a list of all issues.
Using the RF Health Report	Yes	Yes	Tracks problematic radios, changes, errors, and interfering devices.
Using the RF Health Report	**No**	Yes	Identifies discrepancies between access point containment status specified in OV3600 compared to containment status identified by the controller at report run time.
Using the User Session Report	Yes	Yes	Summarizes user data by radio mode, SSID and VLAN, as well as lists all sessions.

Emailing and Exporting Reports

This section describes three ways in which distribute reports from OV3600:

- Emailing Reports in General Email Applications
- Emailing Reports to Smarthost
- Exporting Reports to XML or CSV

Emailing Reports in General Email Applications

Perform these steps to set up email distribution of reports in OV3600:

- All reports contain a link to export the report to an XML file and a text box where you may specify email addresses, separated by commas, to which reports are sent.
- Select **Email This Report** to email the report to the address specified in the text box above the button.

Additional information about email-based report generation is described in "Defining Reports" on page 241, and in "Emailing Reports to Smarthost" on page 244.

Emailing Reports to Smarthost

OV3600 uses Postfix to deliver alerts and reports via email, because it provides a high level of security and locally queues email until delivery. If OV3600 sits behind a firewall, which prevents it from sending email directly to the specified recipient, use the following procedure to forward email to a smarthost.

1. Add the following line to `/etc/postfix/main.cf`:

```
relayhost = [mail.Alcatel-Lucent.com]
```

Where: `mail.Alcatel-Lucent.com` is the IP address or hostname of your smarthost.

2. Run service postfix restart
3. Send a test message to an email address.

```
Mail -v xxx@xxx.com
Subject: test mail
.
CC:
```

4. Press **Enter**.
5. Check the mail log to ensure mail was sent.

```
tail -f /var/log/maillog
```

Exporting Reports to XML or CSV

OV3600 allows you to export individual reports in XML (xhtml) or CSV. You can also export all reports at once and a zip file will be generated with all of the files in CSV format included. These files may be read by an HTML browser or opened in Excel. The CSV files can be opened in any text editor such as MS Notepad or Word..

NOTE

This method of exporting files supports graphics and links, and prevents **Missing File C:\filename.css** error messages.

Transferring Reports Using FTP

Once reports are generated, you can also copy them to any ftp accessible destination using a sample script. Contact Alcatel support for more information.

Chapter 10

Using the OV3600 Helpdesk

This chapter presents the functions, configuration, and use of the **OV3600 Helpdesk**, and includes the following sections:

- "OV3600 Helpdesk Overview" on page 247
- "Monitoring Incidents with Helpdesk" on page 248
- "Creating a New Incident with Helpdesk" on page 249
- "Creating New Snapshots or Incident Relationships" on page 250
- "Using the Helpdesk Tab with an Existing Remedy Server" on page 251

OV3600 Helpdesk Overview

The Helpdesk module of the OmniVista 3600 Air Manager allows front-line technical support staff to take full advantage of the data available in the OmniVista 3600 Air Manager. The OV3600 Helpdesk includes the following features and functions, with additional features described in this chapter:

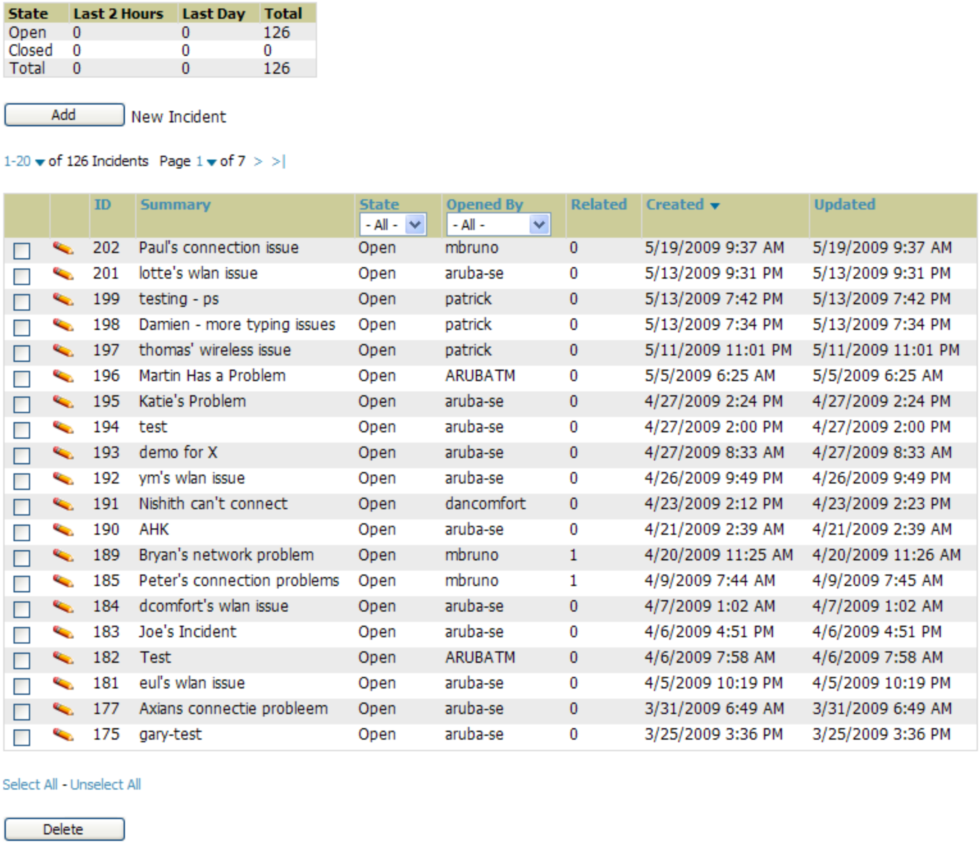
- The **Helpdesk** tab appears to the right of the **Home** tab.
- Users with an **Admin** role have the **Helpdesk** option enabled by default.
- **Admin** users can make the Helpdesk available to users of any role by selecting the **enabled** radio button on the **role detail** page. To edit existing roles, select the **pencil** icon next to a role on the **OV3600 Setup > Roles** page.
- The OV3600 Helpdesk allows you to document incidents associated with users on the network.
- Installing Remedy allows you to disable Helpdesk, and use OV3600 as an interface for creating, viewing, and editing incidents on the existing Remedy server. You can also associate snapshots with Remedy incidents and store them on your OV3600.

  The option to use an external Remedy server is disabled by default. Navigate to the **Helpdesk > Setup** page to enable Remedy. See "Using the Helpdesk Tab with an Existing Remedy Server" on page 251 for more information on how to configure OV3600 to integrate with a Remedy server.

Monitoring Incidents with Helpdesk

For a complete list of incidents, or to open a new incident, navigate to the **Helpdesk > Incidents** page. Figure 183 illustrates the components of the OV3600 **Helpdesk Incidents** page.

Figure 183 ***Helpdesk > Incidents*** *Page Illustration*



State	Last 2 Hours	Last Day	Total
Open	0	0	126
Closed	0	0	0
Total	0	0	126

Add New Incident

1-20 ▾ of 126 Incidents Page 1 ▾ of 7 > >|

		ID	Summary	State - All - ▾	Opened By - All - ▾	Related	Created ▾	Updated
☐	✎	202	Paul's connection issue	Open	mbruno	0	5/19/2009 9:37 AM	5/19/2009 9:37 AM
☐	✎	201	lotte's wlan issue	Open	aruba-se	0	5/13/2009 9:31 PM	5/13/2009 9:31 PM
☐	✎	199	testing - ps	Open	patrick	0	5/13/2009 7:42 PM	5/13/2009 7:42 PM
☐	✎	198	Damien - more typing issues	Open	patrick	0	5/13/2009 7:34 PM	5/13/2009 7:34 PM
☐	✎	197	thomas' wireless issue	Open	patrick	0	5/11/2009 11:01 PM	5/11/2009 11:01 PM
☐	✎	196	Martin Has a Problem	Open	ARUBATM	0	5/5/2009 6:25 AM	5/5/2009 6:25 AM
☐	✎	195	Katie's Problem	Open	aruba-se	0	4/27/2009 2:24 PM	4/27/2009 2:24 PM
☐	✎	194	test	Open	aruba-se	0	4/27/2009 2:00 PM	4/27/2009 2:00 PM
☐	✎	193	demo for X	Open	aruba-se	0	4/27/2009 8:33 AM	4/27/2009 8:33 AM
☐	✎	192	ym's wlan issue	Open	aruba-se	0	4/26/2009 9:49 PM	4/26/2009 9:49 PM
☐	✎	191	Nishith can't connect	Open	dancomfort	0	4/23/2009 2:12 PM	4/23/2009 2:23 PM
☐	✎	190	AHK	Open	aruba-se	0	4/21/2009 2:39 AM	4/21/2009 2:39 AM
☐	✎	189	Bryan's network problem	Open	mbruno	1	4/20/2009 11:25 AM	4/20/2009 11:26 AM
☐	✎	185	Peter's connection problems	Open	mbruno	1	4/9/2009 7:44 AM	4/9/2009 7:45 AM
☐	✎	184	dcomfort's wlan issue	Open	aruba-se	0	4/7/2009 1:02 AM	4/7/2009 1:02 AM
☐	✎	183	Joe's Incident	Open	aruba-se	0	4/6/2009 4:51 PM	4/6/2009 4:51 PM
☐	✎	182	Test	Open	ARUBATM	0	4/6/2009 7:58 AM	4/6/2009 7:58 AM
☐	✎	181	eul's wlan issue	Open	aruba-se	0	4/5/2009 10:19 PM	4/5/2009 10:19 PM
☐	✎	177	Axians connectie probleem	Open	aruba-se	0	3/31/2009 6:49 AM	3/31/2009 6:49 AM
☐	✎	175	gary-test	Open	aruba-se	0	3/25/2009 3:36 PM	3/25/2009 3:36 PM

Select All - Unselect All

Delete

The table in **Helpdesk > Incidents** displays the count of incidents by state and by time. You can sort incidents from within any category of information, whether in sequential or reverse-sequential order. You can display all incidents, or strictly open or closed incidents, and you can display incidents according to the person who created them. Finally, the **Helpdesk > Incidents** page allows you to add or delete incidents.

Table 136 ***Helpdesk > Incidents*** *Top Table*

Column	Description
State	Displays three states as they apply, as follows: - Open (currently under investigation) - Closed (resolved) - The total incident count
Period of time and Total	Shows the count of incidents in the last two hours, the last day, and the total count.

The table at the bottom of the page, as described in Table 137 below, summarizes the incidents that have been reported thus far, and which OV3600 has not yet purged.

Use the **OV3600 Setup > General** page and the **Historical Data Retention** page. Using the **Closed Helpdesk Incidents** field, set the number of days that OV3600 is to retain records of closed Helpdesk incidents. Settings this value to 0 disables this function.

Selecting the **pencil** icon next to any incident opens an edit page where you can modify and update the incident. An incident can be deleted by selecting the checkbox next to it and selecting **Delete** at the bottom of the table.

Table 137 ***OV3600 Helpdesk > Incidents*** *Bottom Table*

Column	Description
ID	Displays the ID number of the incident, which is assigned automatically when the incident is logged.
Summary	Presents a summary statement of the issue or problem—entered by the OV3600 user when the incident is created.
State	The current state of the incident - this can be either open or closed. The drop-down menu at the top of the column can be used to show only open or closed incidents. The default is to show incidents of both states.
Opened By	Displays the username of the OV3600 user who opened the incident. Helpdesk can be made available to users of any role by selecting the **enabled** radio button on the **Role Detail** page. Select the pencil icon next to a role on the **OV3600 Setup > Roles** page.
Related	Displays the number of items that have been associated to the incident. These link different groups, APs or clients to the incident report.
Created	Displays the time and date the incident was created.
Updated	Displays the time and date the incident was last modified by an OV3600 user.

Creating a New Incident with Helpdesk

To create a new Helpdesk incident, select **Add New Incident** underneath the top table. This launches and displays an incident edit page, as illustrated in Figure 184. The page contents are described in Table 138.

Figure 184 ***Add Incident*** *Page Illustration*

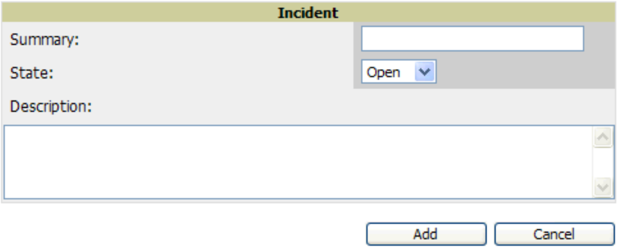


Table 138 ***Helpdesk Incident*** *Edit Page Fields*

Field	Description
Summary	Displays user-entered text that describes a short summary of the incident
State	Provides a drop-down menu with the options "Open" or "Closed"
Description	Provides a longer user-entered text area for a thorough description of the incident.

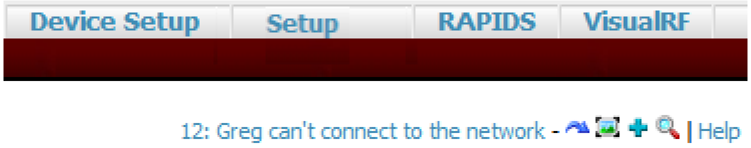
NOTE

The **Incidents** portion of the **Alert Summary** table on other OV3600 pages only increments the counter for incidents that are open and associated to an AP. This field displays incidents based on folder, which is the Top folder on this page and on the **Home > Overview** page. Incidents that are not related to devices in that folder are not counted in the **Alert Summary** table on other pages.

To view all incidents, including those not associated to an AP, use the **Helpdesk > Incidents** page.

Helpdesk icons appear at the top of other OV3600 pages, allowing graphical snapshots and other records to be associated to existing incidents. These appear in the upper right-hand corner next to the **Help** link. Refer to Figure 185.

Figure 185 *Helpdesk Icons on Additional Pages*



12: Greg can't connect to the network - ↷ 🖼 ✚ 🔍 | Help

Table 139 describes the Helpdesk icon components.

Table 139 ***Helpdesk** Icon Components*

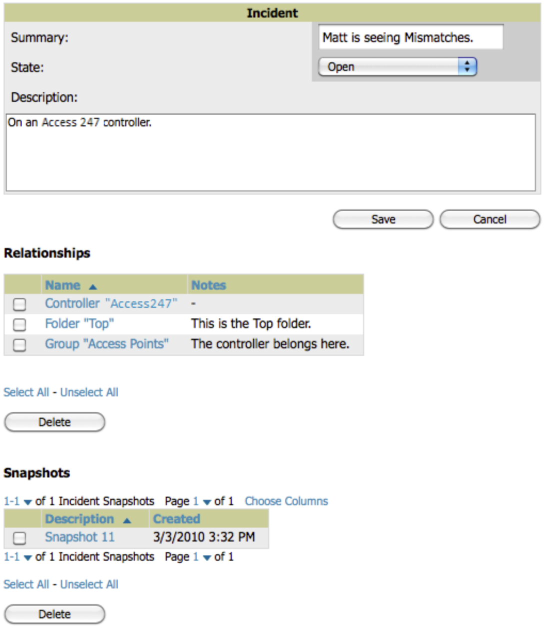
Icon	Description
Current Incident	(ID number and description) Identifies the current incident of focus in the Helpdesk header. Selecting the link brings up the **Incident Edit** page (see above). Mousing over the incident brings up a summary popup of the incident.
↷	Relates the device, group or client to the incident (see below for more details).
🖼	Attaches a snapshot of the page to the incident. This feature can be used to record a screenshot of information and preserve it for future troubleshooting purposes.
✚	Creates a new incident report.
🔍	Choose a new incident from the list of created incidents to be the **Current Incident** (see description of icon above).

Creating New Snapshots or Incident Relationships

Snapshots or relationships can be created by selecting the Helpdesk header icon (see Table 139) on the screen that needs to be documented. Snapshots or relationships can then be related to the current incident in the ensuing popup window. In order to attach snapshots or relationships to another incident, select the **Choose a New Incident** icon to select a new current incident.

Relationships and snapshots appear on the **Incident Edit** page after they have been created. When a relationship is created the user can enter a brief note, and in the **Relationships** table the name of the relationship links to the appropriate page in OV3600. Selecting the snapshot description opens a popup window to display the screenshot. Figure 186 illustrates these GUI tools.

Figure 186 *Relationships and Snapshots on the **Incident Edit** Page*



Incident

Summary:	Matt is seeing Mismatches.
State:	Open
Description:	

On an Access 247 controller.

Relationships

	Name ▲	Notes
□	Controller "Access247"	-
□	Folder "Top"	This is the Top folder.
□	Group "Access Points"	The controller belongs here.

Snapshots

1-1 ▾ of 1 Incident Snapshots Page 1 ▾ of 1 Choose Columns

	Description ▲	Created
□	Snapshot 11	3/3/2010 3:32 PM

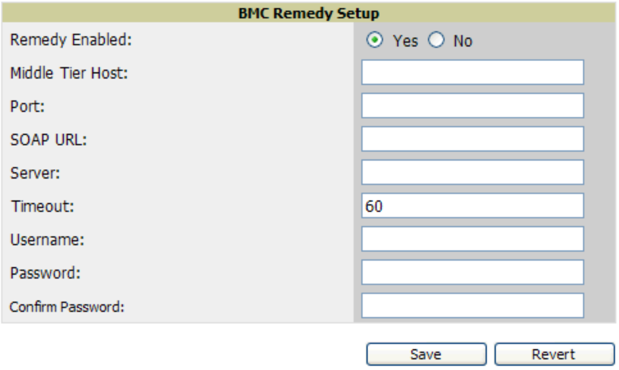
1-1 ▾ of 1 Incident Snapshots Page 1 ▾ of 1

Using the Helpdesk Tab with an Existing Remedy Server

If an external Remedy server exists, you can use the OV3600 **Helpdesk** tab to create, view and edit incidents on the Remedy server. OV3600 can only support integration with a Remedy server if it is a default installation of Remedy 7.0 with no changes to the web service definitions.

To use the Helpdesk tab with a Remedy server, first navigate to the **Helpdesk > Setup** page. In the **BMC Remedy Setup** area, select **Yes** to enable Remedy. This launches a set of fields for information about the Remedy server. Once enabled to use Remedy, the Helpdesk header icons work in the same way for a Remedy-configured Helpdesk as they do for the default OV3600 **Helpdesk**. Figure 187 illustrates this appearance, and Table 140 describes the components. For more details, see "Creating New Snapshots or Incident Relationships" on page 250.

Figure 187 ***Helpdesk > Setup** with Remedy Enabled*



BMC Remedy Setup

Remedy Enabled:	● Yes ○ No
Middle Tier Host:	
Port:	
SOAP URL:	
Server:	
Timeout:	60
Username:	
Password:	
Confirm Password:	

Table 140 *Components of **Helpdesk > Setup** with Remedy Enabled*

Field	Description
Remedy Enabled	If **no** (default) is selected, the existing OV3600 **Helpdesk** functionality is available. If **yes** is selected, the **Helpdesk** functionality is disabled and the **Helpdesk** tab can be configured for use with an existing Remedy server. Fields for server data appear only when Remedy is enabled.

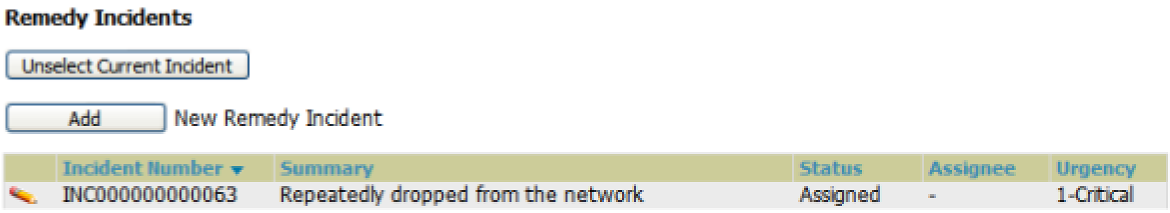
Table 140 *Components of **Helpdesk > Setup** with Remedy Enabled*

Field	Description
Middle Tier Host	The location of the Remedy installation's web server.
Port	The port for the HTTP interface with the web server (this is likely 8080, but there is no default value in OV3600).
SOAP URL	Gateway for web services on Remedy's middle tier host. This is usually arsys/services/ARService, but there is no default value in OV3600.
Server	The location of the backend server where Remedy data is stored.
Timeout	The timeout for HTTP requests (60 seconds by default).
Username	Username for an existing Remedy account; the role of this user defines the visibility OV3600 will have into the Remedy server.
Password and Confirm Password	The password for the Remedy user account.

Once the server settings have been saved and applied, **Helpdesk** features become disabled. OV3600 then displays incident data pulled from the **Remedy** server and push changes back. With the exception of snapshots, OV3600 does not store any Remedy data locally.

To view **Remedy** incidents in OV3600, navigate to the **Helpdesk > Incidents** tab. Figure 188 illustrates the appearance and Table 141 describes the components of this page.

Figure 188 ***Helpdesk > Incidents** with Remedy Enabled*



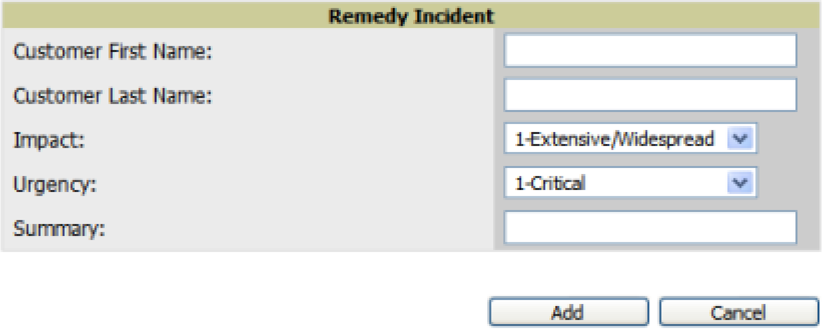
	Incident Number ▾	Summary	Status	Assignee	Urgency
✎	INC000000000063	Repeatedly dropped from the network	Assigned	-	1-Critical

Table 141 ***Helpdesk > Incidents** Components with Remedy Enabled*

Field	Description
Incident Number	Displays a unique identifier for each incident; assigned by the Remedy installation.
Summary	Contains a brief incident summary as entered by OV3600 or Remedy user.
Status	Displays the status as chosen by OV3600 or the Remedy user: ● New ● Assigned ● In Progress ● Pending ● Resolved ● Closed ● Cancelled
Assignee	Assigned by Remedy installation; cannot be changed in OV3600.
Urgency	Displays the urgency level, as chosen by the OV3600 or Remedy User: ● **1** - Critical ● **2** - High ● **3** - Medium ● **4** - Low

To change the current incident in the **Helpdesk** header, select **Unselect Current Incident**. To add a new Remedy incident, select **Add**. To edit an existing Remedy incident, select the pencil icon next to the incident you wish to edit. Refer to Figure 189 and Table 142 for additional illustration and explanation.

Figure 189 ***Helpdesk* > *Incidents* > *Add a New Remedy Incident*** *Page Illustration*



Remedy Incident

Customer First Name:

Customer Last Name:

Impact: 1-Extensive/Widespread

Urgency: 1-Critical

Summary:

Table 142 ***Helpdesk* > *Incidents* > *Add a New Remedy Incident*** *Fields*

Field	Description
Customer First and Last Name	These must match exactly a customer that already exists on the Remedy server. There is no way to create a new customer from OV3600 or to search Remedy customers remotely.
Impact	● 1 - Extensive/Widespread (default) ● 2 - Significant/Large ● 3 - Moderate/Limited ● 4- Minor/Localized
Urgency	● 1 - Critical (default) ● 2 - High ● 3 - Medium ● 4 - Low
Summary	Free-form text field.

NOTE

A new incident is not created if the customer First and Last name do not exist on the Remedy server. However, in this scenario, there is no failure message or warning that the incident was not created.

Once an incident has been created, select the pencil icon in the incident list to edit the information. The status or urgency can be changed as the case progresses, and more detailed information about the incident can be added. Snapshots can also be related to Remedy incidents in the manner described in the Helpdesk section above. However, snapshots are only stored locally on the OV3600 server—they are not pushed to the Remedy server.

Appendix A

Package Management for OV3600

Yum for OV3600

This appendix describes the Yum packaging management system. Alcatel-Lucent recommends running Yum to ensure your packages are up to date, and so that your OV3600 is as secure as possible if you are running RHEL 5 or CentOS 5.

Yum is an automated package management system that verifies OV3600 is running the most recently released RPMs and upgrades any out-of-date packages. Yum accesses the Internet, and downloads and installs new versions of any installed RPMs. It is important to keep the OV3600 RPMs current to close any known security holes in the OS as quickly as possible.

To run Yum on a CentOS 5 machine, follow the instructions below:

1. Before running Yum for the first time, you need to install the GPG key. The GPG key is used to validate the authenticity of all packages downloaded by Yum. To install the GPG key, type **`rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5`**. If the key was not manually installed before Yum is run for the first time, you will be prompted to install and accept a new key.
2. To run Yum manually, log in to the OV3600 console and type **`yum update`** and press **Enter**. If the packages seem to be downloading slowly, press **Ctrl+C** to connect to a new mirror.
3. To configure Yum to run nightly, type **`yum install yum-cron`** and press **Enter**. Then type **`service yum start`** and press **Enter**. Note that yum-cron will default to off if the machine is restarted.
4. To configure yum-cron to start at system startup, type **`chkconfig yum-cron on`** and press **Enter**.
5. In some instances, running Yum may cause a problem with OV3600. If that happens, a good first step is to use SSH to go into the OV3600 server as root, and issue the following command:

   ```
   # root; make
   ```

If that does not resolve the issue, please contact Alcatel-Lucent support.

Appendix B

Third-Party Security Integration for OV3600

This appendix describes the optional integration of third party security products for OV3600, as follows:

- "Bluesocket Integration" on page 257
- "ReefEdge Integration" on page 257
- "HP ProCurve 700wl Series Secure Access Switches Integration" on page 258

Bluesocket Integration

A Bluesocket security scheme for OV3600 has the following prerequisites:

- Bluesocket version 2.1 or higher
- OV3600 version 1.8 or higher
- Completion of **OV3600 Setup > RADIUS Accounting** page

Bluesocket Configuration

Perform these steps to configure a Bluesock security scheme:

1. Log in into the Bluesocket Server via HTTP with proper user credentials.
2. Navigate to the **Users > External Accounting Servers** page.
3. Select **External RADIUS Accounting** from the **Create** drop-down list.
4. Select **Enable server** onscreen.
5. Enter the user-definable **Name** for the OV3600 server.
6. Enter the **Server IP Address** or **DNS entry** for OV3600.
7. Accept the default Port setting of 1813.
8. Enter the **Shared Secret** (matching the OV3600 shared secret).
9. Enter Notes (optional).
10. Select **Save**.
11. If you are using an External LDAP Server, ensure that the accounting records are forwarding to OV3600 upon authentication.
12. Navigate to **Users > External Authentication Servers**.
13. Modify the LDAP server.
14. Ensure under the Accounting server matches the server entered in step 5.
15. Select **Save**.
16. To verify and view the log files on the Bluesocket server, proceed to **Status > Log**.
17. To verify and view the log files on OV3600, proceed to **System > Event Log**.

ReefEdge Integration

A ReefEdge security scheme for OV3600 has the following prerequisites:

- ReefEdge version 3.0.3 or higher

- OV3600 version 1.5 or higher
- Completion of the **OV3600 Setup > Radius Accounting** page configurations, as described in "Integrating a RADIUS Accounting Server" on page 55.

ReefEdge Configuration

Perform these steps to configure a ReefEdge security scheme:

1. Log in into the ReefEdge ConnectServer via HTTP with the proper user credentials.
2. Navigate to the **Connect System > Accounting** page.
3. Select **Enable RADIUS Accounting**.
4. Enter the Primary Server IP Address or DNS entry for OV3600 server.
5. Enter Primary Server Port Number 1813.
6. Enter the Shared Secret (matching the OV3600 shared secret).
7. To verify and view the log files on the **Connect Server** proceed to **Monitor > System Log**.
8. To verify and view the log files on OV3600, proceed to **System > Event Log**.

HP ProCurve 700wl Series Secure Access Switches Integration

A ProCurve security scheme for OV3600 has the following prerequisites:

- HP 700 version 4.1.1.33 or higher
- OV3600 version 3.0.4 or higher
- Completion of the **OV3600 Setup > Radius Accounting** page configurations, as described in "Integrating a RADIUS Accounting Server" on page 55.

Example Network Configuration

In this example, the APs are connected to the Access Switch. The Access Switch routes wireless user traffic to the Employee Network, while bridging AP management traffic. Each AP is presumed to have a static IP address.

Perform these steps for HP ProCurve 700wl Series Configuration, allowing OV3600 to manage APs through **Control** pages.

1. Log in to the Access Control Server via HTTP with proper credentials.
2. Navigate to **Rights > Identity Profiles**.
3. Select **Network Equipment**.
4. Enter the **Name**, **LAN MAC** and ensure the device is identified as an **Access Points in the Identity Profile** section for all access points in the network.

   The Access Points Identity Profile is the default profile for network equipment. Enabling this option instructs the Access Switch to pass management traffic between the Access Points and the Customer's wired network.

HP ProCurve 700wl Series Configuration

This procedure enables the sending of client authentication information to OV3600. Perform the following steps to enable this configuration.

1. Log in to the Access Control Server via HTTP with proper credentials.
2. Navigate to the **Rights > Authentication Policies** configuration page.
3. Select **Authentication Services**.

4. Select **New Services**.
5. Select **RADIUS**.
6. Enter **Name - Logical Name.**
7. Enter **Server** - **OV3600 IP Address.**
8. Enter **Shared Secret**.
9. Enter **Port** - **1812**.
10. Enter the **Shared Secret** and **Confirm** (matching the OV3600 shared secret).
11. Enter **Reauthentication Field** - **Session Timeout**.
12. Enter **Timeout** - **5.**
13. Select the **Enable RADIUS Accounting RFC-2866** check box.
14. Enter **Port** - **1813** for RFC-2866.
15. To verify and view the log files on OV3600, proceed to **System > Event Log**.

Appendix C

Access Point Notes

This appendix contains a few additional notes relevant to Cisco devices monitored by OV3600, and includes the following sections:

- "Resetting Cisco (VxWorks) Access Points" on page 261
- "Cisco IOS Dual Radio Template" on page 263
- "Speed Issues Related to Cisco IOS Firmware Upgrades" on page 264

Resetting Cisco (VxWorks) Access Points

When using any WLAN equipment, it may sometimes be necessary to recover a password and/or to restore the default settings on the equipment. Unlike other access points, the Cisco Aironet hardware and software sometimes do not permit password recovery. In these instances, you may need to first return the equipment to its default state, from which it can then be reconfigured.

For any Cisco VxWorks AP, regardless of the software version being used, you must first connect to the AP via the serial console and then perform the required steps to reset the unit.

Note that Cisco changed the procedure for resetting the AP configuration beginning with software version 11.07. The procedure below helps you determine which software version your AP(s) is currently running and which procedure to use to reset the AP.

Connecting to the AP

Perform these steps to return VxWorks Access Points to their default state and to reset the unit.

1. Connect the COM 1 or COM 2 port on your computer to the RS-232 port on the AP, using a straight-through cable with 9-pin-male to 9-pin-female connectors.
2. Open a terminal-emulation program on your computer.

NOTE

The instructions below assume that you are using Microsoft HyperTerminal; other terminal emulation programs are similar but may vary in certain minor respects.

3. Go to the **Connection Description** window, enter a name and select an icon for the connection, and select **OK**.
4. Go to the **Connect To window** field, and use the pull-down menu to select the port to which the cable is connected, then select **OK**.
5. In the Port Settings window, make the following settings:
   - Bits per second (baud): 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow Control: Xon/Xoff
6. Click **OK**.
7. Press **Enter**.

Determining the Boot-Block Version

The subsequent steps that you must follow to reset the Cisco AP depend on the version of the AP's boot-block. Follow the steps below to determine which boot-block version is currently on your AP, then use the corresponding instructions detailed below.

When you connect to the AP, the Summary Status screen appears. Reboot the AP by pressing CTRL-X or by unplugging and then re-plugging the power connector. As the AP reboots, introductory system information will appear onscreen.

The boot-block version appears in the third line of this text and is labeled Bootstrap Ver.

```
System ID: 00409625854D
Motherboard: MPC860 50MHz, 2048KB FLASH, 16384KB DRAM, Revision 20
Bootstrap Ver. 1.01: FLASH, CRC 4143E410 (OK)
Initialization: OK
```

Resetting the AP (for Boot-Block Versions from 1.02 to 11.06)

Follow these steps to reset your AP if the boot-block version on your AP is greater than or equal to version 1.02 but less than 11.07:

1. If you have not done so already, connect to the AP (see above), select **OK**, and press **Enter**.
2. When the **Summary Status** screen appears, reboot the AP by pressing **CTRL-X** or by unplugging and then re-plugging the power connector.
3. When the memory files are listed under the heading Memory: File, press **CTRL-W** within five seconds to reach the boot-block menu.
4. Copy the AP's installation key to the AP's DRAM by performing the following steps:
   - Press **C** to select **Copy File**.
   - Press **1** to select **DRAM**.
   - Press the selection letter for AP Installation Key.
5. Perform the following steps to reformat the AP's configuration memory bank:
   - Press **CTRL-Z** to reach the Reformat menu.
   - Press ! (**SHIFT-1**) to select **FORMAT Memory Bank**.
   - Press **2** to select **Config**.
   - Press upper-case **Y** (**SHIFT-Y**) to confirm the **FORMAT** command.
   - Press **CTRL-Z** to reach the reformat menu and to reformat the AP's configuration memory bank.
6. Copy the installation key back to the configuration memory bank as follows:
   - Press **C** to select Copy file
   - Press **2** to select Config.
   - Press the selection letter for AP Installation Key.
7. Perform the following steps to run the AP firmware:
   - Press **R** to select Run
   - Select the letter for the firmware file that is displayed.

   The following message appears while the AP starts the firmware: `Inflating` *`<firmware file name>`*.
8. When the **Express Setup** screen appears, begin reconfiguring the AP using the terminal emulator or an Internet browser.

Resetting the AP (for Boot-Block Versions 11.07 and Higher)

Follow these steps to reset your AP if the boot-block version on your AP is greater than 11.07:

1. If you have not done so already, connect to the AP (see above), select **OK**, and press **Enter**.
2. When the **Summary Status** screen appears after you have connected to the AP, reboot the AP by unplugging and then re-plugging the power connector.
3. When the AP reboots and the **Summary Status** screen reappears, type **`:resetall`** and press **Enter**.
4. Type **yes**, and press **Enter** to confirm the command.

NOTE

The :resetall command is valid for only two minutes after the AP reboots. If you do not enter and confirm the:resetall command during that two minutes, reboot the AP again.

5. After the AP reboots and the **Express Setup** screen appears, reconfigure the AP by using the terminal emulator or an Internet browser.

Cisco IOS Dual Radio Template

A dual-radio Cisco IOS AP template is included as reference.

```
! Template created from Cisco Aironet 1240 IOS 12.3(11)JA1 'newName'
!  at 2/12/2007 10:14 AM by user 'admin'
<ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push>

version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname %hostname%
enable secret 5 $1$ceH2$/1BN2DQpOoBAz/KI2opH7/
ip subnet-zero
ip domain name Alcatel-Lucent.com
ip name-server 10.2.24.13
no aaa new-model
dot11 ssid OpenSSID
   authentication open
power inline negotiation prestandard source
username newpassword password 7 05050318314D5D1A0E0A0516
username Cisco password 7 01300F175804
bridge irb
interface Dot11Radio0
 %enabled%
 no ip address
 no ip route-cache
 ssid OpenSSID
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 channel %channel%
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
%if interface=Dot11Radio1%
interface Dot11Radio1
 no ip address
 no ip route-cache
 %enabled%
 ssid OpenSSID
 dfs band 3 block
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 channel %channel%
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
%endif%
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
interface BVI1
%if ip=dhcp%
 ip address dhcp client-id FastEthernet0
%endif%
%if ip=static%
 ip address %ip_address% %netmask%
%endif%
 no ip route-cache
%if ip=static%
ip default-gateway %gateway%
%endif%
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
access-list 111 permit tcp any any neq telnet
snmp-server view iso iso included
snmp-server community public view iso RW
control-plane
bridge 1 route ip
line con 0
line vty 0 4
 login local
end
```

Speed Issues Related to Cisco IOS Firmware Upgrades

OV3600 provides a very robust method of upgrading firmware on APs. To ensure that firmware is upgraded correctly, OV3600 adds a few additional steps which are not included in vendor-supplied management software.

OV3600 Firmware Upgrade Process

1. OV3600 reads the firmware version on the AP to ensure the firmware to which the AP is upgrading is greater than the actual firmware version currently running on the AP.
2. OV3600 configures the AP to initiate the firmware download from OV3600.
3. OV3600 monitors itself and the AP during the file transfer.
4. After a reboot is detected, OV3600 verifies the firmware was applied correctly and all AP configuration settings match those in the OV3600 database
5. OV3600 pushes the configuration if necessary to restore the desired configuration. Some firmware upgrades reconfigure settings.

Cisco IOS access points take longer than most access points because their firmware is larger.

Appendix D

Initiating a Support Connection

The Support Connection Manager establishes a secure point-to-point connection between the customer OV3600 and Alcatel-Lucent's support organization. Using this secure connection, Alcatel-Lucent support engineers can remotely diagnose problems or upgrade software without breaching security and exposing OV3600 to the Internet.

This appendix includes the following sections:

- "Network Requirements" on page 265
- "Procedure" on page 265

Network Requirements

The OV3600 Support Connection initiates a TCP connection on port 23 to Alcatel-Lucent's support server. Please ensure your firewall allows this. The connection can be configured to run on 22, 80, 443 and a few other ports if necessary. Please contact Alcatel-Lucent support if you need to make any changes.

CAUTION

Initiating the support connection will create a point to point tunnel between OV3600 and a support server at Alcatel-Lucent.

Procedure

Perform these steps to initiate a support connection for OV3600:

1. Sign into the serial or regular console with your root login.
2. Type **service support_connection start** at the command line interface.
3. Type **service support_connection status** to verify that the connection is running properly.
4. To end the connection to support, type **service support_connection stop** at the command line interface.

If you have any questions, please contact Alcatel support.

Appendix E

Cisco Clean Access Integration (Perfigo)

This appendix includes the following sections:

Prerequisites for Integrating OV3600 with Cisco Clean Access

- Run Clean Access Software 3.5 or higher
- Run OV3600 version 3.4.0 or higher
- Complete the **OV3600 Setup > RADIUS Accounting** section on OV3600.

Adding OV3600 as RADIUS Accounting Server

Perform these steps to configure Cisco Clean Access integration:

1. Log in to the clean machine server and navigate to the **User Management > Accounting > Server Config** page.
   - Select **Enable RADIUS Accounting**.
   - Input the **OV3600 Hostname** or **IP Address**.
   - For Timeout (sec) - leave default **30**.
   - Ensure the Server Port is set for **1813**.
   - Ensure that the input Shared Secret matches the OV3600 shared secret.
2. Select **Update** to save.

Configuring Data in Accounting Packets

1. Navigate to **User Management > Accounting > Shared Events**.
2. Map the following attributes to corresponding data elements:

```
Framed_IP_Address = "User IP"
User_Name = "LocalUser"
Calling_Station_ID = "User MAC"
```

NOTE

These attribute element pairs are mandatory for username display within OV3600.

Appendix F

HP Insight Install Instructions for OV3600 Servers

To install HP/Compaq Insight Manager on the OV3600, perform the following steps:

1. Use SCP to move the two files over to the server:

- `hpasm-7.8.0-88.rhel4.i386.rpm` <- The actual HP agents
- `hpsmh-2.1.9-178.linux.i386.rpm` <- The HP web portal to the agents

2. Enter **`rpm -i hpasm-7.8.0-88.rhel4.i386.rpm`** at the command line interface.
3. Enter **`hpasm activate`**.

   Take the default values. You will need the SNMP RW and RO strings at this point.
4. Enter **`rpm -i --nopre hpsmh-2.1.9-178.linux.i386.rpm`** at the command line interface. The **`nopre`** syntax component is required to keep the RPM from producing errors on CentOS, as opposed to Red Hat. This rpm *must* be run after the hpasm RPM because the pre-install scripts in the hpsmh RPM are not being run.
5. Enter **`perl /usr/local/hp/hpSMHSetup.pl`**.

   This configures the web server.

   Configure the **Add Group > Administrator** page with a name '**`0`**'.

   Enable IP Binding—type **`1`**.

   At the next interface, enter the IP address and mask of the server.
6. Enter **`/etc/init.d/hpasm reconfigure`**.

   When going through this menu this time, select '**`y`**' to use the existing snmpd.conf.
7. Enter **`vi /etc/snmp/snmpd.conf`**.

   Change the following two lines:

   ```
   rwcommunity xxxstringxxx 127.0.0.1
   rocommunity xxxstringxxx 127.0.0.1
   ```

   Change these lines to read as follows:

   ```
   rwcommunity xxxstringxxx
   rwcommunity xxxstringxxx
   ```
8. Enter **`service snmpd restart`**.
9. Enter **`user add xxusernamexx`**.
10. Enter **`passwd xxusernamexx`** and enter a password for the user.
11. Enter **`vi /etc/passwd`**.

    Scroll to the bottom of the list and change the new users UID and GroupID to **`0`** (fourth and fifth column).
12. Connect to the server using `https://xxx.xxx.xxx.xxx:2381` and the username and password that you created in steps 9 and 10.

Appendix G

Installing OV3600 on VMware ESX (3i v. 3.5)

This appendix provides complete instructions for installing OV3600 on VMware ESX (3i v. 3.5) and includes the following sections:

- "Creating a New Virtual Machine to Run OV3600" on page 271
- "Installing OV3600 on the Virtual Machine" on page 271
- "OV3600 Post-Installation Issues on VMware" on page 272

Creating a New Virtual Machine to Run OV3600

1. Select **Create a new virtual machine** from the VMware Infrastructure Client.
2. Select **Next** to select a **Typical > Virtual Machine Configuration**.
3. Name your virtual machine (OV3600) and then click **Next**.
4. Select an available datastore with sufficient space for the number of APs your OV3600 will manage, choosing the right server hardware to comply with the hardware requirements in this document. Select **Next**.
5. Select the **Linux** radio button and select **Red Hat Enterprise Linux 5 (32-bit)** from the drop-down menu, then click **Next**.
6. Select a minimum of two virtual processors, then click **Next**.
7. Enter **3072** as the minimum virtual RAM (more virtual RAM may be required; refer to the section "Choosing the Right Server Hardware" for a table listing RAM requirements for OV3600). Select **Next**.
8. Accept the VMware default virtual network adapter and click **Next**.
9. Allocate a virtual disk large enough to contain the OV3600 operating system, application and data files (refer to the OV3600 Best Practices Guide for suggested disk space allocations for typical wireless network deployments).
10. Select **Next**.
11. Review the virtual machine settings, then click **Finish** when done.

Installing OV3600 on the Virtual Machine

Running OV3600 installation on a VMware virtual machine is typically done in one of three ways:

1. By writing an OV3600 ISO to CD, inserting the CD into a physical drive on a VMware server, then configure the OV3600 virtual machine to boot from the CD.
2. By copying the OV3600 ISO to the VMware server's datastore, or to a networked filesystem available to the VMware server, then configure the OV3600 virtual machine to boot from the ISO file.
3. By using either a local physical CD or an OV3600 ISO file from the VMware Infrastructure Client, then create a virtual CD on the virtual OV3600 to point to and boot from that device.

Overall, the second option is likely the most efficient method to install OV3600. In addition, after booting the OV3600 virtual machine with either a physical CD or a ISO image file, the installation process with this method is identical to the steps outlined in the *OmniVista 3600 Air Manager Quick Start Guide.*

OV3600 Post-Installation Issues on VMware

By default, OV3600 runs the Linux 'smartd' service for detecting physical disk errors using the S.M.A.R.T. protocol. However, virtual disks do not support the S.M.A.R.T. protocol, so the OV3600 smartd service will fail at startup.

The service can be prevented from starting at boot by running the following commands at the OV3600 command line. Note that the first command prevents the service from starting, the last two commands remove the smartd service from the list of services to shutdown during a reboot or a complete system shutdown.

```
mv /etc/rc.d/rc3.d/S40smartd /etc/rc.d/rc3.d/Z40smartd
mv /etc/rc.d/rc0.d/K40smartd /etc/rc.d/rc3.d/Z40smartd
mv /etc/rc.d/rc6.d/K40smartd /etc/rc.d/rc3.d/Z40smartd
```

To install VMware Tools on OV3600, perform these steps:

1. From the VMware Infrastructure Client, select **Inventory > Virtual Machine** > **Install/Upgrade VMware Tools**.
2. At the OV3600 console type **mkdir /media/cdrom.**
3. Then type **mount /dev/cdrom /media/cdrom**.
4. Next, type c**d /tmp/; tar -xvzf /media/cdrom/VMwareTools-3.5.0-67921.tar.gz\.**

The VMware Tools filename may be different, depending on the version of VMware installed.

NOTE

Desktop environments such as X Windows, GNOME, and KDE, that you will need to use for VMware tools installation will no longer work once you have OV3600 installed.

5. Run the VMware Tools setup and install script by typing the following statement: **/tmp/vmware-toolsdistrib/vmware-install.pl.**
6. During the text-based VMware Tools install, select all default options.
7. Reboot the virtual machine once the VMware Tools install is complete.

Appendix H

Third-Party Copyright Information

OV3600 contains some software provided by third parties (both commercial and open-source licenses).

Source code to third-party open-source packages are available on Alcatel-Lucent's website and by request:

http://service.esd.alcatel-lucent.com

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Google Earth and the Google Earth icon are the property of Google.

Packages

Net::IP:

Net-SNMP:

OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2004, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Crypt::DES perl module (used by Net::SNMP):

Copyright (C) 1995, 1996 Systemics Ltd (http://www.systemics.com/)

All rights reserved.

This library and applications are FREE FOR COMMERCIAL AND NON-COMMERCIAL USE as long as the following conditions are adhered to.

Copyright remains with Systemics Ltd, and as such any Copyright notices in the code are not to be removed. If this code is used in a product, Systemics should be given attribution as the author of the parts used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Systemics Ltd (http://www.systemics.com/)

THIS SOFTWARE IS PROVIDED BY SYSTEMICS LTD ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR

BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Perl-Net-IP:

Copyright (c) 1999 - 2002 RIPE NCC

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of the author not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS; IN NO EVENT SHALL AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Berkeley DB 1.85:

Copyright (c) 1987, 1988, 1990, 1991, 1992, 1993, 1994, 1996, 1997, 1998 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SWFObject v. 1.5:

Flash Player detection and embed - http://blog.deconcept.com/swfobject/

SWFObject is (c) 2007 Geoff Stearns and is released under the MIT License

mod_auth_tacacs - TACACS+ authentication module:

Copyright (c) 1998-1999 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index