OmniVista 3600 Air Manager (OV3600)

Version 7.0

User Guide

www.alcatel-lucent.com/enterprise
Part Number: 0510710-01

Copyright

© 2010 Alcatel-Lucent. Alcatel, Lucent, Alcatel-Lucent, and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All rights reserved. All other trademarks are the property of their respective owners. While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent a commitment on the part of Alcatel-Lucent.

Contents

Preface 9

Document Organization 9
Text Conventions 10
Contacting Alcatel-Lucent 11

Chapter 1 Introduction to the OmniVisa Air Manager (OV3600) 13

OV3600—A Unified Wireless Network Command Center 13
VisualRF™ 13
RAPIDS™ 13
Integrating OV3600 into the Network and Organizational Hierarchy 14

Chapter 2 Installing OV3600 17

OV3600 Hardware Requirements and Installation Media 17
Installing Linux CentOS 5 (Phase 1) 17
Installing OV3600 Software (Phase 2) 18
Getting Started 18
Step 1: Configuring Date and Time, Checking for Prior Installations 18
Date and Time 18
Previous OV3600 Installations 19
Step 2: Installing OV3600 Software, Including OV3600 20
Step 3: Checking the OV3600 Installation 20
Step 4: Assigning an IP Address to the OV3600 System 20
Step 5: Naming the OV3600 Network Administration System 21
Step 6: Assigning a Host Name to the OV3600 21
Step 7: Changing the Default Root Password 21
Completing the Installation 21
Configuring and Mapping Port Usage for OV3600 22
OV3600 Navigation Basics 23
Status Section 24
Navigation Section 25
Activity Section 27
Help Links in the GUI 27
Common List Settings 27
Buttons and Icons 28
Getting Started with OV3600 30
Completing Initial Login 30

Chapter 3 Configuring OV3600 31

Before You Begin 31
Formatting the Top Header 31
Customizing Columns in Lists 32
Resetting Pagination Records 33
Using the Pagination Widget 34
Using CSV Export for Lists and Reports 35
Defining Graph Display Preferences 35
Customizing the Overview Subtab Display Using Home > Customize Dashboard 36

Setting Severe Alert Warning Behavior 37
Defining General OV3600 Server Settings 38
What Next? 47
Defining OV3600 Network Settings 48
What Next? 49
Creating OV3600 Users 50
What Next? 51
Creating OV3600 User Roles 52
What Next? 54
Enabling OV3600 to Manage Your Devices 54
Configuring Communication Settings for Discovered Devices 55
Loading Device Firmware onto OV3600 (Optional) 59
Overview of the Device Setup > Upload Files Page 59
Loading Firmware Files to OV3600 60
Using Web Auth Bundles in OV3600 62
Configuring TACACS+ and RADIUS Authentication 63
Configuring TACACS+ Authentication 63
What Next? 64
Configuring RADIUS Authentication and Authorization 65
Integrating a RADIUS Accounting Server 66
What Next? 67
Configuring Cisco WLSE and WLSE Rogue Scanning 68
Introduction to Cisco WLSE 68
Configuring WLSE Initially in OV3600 68
Adding an ACS Server for WLSE 69
Enabling Rogue Alerts for Cisco WLSE 69
Configuring WLSE to Communicate with APs 69
Discovering Devices 69
Managing Devices 69
Inventory Reporting 70
Defining Access 70
Grouping 70
Configuring IOS APs for WDS Participation 70
WDS Participation 70
Primary or Secondary WDS 70
Configuring ACS for WDS Authentication 71
Configuring Cisco WLSE Rogue Scanning 71
What Next? 72
Configuring ACS Servers 73
What Next? 74
Integrating OV3600 with an Existing Network Management Solution (NMS) 75
What Next? 76
Auditing PCI Compliance on the Network 76
Introduction to PCI Requirements 76
PCI Auditing in the OV3600 Interface 77
Enabling or Disabling PCI Auditing 78
What Next? 79
Deploying WMS Offload 79
Overview of WMS Offload in OV3600 79
General Configuration Tasks Supporting WMS Offload in OV3600 80
Additional Information Supporting WMS Offload 80
Chapter 4 Configuring and Using Device Groups in OV3600 81
OV3600 Group Overview 83
Viewing All Defined Device Groups 83
Editing Columns on the Groups > List Page and Additional Pages 85

Configuring Basic Group Settings 87
What Next? 95
Configuring Group Security Settings 96
Configuring Group SSIDs and VLANs 99
Adding and Configuring Group AAA Servers 103
Configuring Radio Settings for Device Groups 105
An Overview of Cisco WLC Configuration 112
Accessing Cisco WLC Configuration 112
Navigating Cisco WLC Configuration 112
Configuring WLANs for Cisco WLC Devices 113
Defining and Configuring LWAPP AP Groups for Cisco Devices 115
Viewing and Creating AP Groups 115
Configuring Cisco Controller Settings 116
Configuring Wireless Parameters for Cisco Controllers 116
Configuring Security Parameters and Functions 116
Configuring Management Settings for Cisco Controllers 117
Configuring Group PTMP/WiMAX Settings 118
Configuring Proxim Mesh Radio Settings 123
Configuring Group MAC Access Control Lists 125
Specifying Minimum Firmware Versions for APs in a Group 126
Comparing Device Groups 127
Deleting a Group 128
Changing Multiple Group Configurations 128
Modifying Multiple Devices 129
Using Global Groups for Group Configuration 132

Chapter 5 Discovering, Adding, and Managing Devices 135

Device Discovery Overview 135
Discovering and Adding Devices 135
SNMP/HTTP Scanning 136
Adding Networks for SNMP/HTTP Scanning 136
Adding Credentials for SNMP/HTTP Scanning 137
Defining a SNMP/HTTP Scan Set 138
Running a Scan Set 140
What Next? 141
Enabling Cisco Discovery Protocol (CDP) 141
Assigning Devices to OV3600 from APs/Devices > New Page 142
Manually Adding Individual Devices 144
Adding Devices with the Device Setup > Add Page 144
Adding Multiple Devices from a CSV File 148
Adding Universal Devices 149
Assigning Devices to the Ignored Page 150
Monitoring Devices 151
Viewing Device Monitoring Statistics 151
Understanding the APs/Devices > Monitor Pages for All Device Types 156
Monitoring Data Specific to Wireless Devices 157
Monitoring Data Specific to Wired Devices (Routers and Switches) 163
Understanding the APs/Devices > Interfaces Page 164
What Next? 165
Auditing Device Configuration 166
Using Device Folders (Optional) 167
Configuring and Managing Devices 168
Moving a Device from Monitor Only to Manage Read/Write Mode 168

Configuring AP Settings 169
Configuring Device Interfaces for Cisco Catalyst Switches 176
Configuring Cisco Router and Switch Interface Settings 179
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 185. 179
Individual Device Support and Firmware Upgrades 179
Troubleshooting a Newly Discovered Device with Down Status 182

Chapter 6 Creating and Using Templates 185

Group Templates 186
Supported Device Templates 186
Template Variables 186
Viewing and Adding Templates 187
Configuring General Template Files and Variables 191
Configuring General Templates 191
IOS Configuration File Template: 192
Device Configuration File on APs/Devices > Audit Configuration Page 192
Using Template Syntax 193
Using Directives to Eliminate Reporting of Configuration Mismatches 193
Using Conditional Variables in Templates 194
Using Substitution Variables in Templates 194
Using AP-Specific Variables 195
Configuring Cisco IOS Templates 196
Applying Startup-config Files 196
WDS Settings in Templates 196
SCP Required Settings in Templates 197
Supporting Multiple Radio Types via a Single IOS Template 197
Configuring Single and Dual-Radio APs via a Single IOS Template 198
Configuring Cisco Catalyst Switch Templates 198
Configuring Symbol Controller / HP WESM Templates 198
Configuring Clustering and Redundancy 200
Changing Redundancy Configuration 201
Adding Clustering Members 201
Configuring a Global Template 202

Chapter 7 Using RAPIDS and Rogue Classification 205

Overview Tab 205
List 207
Viewing Ignored Rogue Devices 210
Using RAPIDS Workflow to Process Rogue Devices 211
RAPIDS Setup 211
Basic Configuration 211
Containment Options 212
Additional Settings 213
RAPIDS Rules 214
Controller Classification with WMS Offload 214
Device OUI Score 215
Rogue Device Threat Level 215
Viewing and Configuring RAPIDS Rules 215
Deleting or Editing a Rules 219
Recommended RAPIDS Rules 219
Using RAPIDS Rules with Additional OV3600 Functions 219
Score Override 220
Audit Log 221

Additional Rogue Device Resources 221
Additional Security-Related Topics 221

Chapter 8 Performing Daily Administration in OV3600 223

Creating and Using Triggers and Alerts 224
Overview of Triggers and Alerts 224
Viewing Triggers 224
Creating New Triggers 224
Setting Triggers for Devices 227
Setting Triggers for Radios 228
Setting Triggers for Discovery 230
Setting Triggers for Users 231
Setting Triggers for RADIUS Authentication Issues 233
Setting Triggers for IDS Events 234
Setting Triggers for OV3600 Health 235
Delivering Triggered Alerts 235
Viewing Alerts 236
Responding to Alerts 237
Monitoring and Supporting WLAN Users 238
Overview of the Users Pages 238
Monitoring WLAN Users With the Users > Connected and Users > All Pages 239
Supporting Guest WLAN Users With the Users > Guest Users Page 241
Supporting Users on Thin AP Networks With the Users > Tags Page 244
Evaluating and Diagnosing User Status and Issues 245
Evaluating User Status with the Users > User Detail Page 245
Using the Deauthenticate User Feature 246
Evaluating User Status with the Users > Diagnostics Page 246
Introduction and Overview of the Diagnostics Page 246
Supporting OV3600 Stations with the Master Console 250
Adding a Managed OV3600 with the Master Console 250
Monitoring and Supporting OV3600 with the Home Pages 252
Monitoring OV3600 with the Home > Overview Page 252
Viewing and Updating License Information with the Home > License Page 255
Searching OV3600 with the Home > Search Page 256
Accessing OV3600 Documentation with the Home > Documentation Page 257
Configuring Your Own User Information with the Home > User Info Page 258
Monitoring and Supporting OV3600 with the System Pages 259
Using the System > Status Page 260
Using the System > Event Logs Page 261
Using the System > Configuration Change Jobs Page 262
Using the System > Performance Page 263
Upgrading OV3600 265
Upgrade Instructions 265
Upgrading Without Internet Access 265
Backing Up OV3600 266
Overview of Backups 266
Viewing and Downloading Backups 266
Running Backup on Demand 266
Restoring from a Backup 266
OV3600 Failover 267
Navigation Section of OV3600 Failover 267
Adding Watched OV3600 Stations 267

Chapter 9 Creating, Running, and Emailing Reports 269

Overview of OV3600 Reports 269
Reports > Definitions Page Overview 269
Reports > Generated Page Overview 271

Using Daily Reports 272
Viewing Generated Reports 272
Using Custom Reports 273
Using the Capacity Planning Report 274
Using the Configuration Audit Report 275
Using the Device Summary Report 276
Using the Device Uptime Report 279
Using the IDS Events Report 280
Using the Inventory Report 281
Using the Memory and CPU Usage Report 282
Using the Network Usage Report 284
Using the New Rogue Devices Report 285
Using the New Users Report 287
Using the PCI Compliance Report 288
Using the Port Usage Report 289
Using the RADIUS Authentication Issues Report 291
Using the Rogue Containment Audit Report 292
Using the User Session Report 292
Defining Reports 296
Emailing and Exporting Reports 299
Emailing Reports in General Email Applications 299
Emailing Reports to Smarthost 300
Exporting Reports to XML or CSV 300
Transferring Reports Using FTP 300

Chapter 10 Using the OV3600 Helpdesk 301
OV3600 Helpdesk Overview 301
Monitoring Incidents with Helpdesk 302
Creating a New Incident with Helpdesk 303
Creating New Snapshots or Incident Relationships 304
Using the Helpdesk Tab with an Existing Remedy Server 305

Appendix A Package Management for OV3600 309
Yum for OV3600 309
Package Management System Advisories for OV3600 309

Appendix B Third-Party Security Integration for OV3600 311
Bluesocket Integration 311
Bluesocket Configuration 311
ReefEdge Integration 311
ReefEdge Configuration 312
HP ProCurve 700wl Series Secure Access Controllers Integration 312
Example Network Configuration 312
HP ProCurve 700wl Series Configuration 312

Appendix C Access Point Notes 315
Resetting Cisco (VxWorks) Access Points 315
Connecting to the AP 315
Determining the Boot-Block Version 316
Resetting the AP (for Boot-Block Versions from 1.02 to 11.06) 316
Resetting the AP (for Boot-Block Versions 11.07 and Higher) 316
Cisco IOS Dual Radio Template 317
Speed Issues Related to Cisco IOS Firmware Upgrades 318
OV3600 Firmware Upgrade Process 318

Appendix D Initiating a Support Connection 321
Network Requirements 321

Procedure 321

Appendix E Cisco Clean Access Integration (Perfigo) 323

Prerequisites for Integrating OV3600 with Cisco Clean Access: 323

Adding OV3600 as RADIUS Accounting Server 323

Configuring Data in Accounting Packets 323

Appendix F HP Insight Install Instructions for OV3600 Servers 325

Appendix G Installing OV3600 on VMware ESX (3i v. 3.5) 327

Creating a New Virtual Machine to Run OV3600 327

Installing OV3600 on the Virtual Machine 327

OV3600 Post-Installation Issues on VMware 328

Appendix H Third-Party Copyright Information 329

Packages 329

Net::IP: 329

Net-SNMP: 329

Crypt::DES perl module (used by Net::SNMP): 332

Perl-Net-IP: 333

Berkeley DB 1.85: 334

SWFObject v. 1.5: 334

mod_auth_tacacs - TACACS+ authentication module: 334

This preface provides an overview of this guide, a list of all documentation available for OV3600 7.0, including contact information for Alcatel Lucent, and includes the following sections:

- "Document Organization" on page 9
- "Text Conventions" on page 10
- Contacting Alcatel-Lucent

Document Organization

This user guide includes instructions and examples of the graphical user interface (GUI) for installation, configuration, and daily operation of OmniVista Air Manager, Version 7.0. 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 7.0.

Table 1 *Document Organization and Purposes*

Chapter	Description
Chapter 1, “Introduction to the OmniVisa Air Manager (OV3600)”	Introduces and presents the OmniVista Air Manager, Version 7.0, OV3600 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 7.0, 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 7.0.
Chapter 8, “Performing Daily Administration in OV3600”	Describes common daily operations and tools in OV3600 7.0, 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 7.0.
Chapter 10, “Using the OV3600 Helpdesk”	Describes how to use the OV3600 7.0 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 7.0.

Table 1 *Document Organization and Purposes*

Chapter	Description
Appendix C, “Access Point Notes”	Provides guidelines and suggestions for Access Point devices in OV3600.
Appendix D, “Initiating a Support Connection”	Provides instructions about how to create and use a support connection between OV3600 and Alcatel Lucent Wireless 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 7.0 servers.
Appendix G, “Installing OV3600 on VMware ESX (3i v. 3.5)”	Provides instructions for an alternative installation option on VMware ESX for OV3600 7.0.
Appendix H, “Third-Party Copyright Information”	Presents multiple copyright statements from multiple equipment vendors that interoperate with OV3600 7.0.
Index	Provides extensive citation of and links to document topics, with emphasis on the OV3600 7.0 GUI and tasks relating to OV3600 7.0 installation and operation.

Text Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Table 2 *Text Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: • Sample screen output • System prompts • Filenames, software devices, and specific commands when mentioned in the text
`Commands`	In the command examples, this bold font depicts text that you must type exactly as shown.
<*Arguments*>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: `# send <text message>` In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
`[Optional]`	In the command examples, items enclosed in brackets are optional. Do not type the brackets.
`{Item A | Item B}`	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

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

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

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

Indicates a risk of personal injury or death.

Contacting Alcatel-Lucent

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 to the OmniVisa Air Manager (OV3600)

Thank you for choosing the OmniVista Air Manager. 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 Air Manager. This chapter includes the following topics:

- "OV3600—A Unified Wireless Network Command Center" on page 13
- "OV3600 Navigation Basics" on page 23
- "Integrating OV3600 into the Network and Organizational Hierarchy" on page 14

If you have any questions or comments, please contact Alcatel-Lucent Technical support at Esd.support@alcatel-lucent.com.

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

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

- OV3600 wireless network management software
- *VisualRF* location and RF mapping software module
- *RAPIDS* rogue access point detection software module

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

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.

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, help systems, indoor wireless access points, mesh devices, and WiMAX 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 utilizing a variety of protocols.

The power, performance, and usability of the OV3600 solution become more apparent when considering the diverse components within a Wireless LAN. Table 1 itemizes such network components, as an example.

Table 1 *Components of a Wireless LAN*

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 Controller	Used in conjunction with thin APs to coordinate authentication and roaming
NMS	Network Management Systems and Event Correlation (OpenView, Tivoli, and so forth)
RADIUS Auth.	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 authenticated OV3600 administrative users
Routers/Switches	Provide OV3600 with data for user information and AP and Rogue discovery
Help Desk Systems	Remedy EPICOR

Table 1 *Components of a Wireless LAN*

Component	Description
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.

Further flexibility and administrative power include the following benefits:

- 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 give 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 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 22
- "OV3600 Navigation Basics" on page 23
- "Getting Started with OV3600" on page 30

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 Air Manager. OV3600 supports any hardware that is Red Hat Enterprise Linux 5 certified.

OV3600 hardware requirements vary by version. As additional features are added to OV3600, increased hardware resources become necessary. For the most recent hardware requirements, download the *OV3600 Hardware Sizing Guide* from the http://airwave.com/download/docs/70/AWMSSizingGuide.pdf page, or contact Alcatel-Lucent Technical support at Esd.support@alcatel-lucent.com.

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 7.0 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**.

NOTE

When you press Enter, all existing data on the hard drive is erased.

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:
```

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. For more information, see http://kb.airwave.com/?sid=50140000000Merd.

1. Allow the installation process to continue in automatic fashion. 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 automatically reboots and ejects the installation CD.
2. 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 **smp** 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 `./ov3600-install` command.

   Type `./ov3600-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.*

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.

Changing these settings after the installation can cause a loss of graphical data, and you should 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 20. 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)?
```

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

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 have the option of monitoring progress in more detail should you wish to do so:

- To view detailed output from the OV3600 software installer, press **Alt-F9** or **Ctrl-Alt-F9**.
- Pressing **Alt-F1** or **Ctrl-Alt-F1** returns you to the main console.

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, OV3600 Setup --> Network Tab
```

1. Enter the network information.

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:
```

1. 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 message 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 message 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:
```

1. 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.

   Alcatel Lucent recommends keeping this password 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 Lucent Support for instructions on resetting it.

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/OV3600-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 Stations with the Master Console" on page 250 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 2 *OV3600 Protocol and Port Chart*

Port	Type	Protocol	Description	Dataflow Direction	Device Type
21	TCP	FTP	Configure devices and FW distribution	>	Legacy AP (Cisco 4800)
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	HTTP	Firmware upgrades	<	Colubris devices
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

Table 2 *OV3600 Protocol and Port Chart (Continued)*

Port	Type	Protocol	Description	Dataflow Direction	Device Type
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	<	AP 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	<	Aruba/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 follows:

- 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 illustrates these sections.

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

Status Section

The **Status** section provides 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 7.0 introduces 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 259.

The table below describes these elements in further detail.

Table 3 *Status Section Components of the OV3600 Graphical User Interface (GUI)*

Field	Description
New Devices	The number of wireless APs or wireless LAN switches/controllers that have been discovered by OV3600 but not yet managed by network administrators. When you click this link, OV3600 directs you to a page that displays a detailed list of devices awaiting authorization.
Up (Wired, Wireless, and combined**)**	The number of managed, authorized devices that are currently responding to OV3600 requests. When you click this link, OV3600 will direct you to a page that displays a detailed list of all **Up** devices.
Down (Wired, Wireless, and combined)	The number of managed, authorized devices that are not currently responding to OV3600 SNMP requests. When you click this link, OV3600 will direct you to a page that displays 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.
Users	The number of wireless users currently associated to the wireless network via all the APs managed by OV3600. When you click this link, OV3600 directs you to a page that contains a list of users that are associated.
Alerts	Displays the number of non-acknowledged OV3600 alerts generated by user-configured triggers. When you click this link, OV3600 directs you to a page containing 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. However, 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 259.
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 bar is a static navigation bar containing tabs for the main components of OV3600, while the lower bar is context-sensitive and displays the sub-menus for the highlighted tab.

Table 4 *Components and Sub-Menus of the OV3600 Navigation Screen*

Main Tab	Description	Sub-Menus
Home	The **Home** pages provide 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. The **Home > Overview** page provides 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 252.	• 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 301.	• Incidents • Setup

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 81.
	NOTE: Some of the focused sub-menus will not appear for all groups. Focused sub-menus are visible based on the device type field on the **Groups > Basic** page. This sub-menu 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 Sub-Menus
		  ◦ Monitor
		  ◦ Basic
		  ◦ Templates
		  ◦ Security
		  ◦ SSIDs
		  ◦ AAA Servers
		  ◦ Radio
		  ◦ Aruba/Alcatel-Lucent Config
		  ◦ Cisco WLC Config
		  ◦ PTMP/WiMAX
		  ◦ Proxim Mesh
		  ◦ Colubris
		  ◦ MAC ACL
		  ◦ Firmware
		  ◦ Compare (Master Console Only)

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 135.
	NOTE: When specified, device-level settings override the default Group-level settings.
		• List
		• New
		• Up
		• Down
		• Mismatched
		• Ignored
		• Focused Sub-Menus
		  ◦ Manage
		  ◦ Audit
		  ◦ Compliance
		  ◦ Interfaces
		  ◦ Containment Status

Table 4 *Components and Sub-Menus of the OV3600 Navigation Screen (Continued)*

Main Tab	Description	Sub-Menus
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 238.	• 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 269.	• Generated • Definition • Focused Sub-Menus ◦ Details
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 260.	• Status • Event Log • Triggers • Alerts • Configuration Change Jobs • Firmware Upgrade Jobs • Performance
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 54.	• Discover • Add • Communication • Alcatel Lucent/Alcatel Lucent Configuration • 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 31. **NOTE:** The **OV3600 Setup** pages may not be visible, depending on the role and license set in OV3600.	• General • Network • Users • Roles • Authentication • 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 205. **NOTE:** The RAPIDS pages may not be visible, depending on the role and license set in OV3600.	• Overview • Rogue APs • 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*. **NOTE:** VisualRF may not be visible, depending on the role and license set in OV3600.	• Overview • Floor Plans • Campus/Building • Setup • Import

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 clicked, this launches a PDF document with information describing the OV3600 page that is currently displayed.

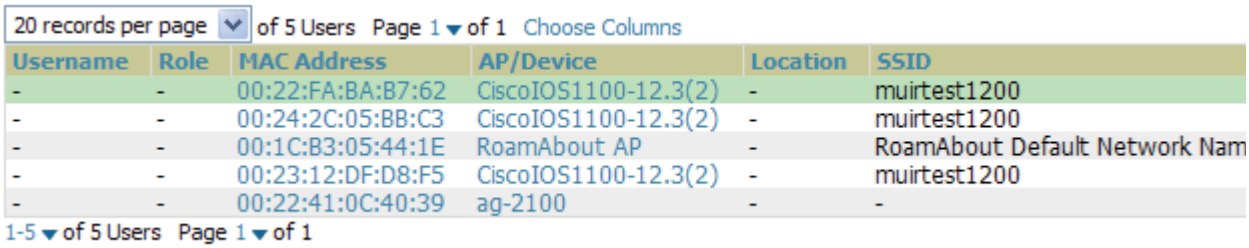
NOTE

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

Common List Settings

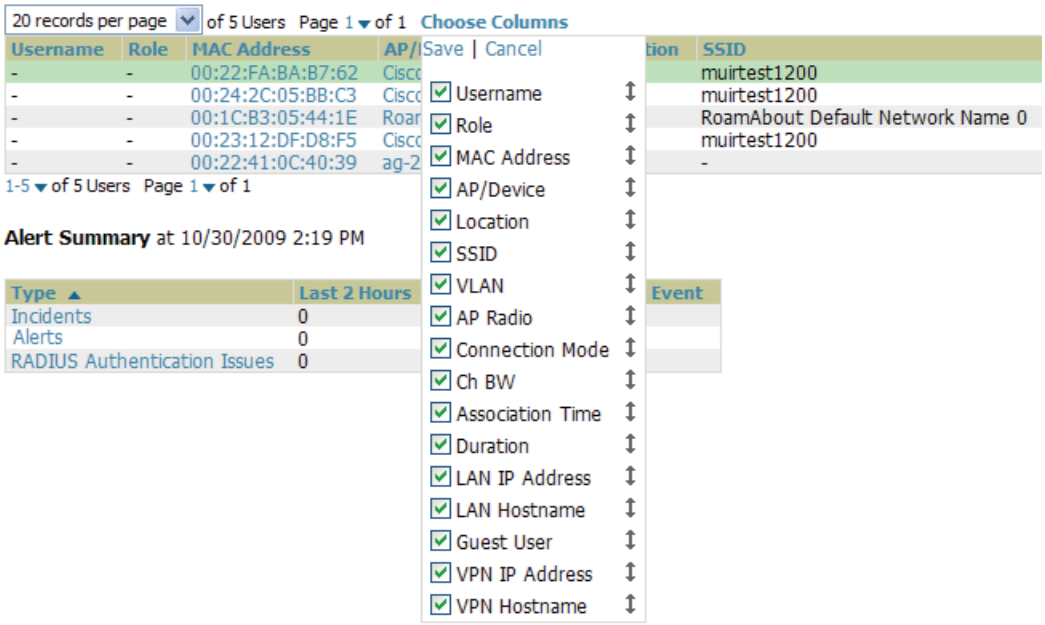
All of the lists in OV3600 have some common options. All lists are paginated with a configurable number of items per page, as shown in Figure 2.

Figure 2 *Example of* **Common List Settings** *Configurable Attributes*



Clicking on the left most down arrow allows you to set how many rows appear on one page of the list. The next down arrow is used to jump to a specific page in the list. Clicking it will bring up a drop down menu that allows you to select the exact page you would like to view, as shown in Figure 3.

Figure 3 **Common List Settings Choose Columns** *Illustration*



The **Choose Columns** option allows you to configure the columns that are presented in the list and the order in which they are presented. To disable a column simply uncheck the checkbox. To reorder the columns,

click and drag a specific row to the appropriate new position. When you are satisfied with the enabled columns and their order, click on the save button.

These settings are user specific. To reset them to the defaults click the **Reset List Preferences** button on the **Home > User Info** page.

Buttons and Icons

Standard buttons and icons are used consistently from screen to screen throughout the OV3600 user pages and GUI, as itemized in the following table:

Table 5 *Standard Buttons and Icons of the OV3600 User Page*

Buttons and Icons	Appearance[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 205 as one example of drag-and-drop.
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).

Table 5 *Standard Buttons and Icons of the OV3600 User Page (Continued)*

Buttons and Icons	Appearance[a]	Description
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 flash 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.
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 flash graphs to the range specified with the time-range bar.
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 Graph in New Window		Displays flash graphs in a new window.
VisualRF		Links to VisualRF - real time visualization.

Table 5 *Standard Buttons and Icons of the OV3600 User Page (Continued)*

Buttons and Icons	Appearance[a]	Description
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. This topic requires successful completion of installation, as described earlier in this chapter. This topic prepares the administrator for wider deployment and device support and operations once initial startup is complete.

Completing Initial Login

Use your browser to navigate to the static IP address assigned to the internal page of the OV3600. Once your session launches, the **Authentication Dialog Box** appears as shown in Figure 4.

Figure 4 *Authentication Dialog Box*

Perform these steps to complete the initial login.

1. Enter User name: **admin**
2. Enter Password: **admin**
3. Click: **OK**

NOTE

OV3600 pages are protected via SSL.

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

NOTE

Alcatel Lucent recommends changing the default login and password on the **OV3600 Setup > Users** page. Refer to the procedure "Creating OV3600 User Roles" on page 52 for additional information.

Chapter 3

Configuring OV3600

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

- "Formatting the Top Header" on page 31
- "Customizing Columns in Lists" on page 32
- "Resetting Pagination Records" on page 33
- "Using the Pagination Widget" on page 34
- "Using CSV Export for Lists and Reports" on page 35
- "Defining Graph Display Preferences" on page 35
- "Customizing the Overview Subtab Display Using Home > Customize Dashboard" on page 36
- "Setting Severe Alert Warning Behavior" on page 37
- "Defining General OV3600 Server Settings" on page 38
- "Defining OV3600 Network Settings" on page 48
- "Creating OV3600 Users" on page 50
- "Creating OV3600 User Roles" on page 52
- "Enabling OV3600 to Manage Your Devices" on page 54
- "Configuring TACACS+ and RADIUS Authentication" on page 63
- "Configuring Cisco WLSE and WLSE Rogue Scanning" on page 68
- "Configuring ACS Servers" on page 73
- "Integrating OV3600 with an Existing Network Management Solution (NMS)" on page 75
- "Auditing PCI Compliance on the Network" on page 76
- "Deploying WMS Offload" on page 79

NOTE

Additional configurations of multiple types are available after basic configuration is complete, as shown in this chapter.

Before You Begin

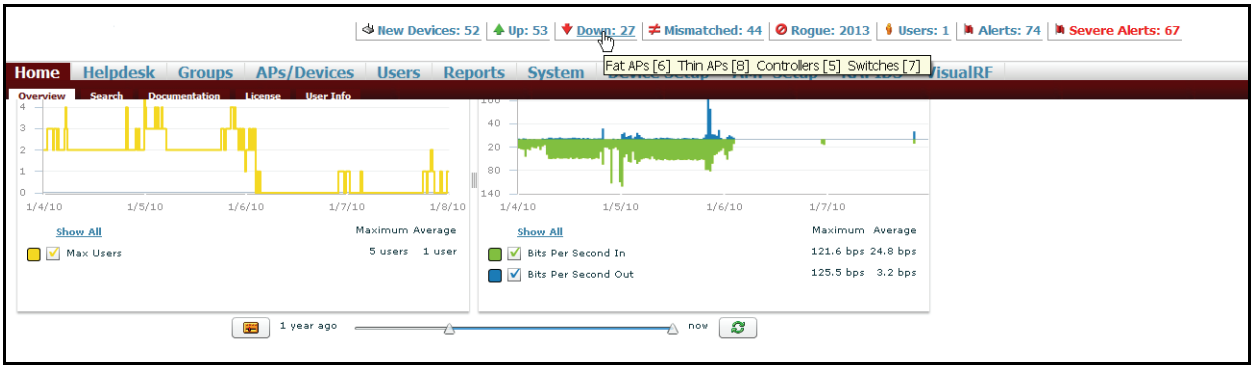
Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document. Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

Formatting the Top Header

The OV3600 interface centers around a horizontal row of tabs corresponding to high level components, with nested subtabs pertaining to relevant information and features within that component. Above the component tabs reside a row of statistics hyperlinks representing many commonly used subtabs. These hyperlinks provide two things: an ability to view certain key statistics by mousing over, such as number and type of **Down** devices (Fat APs, switches for example), and a short cut to certain frequently viewed subtabs. Clicking the Down hyperlink is the same as clicking **APs/Devices > Down**, to use the same example.

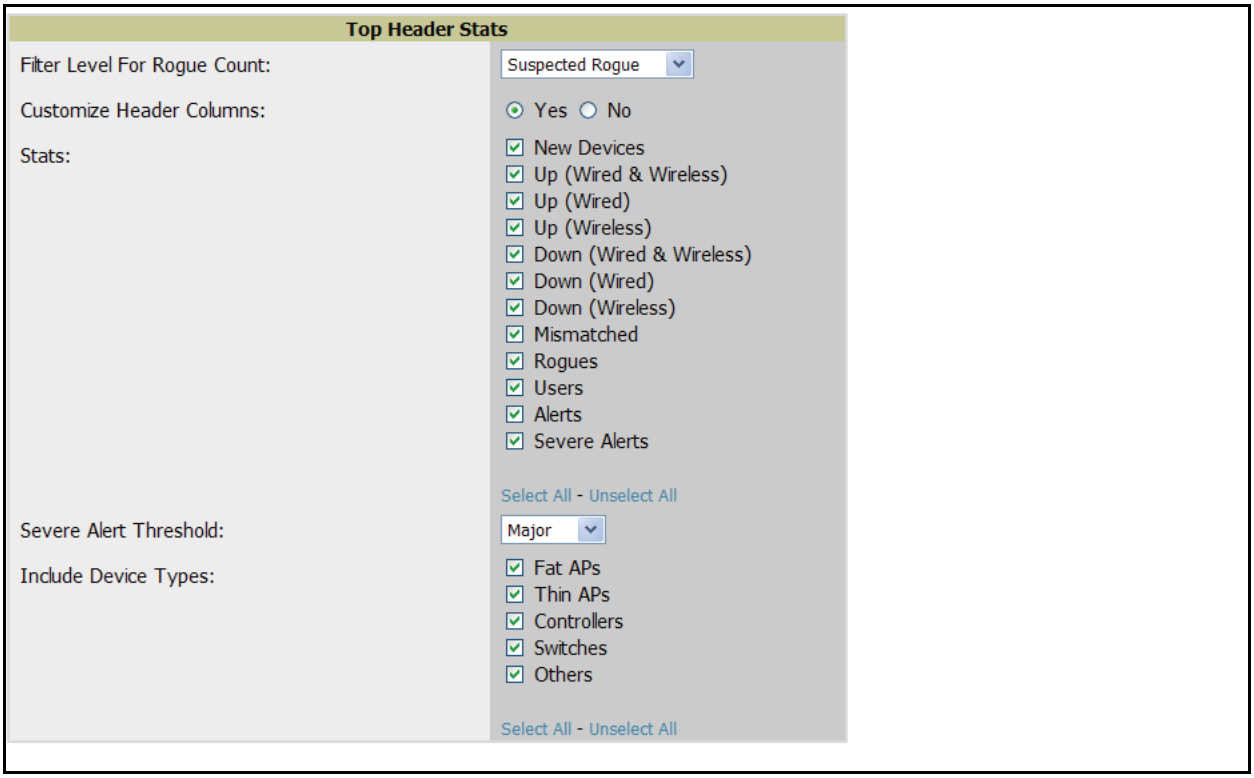
Figure 5 illustrates the navigation bar. For more details on hyperlinks, tabs and submenus, see "OV3600 Navigation Basics" on page 23.

Figure 5 *Navigation Bar Displaying Home Subtabs and* ***Down Device*** *Statistics*



You can control which **Top Header Stats** links appear across the entire product from the **OV3600 Setup > General** page, as described in "Defining General OV3600 Server Settings" on page 38. Top Header Stats hyperlinks can also be customized for individuals, according to individual user roles from the **Home > User Info** page by clicking the **Yes** radio button in the **Top Header Stats** pane. There you can select which statistics are displayed for what device types, and override choices made from the **OV3600 Setup** page. All possible display options are shown in Figure 6, and these fields are described in detail in "Monitoring and Supporting OV3600 with the Home Pages" on page 252.

Figure 6 *Top Header Stats Display Options*



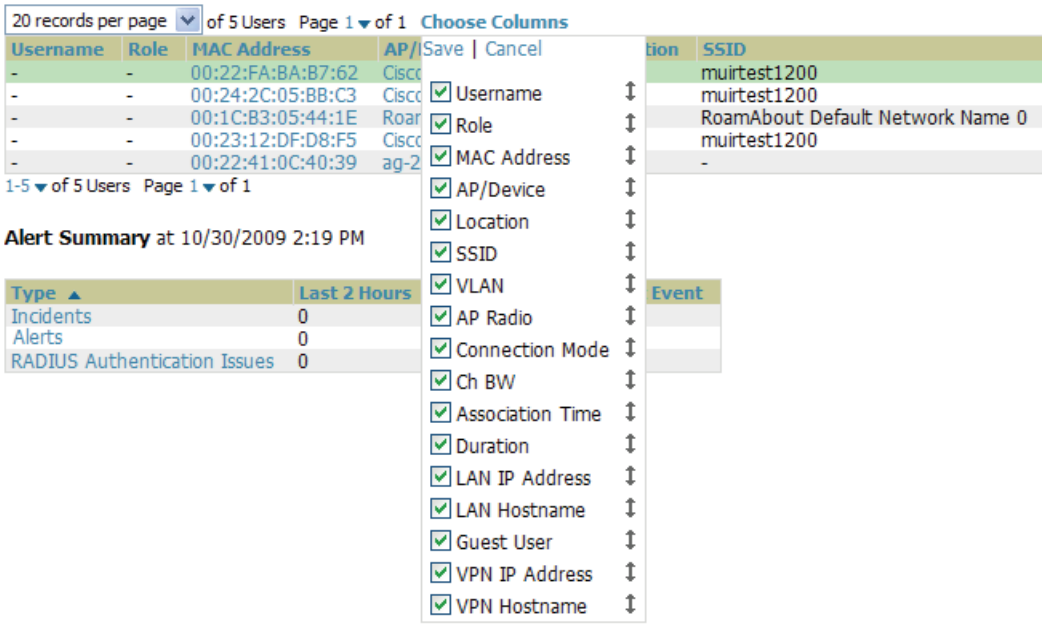
You can also set the severity level of critical alerts displayed for a given user role. For details including a description of what constitutes a severe alert, see "Setting Severe Alert Warning Behavior" on page 37.

Customizing Columns in Lists

You can determine which columns are displayed in any OV3600 table by selecting or deselecting its checkbox from the dropdown list made visible by clicking **Choose Columns** as shown in Figure 7. Using the

up/down arrows to the right of each column title, you can change the order in which the column heads appear with the upper most column in the dropdown list correlating to the left most column in the table. As shown in Figure 7, **Username** if it remains checked will appear as the left most column, **Role** will appear to the right of that, and so on.

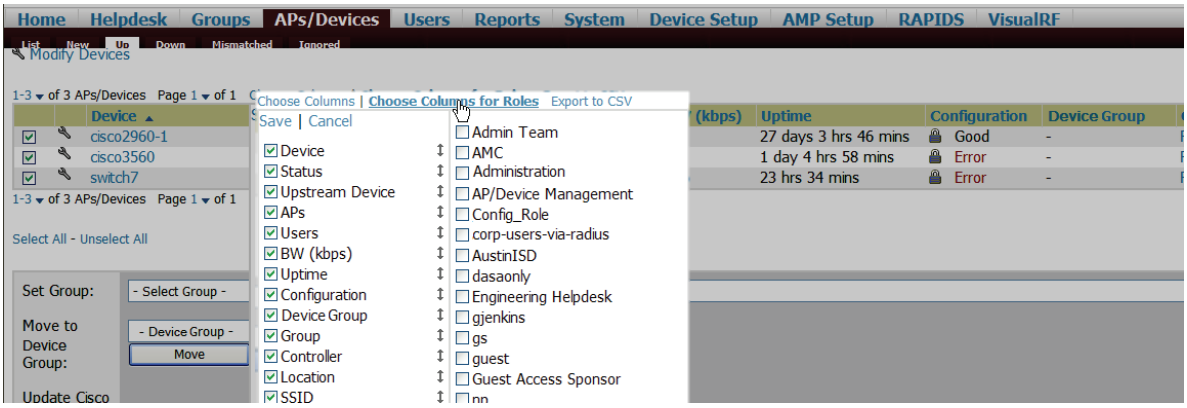
Figure 7 ***Choose Columns*** *Dropdown List*



For more information on the universal list elements, see "Common List Settings" on page 27.

You can also control which column heads appear for each user role by selecting the **Yes** radio button in the **Customize Header Columns** field, as also appears in Figure 6. This exposes the **Choose Columns for Roles** dropdown menu in all tables shown in Figure 8. The right hand column shows the user roles already customized, if any, for your particular production environment. The left hand column allows you to establish left to right columns and order them using the up and down arrows alongside the column head entries. The column heads and user roles displayed are set to their defaults, but can always be customized further, as needed.

Figure 8 *Table With* ***Choose Columns for Roles Menu*** *Selected*

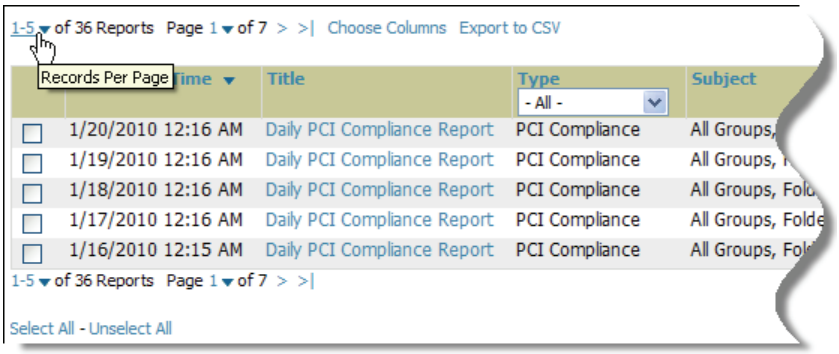


Resetting Pagination Records

You can control how many records appear in any list individually by clicking the link with **Records Per Page** mouseover text at the top left of each table, as shown in Figure 9. OV3600 stores each list's pagination

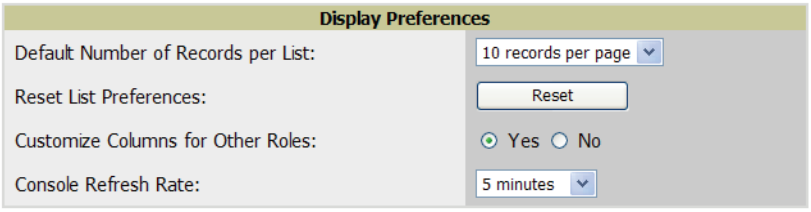
preferences so once you have customized the table (by choosing **Custom** from the **Records Per Page** dropdown menu and entering 5), each time you return to the **Generated Reports** list, it will always show just 5 records at a time, as in this example.

Figure 9 Records Per Page *Drop Down Menu*



If for some reason you would like to reset all OV3600 list Records Per Page preferences, you can select **Reset** in the **Display Preferences** pane of the **Home > User Info** page. The **Display Preferences** pane is shown in Figure 10.

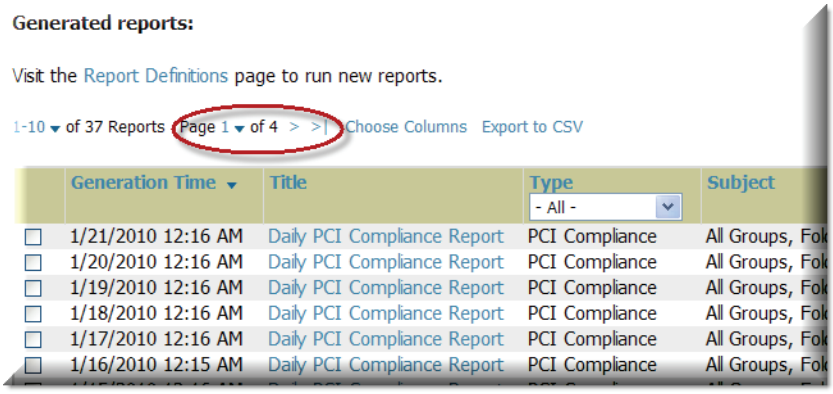
Figure 10 ***Display Preferences*** *Pane*



Using the Pagination Widget

The pagination widget is located at the top and bottom of every list table, as shown in Figure 11.

Figure 11 *Pagination Widget*

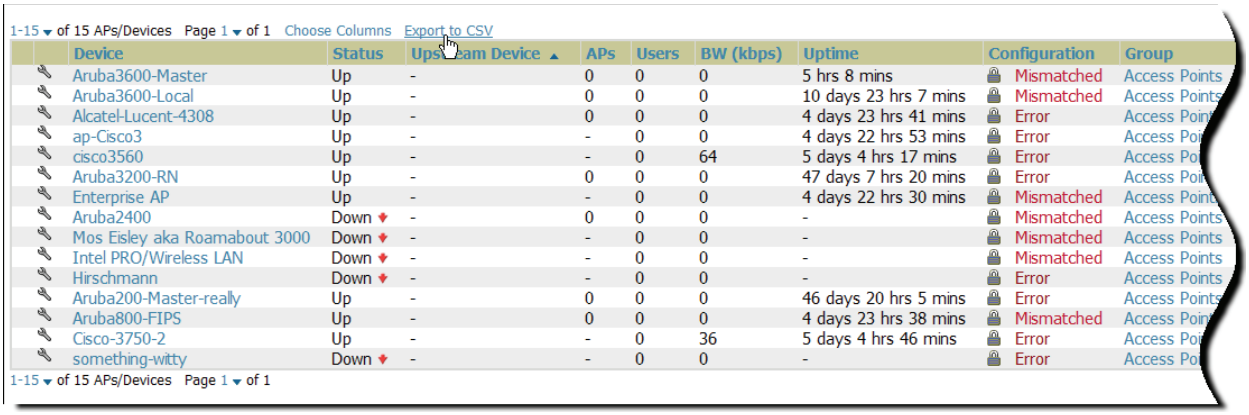


As you mouse over it, you will see **Jump to Page**. Click the down arrow next to where it says **Page 1**, and a dropdown list appears with all the page numbers listed for that table. From here, you can jump to any portion of the table. You can browse the pages of any list table using the right pointing arrows on the outermost sides of the pagination widget. Using the mouseover text as a guide, you can to jump to the next or previous and first or last pages of the table.

Using CSV Export for Lists and Reports

Wherever you see an **Export to CSV** setting above a list, you can export the data shown into a CSV file that you can open as a Microsoft Excel spreadsheet or in any text editor. All vertical and horizontal columns appearing in the table will also appear in the exported data file. See Figure 12 for an example of a list with the **Export to CSV** option selected.

Figure 12 *List with* **Export to CSV** *Selected*

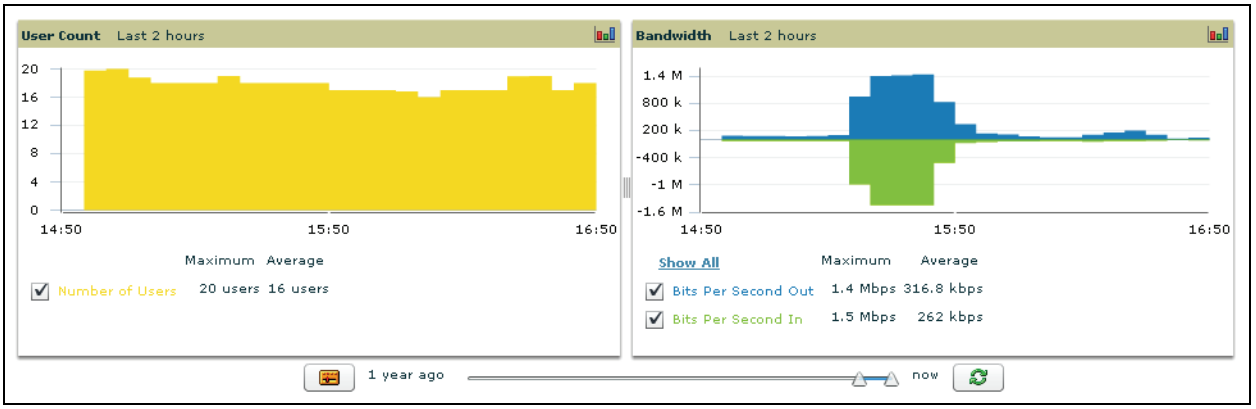


OV3600 also enables CSV exporting of all report types. For more information, see "Using Custom Reports" on page 273.

Defining Graph Display Preferences

Many of the graphs in OV3600 are flash-based, which allows you change graph attributes, as shown in Figure 13.

Figure 13 *Flash Graphs on the* ***Home Overview*** *Page*



This flash-enabled GUI allows for custom settings and adjustments, and the following examples illustrate some changes you can make or functions that are supported:

- 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).

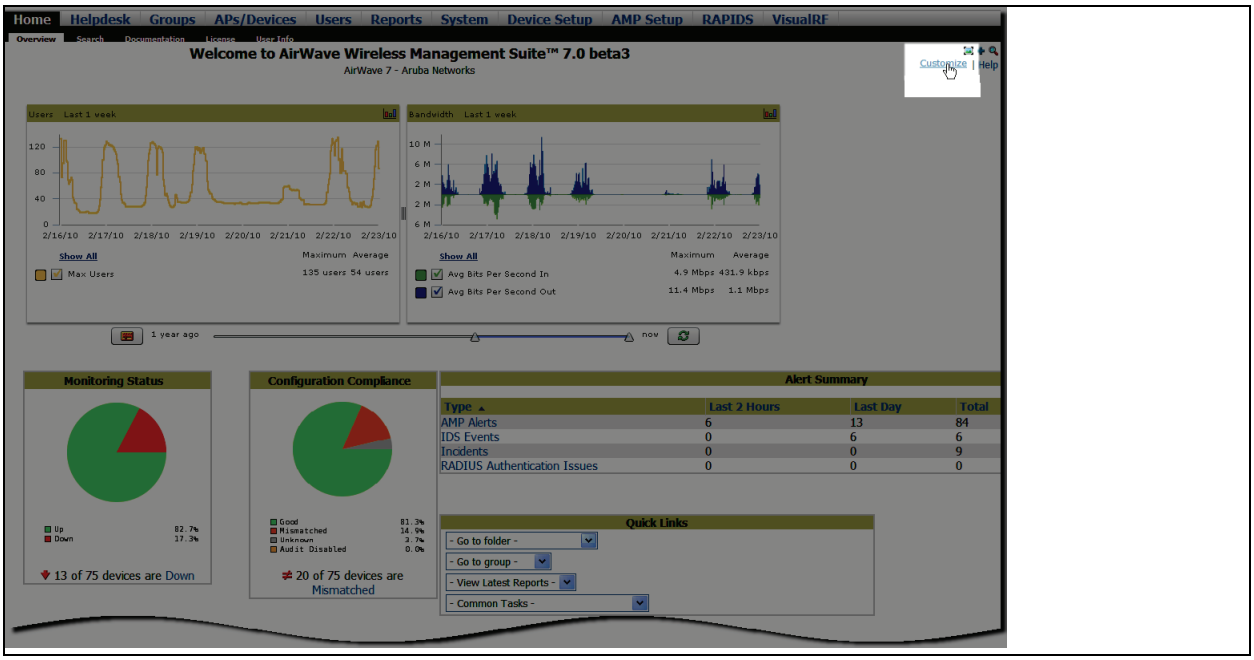
- For non-flash graphs, click the graph to open a popup window that shows historical data.

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 OV3600 through the 5.3 Version. Contact Alcatel Lucent support for more information on activating this feature in the OV3600 database.

Customizing the Overview Subtab Display Using Home > Customize Dashboard

You can rearrange or omit altogether widgets appearing on the **Home > Overview** dashboard by clicking **Customize** to the right of this window, as shown in Figure 14.

Figure 14 *Customize Button on the* ***Home Overview*** *Page*



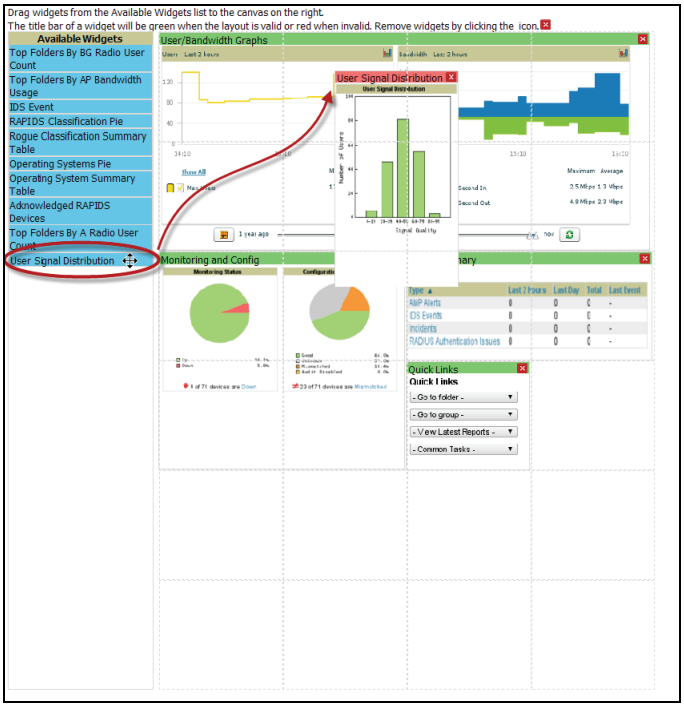
The **Customize** workspace is shown in Figure 15.

Figure 15 **Customize Overview** *Page*

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

Drag the widgets you want to appear on the **Overview** dashboard across to the gridlines and arrange them in the right pane, 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, as shown in Figure 16.

Figure 16 *Example of Improper Widget Placement*



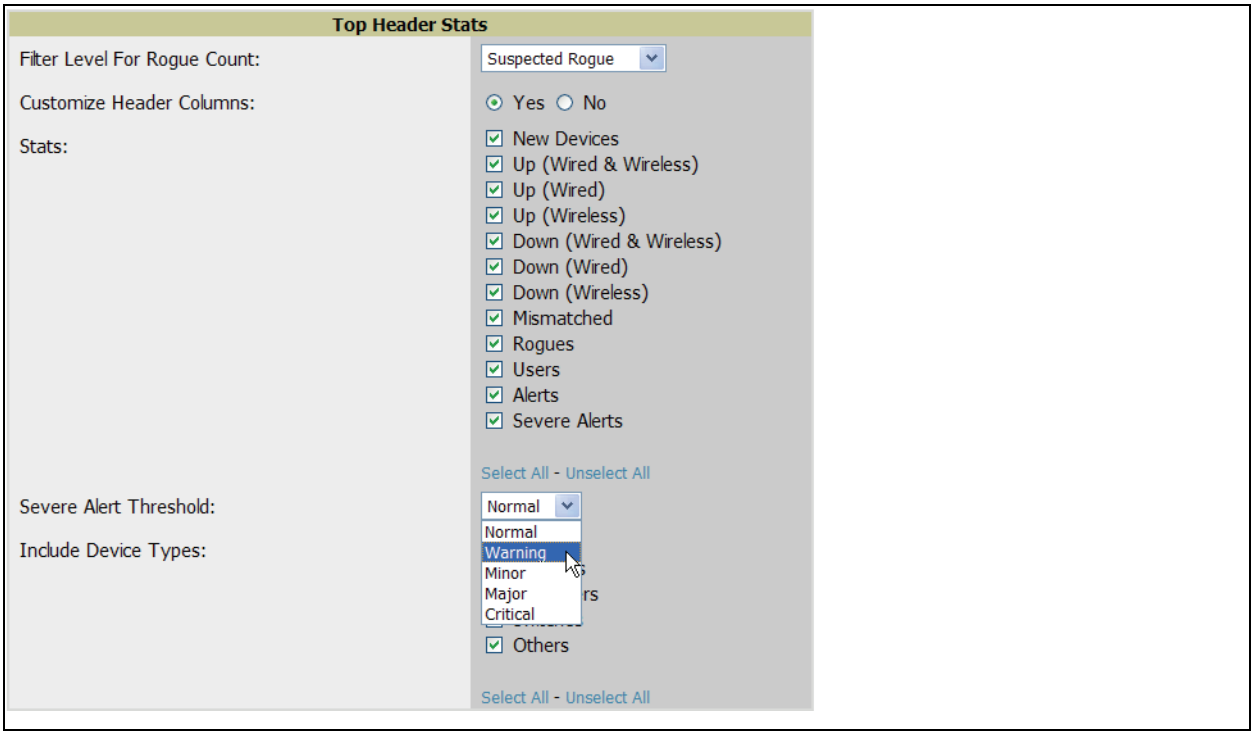
Green widgets are those that are properly placed and set to appear when you click **Save**. Widgets that remain in the left pane will not appear (although they can be returned at a later time, or reinstated by clicking **Restore Defaults**).

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 configured on the **Home > User Info** page to be enabled to view critical alerts can see severe alerts. The **Severe Alert Threshold** dropdown menu,

located in the Top Header Stats pane of the **Home > User Info** page, with all options displayed is shown in Figure 17.

Figure 17 Severe Alert Threshold *Dropdown Menu*

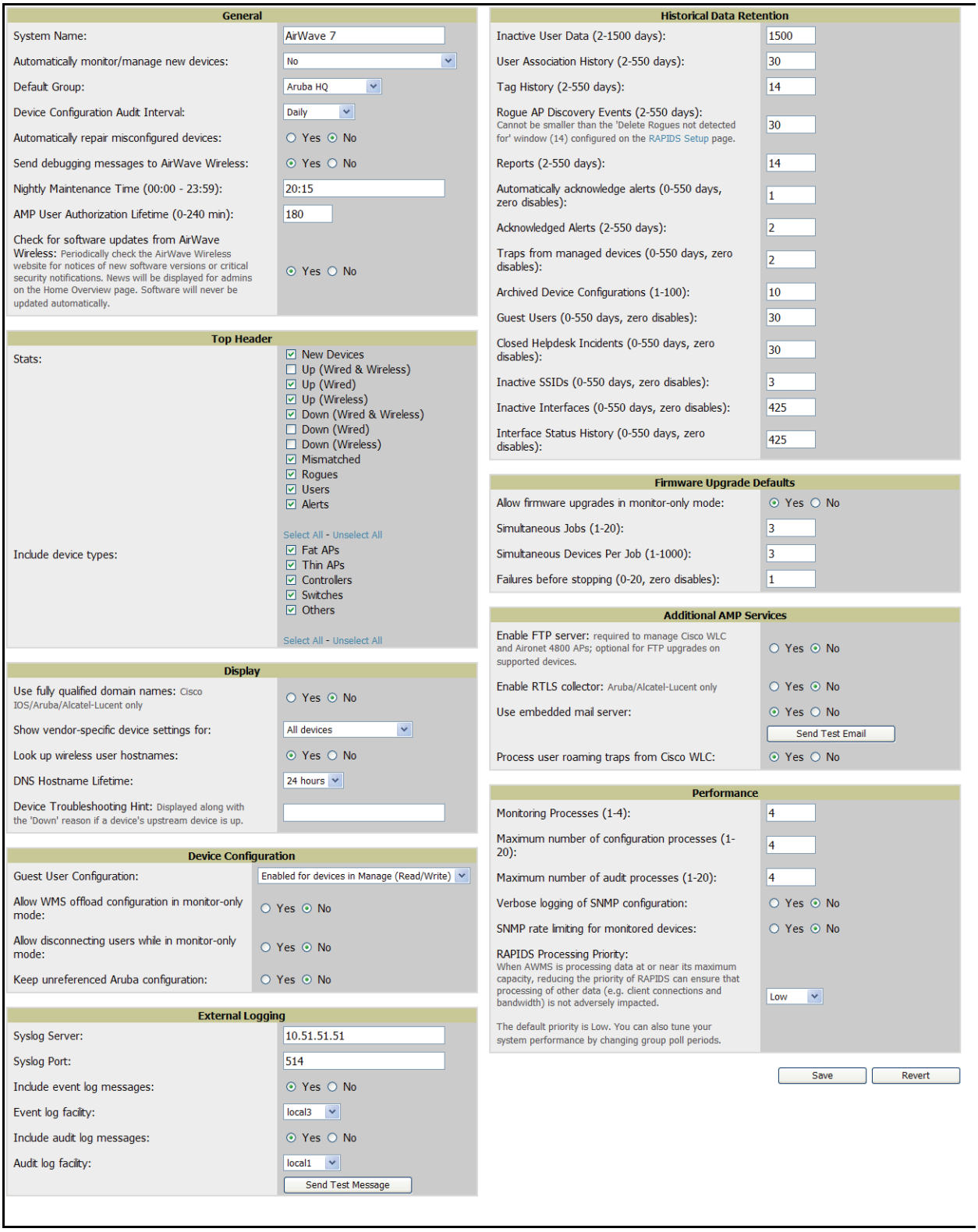


Defining General OV3600 Server Settings

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 18 illustrates the **OV3600 Setup > General** page:

Figure 18 OV3600 Setup > General *Page Illustration*



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 6:

Table 6 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. • When devices are in **Monitor Only** mode, 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. • When devices are 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. 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.
Default Group	NA	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 81.
Device Configuration Audit Interval	Daily	If enabled, this setting defines the interval of OV3600 queries, in which each device 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 to Alcatel Lucent	Enabled	If enabled, OV3600 automatically emails any system errors to the Alcatel Lucent Support Center to assist in debugging.
Nightly Maintenance Time (00:00 - 23:59)	04:15	Specifies the 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.

Table 6 OV3600 *Setup > General > General* Section Fields and Default Values *(Continued)*

Setting	Default	Description
Check Updates from Alcatel Lucent	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** by checking the corresponding check box. The selected options will be displayed at the top of GUI. For more detailed information about each option, refer to Table 3 on page 24.

3. On the **OV3600 Setup > General** page, locate the **Display Options** section and adjust settings as required. The **Display Options** section configures which **Group** tabs and options appear by default in new device groups.

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

Table 7 describes the settings and default values in this section.

Table 7 ***OV3600 Setup > General > Display Options*** *Section 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, Aruba, 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 at the individual group level.
Look Up Wireless User Hostnames	Yes	Enables OV3600 to look up automatically 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. Select a time duration from the drop-down menu. Options are as follows: • 1 hour • 2 hours • 4 hours • 12 hours • 24 hours
AP 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 **Configuration Options** section and adjust settings as required. The settings in this field configure whether certain changes can be pushed to devices in **Monitor Only** mode. Table 8 describes the settings and default values of this section.

Table 8 ***OV3600 Setup > General > Configuration Options*** *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 (for Aruba/Alcatel-Lucent devices only)	No	When **Yes** is selected, you can enable the Aruba/Alcatel-Lucent 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.
Desire all global Alcatel Lucent Configuration	No	Allows OV3600 to retain unused Aruba/Alcatel-Lucent OS configuration profiles. You can define profiles on a WLAN switch but it is not necessary to reference them from a virtual AP configuration or other component of Aruba/Alcatel-Lucent Configuration. Normally OV3600 deletes unreferenced profiles, but this setting retains them when enabled with **Yes**. **NOTE:** If this setting is enabled with **Yes**, then all profiles are pushed to all controllers. In this case, you cannot have different configurations for different controllers.

5. On the **OV3600 Setup > General** page, locate the **External Logging** section and adjust settings as required. Use this section to configure OV3600 to send audit and system events to an external syslog server. Table 9 describes these settings and default values.

Table 9 ***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 10 describes the settings and default values of this section. Many settings can be set to have no expiration date, such that the information will remain in the OV3600 indefinitely, as noted.

Table 10 ***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 or convention centers. 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.
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 OV3600 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 OV3600 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. Setting this value to 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 OV3600 database.
Inactive SSIDs (0-550 days, zero disables)	425	Sets the number of days OV3600 retains historical information after OV3600 last saw a client on a specific SSID. Setting this value to 0 disables this function, and inactive SSIDs will never expire or be deleted from the OV3600 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 OV3600 database.

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

Setting	Default	Description
Interface Status History (0-550 days, zero disables)	425	Sets the number of days OV3600 retains historical information on interface status. Setting this value to 0 disables this function.

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 11 describes the settings and default values of this section.

Table 11 *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.
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 12 describes the settings and default values of this section.

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

Setting	Default	Description
Enable FTP Server	No	Enables or disables the FTP server on OV3600. The FTP server is only used to manage 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 controllers to send RTLS packets to VisualRF. The RTLS server IP address must be configured on each controller. This function is used for VisualRF to improve location accuracy and to locate chirping asset tags. This function is supported only for Aruba and Alcatel-Lucent devices. With selection of **Yes**, the following additional fields appear: • **RTLS Port**—Specify the port for the RTLS server. • **RTLS Username**—Enter the user name supported by the RTLS server. • **RTLS Password**—Enter the RTLS server password.

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

Setting	Default	Description
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. Clicking 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.

9. On the **OV3600 Setup > General** page, locate the **Performance Tuning** 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 13 describes the settings and default values of this section.

Table 13 **OV3600 Setup > General >** ***Performance Tuning*** *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.
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	Enables or disables a maximum bandwidth consumption threshold for each port for monitored devices. This setting prevents unnecessary SNMP traffic from compromising device performance. Alcatel Lucent recommends enabling this setting when monitoring Aruba/Alcatel Lucent devices.
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) are not adversely impacted. The default priority is **Low**. You can also tune your system performance by changing group poll periods.

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

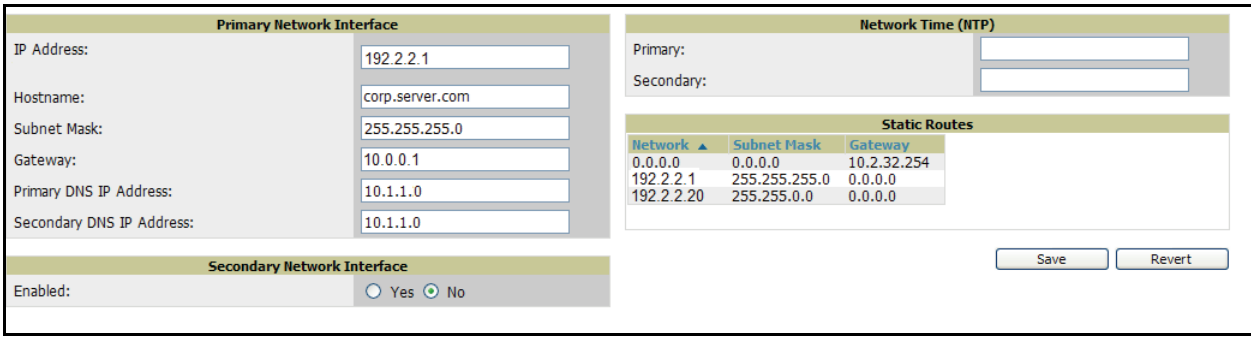
What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

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 19 illustrates the contents of this page.

Figure 19 ***OV3600*** **Setup > Network** *Page* **Illustration**



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 14 describes the settings and default values.

Table 14 ***OV3600 Setup > Network > 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 static IP address.
Hostname	None	Sets the DNS name assigned to the OV3600 server.
Subnet Mask	None	Sets the subnet mask for the OV3600 primary network interface.
Gateway	None	Sets the default gateway for the OV3600 network interface.
Primary DNS IP	None	Sets the primary DNS IP address for the OV3600 network interface.
Secondary DNS IP	None	Sets the secondary DNS IP address for the OV3600 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.

Specifying NTP servers is optional. NTP servers synchronize the time on the OV3600 server, not on individual access points. Secondary network interface options may include multiple telnet terminal configurations, DHCP/BOOTP auto-configuration, time zone offsets, daylight savings time, and NTP addressing modes such as unicast, broadcast, and multicast. Secondary NTP information is only supported on OV3600 that have multiple interfaces.

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 15 describes the settings and default values in more detail.

Table 15 ***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 Network Time Protocol server.
Secondary	ntp2.yourdomain.com	Sets the IP address or DNS name for the secondary Network Time Protocol 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.

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

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

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

Creating OV3600 Users

OV3600 installs with only one OV3600 user—the **administrator or admin** user. The **admin** user has these parameters authorizations within OV3600:

- The **admin** user is able to define additional users with varying levels of privilege, be it manage read/write or monitoring.
- The **admin** user can limit the viewable devices as well as the type of access a user has to the devices.

For each general user **that you add, you define** a **Username**, **Password** and a **Role**. You use the username and password when logging into OV3600. It is helpful to 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.

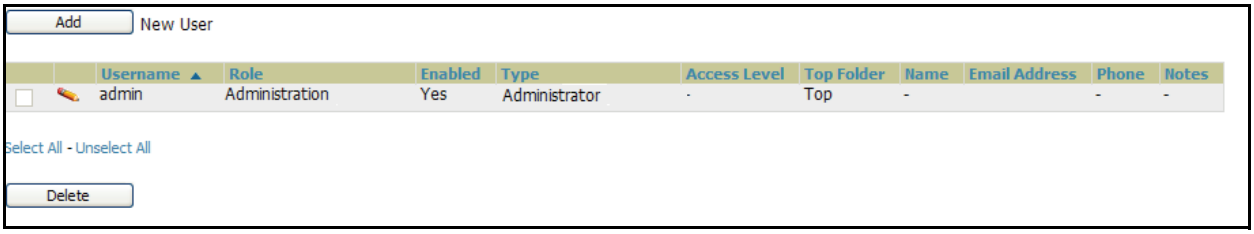
The ***user* role** defines the user type, access level, and the top folder for that user. User roles are defined on the **OV3600 Setup > Roles** page. Refer to the next procedure in this chapter for additional information, "Creating OV3600 User Roles" on page 52.

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.

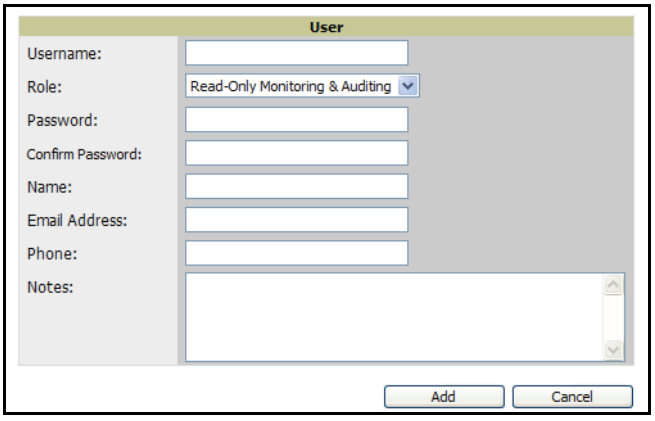
1. Navigate to the **OV3600 Setup > Users** page. This page displays all users currently configured in OV3600. Figure 20 illustrates the contents and layout of this page.

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



2. Click **Add** to create a new user, click the pencil icon to edit an existing user, or select a user and click **Delete** to remove that user from OV3600. When you click **Add** or the edit icon, the **Add User** page appears, illustrated in Figure 21.

Figure 21 ***OV3600 Setup > Users > Add/Edit User*** *Page Illustration*



3. Enter or edit the settings on this page. Table 16 describes these settings in additional detail.

Table 16 ***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. Because the default user's password is identical to the name, Alcatel Lucent strongly recommends that your change this password. Alcatel Lucent strongly recommends that you immediately change the default OV3600 "**admin**" password for **admin** users.
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. Click **Add** to create the new user, click **Save** to retain changes to an existing user, or click **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 additional OV3600 pages and functions relevant to that user.

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.

In prior OV3600 versions, user roles could be assigned only to a single top folder, such as "West Coast" or "European Stores", for example. User roles can now 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.

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

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. 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. In prior OV3600 releases, OV3600 user roles could only be assigned to a single top folder (such as "West Coast" or "European Stores"). 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.

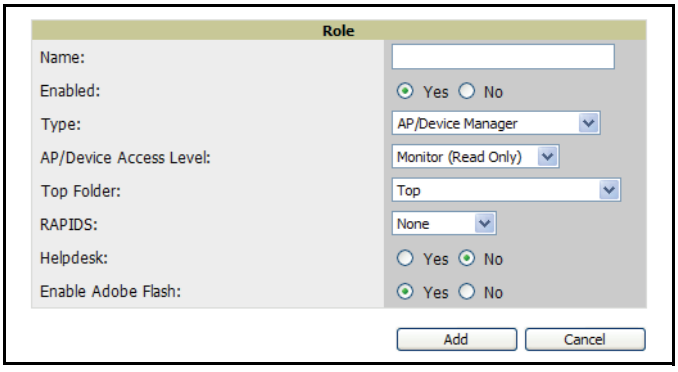
Perform the following steps to view, add, edit, or delete user **Roles**:

1. Navigate to the **OV3600 Setup > Roles** page. This page displays all roles currently configured in OV3600. Figure 22 illustrates the contents and layout of this page.

Figure 22 ***OV3600 Setup > Roles*** *Page Illustration*

2. Click **Add** to create a new role, click the pencil icon to edit an existing role, or select a role and click **Delete** to remove that role from OV3600. When you click **Add** or the edit icon, the **Add Role** page appears, illustrated in Figure 23.

Figure 23 ***OV3600 Setup > Roles > Add/Edit Role*** *Page Illustration*



3. Enter or edit the settings on this page. Table 16 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 17 describes the settings and default values of this section.

Table 17 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.
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. The administrator can view and edit all settings and all APs in OV3600. 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. • **Alcatel Lucent Management Client**—Defines the OV3600 user. 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 have read/write access to the viewable devices and Groups. They can change all OV3600 settings for the devices and Groups they can view. • **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. Monitor users cannot view the **APs/Devices > Audit** page which may contain sensitive information, including AP passwords. Monitor-only users also have read-only access to VisualRF.
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. Prior to Version 6.3, OV3600 user roles could be assigned only to a single top folder, such as "West Coast" or "European Stores", for example. User roles can now 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.

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

Setting	Default	Description
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.

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

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 Airespace/WLC wireless LAN controllers when they are present on the network.

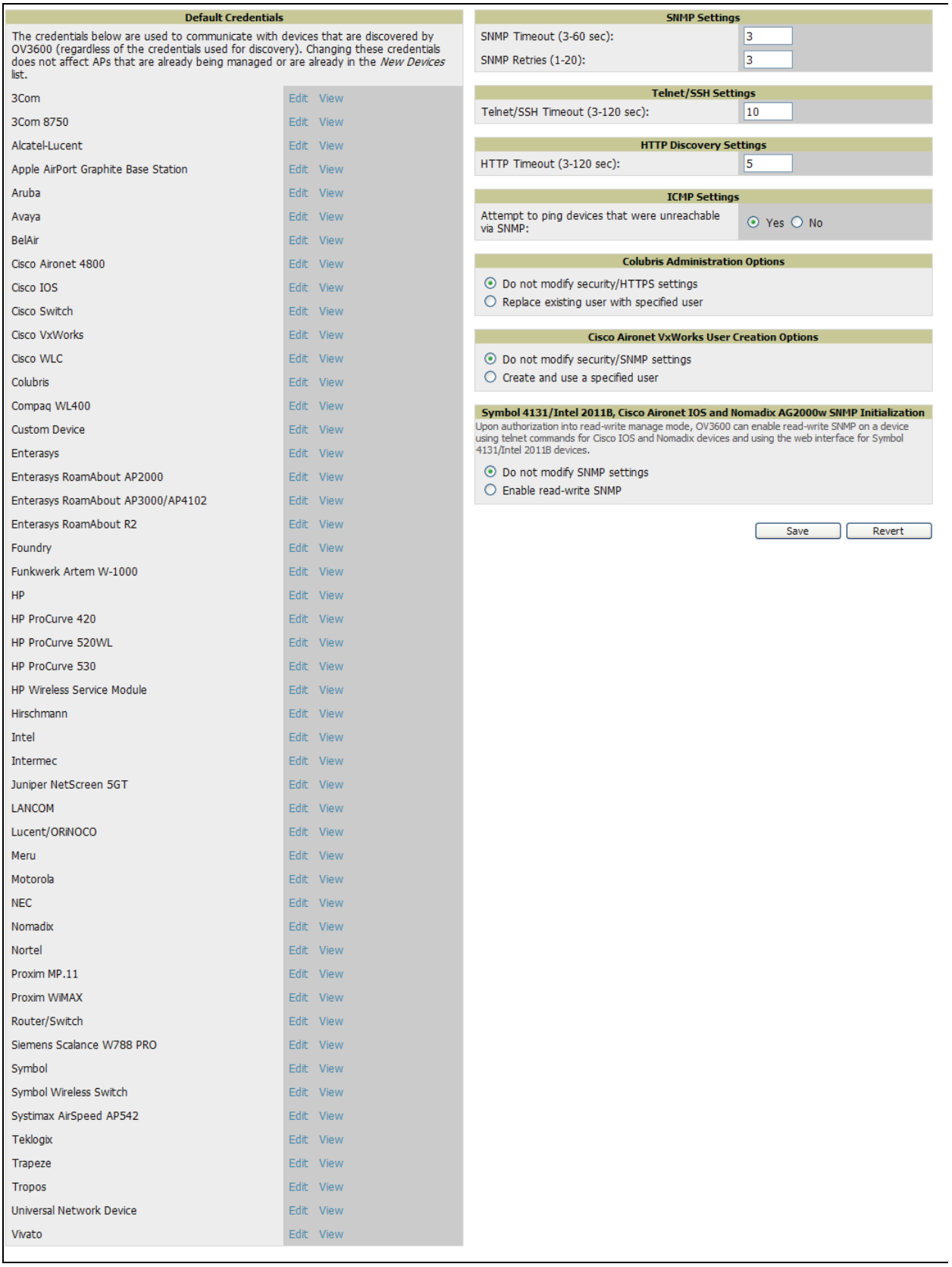
This section contains the following procedures:

- Configuring Communication Settings for Discovered Devices
- Loading Device Firmware onto OV3600 (Optional)
  - Overview of the Device Setup > Upload Files Page
  - Loading Firmware Files to OV3600
    - Overview of the Device Setup > Upload Files Page
    - Loading Firmware Files to OV3600
    - Using Web Auth Bundles in 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 24.

Figure 24 ***Device Setup > Communication*** *Page Illustration*



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.

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** area, and enter or revise the following information. Table 18 lists the settings and default values.

Table 18 ***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. If OV3600 does not receive an SNMP response from the device after the specified number of retries, OV3600 classifies that device as `Down`.

3. On the **Device Setup > Communication** page, locate the **Telnet/SSH Settings** section, and complete or adjust the default value for the field in this section. Table 19 lists the setting and default value.

Table 19 ***Device Setup > Communication > Telnet/SSH Settings*** *Fields and Default Values*

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

4. 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 20 lists these settings and default values.

Table 20 ***Device Setup > Communication > HTTP Discovery Settings*** *Fields and Default Values*

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

5. On the **Device Setup > Communication** page, locate the **ICMP Settings** section. Complete the settings or revise the default values as required. Table 21 itemizes the setting and default value of this section.

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

Setting	Default	Description
Attempt to ping down devices	Yes	Enables a function that applies when an AP is unreachable over SNMP. • When **Yes** is selected, this option has OV3600 attempt 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.

6. On the **Device Setup > Communication** page, locate the **Colubris Administration Options** section You only need to provide this information if you use Colubris APs on your network. Select one of the options listed. Figure 25 illustrates this section and Table 22 explains related fields.

Figure 25 ***Device Setup > Communication > Colubris Administration Options*** *Section Illustration*

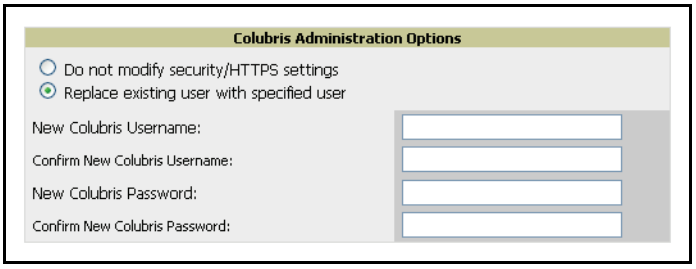


Table 22 ***Device Setup > Communication > Colubris Administration Options*** *Fields and Default Values*

Setting	Default	Description
Do not modify security/HTTPS settings	N/A	Enables OV3600 to use only an existing user account on the AP. This user account must have all permissions set. The user accounts are defined in the **Colubris Username/Password** section in the **Default Secrets** area.
Replace existing user with specified user	Disabled	When enabled, this setting allows you to define a new Colubris username and password on each Colubris AP.
New Colubris Username and Password	N/A	Specifies the username and password to be used only if the option **Replace existing user with specified user** is selected.

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 23 describes the settings and default values of this section.

Table 23 ***Device Setup > Communication > 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/Intel 2011b and Cisco Aironet IOS SNMP Initialization** area. You only need to provide this information if you use Symbol 4131, Intel 2011b, or Cisco Aironet IOS access points. Select one of the options listed. Table 24 describes the settings and default values.

Table 24 ***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.

9. On the **Device Setup > Communication** page, locate the **Symbol 4131/Intel 2011b and Cisco Aironet IOS SNMP Initialization** area. You only need to provide this information if you use Symbol 4131, Intel 2011b, or Cisco Aironet IOS access points. Select one of the options listed. Table 25 describes the settings and default values.

Table 25 ***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.

Loading Device Firmware onto OV3600 (Optional)

Overview of the Device Setup > Upload 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 Files** page.

Figure 26 illustrates the **Upload Files** page, which 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 on this **Upload File** page appear as options in the drop-down menus on the **Group > Firmware** page and on individual **AP/Device > Manage** pages. These firmware files can be applied automatically to devices through OV3600.
- Use the **OV3600 Setup** page to configure OV3600-wide default firmware options.

Figure 26 ***Device Setup > Upload Files*** *Page Illustration*

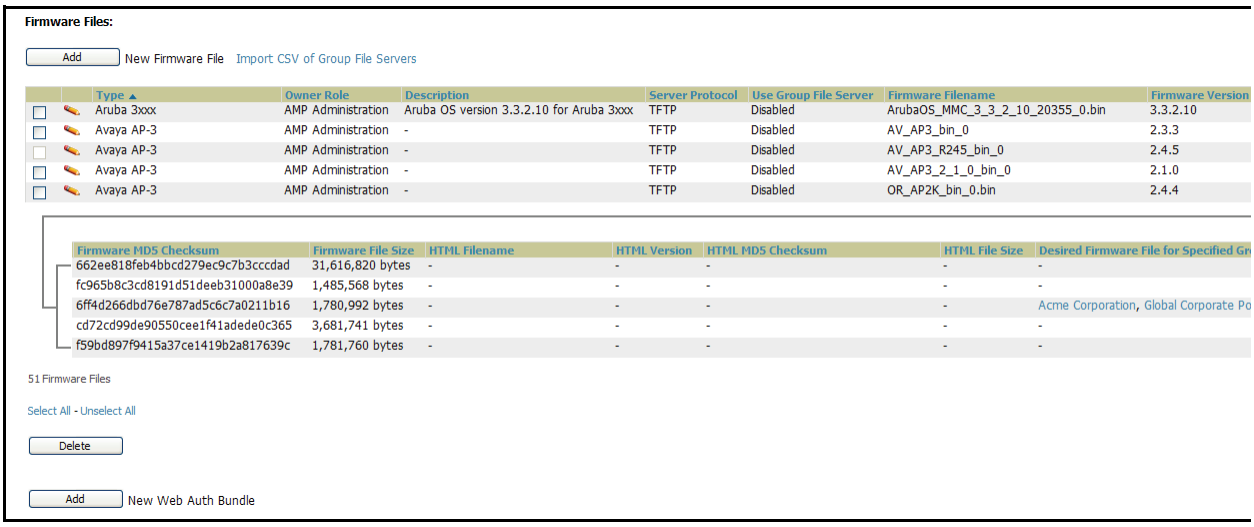


Table 26 below itemizes the contents, settings, and default values for the **Upload Files** page.

Table 26 ***Device Setup > Upload 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.

Table 26 ***Device Setup > Upload Files*** *Fields and Default Values (Continued)*

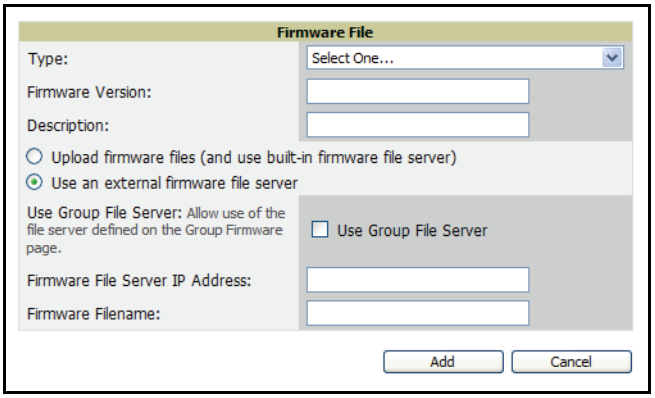
Setting	Default	Description
Firmware Filename	None	Displays the name of the file that was uploaded to OV3600 and to be transferred to an AP when the file is used in an upgrade.
Firmware Version	None	Displays the firmware version number. This is a user-configurable field.
Firmware MD5 Checksum	None	Displays 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. Browse to the **Device Setup > Upload Files** page.
2. From the **Upload Files** page, click the **Add** button. The **Add Firmware File** dialog box appears. Figure 27 illustrates this page.

Figure 27 ***Device Setup > Upload Files > Add New Firmware*** *Page Illustration*



3. Click the **Supported Firmware Versions and Features** link to view a list of 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. See "Contacting Alcatel-Lucent" on page 11.

4. Enter the appropriate information and click the **Add** button. The file uploads to OV3600 and once complete, this file appears on the **Device Setup > Upload Files** page. This file also appears on additional pages that display firmware files (such as the **Group > Firmware** page and on individual **AP/Device > Manage** pages).
5. You can also import a CSV list of groups and their external TFTP firmware servers. Table 27 itemizes the settings of this page.

Table 27 ***Supported Firmware Versions and Features*** *Fields and Default Values*

Setting	Default	Description
Type	None	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 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.
Description	None	Provides a user-configurable text description of the firmware file.
Upload firmware files (and use built-in firmware file server)	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. **NOTE:** If you select FTP, OV3600 uses an anonymous user for file upload.
Use Group File Server	Disabled (not selected)	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.
TFTP Server IP	None	Provides the IP address of the External TFTP Server (like SolarWinds) that is used for the firmware upgrade. This option displays when the user selects **Use a Different TFTP server** option.
Firmware Filename	None	Enter the filename of the firmware file that needs to be uploaded. Ensure that the firmware file is in the TFTP root directory. Click the **Browse** button to locate the appropriate Intel or Symbol HTML firmware file on your network.

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. Click **Add** to import the firmware file.
7. To delete a firmware file that has already been uploaded to OV3600, return to the **File Upload** page, select the checkbox for the firmware file and click **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

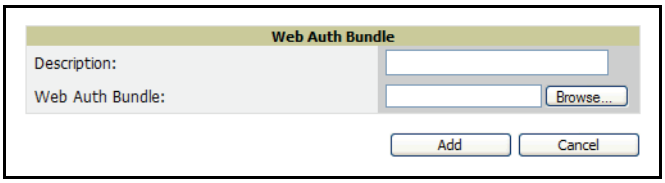
Web authentication bundles are configuration files that support Cisco Airespace/WLC wireless LAN controllers. This procedure requires that you have local or network access to a Web Auth configuration file for Cisco Airespace/WLC devices.

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

1. Navigate to the **Device Setup > Upload 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. Click **Add New Web Auth Bundle** to create a new Web Auth bundle, or click 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 clicking **Delete**.

   When you add or edit a Web Auth bundle, the **Web Auth Bundle** page appears, as illustrated in Figure 28.

Figure 28 ***Add Web Auth Bundle*** *Page Illustration*



3. Enter a descriptive label in the description field. This is the label by which you identify and track Web Auth bundles on the **Device Setup > Upload Files** page once they are present in OV3600.
4. Enter the path and filename of the Web Auth configuration file in the **Web Auth Bundle** field. Click **Browse** to locate the file with the browsing method, as required.
5. Click **Add** to complete the Web Auth bundle creation, or click **Save** if replacing a previous Web Auth configuration file, or click **Cancel** to abort the Web Auth integration.
6. The **Device Setup > Upload** files page displays your changes.

For additional information and a case study that illustrates the use of Web Auth bundles with Cisco Airespace/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:

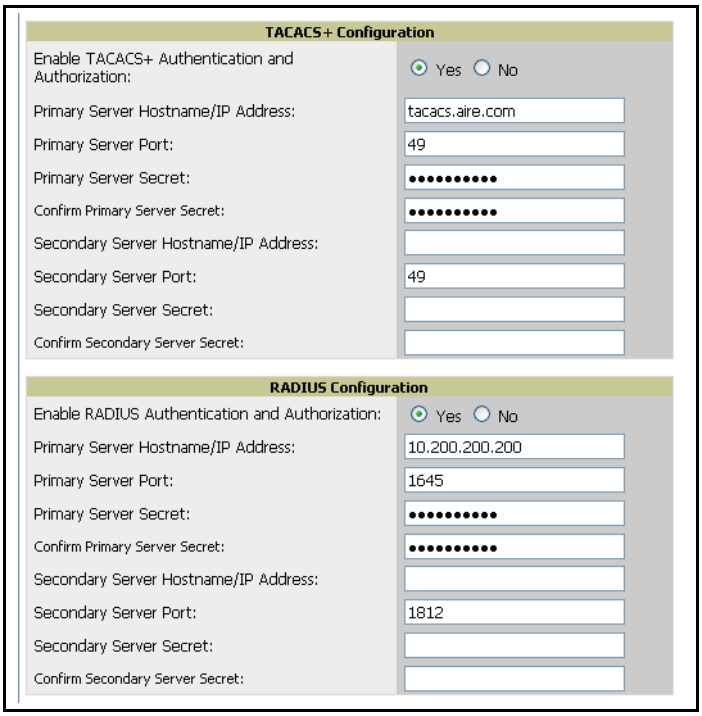
- Configuring TACACS+ Authentication
- Configuring RADIUS Authentication and Authorization
- Integrating a RADIUS Accounting Server

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. Perform these steps to configure TACACS+ authentication:

1. Navigate to the **OV3600 Setup > Authentication** page. This page displays current status of TACACS+. Figure 29 illustrates this page when neither TACACS+ nor RADIUS authentication is enabled in OV3600.

Figure 29 ***OV3600 Setup > Authentication*** *Page Illustration*



2. Click **No** to disable or **Yes** to enable TACACS+ authentication. If you click **Yes**, several new fields appear. Complete the fields described in Table 28.

Table 28 ***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 TCP port for the primary TACACS+ server.
Primary Server Secret	N/A	Specify the primary shared secret for the primary TACACS+ server, and confirm in the **Confirm** field.

Table 28 ***OV3600 Setup > Authentication*** *Fields and Default Values (Continued)*

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

3. Click **Save** to retain these configurations, 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.
   - Click **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, click **Add Entry** to add an AAA client.
   - 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 click **submit** + **restart**.

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?

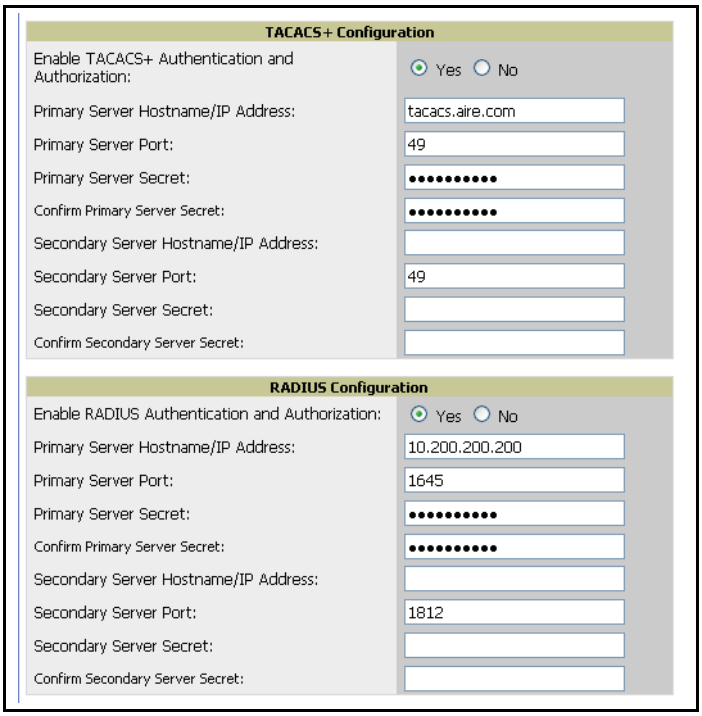
- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

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. Navigate to the **OV3600 Setup > Authentication** page. This page displays current status of RADIUS. Figure 30 illustrates this page when neither TACACS+ nor RADIUS authentication is enabled in OV3600.

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



2. Click **No** to disable or **Yes** to enable TACACS+ nor RADIUS authentication. If you click **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 RADIUS server.
Primary Server Port	49	Enter the TCP port for the primary RADIUS server.
Primary Server Secret	N/A	Specify the primary shared secret for the primary RADIUS server, and confirm in the **Confirm** field.
Secondary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the secondary RADIUS server.
Secondary Server Port	49	Enter the TCP port for the secondary RADIUS server.
Secondary Server Secret	N/A	Enter the shared secret for the secondary RADIUS server.

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

NOTE

OV3600 checks the local username and password store before checking with the RADIUS server. If the user is found locally, the local password and local role apply. When using RADIUS, 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 RADIUS server goes down.

As an optional configuration, OV3600 supports RADIUS server accounting. Use the **OV3600 Setup > RADIUS Accounting** page enables this configuration. This capability is not required for basic OV3600 operation, but can increase the user-friendliness of OV3600 administration in large networks. Figure 31 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 31 illustrates the display of RADIUS accounting clients already configured, and Figure 32 illustrates the **Add RADIUS Accounting Client** page.

Figure 31 ***OV3600 Setup > RADIUS Accounting*** *Page Illustration*

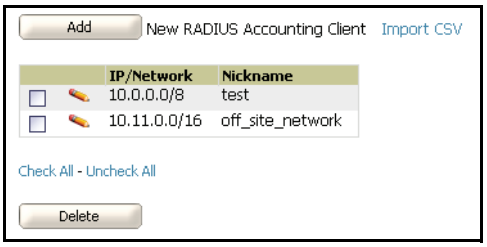
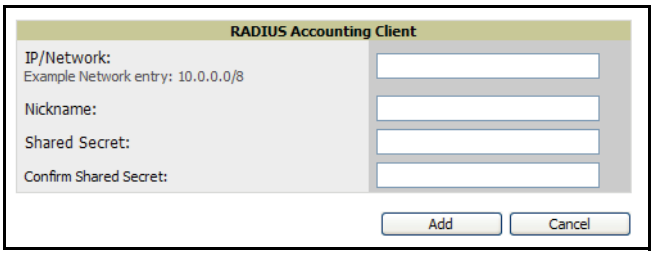


Figure 32 ***OV3600 Setup > RADIUS > Add RADIUS Accounting Client*** *Page Illustration*



1. To specify the RADIUS authentication server or network, browse to the **OV3600 Setup > RADIUS Accounting** page and click **Add**, illustrated in Figure 32, and provide the information described in Table 30.

Table 30 ***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).
(Confirm) Shared Secret	None	Sets the Shared Secret that is used to establish communication between OV3600 and the RADIUS authentication server.

2. Click **Add**.

What Next?

- For additional 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 311.
- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

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 31 describes these components.

Table 31 *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. Navigate 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. Click **Save**.

Enabling Rogue Alerts for Cisco WLSE

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

Additional information about rogue device detection is available in "Configuring Cisco WLSE Rogue Scanning" on page 71.

Configuring WLSE to Communicate with APs

1. Navigate to the **Device Setup > Discover** page.
2. Configure **SNMP Information** (click for additional information).
3. Configure HTTP Information (click for additional information).
4. Configure Telnet/SSH Credentials (click for additional information).
5. Configure HTTP ports for IOS access points (click for additional information).
6. Configure WLCCP credentials (click for additional information).
7. Configure AAA information (click for additional 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. Navigate to the **Device > Managed Devices > Discovery Wizard** page.
2. Import devices from a file (click for additional information).
3. Import devices from Cisco Works (click for additional information).
4. Import using CDP (click for additional information).

Managing Devices

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

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. Navigate to **Device > Discover > Advanced Options**.

2. Select the method to bring APs into management **Auto**, or specify via filter (click for additional information).

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. Navigate to **Devices > Inventory > Run Inventory**.
2. **Run Inventory** executes immediately between WLSE polling cycles (click for additional information).

Defining Access

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

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

Grouping

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

1. Navigate 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.

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. Navigate to the **Wireless Services > AP** page.
3. Click **Enable participation in SWAN Infrastructure.**
4. Click **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. Navigate 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. Navigate to the **Security > Server Manager** page.
5. Enter the **IP address** and **Shared Secret** for the ACS server.
6. Click the **Apply** button.
7. Navigate to the **Wireless Services > WDS > Server Group** page.
8. Enter the WDS Group of AP.
9. Select the **ACS server** in the **Priority 1** drop- down menu.
10. Click the **Apply** button.

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. Navigate to the **System Configuration > ACS Certificate Setup** page.
3. Install a New Certificate by clicking the **Install New Certificate** button, or skip to the next step if the certificate was previously installed.
4. Click the **User Setup** button in the left frame.
5. Enter the **Username** that will be used to authenticate into the WDS and click **Add/Edit** button.
6. Enter the **Password** that will be used to authenticate into the WDS and click the **Submit** button.
7. Navigate 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 click the **Submit** button.

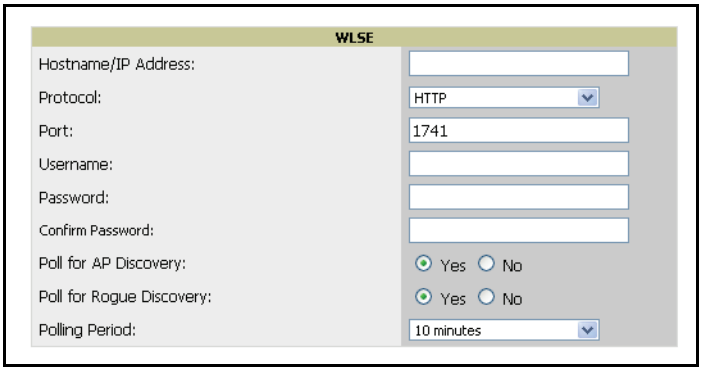
For additional and more general information about ACS, refer to "Configuring ACS Servers" on page 73.

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

Figure 33 ***OV3600 Setup > WLSE > Add WLSE*** *Page Illustration*



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 click **Add**. Complete the fields in this page. Table 32 describes the settings and default values.

Table 32 ***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.
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, click the **Save** button. 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?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

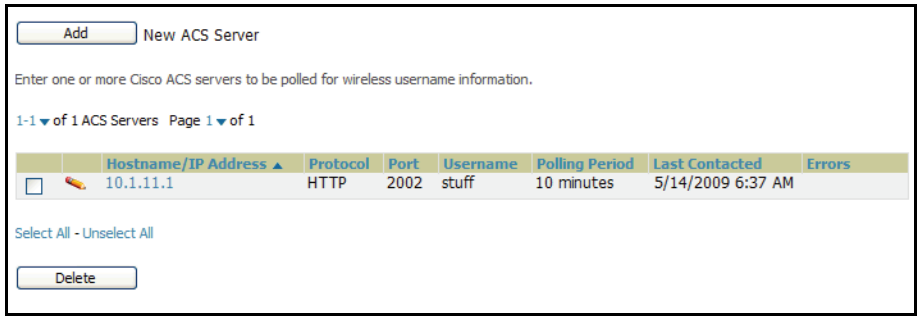
Configuring ACS Servers

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 networks wireless users. Refer to the "Configuring TACACS+ and RADIUS Authentication" on page 63 section if you want to use your ACS server to manage your OV3600 users.

Perform these steps to configure ACS servers:

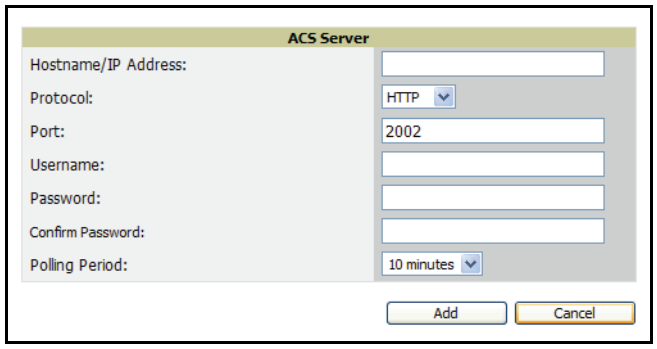
1. Navigate to the **OV3600 Setup > ACS** page. This page displays current ACS information, as illustrated in Figure 34.

Figure 34 ***OV3600 Setup > ACS*** *Page Illustration*



2. Click **Add** to create a new ACS server, or click a pencil icon to edit an existing server. To delete an ACS server, select that server and click **Delete**. When clicking **Add** or edit, the **Details** page appears, as illustrated in Figure 35.

Figure 35 ***OV3600 Setup > ACS > Add/Edit Details*** *Page Illustration*



3. Complete the settings on the **OV3600 Setup > ACS > Add/Edit Details** page. Table 33 describes these fields:

Table 33 ***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.

Table 33 ***OV3600*** **Setup > ACS > Add/Edit Details** *Fields and Default Values (Continued)*

Field	Default	Description
Polling Period	10 min	Launches a drop-down menu that specifies how frequently OV3600 polls the ACS server for username information.

4. Click **Add** to finish creating the new ACS server, or click **Save** to finish editing an existing ACS server.
5. The ACS server must have logging enabled for passed authentications. To configure your ACS server to log the required information, you must 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, click the **Logging** link.
   - Under **Enable Logging**, click the **CSV Passed Authentications** link. The default logging options function and support OV3600. These include the two columns OV3600 requires: **User-Name** and **Caller-ID**.

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

Integrating OV3600 with an Existing Network Management Solution (NMS)

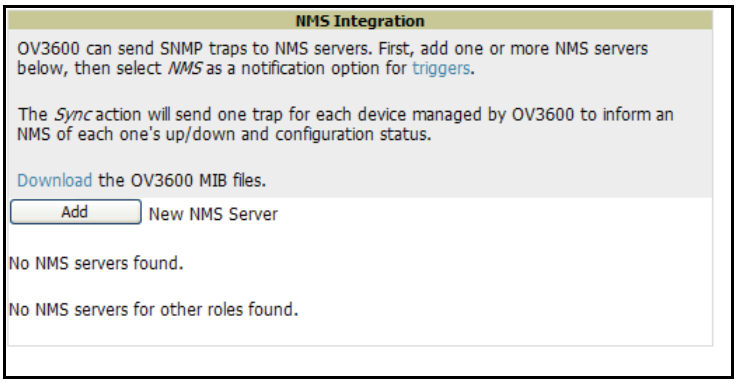
This is an optional configuration. The **OV3600 Setup > NMS** configuration page allows OV3600 to integrate with other Network Management Solution (NMS) consoles. This configuration enables advanced and interoperable functionality as follows:

- 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 Alcatel Lucent support.

Perform these steps to configure NMS support in OV3600:

1. Navigate to the **OV3600 Setup > NMS** page, illustrated in Figure 36.

Figure 36 ***OV3600 Setup > NMS Integration*** *Page Illustration*



2. Click **Add to integrate a new NMS server, or click the pencil icon to edit an existing NMS server.** Provide the information described in Table 34:

Figure 37 ***OV3600 Setup > NMS Integration Add/Edit*** *Page Illustration*

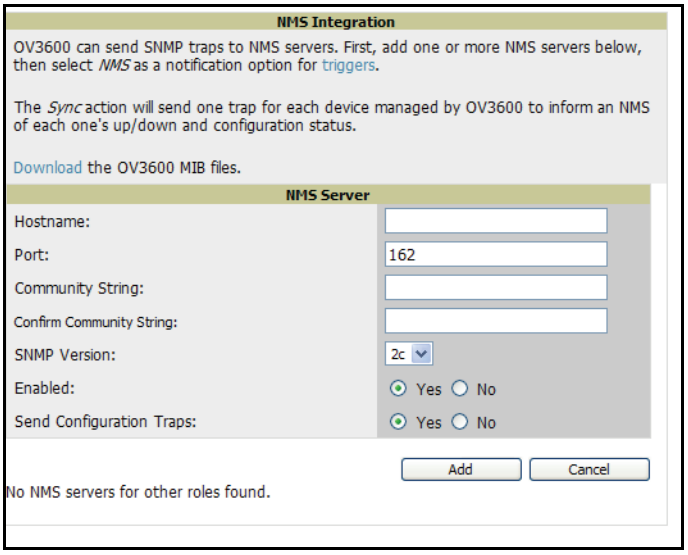


Table 34 ***OV3600 Setup > NMS Integration Add/Edit*** *Fields and Default Values*

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

Table 34 ***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 **OV3600 Setup > NMS Integration Add/Edit** page features the **Netcool/OMNIbus Integration** link. IBM Tivoli Netcool/OMNIbus is operations management software that enables automated event correlation and additional features resulting in optimized network uptime. Click this link for additional information, specifications, and brief instructions for installation with OV3600.
4. The **OV3600 Setup > NMS Integration Add/Edit** page features the **HP ProCurve Manager Integration** link. Click this link for additional information, zip file download, and brief instructions for installation with OV3600. Click **Add** on the **OV3600 Setup > NMS Integration Add/Edit** page to finish creating the NMS server, or click **Save** to complete configuration of an existing NMS server.

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

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 78.
- The **Reports > Definitions** page allows you to create custom-configured and custom-scheduled PCI Compliance reports. See "Reports > Definitions Page Overview" on page 269.
- 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 click. Refer to "Reports > Generated Page Overview" on page 271.
- 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 78.
- The **PCI Compliance Report** offers additional information. Refer to "Using the PCI Compliance Report" on page 288. 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.

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.

Table 35 *PCI Requirements and Support in OV3600*

PCI 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**: When this PCI requirement is disabled in OV3600, firewall router and device configurations are not checked for PCI compliance in firewall configuration, and **Pass** or **Fail** status is not reported nor 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**: When this PCI requirement is disabled in OV3600, 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**: When this PCI requirement is disabled in OV3600, device passwords and other vendor default settings are not checked for PCI compliance.

Table 35 *PCI Requirements and Support in OV3600*

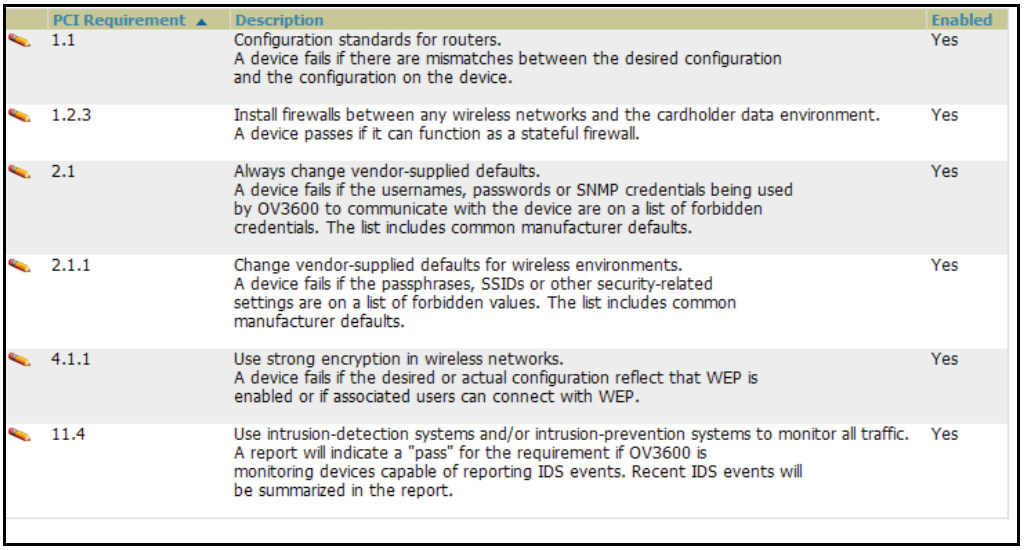
PCI Requirement	Description
2.1.1	Changing vendor-supplied defaults for wireless environments **When Enabled**: A device fails requirement 2.1.1 if the passphrases, SSIDs, or other security-related settings are on a list of forbidden values that OV3600 establishes and tracks. The list includes common vendor default passwords. The user can input new values to achieve compliance. **When Disabled**: When this PCI requirement is disabled in OV3600, then 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**: When this PCI monitoring function is disabled in OV3600, then OV3600 cannot establish a pass or fail status with regard to PCI encryption requirements on the network.
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**: When this function is disabled, then 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 35.

1. To determine what PCI Compliance standards are enabled or disabled on OV3600, navigate to the **OV3600 Setup > PCI Compliance** page, illustrated in Figure 38.

Figure 38 ***OV3600 Setup > PCI Compliance*** *Page Illustration*

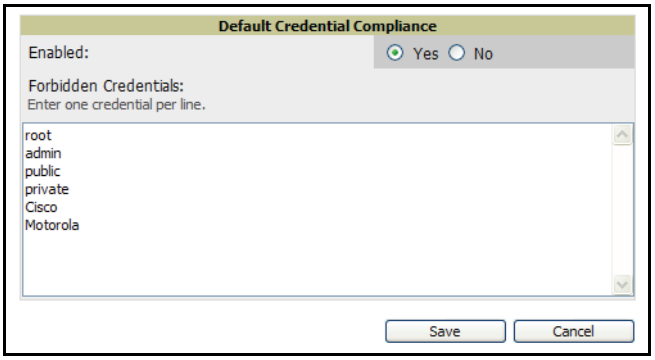


	PCI Requirement ▲	Description	Enabled
✎	1.1	Configuration standards for routers. A device fails if there are mismatches between the desired configuration and the configuration on the device.	Yes
✎	1.2.3	Install firewalls between any wireless networks and the cardholder data environment. A device passes 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, click the **pencil** icon next to the compliance category you wish to change. 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 39 illustrates one example.

Figure 39 ***Default Credential Compliance*** *for PCI Requirements*



4. Click **Save** to retain the settings. The **PCI Compliance** page should reflect changes on the next viewing.
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. Navigate to the **APs/Devices > List** page, click a specific device, and the **Monitor** page for that device displays. The **Monitor** page displays a **Compliance** page in the menu bar.
   b. Click the **Compliance** page to view complete PCI compliance auditing for that specific device.

What Next?

- For additional 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 311.
- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel Lucent support remains available to you for any phase of OV3600 installation. See "Contacting Alcatel-Lucent" on page 11.

Deploying WMS Offload

Overview of WMS Offload in OV3600

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

- Aruba OS Version 2.5.4 or later
- OV3600 Version 6.0 or later

The *Aruba/Alcatel-Lucent 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 Aruba/Alcatel-Lucent WMS functionality.

In OV3600 Version 6.1 and Version 6.2, WMS Offload is the ability to offload the WMS server data and GUI functions into OV3600. WMS master controllers provide this data so that OV3600 can support rigorous network monitoring capabilities. Additional support for WMS Offload continues with newer versions of OV3600.

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 Aruba/Alcatel-Lucent infrastructure.
   - Enable WMS offload.
   - Configure SNMP communication.
   - Create a proper policy for monitoring Aruba/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 Aruba/Alcatel-Lucent-specific monitoring features.
   - Enable remote AP and wired network monitoring.
   - View controller license information.
5. Convert existing floor plans to VisualRF, to include the following elements:
   - MMS
   - AOS
   - RF Plan
6. Use RTLS for increasing location accuracy (optional).
   - Enable RTLS service on the OV3600 server.
   - Enable RTLS on Aruba/Alcatel-Lucent Infrastructure.

Additional Information Supporting WMS Offload

For additional information, including detailed concepts, configuration procedures, restrictions, Aruba/Alcatel-Lucent 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 the Alcatel Lucent OmniVista Air Manager (OV3600), and includes the following topics:

- "OV3600 Group Overview" on page 83
- "Configuring Basic Group Settings" on page 87
- "Configuring Group Security Settings" on page 96
- "Configuring Group SSIDs and VLANs" on page 99
- "Adding and Configuring Group AAA Servers" on page 103
- "Configuring Radio Settings for Device Groups" on page 105
- "An Overview of Cisco WLC Configuration" on page 112
- "Configuring WLANs for Cisco WLC Devices" on page 113
- "Configuring Cisco Controller Settings" on page 116
- "Configuring Wireless Parameters for Cisco Controllers" on page 116
- "Configuring Security Parameters and Functions" on page 116
- "Configuring Management Settings for Cisco Controllers" on page 117
- "Configuring Group PTMP/WiMAX Settings" on page 118
- "Configuring Proxim Mesh Radio Settings" on page 123
- "Configuring Group MAC Access Control Lists" on page 125
- "Specifying Minimum Firmware Versions for APs in a Group" on page 126
- "Comparing Device Groups" on page 127
- "Deleting a Group" on page 128
- "Changing Multiple Group Configurations" on page 128
- "Modifying Multiple Devices" on page 129
- "Using Global Groups for Group Configuration" on page 132

Focused sub-menus can vary significantly from one device group to another—one or more sub-menus may not appear, depending on the **Default Group** display option selected on the **OV3600 Setup > General** page and the types of devices you add to OV3600.

The **Groups** tab can have the following pages or focused sub-menus:

- **List**—This page is the default page in the **Groups** section of OV3600. This page lists all groups currently configured in OV3600 and provides the foundation for all group-level configurations. See "Viewing All Defined Device Groups" on page 83. In the case of WLAN switches and configuration, refer also to the *Alcatel Lucent Configuration Guide*.

- **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 device-level activity in a given group. Several procedures in this chapter cite the **Groups > Monitor** page.

The **Incidents** portion of the **Alert Summary** table only increments the counter for incidents that are open and associated to an AP. The incidents are based on the Top folder on the **Groups > Monitor** page and on the **Home > Overview** page. Incidents that are not related to devices in that folder are not counted in this **Alert Summary**.

To view all incidents, including those not associated to an AP, navigate to the **Helpdesk > Incidents** page.

- **Basic**—This sub-menu page appears when you create a new group with the **Add** button 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 87.
- **Templates**—This page manages templates for any device group. 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 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 185.
- **Security**—This page defines general security settings for device groups, to include TACACS+, RADIUS, encryption, and additional security settings on devices. Refer to "Configuring Group Security Settings" on page 96.
- **SSIDs**—This page sets SSIDs, VLANs, and related parameters in device groups. Refer to "Configuring Group SSIDs and VLANs" on page 99.
- **AAA Servers**—This page configures authentication, authorization, and accounting settings in support of TACACS+ and RADIUS servers for device groups. Refer to "Adding and Configuring Group AAA Servers" on page 103.
- **Radio**—This page defines general 802.11 radio settings for device groups. Refer to "Configuring Radio Settings for Device Groups" on page 105.
- **Alcatel Lucent Configuration**—This page manages Aruba/Alcatel-Lucent Device Groups, AP Overrides, and other profiles specific to Aruba/Alcatel-Lucent devices on the network. Use this page in combination with the **Device Setup > Alcatel Lucent Configuration** page. For additional information, refer to the *Aruba/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 116.
- **PTMP/WiMAX**—This page defines settings specific to Proxim MP devices when present. Refer to "Configuring Group PTMP/WiMAX Settings" on page 118.
- **Proxim Mesh**—This page defines mesh AP settings specific to Proxim devices when present. Refer to "Configuring Proxim Mesh Radio Settings" on page 123.
- **MAC ACL**—This page defines MAC-specific settings that apply to Proxim, Cisco Vxworks, Symbol, Intel and Procurve520 devices when present. Refer to "Configuring Group MAC Access Control Lists" on page 125.
- **Firmware**—This page manages firmware files for many devices. "Specifying Minimum Firmware Versions for APs in a Group" on page 126.
- **Compare**—This page allows you to compare line item-settings between two device groups. On the **Groups > List** page, click **Compare Two Groups**, select the two groups from the drop-down menus, then

click **Compare**. The **Compare** page allows you to edit any line-item configuration for either of the two groups you compare. “Comparing Device Groups” on page 127.

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

- “Deleting a Group” on page 128
- “Changing Multiple Group Configurations” on page 128
- “Modifying Multiple Devices” on page 129
- “Using Global Groups for Group Configuration” on page 132

OV3600 Group Overview

Enterprise APs, controllers, routers, and switches are complex devices with 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 groups, with the following functions and benefits:

- OV3600 allows certain settings to be managed efficiently at a "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 variable appropriate for your business needs.
- *Devices* within a group may be from different vendors or hardware models—the core requirement and benefit of this approach is that 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.

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

With OV3600, you can create as many different groups as required. OV3600 users usually establish groups that range in size from five to 100 wireless devices.

Group configuration can be enhanced with the OV3600 *Global Groups* feature; this feature allows you to create global groups with master configurations that are pushed to individual subscriber groups. More information is available in “Using Global Groups for Group Configuration” on page 132 as well as the section on the “Supporting OV3600 Stations with the Master Console” on page 250.

Viewing All Defined Device Groups

To display a list of all groups that have been defined in OV3600, browse to the **Groups > List** page, illustrated in Figure 40. Table 36 describes the contents and functions of this page.

Figure 40 ***Groups > List*** *Page Illustration*

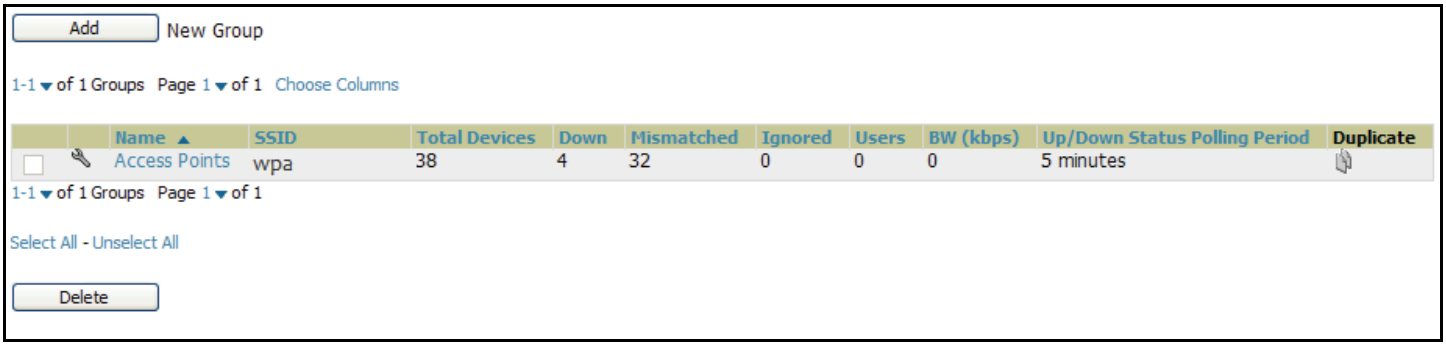


Table 36 ***Groups > List*** *Page Fields and Default Values*

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 87.
Manage (wrench icon)	The wrench icon for any existing group provides a hyperlink to the **Groups > Basic** configuration page to begin editing Group configuration settings for that group.
Name	Displays a user-defined name that 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).
Is Global Group	Identifies whether or not the group has been identified as a global group that can be used to configure subscriber groups. Global groups cannot contain APs and are visible by users of any role.
Global Group	Displays the global group to which the group is subscribed, if any.
SSID	Column represents the Service Set Identifier (SSID) assigned to all devices within the group.
Total Devices	Column represents the total number of devices contained in the group, including APs, wireless controllers and routers or switches.
Down	Column represents 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	Column represents the number of access points or wireless controllers within the group that are in a mismatched state.
Ignored	Column displays the number of ignored devices in that group.
Users	Column represents 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 (kbps)	Column represents a running average of the sum of bytes in and bytes out for the managed radio page.
Up/Down Status Polling Period	Column represents 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.
Duplicate	Column represents a hyperlink, and the link creates a new group with the name **Copy of <Group Name>** with the same group configuration.

NOTE

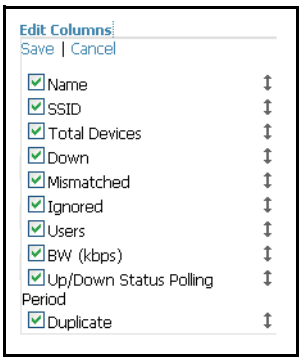
When you first configure OV3600, there is only one default group labeled **Access Points**. If you have no other groups configured, refer to "Configuring Basic Group Settings" on page 87.

Editing Columns on the Groups > List Page and Additional Pages

Perform the following steps to edit the columns that appear on the **Groups > List** page. All additional list and reports pages in OV3600 Version 7.0 and later allow you to edit the presence and sequence of columns in this manner:

1. Above the list or report, click **Edit Columns**. The supported columns appear in a popup window, as illustrated in Figure 41:

Figure 41 ***Edit Columns*** *Illustration for the* ***Groups > List*** *Page*



2. To remove one or more columns from the **Groups > List** page, click to remove the check mark from the associated checkbox.
3. To change the sequence in which columns appear on the **Groups > List** page, place your cursor over the drag-and-drop icon, left click, move the column to the new position, and release.
4. Click **Save** to retain your settings. The **Groups > List** page displays your changes.

The following pages include columns able to be edited for data display:

- **Home > Search** (results)
- **Helpdesk > Incidents**
- **Groups > List**
- **Groups > Monitor**
- **Groups > Cisco WLC Config**
- **APs/Devices > List**
- **APs/Devices > New**
- **APs/Devices > Up**
- **APs/Devices > Down**
- **APs/Devices > Mismatched**
- **APs/Devices > Ignored**
- **Users > Connected**
- **Users > All**
- **Users > Guest Users**
- **Users > Tags**
- **Reports > Generated**
- **Reports > Definitions (defining report setup)**
- **Device Setup > Discover**
- **Device Setup > Alcatel Lucent Configuration** (and several additional pages in this section)
- **OV3600 Setup > NMS**

- **OV3600 Setup > RADIUS Accounting**
- **RAPIDS > Rogue APs**
- **RAPIDS > Score Override**

Configuring Basic Group Settings

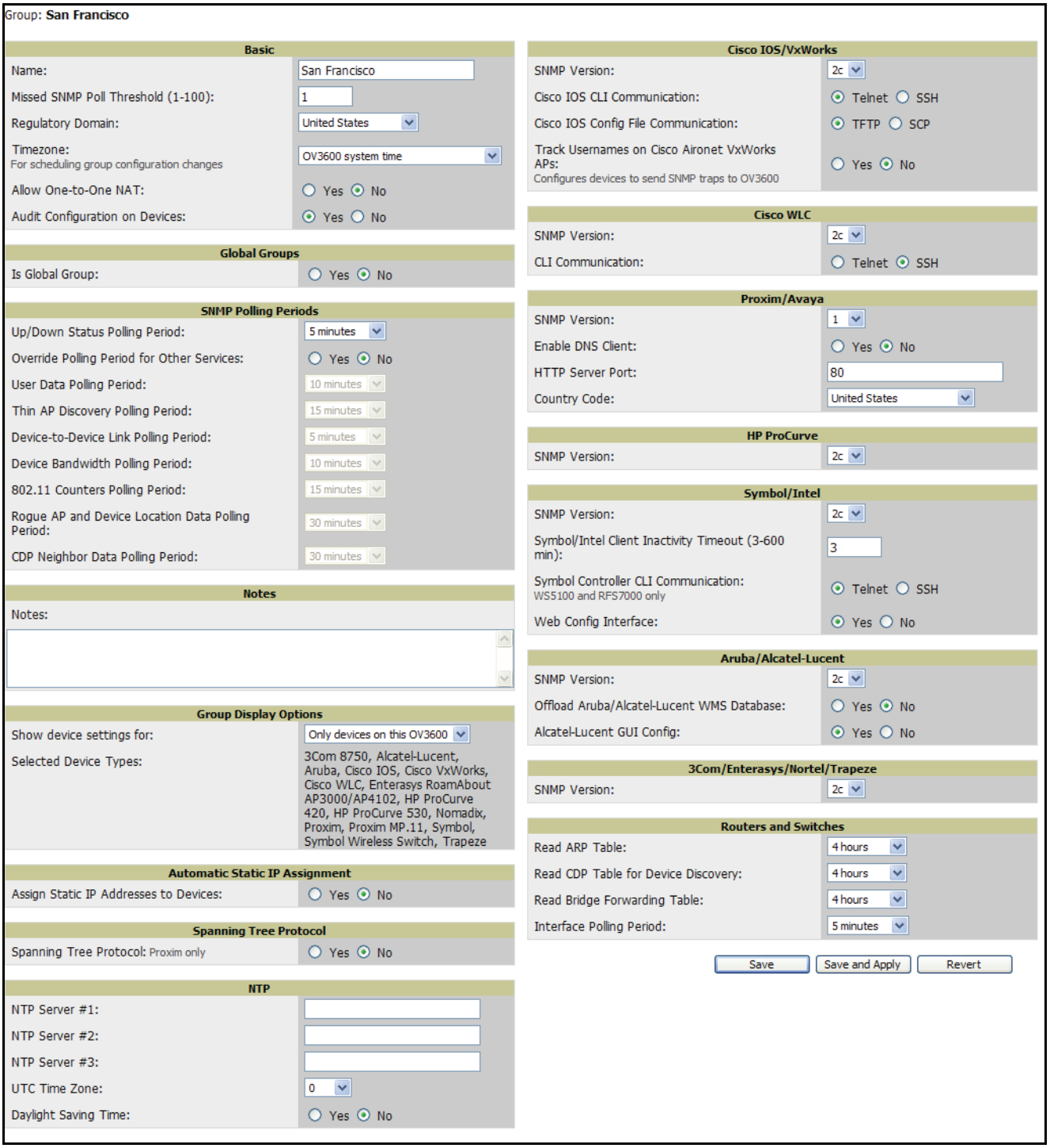
The first default device group that OV3600 sets up is the **Access Points** group, but you can use this procedure to add and configure any device group. Perform these steps to configure basic group settings, then continue to additional procedures to define additional settings as required.

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

   To edit an existing device group, click the **manage** (wrench) icon next to the group. The **Group > Basic** page appears. If you hover your cursor over an existing group's manage (wrench) icon, a popup menu appears after a moment, and allows you to click **Basic**, **Templates**, **Security**, **SSIDs**, **AAA Servers**, or **Radio** to edit those pages as desired.

Figure 42 illustrates the **Groups > Basic** page. Page content differs according to the devices that a group contains. This page may change over time as you add or remove devices from the group.

Figure 42 ***Groups > Basic*** *Page Illustration*



3. Define the settings in the **Basic** and **Global Group** sections. Table 37 describes several typical settings and default values of this **Basic** section.

Table 37 ***Groups > Basic*** *Page >* ***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 user-definable name to uniquely identify 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).
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 for Groups	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.
Global Groups	No	When enabled, this field allows you to define the device group to be a global group. Refer also to “Using Global Groups for Group Configuration” on page 132.

4. Complete the **SNMP Polling Periods** section. The information in this section overrides default settings. Table 38 describes the SNMP polling settings.

Table 38 ***Groups*** *>* ***Basic*** *Page >* ***SNMP Polling Period*** *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** configuration page. Alcatel Lucent recommends an initial polling interval of **5** minutes for most networks.
Override Polling Period for Other Services	No	Radio button enables or disables overriding the base SNMP Polling Period. If you select Yes for this field, then the other settings in the SNMP Polling Periods section are activated, and you can override default values.
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.
Device Bandwidth Polling Period	5 minutes	Sets the interval at which OV3600 polls for the bandwidth being used by a device.
802.11 Counters Polling Period	5 minutes	Sets time between SNMP polls for 802.11 Counter information.

Table 38 ***Groups*** **>** ***Basic*** *Page* **>** ***SNMP Polling Period*** *Fields and Default Values (Continued)*

Setting	Default	Description
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 39 describes the settings and default values.

Table 39 ***Groups > Basic*** *Page* **>** ***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 perform a **Save and Apply** action on the group. • **Only Devices on this OV3600**—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 the OV3600 configuration page • **Selected device types**—Allows the user to specify the device types for which OV3600 displays Group settings.
Selected Device Types	Disabled	If you chose to display selected device types, then this option appears, allowing you to select the device types for which OV3600 displays group settings. Click **Select devices in this group** for a quick way to display only devices in the current 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 40 describes the settings and default values.

Table 40 ***Groups > Basic*** *Page* **>** ***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.

Table 40 ***Groups > Basic*** *Page >* ***Automatic Static IP Assignment*** *Fields and Default Values*

Setting	Default	Description
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 WLSE devices and Proxim APs, locate the Spanning Tree Protocol section on the **Groups > Basic** configuration page. Adjust these settings as required. Table 41 describes the settings and default values.

Table 41 ***Groups > Basic*** *Page,* ***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.
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 42 describes the settings and default values.

Table 42 ***Groups > Basic*** *Page,* ***NTP*** *Fields and Default Values*

Setting	Default	Description
NTP Server #1,2,3	None	Sets the IP address of the NTP server that is 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 43 describes the settings and default values.

Table 43 ***Groups > Basic*** *Page,* ***Cisco IOS/VxWorks*** *Fields and Default Values*

Setting	Default	Description
Cisco IOS SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the AP.

Table 43 ***Groups > Basic*** *Page,* ***Cisco IOS/VxWorks*** *Fields and Default Values (Continued)*

Setting	Default	Description
Cisco IOS 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.
Cisco IOS Config File Communication	TFTP	Sets 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 44 describes the settings and default values.

Table 44 ***Group > Basic*** *Page,* ***Cisco WLC*** *Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies 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.

When configuring Cisco WLC controllers, refer also to "Configuring Wireless Parameters for Cisco Controllers" on page 116.

12. To configure Proxim/Avaya specific settings locate the **Proxim/Avaya** section and adjust these settings as required. Table 45 describes the settings and default values.

Table 45 ***Groups > Basic*** *Page,* ***Proxim/Avaya*** *Fields and Default Values*

Setting	Default	Description
SNMP Version	1	Drop-down menu specifies 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	OV3600 sets this port as the HTTP server port on all Proxim APs in the group.

Table 45 *Groups > Basic* Page, *Proxim/Avaya* Fields and Default Values (Continued)

Setting	Default	Description
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 420 specific settings, locate the **HP ProCurve 420** section and adjust these settings as required. Table 46 describes the settings and default values.

Table 46 *Groups > Basic* Page, *HP ProCurve 420* Fields and Default Values

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies 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 page (CLI) communication. Selecting **telnet** will send the data in clear text via telnet.
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the AP.

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

14. To configure Symbol or Intel-specific settings, locate the **Symbol/Intel** section and adjust these settings as required. Table 47 describes the settings and default values of this section.

Table 47 *Groups > Basic* Page, *Symbol/Intel* Fields and Default Values

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the device.
Symbol/Intel Client Inactivity Timeout (3-600 min)	3	Sets the minutes of inactivity after which a client associated to an Intel or 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	Select which connection type is to support the command-line interface (CLI) connection. The options are **Telnet** and secure shell (**SSH**). This is supported for WS5100 and RFS7000 devices only.
Web Config Interface	Yes	Enables or disables the **`http/https`** configuration page for the Symbol 4131 and Intel 2011 devices.

15. To configure Aruba/Alcatel Lucent-specific settings, locate the **Aruba/Alcatel Lucent** section and adjust these settings as required. Table 48 describes the settings and default values of this section.

Table 48 *Groups > Basic* Page, *Aruba/Alcatel Lucent* Fields and Default Values

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the AP.

Table 48 ***Groups > Basic*** *Page,* ***Aruba/Alcatel Lucent*** *Fields and Default Values (Continued)*

Setting	Default	Description
Offload Aruba/ Alcatel Lucent WMS database	No	Configures commands previously documented in the *Alcatel Lucent Best Practices Guide*. See the current *Best Practices* guide for more information about this feature. 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 controller. The command can be pushed to controllers in manage mode (also without rebooting the controller) if the **Allow WMS Offload** setting on the OV3600 configuration page is changed to **Yes**.
Aruba/Alcatel-Lucent GUI Config	Yes	Enables or disables OV3600 support for the Aruba/Alcatel-Lucent configuration interface. This setting relates to the Device Setup > Aruba/Alcatel-Lucent Configuration page and all related operations. For additional information, refer to the *Aruba/Alcatel-Lucent Configuration Guide*.

16. To configure settings for 3Com, Enterasys, Nortel, or Trapeze devices, locate the **3Com/Enterasys/Nortel/ Trapeze** section and adjust these settings as required. Table 49 describes the settings and default values of this section.

Table 49 ***Groups > Basic*** *Page,* ***3Com/Enterasys/Nortel/Trapeze*** *Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the AP.

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

Table 50 ***Groups > Basic*** *Page,* ***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.
Interface Polling Period	5 minutes	Sets the frequency in which network interfaces are polled. This setting can be disabled, or set to poll bridge forwarding tables from switches in a range from every 15 seconds to 12 hours.

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.

Table 51 ***Groups > Basic*** *Page,* ***Universal Devices, Routers and Switches*** *Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate with universal devices on the network.

19. Click **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 Access Points group. **Save** is a good option if you intend to make additional device changes in the Access Points group, and wish to wait until all configurations are complete before you push all configurations at one time.

    Click **Save and Apply** to save and push these configurations to devices immediately in the Access Points group, or click **Revert** to return to the most recently saved settings.

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.

Configuring Group Security Settings

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

1. Select the device group for which to define security settings from the **Groups > List** page.
2. Select the **Groups > Security** page. Some controls on this page interact with additional OV3600 pages. Figure 43 illustrates this page and Table 52 explains the fields and default values.

Figure 43 ***Groups > Security*** *Page Illustration*

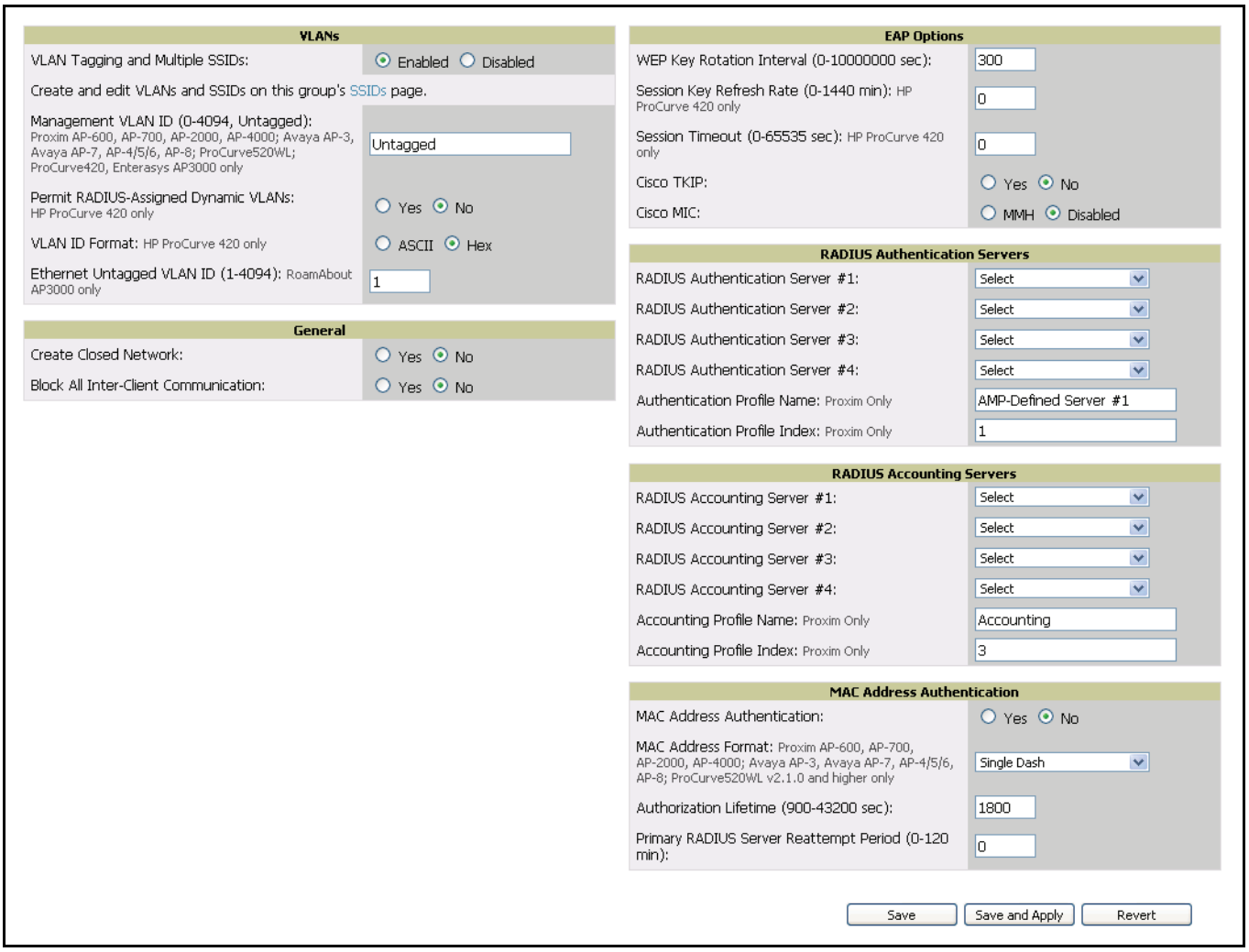


Table 52 ***Groups > Security*** *Page Fields and Default Values*

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 99.

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

Setting	Default	Description
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:** Alcatel Lucent recommends creating a closed network to make it more difficult for intruders to detect your wireless network.
Block All Inter-client Communication	No	If enabled, this setting blocks client devices associated with an AP from communicating with other client devices on the wireless network. **NOTE:** This option may also be identified as PSPF (Publicly Secure Packet Forwarding), which can be useful for enhanced security on public wireless networks.
EAP Options Section		
WEP Key Rotation Interval	300	Sets the frequency at which the Wired Equivalent Privacy (WEP) keys are rotated in the device group being configured. The supported range is from 0 to 10,000,000 seconds.
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.

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

Setting	Default	Description
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 Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8, HP ProCurve 520WL, ProCurve 420 v2.1.0 and higher.
Authorization Lifetime	1800	Sets the amount of time a user can be connected before reauthorization is required. The supported range is from 900 to 43,200 seconds.
Primary RADIUS Server Reattempt Period	0	Specifies the time (in minutes) that the AP awaits responses from the primary RADIUS server before communicating with the secondary RADIUS server, and so forth

3. Click **Save** to retain these Security configurations for the group, click **Save and Apply** to retain and push these configurations, or click **Revert** to return to the last saved security settings for this group.
4. Continue with additional security-related procedures in this document for additional TACACS+, RADIUS, and SSID settings for device groups, as required.

Configuring Group SSIDs and VLANs

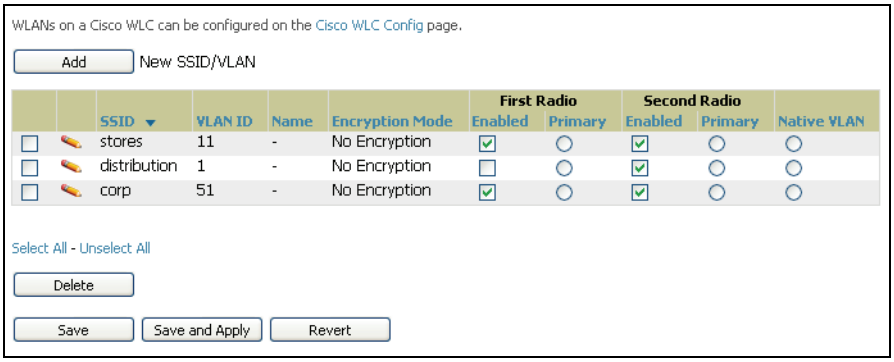
The **Groups > SSIDs** configuration page allows you to create and edit SSIDs and VLANs that apply to a device group. Perform these steps to create or edit VLANs and to set SSIDs.

NOTE

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

Figure 44 illustrates an example of the **Groups > SSIDs** page.

Figure 44 ***Groups > SSIDs*** *Page Illustration*



NOTE

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

NOTE

Multiple VLANs and SSIDs are supported only on Cisco access points.

1. Navigate to the **Groups > List** page and select the group for which to define SSIDs/VLANs by clicking the group name. Alternatively, click **Add** to create a new group, define a group name. In either case, the **Groups > Monitor** page appears.
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*

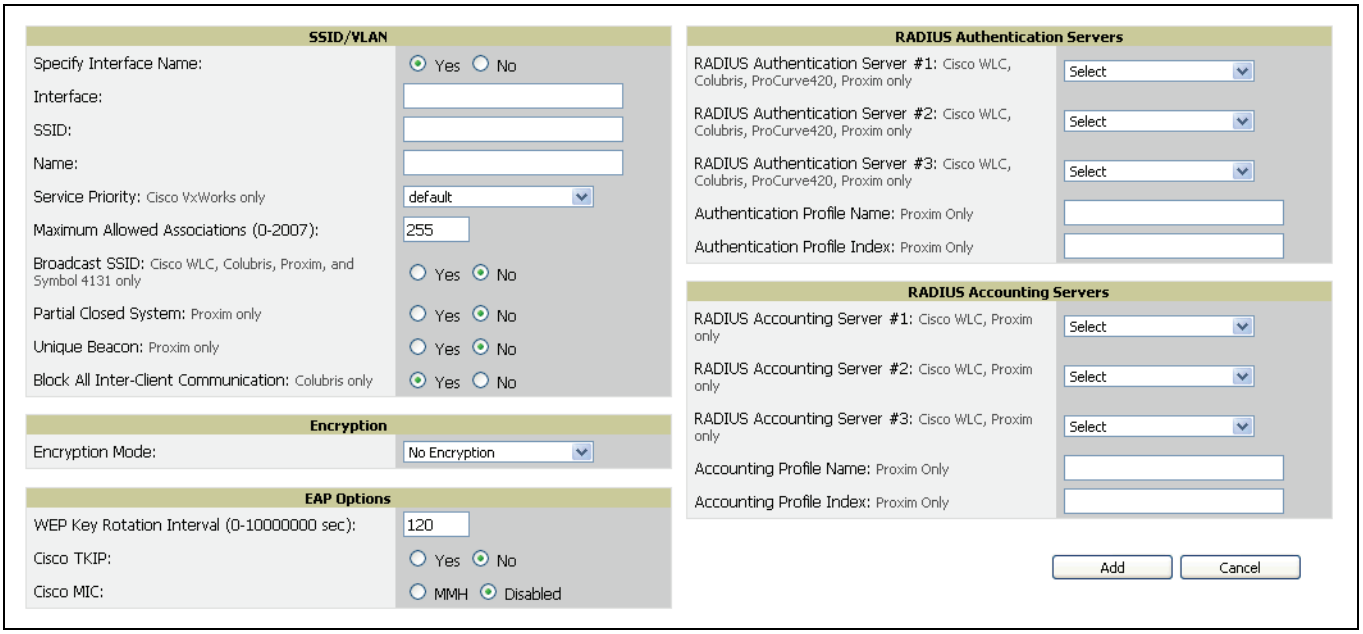
Setting	Description
SSID	Displays the SSID associated with the VLAN.
VLAN ID	Identifies the number of the primary VLAN SSID on which encrypted or unencrypted packets can pass between the AP and the switch.
Name	Displays the name of the VLAN.
Encryption Mode	Displays the encryption on the VLAN.
First or Second Radio Enabled	Checkbox enables the VLAN, SSID and Encryption Mode on the radio control.
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 Create Closed Network below) in which the APs broadcast an SSID, the Primary SSID is the one that is broadcast.

Table 53 ***Groups > SSIDs*** *Fields and Descriptions (Continued)*

Setting	Description
Native VLAN	Selects 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. Some AP types do not require a native VLAN. For those APs, you need to create a dummy VLAN, disable it on both radio controls and ensure that it has the highest VLAN ID.

3. Click **Add** to create a new SSID or VLAN, or click 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 45 and explained in Table 54.

Figure 45 ***Groups > SSIDs > Add SSID/VLAN*** *Page Illustration*



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.

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

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

Setting	Default	Description
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 and none for Colubris.
Broadcast SSID (Proxim 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	For Colubris only, 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: • **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**—This encryption type is based on the WEP algorithm. • **Require Leap**—Lightweight Extensible Authentication Protocol • **802.1x+WEP**—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

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 (seconds)	120	Time (in seconds) between WEP key rotation on the AP.

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

Setting	Default	Description
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 (Colubris, ProCurve420, Proxim only)	None	Drop-down menu to select RADIUS Authentication servers previously entered on the **Group > 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, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.
Authentication Profile Index (Proxim Only)	None	Sets the Authentication Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.

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

You may need to return to the **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 **Group > 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, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.
Accounting Profile Index (Proxim Only)	None	Sets the Accounting Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.

10. Click **Save** to retain these **Security** configurations for the group, click **Save and Apply** to retain and push these configurations, or click **Revert** to return to the last saved security settings for this group.

11. Continue with additional security-related procedures in this document for additional TACACS+, RADIUS, and SSID settings for device groups, as required.

Adding and Configuring Group AAA Servers

Configure RADIUS servers on the **Group > AAA Servers** page. TACACS+ servers are configured as a part of Cisco WLC configuration, In that case, refer to "Configuring Security Parameters and Functions" on page 116.

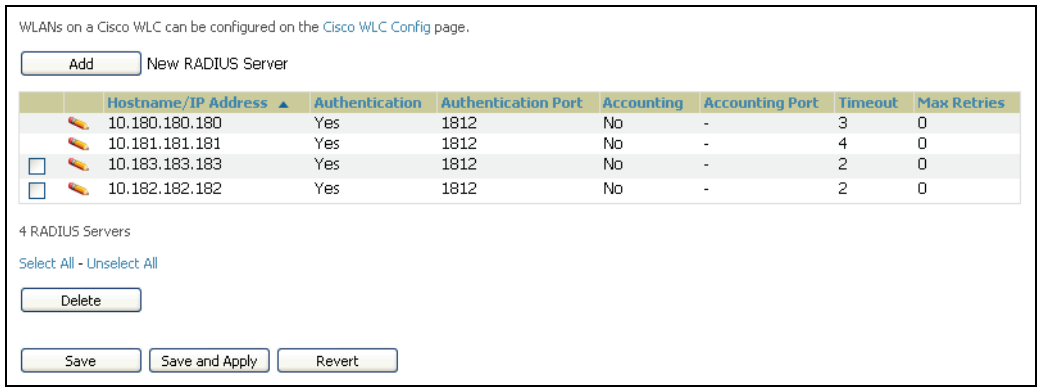
Once defined on this page, RADIUS servers are selectable in the drop-down menus on the **Groups > Security and Groups > SSIDs** configuration pages. Perform these steps to create RADIUS servers.

NOTE

TACACS+ servers are configurable only for Cisco WLC devices. Refer to "Configuring Wireless Parameters for Cisco Controllers" on page 116.

1. Navigate to the **Groups > List** page and select the group for which to define AAA servers by clicking the group name. Alternatively, click **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 **AAA Servers** page. The **AAA Servers** page appears, enabling you to add a RADIUS server. Figure 46 and Figure 47 illustrate this page for AAA RADIUS Servers:

Figure 46 ***Groups > AAA Servers*** *Page Illustration*



3. To add a RADIUS server or edit an existing server, click the **Add New RADIUS Server** button or click the corresponding pencil icon to edit an existing server. Table 59 describes the settings and default values of the **Add/Edit** page.

Figure 47 ***Adding a RADIUS Server*** *Page Illustration*

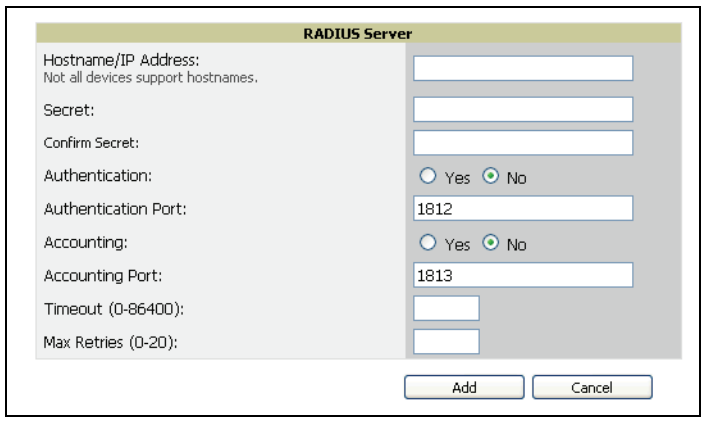


Table 59 ***Adding a RADIUS Server*** *Fields and Default Values*

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. Click **Add** to complete the creation of the RADIUS server, or click **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 clicking **Reports > Generated**, scrolling to the bottom of the page, and clicking **Latest RADIUS Authentication Issues Report**.

OV3600 first checks its own database prior to checking the RADIUS server database.

5. To make additional RADIUS configurations for device groups, use the **Groups > Security** page, and refer to "Configuring Group Security Settings" on page 96.

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.

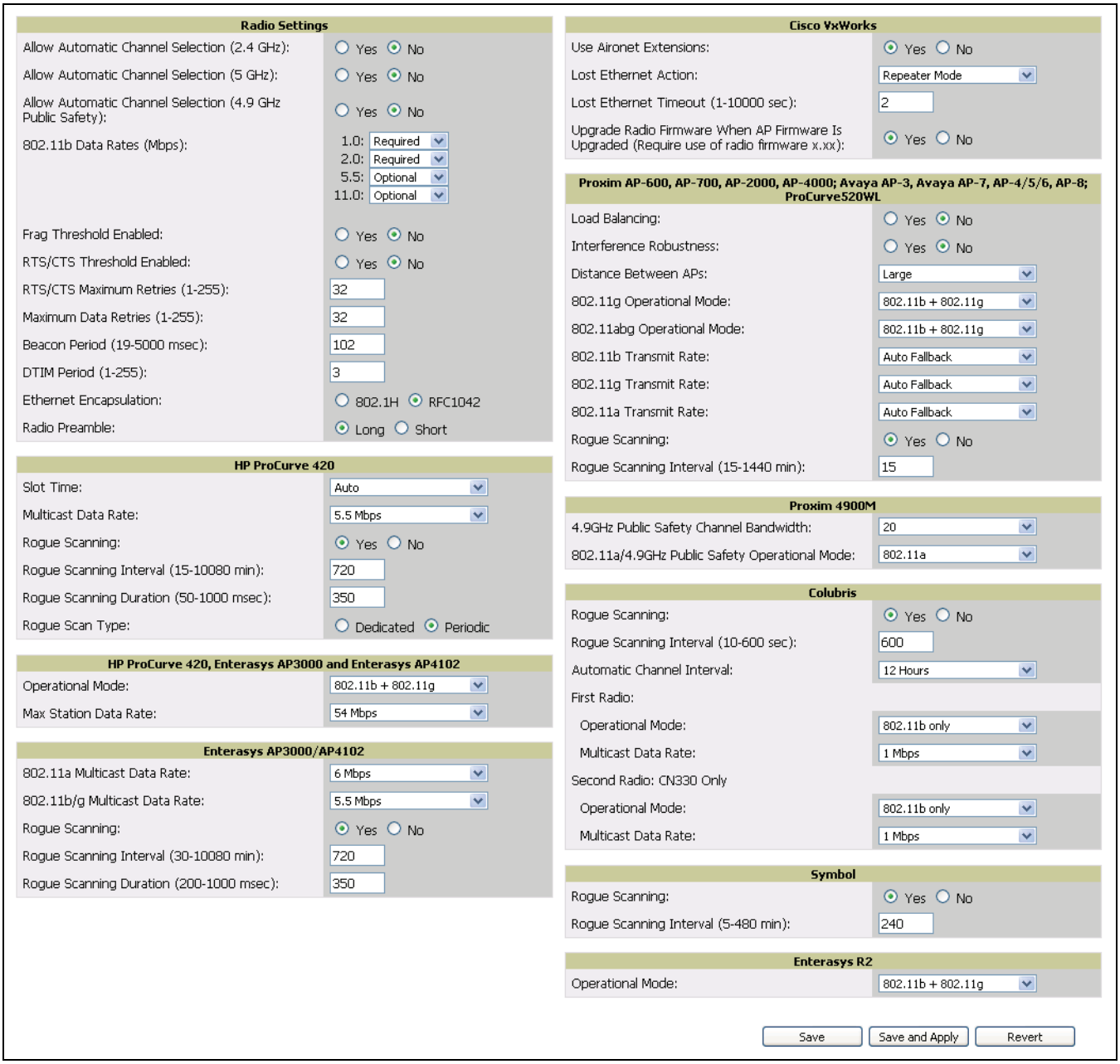
NOTE

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. Navigate to the **Groups > List** page and select the group for which to define radio settings by clicking the group name. Alternatively, click **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Navigate to the **Groups > Radio** page. Figure 48 illustrates this page.

Figure 48 ***Groups > Radio*** *Page Illustration*



3. Locate the **Radio Settings** area and adjust these settings as required. Table 60 describes the settings and default values.

Table 60 ***Groups > Radio*** *Fields and Default Values*

Setting	Default	Description
Allow Automatic Channel Select (2.4, 5 GHz and 4.9GHz)	No	If enabled, whenever the AP is rebooted it uses its radio to scan the airspace and automatically 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 (Mb/sec)	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, Alcatel Lucent recommends leaving 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.
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, Alcatel Lucent recommends leaving 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.
Beacon Period (19-5000 Kμsec)	100	Time between beacons (in kilo microseconds).
DTIM Period (1-255)	2	DTIM alerts power-save devices that a packet is waiting for them. This setting configures DTIM packet frequency as a multiple of the number of beacon packets. The DTIM Interval indicates how many beacons equal one cycle.
Ethernet Encapsulation	RFC1042	This setting selects either the RFC1042 or 802.1h Ethernet encapsulation standard for use by the group.

Table 60 ***Groups > Radio*** *Fields and Default Values (Continued)*

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

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

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

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 61 describes the settings and default values.

Table 61 ***HP ProCurve 420*** *Fields and Default Values in* ***Proprietary Settings***

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.
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 of the **Proprietary Settings** area, and define the settings. Table 62 describes the settings and default values of this page.

Table 62 ***HP ProCurve 240, Enterasys AP 3000 and AP 4102*** *Fields and Default Values in* ***Proprietary Settings*** *Section*

Setting	Default	Description
Operational Mode	802.11b + 802.11g	Sets the radio operational mode for all of the ProCurve 420s, Enterasys 3000s and 4102sin 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 of the **Proprietary Settings** area, and define the settings. Table 63 describes the settings and default values of this page.

Table 63 ***Enterasys AP3000*** *and* ***Enterasys AP4102 > Proprietary Settings*** *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 64 describes the settings and default values of this page.

Table 64 ***Groups > VxWorks*** *Proprietary Settings 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 64 ***Groups > VxWorks*** *Proprietary Settings 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 65 describes the settings and default values.

Table 65 ***Groups > LWAPP APs, Proprietary Settings*** *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 abg 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.

Table 65 ***Groups > LWAPP APs, Proprietary Settings*** *Fields and Default Values (Continued)*

Setting	Default	Description
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 access points in the group (with the appropriate firmware) will passively scan for rogue access points at the specified interval. This rogue scan will not break users' association to the network. **NOTE:** This feature can affect the data performance of the access point.
Rogue 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 66 describes the settings and default values.

Table 66 ***Proxim 4900, Proprietary Settings*** *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 Colubris-only settings in this device group, locate the **Colubris** section and define the required fields. Table 67 describes the settings and default values.

Table 67 ***Colubris****-only Fields and Default Values in* ***Proprietary Settings*** *Section*

Setting	Default	Description
Rogue Scanning	Yes	If enabled, Colubris access points 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 (10-600 secs)	600	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.
Automatic Channel Interval	12 Hours	Sets the frequency by which APs monitor radio channels for availability and activity.
First Radio	802.11b only 1 Mbps	Sets the operational mode and multicast data rate for the first Colubris radio.
Second Radio (CN330 only)	802.11b only 1 Mbps	Sets the operational mode and multicast data rate for the second Colubris radio, supported only for the Colubris CN330.

12. To configure Symbol-only settings, locate the **Symbol** section and define the required fields. Table 68 describes the settings and default values.

Table 68 ***Symbol****-only Fields and Default Values in* ***Proprietary Settings*** *Section*

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.

13. To configure Enterasys R2 settings, locate the **Enterasys R2** section and define the required fields. Table 68 describes the settings and default values.

Table 69 ***Enterasys*** *Section Fields and Default Values*

Setting	Default	Description
Operational Mode	802.11b + 802.11g	Drop-down menu defines the 802.11 settings to support with the Enterasys radio devices in this group. Supported options are as follows: • 802.11a only • 802.11b only • 802.11g only • 802.11b + 802.11g

14. Click **Save** when radio configurations as described above are complete, or click **Save and Apply** to retain changes and push them to network devices. Click **Revert** to return to the last saved 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

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

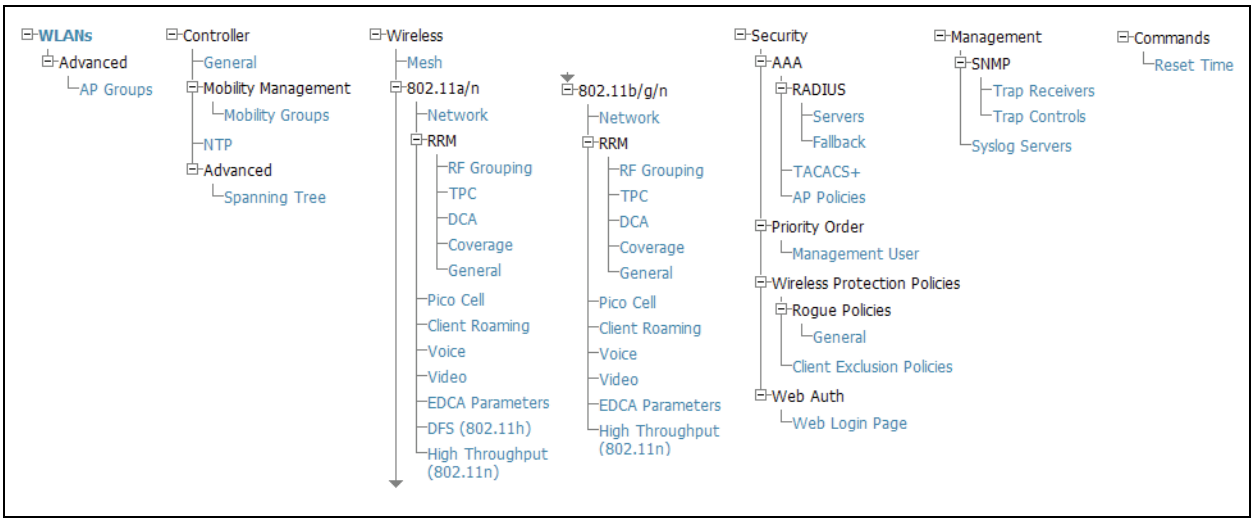
1. Navigate to the **Groups > List** page and select a group that has been defined to support Cisco devices. Click the group name, or the Manage (wrench) icon, and the **Cisco WLC Config** option appears in the navigation pane at the top.
2. Navigate to the **Groups > List** page and create a new group to support Cisco devices with these steps:
   - Click **Add** from the **Groups > List** page to create a new group, enter a group name, and click **Add**.
   - Once OV3600 prompts you with the **Groups > Basic** page, ensure that you enable device specific settings for **Cisco WLC**.
   - Once you click **Save** or **Save and Apply**, then the **Groups > Cisco WLC Config** sub-menu 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 49 and Figure 50 illustrate this navigation pane.

Figure 49 ***Groups > Cisco WLC Config*** *page illustration, contracted view*

Figure 50 ***Groups > Cisco WLC Config*** *page illustration, expanded view*

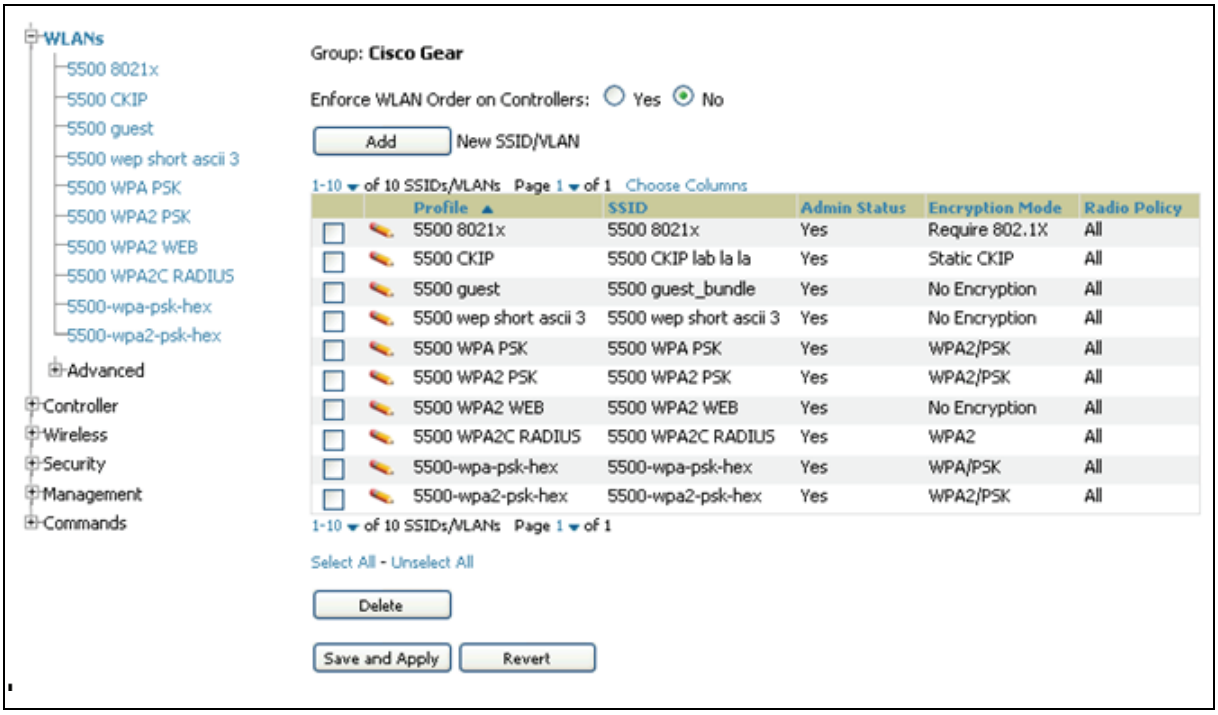


Configuring WLANs for Cisco WLC Devices

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. Navigate to the **Groups > Cisco WLC Config** page, and click **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 51 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 51 ***Groups > Cisco WLC Config > WLANS*** *page illustration*



3. To add or edit SSIDs or VLANs that are dedicated to Cisco WLC devices, either click the **Add New SSID/VLAN** button, or click 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 52 ***Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > General*** *Tab Illustration*

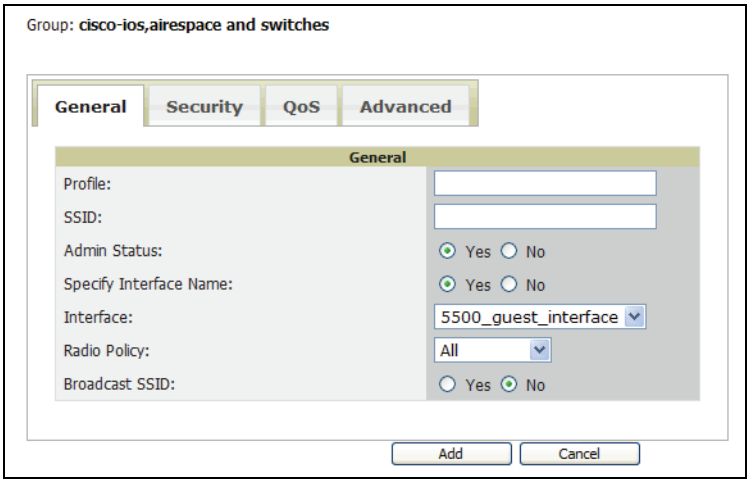


Figure 53 ***Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > Security*** *Tab Illustration*

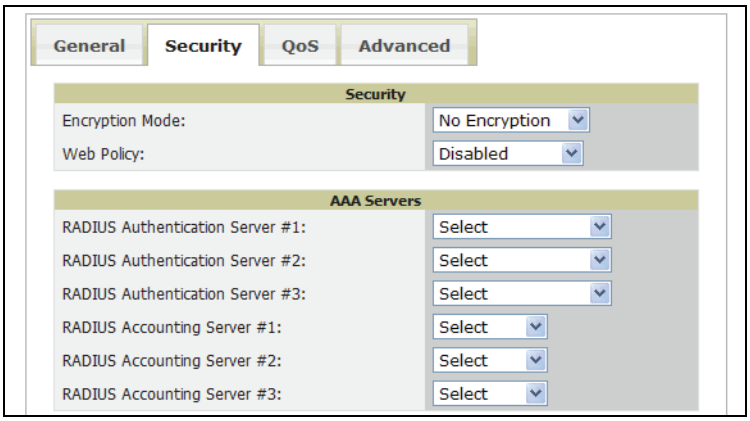


Figure 54 ***Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > QoS*** *Tab Illustration*

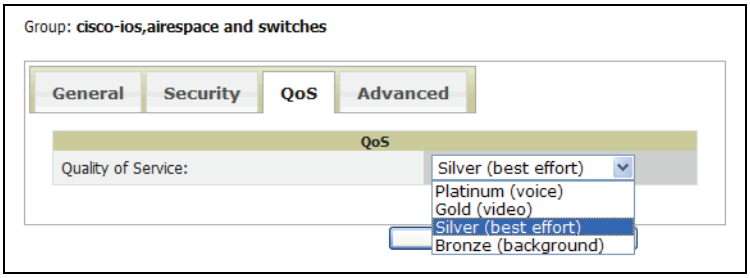
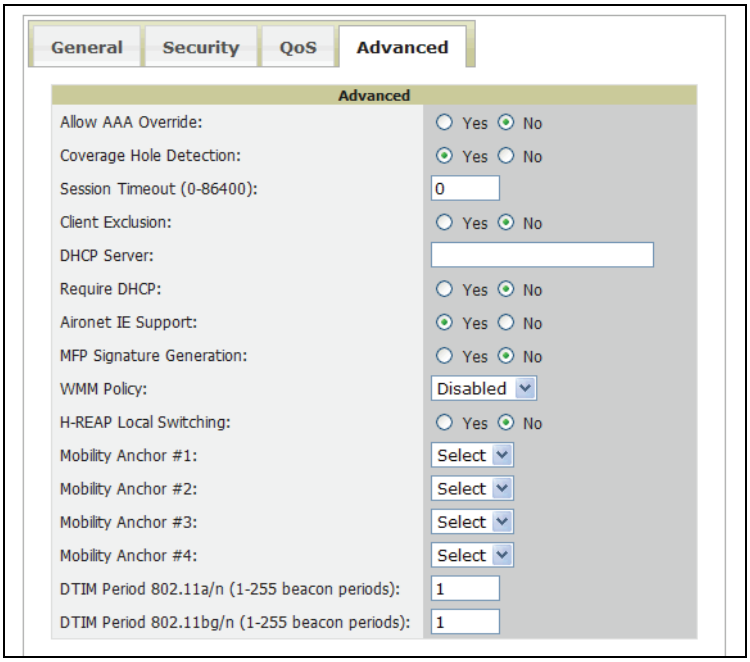


Figure 55 ***Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > Advanced*** *Tab Illustration*



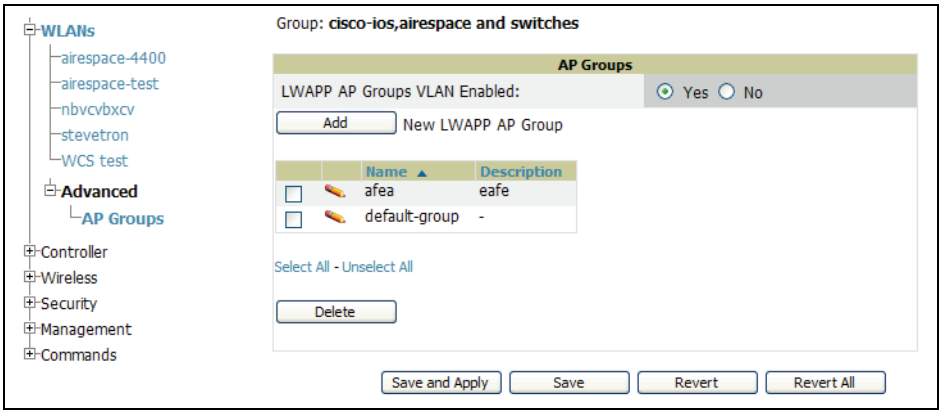
Defining and Configuring LWAPP AP Groups for Cisco Devices

The **Groups > Cisco WLC Config > WLANs > Advanced > AP Groups** page allows the user 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. Navigate to the **Groups > Cisco WLC Config** page, and click **WLANs > Advanced > AP Groups** in the navigation pane at left. This page displays the configured LWAPP APs. Figure 56 illustrates this page.

Figure 56 ***Groups > Cisco WLC Config > WLANS > Advanced > AP Groups*** *Page Illustration*



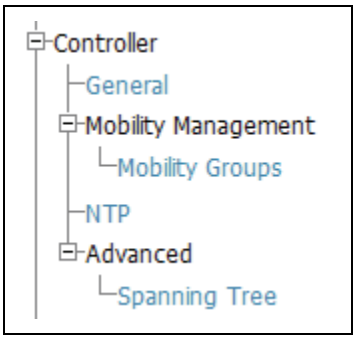
2. To add a new LWAPP AP group, click **Yes** in the **AP Groups** section. Additional controls appear.
3. Click the **Add** button to create a new LWAPP AP group. To edit an existing LWAPP AP group, click the pencil icon next to that group. Add one or more SSIDs and the interface/VLAN ID mapping on the **Add/Edit** page of the LWAPP AP Group.
4. Click **Save and Apply** to push these settings to the Cisco WLC controllers immediately, or click **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, Cisco mobility groups to be supported on Cisco controllers, Network Transfer Protocol (NTP), and Spanning Tree Protocol settings.

Navigate to the **Groups > Cisco WLC Config > Controller** page. This navigation is illustrated in Figure 57.

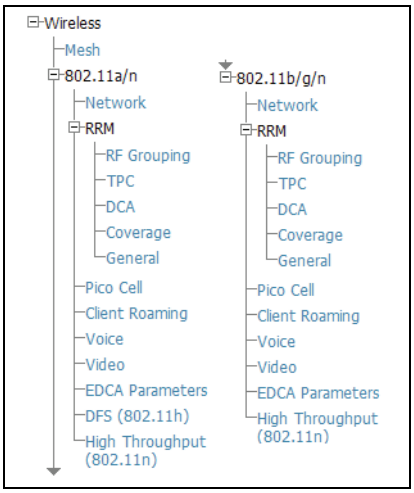
Figure 57 ***Groups > Cisco WLC Config > Controller*** *Navigation*



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 58.

Figure 58 ***Groups > Cisco WLC Config > Wireless*** *Navigation Illustration*



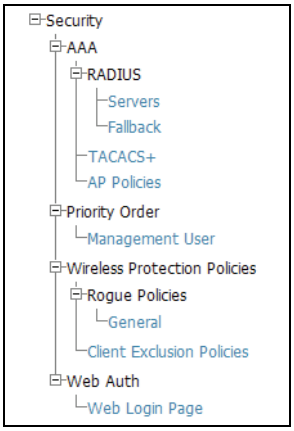
Configuring Security Parameters and Functions

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 59 illustrates these components and this navigation:

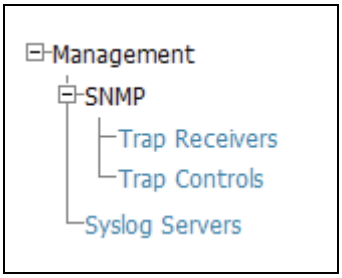
Figure 59 ***Groups > Cisco WLC Config > Security*** *Navigation Illustration*



Configuring Management Settings for Cisco Controllers

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, navigate to the **Groups > Cisco WLC Config > Management** page, illustrated in Figure 60.

Figure 60 ***Groups > Cisco WLC Config > Management*** *Navigation Illustration*



Configuring Group PTMP/WiMAX Settings

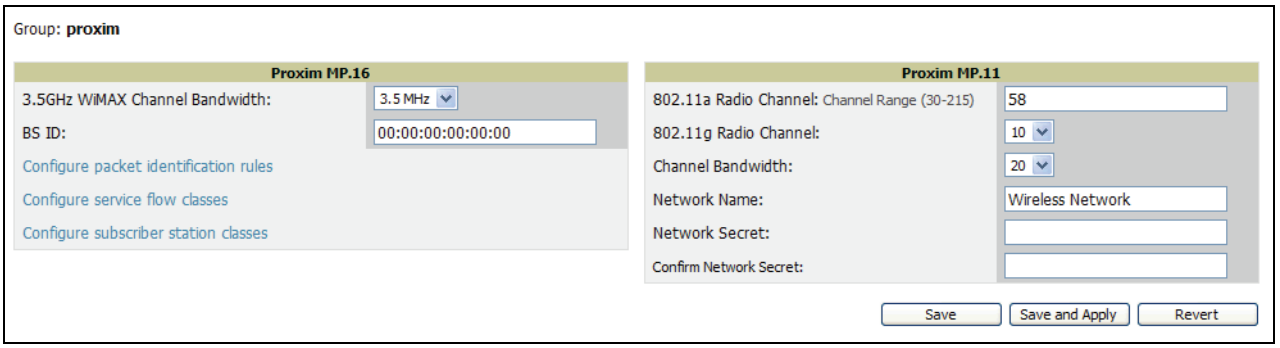
The **Groups > PTMP/WiMAX** configuration page configures Point-to-Multipoint and WiMAX settings for all subscriber and base stations in the device group. Subscriber stations must be in the same group as all base stations with which they might connect.

Packet identification rules (PIR) are used to identify traffic types. Service flow classes define the priority given to traffic. Subscriber Station classes link traffic types (PIRs) with service flow classes to fully define how packets should be handled.

Perform the following steps to configure these functions.

1. Navigate to the **Groups > List** page and select the group for which to define PTMP/WiMAX settings by clicking the group name. Alternatively, click **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Click the PTMP/WiMAX tab in the OV3600 navigation menu. Figure 61 illustrates this page.

Figure 61 ***Groups > PTMP/WiMAX*** *Page Illustration*



3. Define the settings on this page. Table 70 describes the settings and default values.

Table 70 ***Groups > PTMP/WiMAX*** *Fields and Default Values*

Setting	Default	Description
Proxim MP.16 Section		
3.5GHz WiMAX Channel Bandwidth	3.5GHz	Sets the frequency used by the WiMAX devices in the group.
BSID	00:00:00:00:00:00	Defines the BSID used by the subscriber stations in the group. To define the BSID for a base station, refer to its **APS/Devices > Manage** configuration page.
Configure Packet Identification Rules	N/A	This link takes you to the list of packet identification rules for the group being configured. You can select rules to apply and add new rules, then return to the Group WiMAX page.
Configure Service Flow Classes	N/A	This link takes you to the list of service flow classes for the group being configured. You can select service flow classes to apply and add new classes, then return to the Group WiMAX page.
Configuration Subscriber Station Classes	N.A	This link takes you to the list of subscriber station classes. You can select subscriber station classes to apply and add new classes, then return to the Group WiMAX page.
Proxim MP.16 Section		

Table 70 ***Groups > PTMP/WiMAX*** *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. To configure packet identification rules, click the **Configure packet identification rules** link on the **Groups > PTMP/Wimax** configuration page and define the settings as required. Packet identification rules are used to define which packets match a subscriber station class. Figure 62 illustrates this page and Table 71 describes the settings and default values.

Figure 62 ***Groups > PTMP/WiMAX Configuring Packet Identification Rules*** *Page Illustration*

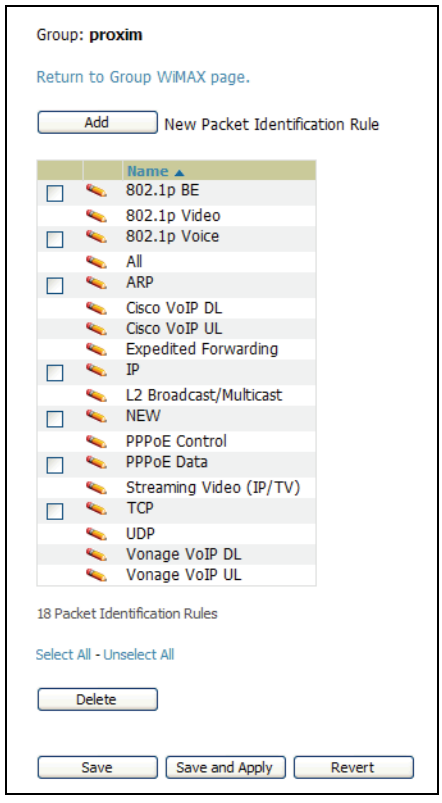


Table 71 ***Groups > PTMP/WiMAX Configuring Packet Identification Rules*** *Fields and Default Values*

Setting	Default	Description
Name	None	Text field defines a name for the PIR. The name should be meaningful and descriptive. The name is used to define the subscriber station class.
Use IP TOS	No	Identifies packets based on IP Type-of-Service for the PIR.

Table 71 ***Groups > PTMP/WiMAX Configuring Packet Identification Rules*** *Fields and Default Values*

Setting	Default	Description
Minimum TOS Value (positive integer)	0	Specifies the minimum TOS used to identify packets.
Maximum TOS Value (positive integer)	0	Specifies the maximum TOS used to identify packets
Mask (positive integer)	0	Specifies the TOS mask used to identify packets.
Use Ethernet Type	No	Identifies packets based on Ethernet type settings.
Ethernet Type	DIX SNAP	Drop-down menu specifies the Ethernet types used to identify a packet.
Ethernet Value (positive integer)	0	Identifies packets that have a specific ethernet value.
Ethernet Priority	No	Identifies packets based on Ethernet Priority settings.
Ethernet Priority Minimum (0-7)	None	Identifies packets that meet a minimum priority.
Ethernet Priority Maximum (0-7)	0	Identifies packets that meet a maximum priority.
Use VLAN ID	No	Identifies packets based on the VLAN ID.
VLAN ID (positive integer)	0	Specifies the VLAN that will be used to identify packets.
Use Source IP Address	No	Identifies packets based on source IP address.
Source IP address	None	Defines the source IP addresses that will be used to identify packets.
Use Destination IP Address	No	Identifies packets based on destination IP address.
Destination IP Address	None	Defines the destination IP addresses that will be used to determine identify packets.
Use IP Protocol	No	Identifies packets based on IP protocol.
IP Protocol (0-255)	None	Identifies packets that have a specific IP Protocol value.
Use Source MAC Address	No	Identifies packets based on Source MAC address.
Source MAC Address	None	Defines that packets from this MAC address match this PIR.
Use Destination MAC Address	No	Identifies packets based on Destination MAC address
Destination MAC Address	None	Defines that packets to this destination MAC address match this PIR.

5. To configure service flow classes, click the **Configure service flow classes** link on the **Groups > PTMP/Wimax** configuration page, and define the settings. Service flow classes are used to describe how the device handles traffic. Figure 63 illustrates this page and Table 72 describes settings and default values.

Figure 63 ***Groups > PTMP/WiMAX Configuring Service Flow Classes*** *Page Illustration*

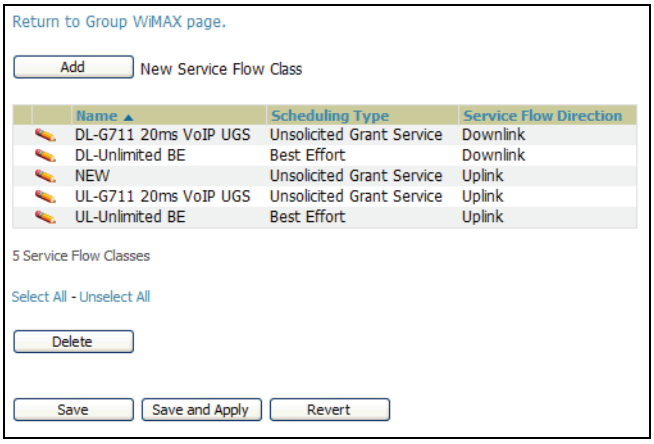


Table 72 ***Groups > PTMP/WiMAX Configure Service Flow Classes*** *Fields and Default Values*

Setting	Default	Description
Name	None	Text field defines the name of the Service Flow Class. The name should be meaningful and descriptive. The name is used to define the subscriber station class.
Scheduling Type	Best Effort	Drop-down menu specifies the scheduling priority for the Service Flow Class. There are two options as follows: • **Best Effort**—Maximum sustained data rate and traffic priority • **Unsolicited Grant Service**—Maximum sustained data rate, maximum latency and tolerable jitter.
Service Flow Direction	Uplink	Defines the direction of the service.
Maximum Sustained Data Rate (in Kbps)	0	Sets the maximum sustained data rate for this service class. The base station does not allow the data rate to exceed this value.
Traffic Priority (0-7)	7	Sets the priority of the traffic from 0 - 7 with 7 getting the highest priority.

6. To configure subscriber station classes, click the **Configure subscriber station classes** link on the **Groups > PTMP/Wimax** configuration page. Subscriber station classes link packet identification rules and service flow classes. Figure 64 illustrates this page and Table 73 describes the settings and default values.

Figure 64 ***Groups > PTMP/WiMAX Configuring Subscriber Station Classes*** *Page Illustration*

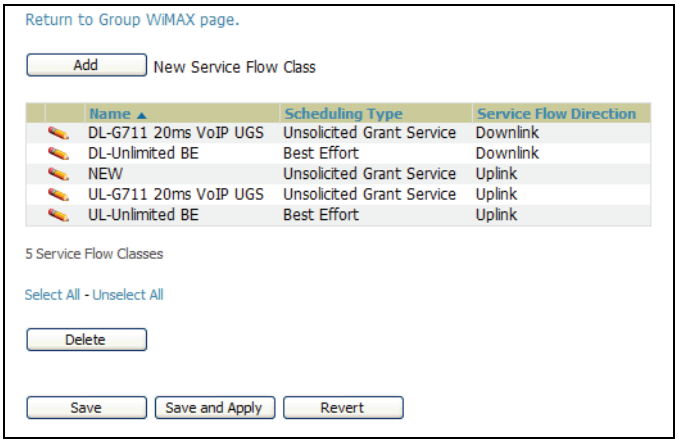


Table 73 ***Groups > PTMP/WiMAX Configuring Subscriber Station Classes*** *Fields and Default Values*

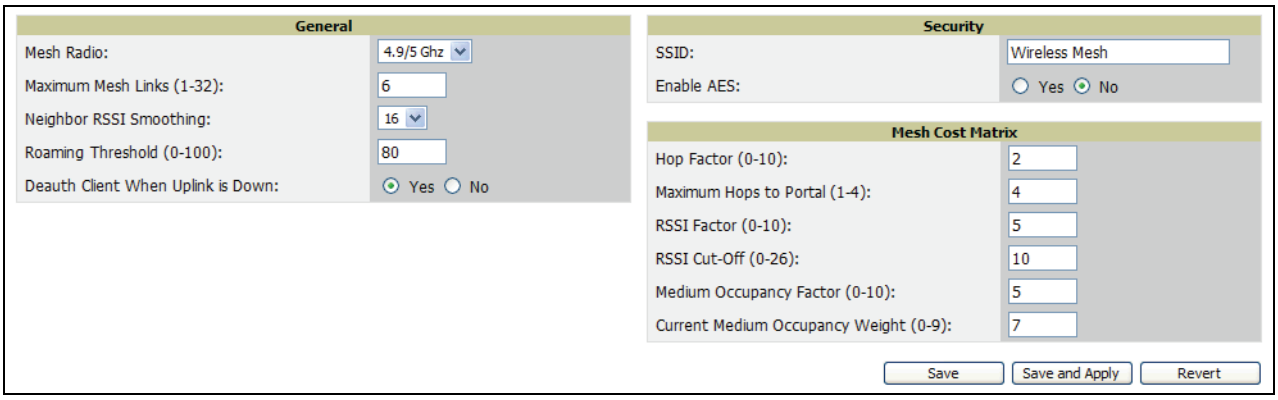
Setting	Default	Description
Name	None	Text field that defines the name of the Subscriber Station Class. The name should be meaningful and descriptive.
VLAN Mode	Transparent	Defines the VLAN mode.
Service Flows	None	Checkbox field that defines the service flow classes that apply to this Subscriber Station Class.
Packet Identification Rules	None	Define the priority for all of the packet identification rules.

7. Click **Save and Apply** when configurations are complete and to push this configuration to controllers, or click **Save** to retain these settings prior to pushing to controllers at a later time.

Configuring Proxim Mesh Radio Settings

1. Navigate to the **Groups > Proxim Mesh** configuration page to configure Mesh-specific radio settings.
2. Define the settings as required for your network. Figure 65 illustrates this page. Table 73 and Table 75 describe the settings and default values.

Figure 65 ***Groups > Proxim Mesh*** *Page Illustration*



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

Table 74 ***Groups > Mesh Radio Settings > 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.
De-auth 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 75 ***Groups > Mesh Radio Settings > 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 Count 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 76 describes these settings and default values.

Table 76 ***Groups > Mesh Radio Settings > Mesh Count 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.
Minimum RSSI Cutoff	10	Specifies the minimum RSSI needed to become a mesh neighbor.
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. Click **Save** when configurations are complete to retain these settings. Click **Save and Apply** to retain these settings and push them to devices in the group. Click **Revert** to cancel out of these changes and return to the most recently saved changes.

Configuring Group MAC Access Control Lists

This configuration is optional. If you use Symbol 4121/4131, Intel 2011/2011b, 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.

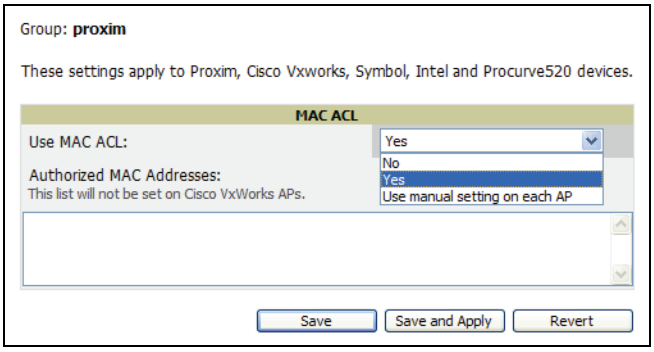
NOTE

If **User 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 66 illustrates this configuration page.

Figure 66 ***Groups > MAC ACL*** *Page Illustration*



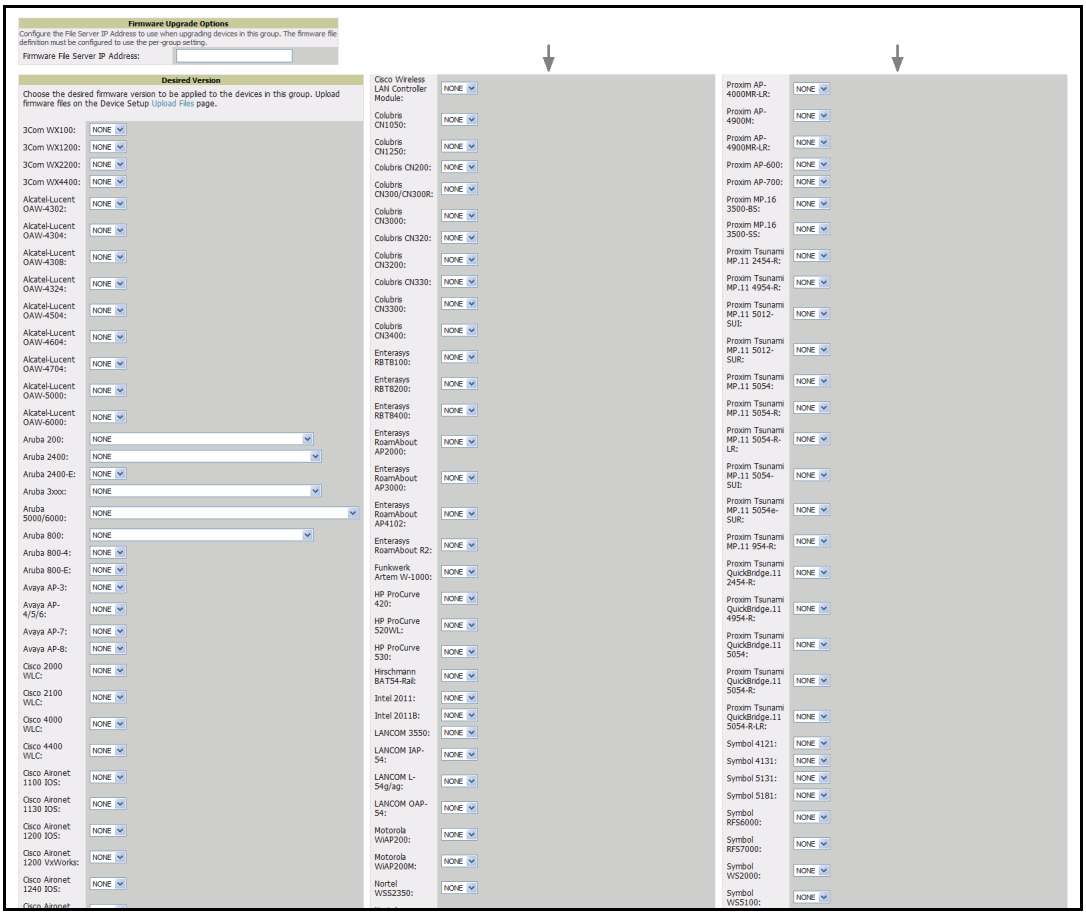
2. Select **Yes** on the **Use MAC ACL** drop-down menu. Enter all authorized MAC addresses, separated by white spaces.
3. Click **Save** when configurations are complete to retain these settings. Click **Save and Apply** to retain these settings and push them to devices in the group. Click **Revert** to cancel out of these changes and return to the most recently saved 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 67 illustrates this page.

Figure 67 ***Groups > Firmware*** *Page Illustration (Partial View)*



2. For each device type in the group, use the pull-down menu to specify the minimum acceptable firmware version. If no firmware versions are listed, you must browse to the **Device Setup > Firmware** configuration page to upload the firmware files to OV3600.
3. Click **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. Click **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 the OV3600 configuration page.
7. Browse to the **Groups > List** configuration page. See Figure 41 for the **Groups > List** configuration page.

8. From the list of groups, check the **Default** radio button next to the desired default group to make it the default.

Comparing Device Groups

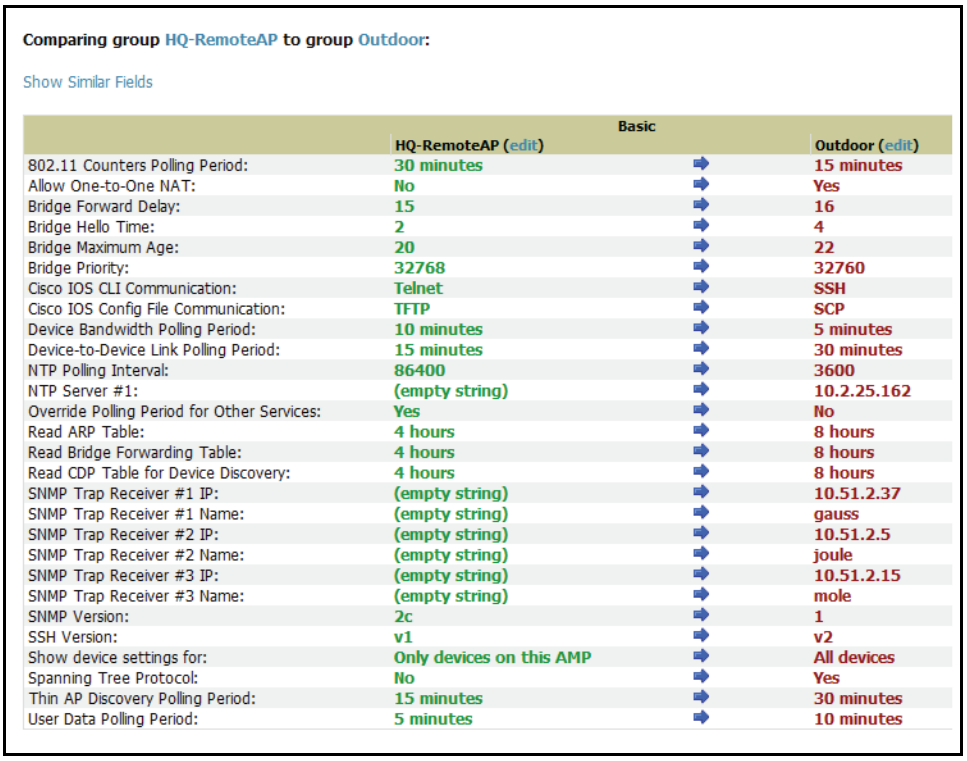
You can compare two existing device groups with a detailed line-item comparison. Group comparison allows several levels of analysis to include the following:

- 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, click **Compare two groups**. Two drop-down menus appear.
2. Select the two groups to compare to each other in the drop-down menus, and click **Compare**. The **Compare** page appears, displaying some or many configuration categories. Figure 68 illustrates this page.

Figure 68 *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
SNMP Trap Receiver #1 IP:	(empty string)	10.51.2.37
SNMP Trap Receiver #1 Name:	(empty string)	gauss
SNMP Trap Receiver #2 IP:	(empty string)	10.51.2.5
SNMP Trap Receiver #2 Name:	(empty string)	joule
SNMP Trap Receiver #3 IP:	(empty string)	10.51.2.15
SNMP Trap Receiver #3 Name:	(empty string)	mole
SNMP Version:	2c	1
SSH Version:	v1	v2
Show device settings for:	Only devices on this AMP	All devices
Spanning Tree Protocol:	No	Yes
Thin AP Discovery Polling Period:	15 minutes	30 minutes
User Data Polling Period:	5 minutes	10 minutes

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, click **Show Similar Fields** at the top left of the page. The result may be a high volume of information.
     - Click **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 clicking **Edit** in the corresponding column heading. The appropriate configuration page appears.
- If you make and save changes to either or both groups, navigate back to the **Groups > List** page and click **Compare two groups**. Select the same two groups again for updated information.
- Additional topics in this document or in the *Alcatel Lucent Configuration Guide* 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:

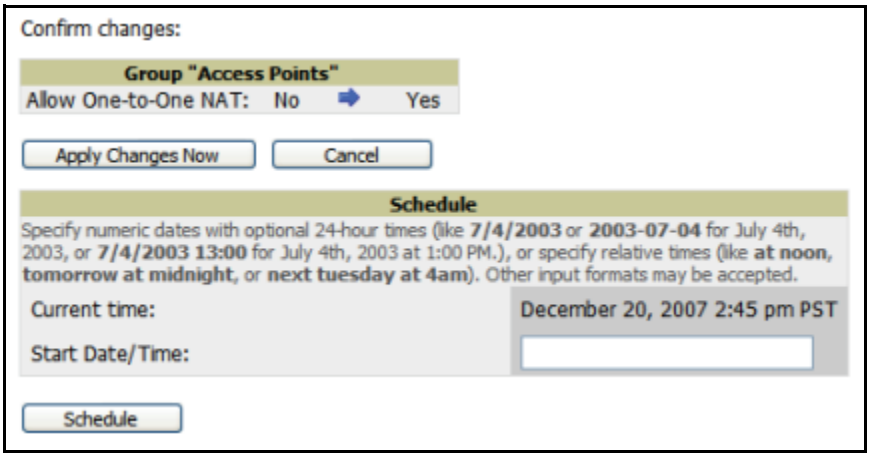
1. Browse to the **Groups > List** configuration page.
2. Ensure that the Group you wish to delete is not marked as the **default** group. OV3600 does not permit you to delete the current default Group.
3. Ensure there are no devices in the Group you wish to delete. OV3600 does not permit you to delete a Group that still contains managed devices. You must move all devices to other Groups before deleting a Group.
4. Select the checkbox and click **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. Click 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 navigate 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, or click **Save and Apply** to save and push configurations.
4. When all changes for the group are complete click the **Save and Apply** button. Figure 69 illustrates the confirmation message that appears.

Figure 69 *Configuration Change Confirmation*



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** —This button applies the changes immediately to access points within the group. If you wish to edit multiple groups you must use the Preview button.
   - **Schedule**—This button 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 **Group > Basic** configuration page.

- **Cancel**—This button cancels the application of changes (immediately or scheduled).

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

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

Modifying Multiple Devices

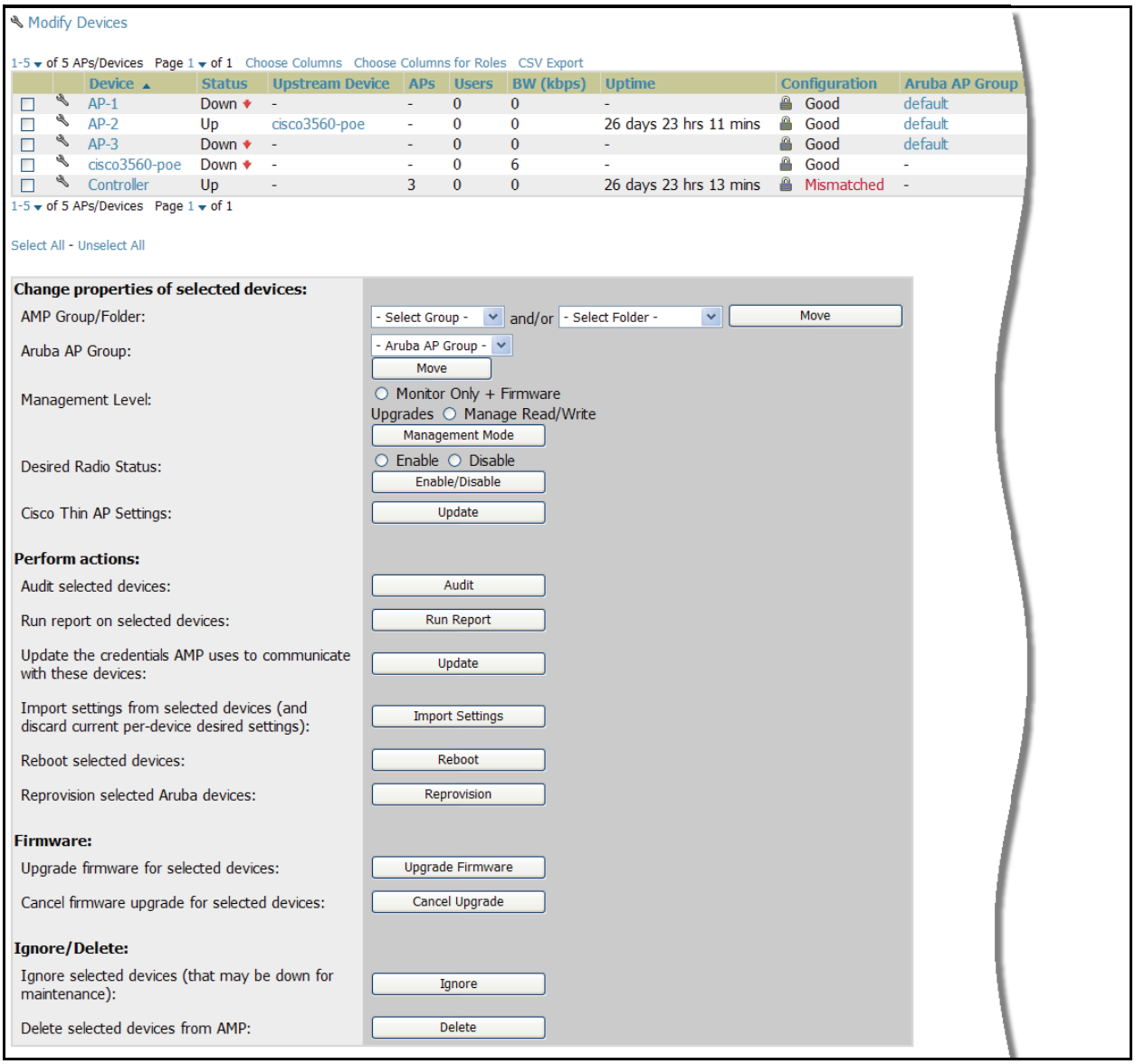
OV3600 provides a very powerful utility that modifies all APs or a subset of access points unrelated to the typical OV3600 group construct. This utility provides the ability to delete simultaneously multiple devices, migrate multiple devices to another group and/or folder, update credentials and optimize channels. Perform these steps to modify multiple devices.

1. To modify multiple devices, navigate to one of the following pages:
   - **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

2. Click **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. Figure 70 illustrates this page.

Figure 70 ***Modify Multiple Devices*** *Section Illustration*



3. Select one or more devices that are to share the configurations. Click inside the checkbox for each device to modify.
4. In the Modify Multiple Devices section, click 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 77 describes these action and controls.

Table 77 ***Modify Multiple Devices*** *Section Fields and Default Values*

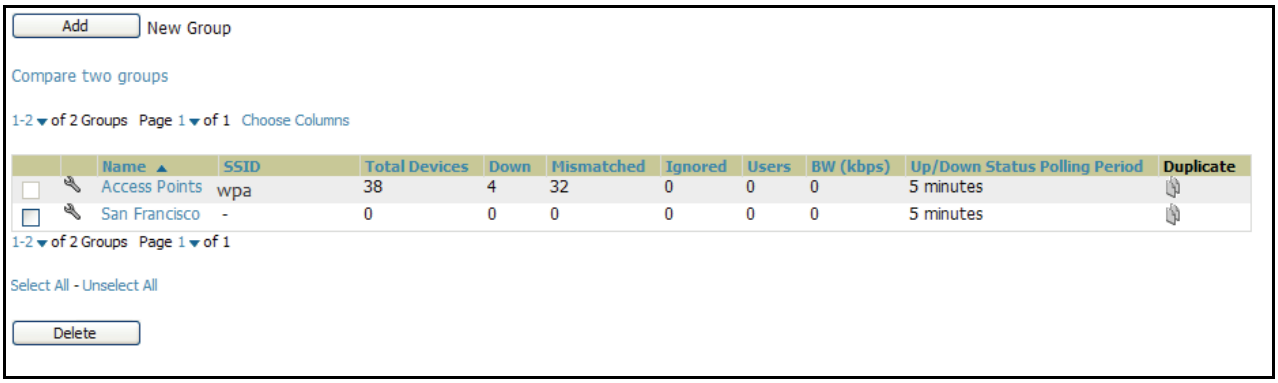
Action	Description
Set Group/Folder	Move the selected devices to a new group or folder. If the AP is in managed mode when it is moved to a new group, it will be reconfigured.
Move to Aruba/Alcatel-Lucent AP Group	Moves the selected APs to a new group or folder. If the AP is in managed mode when it is 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, is now available here.
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 273.
Update the credentials OV3600 uses to communicate with these devices	**Update...** changes the credentials OV3600 uses to communicate with the device. **Update...** 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 Aruba/ Alcatel-Lucent devices	Configures the controller 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.
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 clicking the **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 navigate to the **Groups > List** configuration page. Click the **Add** button to add a new group, or click the name of the group to edit settings for an existing group. Click the **Duplicate** icon to create a new group with identical configuration to an existing group.

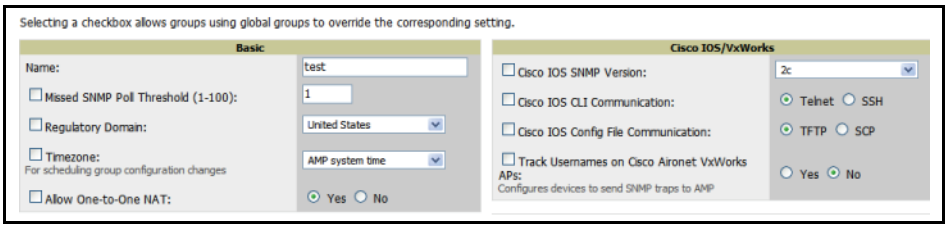
- To have global group status, a group must contain no devices; accordingly, access points can never be added to a global group. Global groups are visible to users of all roles, so they may not contain devices, which can be made visible only to certain roles. Figure 71 illustrates this configuration page.

Figure 71 ***Groups > List*** *Page Illustration*



- To set a group as a global group, navigate 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 check box next to fields on the **Basic, Security, SSIDs, AAA Servers, Radio, Cisco WLC Config, LWAPP APs, PTMP/WiMAX, Proxim Mesh** and **MAC ACL** tabs. Figure 72 illustrates this configuration page.

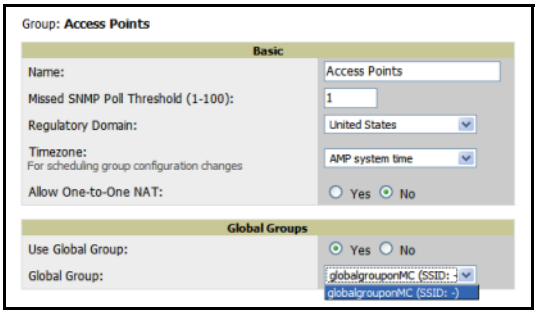
Figure 72 ***Groups > Basic Page*** *for a Global Group*



- 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 (navigate to the **Groups > SSIDs** configuration page and click the **Add** button). Global templates are also configurable as part of global groups; see "Creating and Using Templates" on page 185 for more information.
- Once global groups have been configured, groups may be created or configured to subscribe to a particular global group. Navigate to the **Group > 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

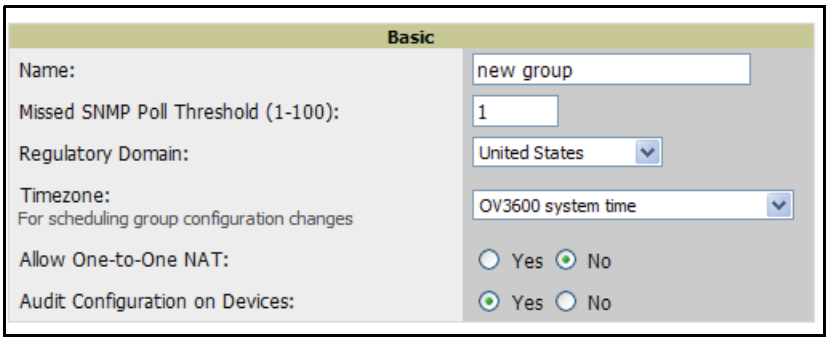
drop-down menu. Then click **Save and Apply** to push the configuration from the global group to the subscriber group. Figure 73 illustrates this page.

Figure 73 ***Groups > Basic > Managed*** *Page Illustration*



- 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.
- In the example below, the field **Name** was overridden with the checkbox in the global group, so it can be configured for each subscriber group. The other four fields in the **Basic** section were not overridden, so they are static fields that will be the same for each subscriber group. These fields can be altered only on the global group.

Figure 74 ***Groups > Basic > Managed*** *Illustration for a Subscriber 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 Stations with the Master Console" on page 250.

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 **OV3600 Device Setup** tab:

- "Device Discovery Overview" on page 135
- "Discovering and Adding Devices" on page 135
- "Monitoring Devices" on page 151
- "Configuring and Managing Devices" on page 168
- "Troubleshooting a Newly Discovered Device with Down Status" on page 182

Device Discovery Overview

Once you have deployed OV3600 on the network, the next step is to discover all existing APs connected to your network. OV3600 has added the ability to discover and provision Cisco edge switches, and the ability to discover and monitor HP ProCurve and NetGear edge switches. You can gather statistics and generate reports displaying wired port usage, and error counting. Individual interface monitoring and configuration has also been added.

OV3600 allows device discovery in the following ways, all of which are described in this chapter:

- **SNMP/HTTP scanning**—This is the primary method for OV3600 to discover devices on your network, and this discovery method contains four specific procedures. The interface that configures this discovery method is the **Device Setup > Discovery** page. See "SNMP/HTTP Scanning" on page 136.
- **Cisco Discovery Protocol (CDP)**—OV3600 enhances support for CDP by discovering a device's CDP neighbors. See "Enabling Cisco Discovery Protocol (CDP)" on page 141.
- **Manual device entry**—This method of discovery applies when the devices are already on your network. The **admin** user adds devices manually with known device information. See the following section for information and procedures:
  - "Assigning Devices to OV3600 from APs/Devices > New Page" on page 142
  - "Manually Adding Individual Devices" on page 144
  - "Adding Multiple Devices from a CSV File" on page 148
  - "Adding Universal Devices" on page 149
- **Controller-driven device discovery**—Thin APs will automatically be added to the network when you add their controller to OV3600.

Discovering and Adding Devices

Devices are prepared for discovery in the ways described in the previous section. This section describes the following topics:

- SNMP/HTTP Scanning
- Enabling Cisco Discovery Protocol (CDP)
- Assigning Devices to OV3600 from APs/Devices > New Page
- Manually Adding Individual Devices

SNMP/HTTP Scanning

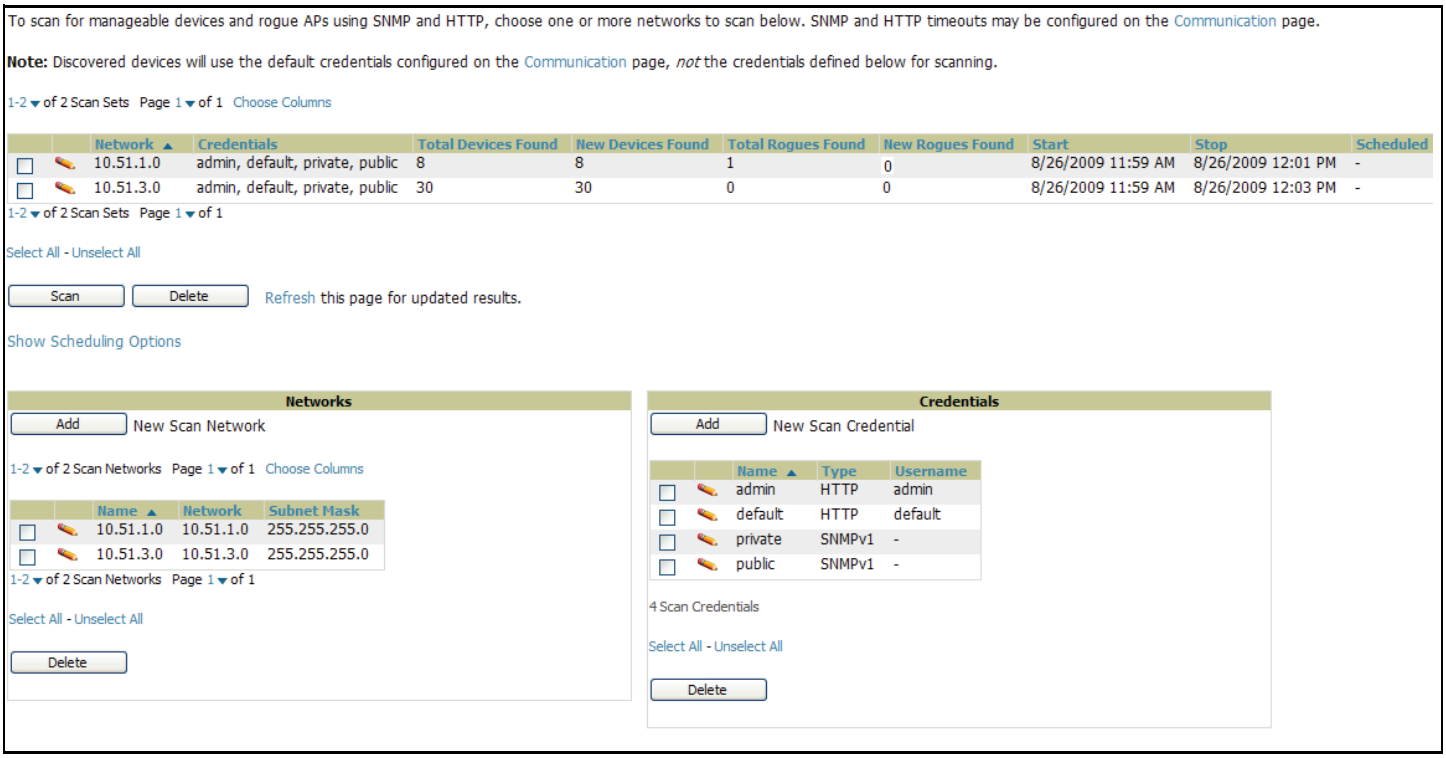
SNMP/HTTP scanning is the primary method for discovering devices on your network, including the discovery of rogue devices. Enable this scanning method from the **Device Setup > Discover** page.

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.

Figure 75 illustrates the **Device Setup > Discover** page.

Figure 75 ***Device Setup > Discover*** *Page Illustration*

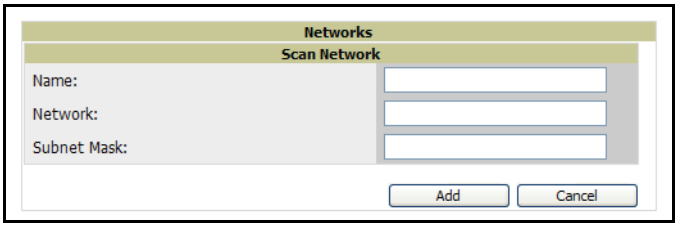


Adding Networks for SNMP/HTTP Scanning

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

1. Navigate to the **Device Setup > Discover** page, and locate the **Networks** section.
2. In the **Networks** section, click **Add New Scan Network**. The **Scan Network** page appears, as shown in Figure 76. Alternatively, you can edit an existing scan network by clicking the corresponding pencil icon. The **New/Edit Networks** page also appears in this instance.

Figure 76 ***Device Setup > Discover > New Network*** *Section Illustration*



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. Click **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.

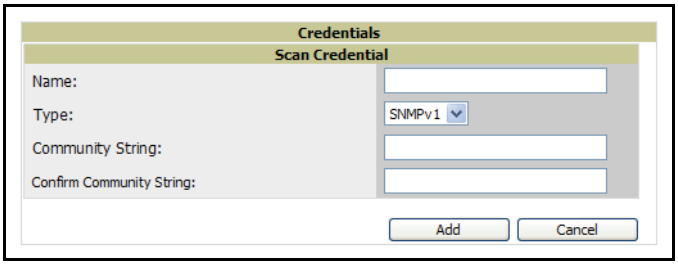
Adding Credentials for SNMP/HTTP Scanning

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, click **Add** New Scan Credential. Figure 77 illustrates this page.

Figure 77 ***Device Setup > Discover > Add/Edit New Scan Credential*** *Section Illustration*



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, we advise that you perform scans using SNMP for device discovery, but the following are considerations you should factor in to 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 > SNMP** page.

NOTE

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

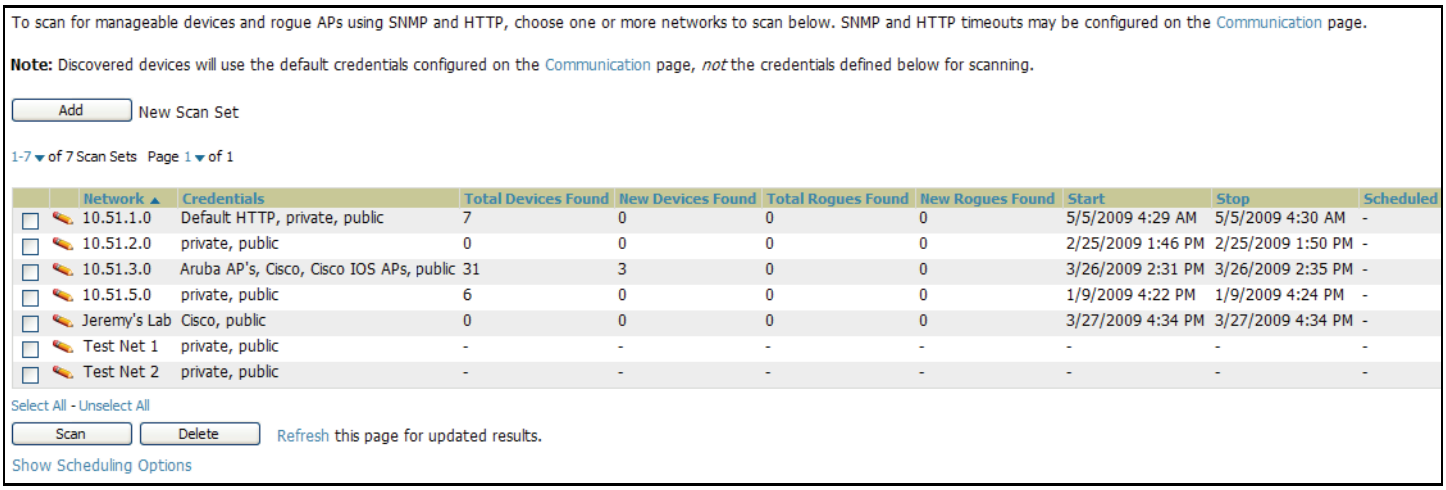
6. Click **Add**. The **Device Setup > Discover** page displays the new scan credential or credentials just created or edited.
7. Repeat these steps to add as many credentials as you require.
8. Once scan networks and scan credentials are defined, combine them by creating scan sets using the next procedure titled "Defining a SNMP/HTTP Scan Set" on page 138.

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. Figure 75, shown previously, illustrates this page. The **Scan Set** pane is illustrated in Figure 78.

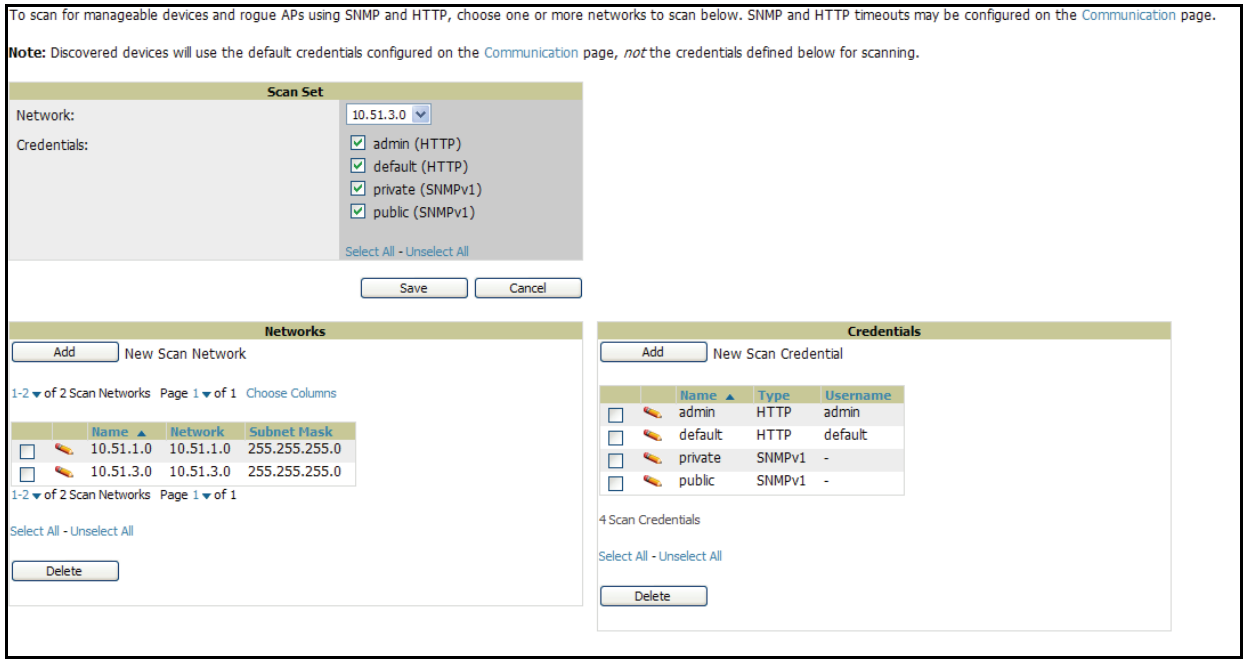
Figure 78 ***Device Setup > Discover > Scan Sets*** *Section Illustration*



2. Click **Add New Scan Set**, and the **Scan Set** section displays. Below the **Scan Set** section, the **Networks** and **Credentials** sections display all scan components configured so far. If you wish to create a new

network, or new scanning credentials, you can click Add in either of these fields to create new components prior to creating a scan set. Figure 79 illustrates the **Add New Scan Set** page.

Figure 79 ***Device Setup > Discover > Add New Scan Set*** *Page Illustration*



3. Select the **Network**(s) to be scanned and the **Credential(s)** to be used. You may select as many networks and credentials as you would like. OV3600 defines a unique scan for each **Network-Credential** combination.
4. Click the **Add** button to create the selected scans. The newly defined scans appear in a list at the top of the **Device Setup > Discover** page.
5. To edit an existing scan, click 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 140.

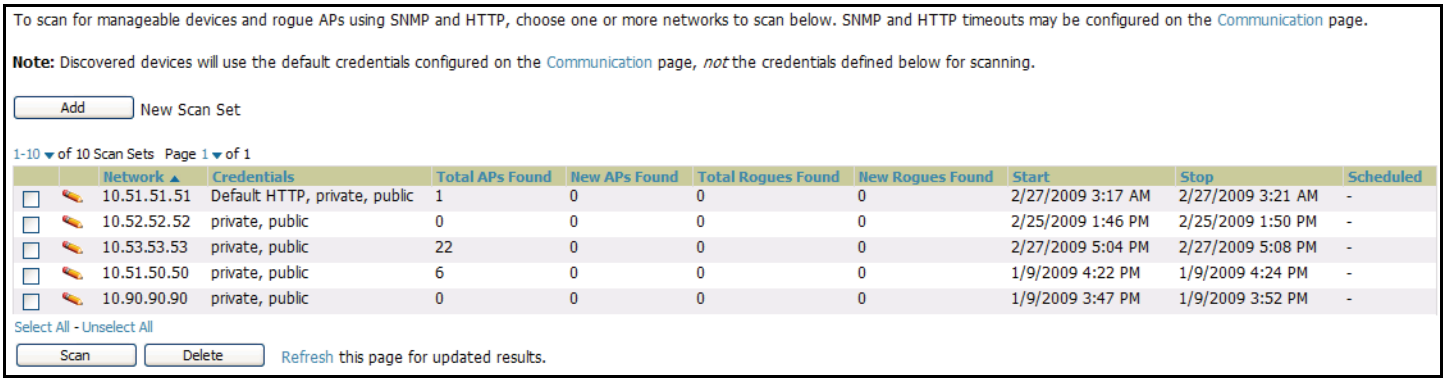
Scheduling an HTTP scan to run daily on your network can help you to discover rogues. Some consumer access points, most D-Link, Linksys, NetGear models, do not support SNMP and are found only on the wired side with an HTTP scan. These devices are discovered only if they have a valid IP address. Proper credentials are not required to discover these access points. Wireless scans and the Alcatel Lucent Management Client 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 **Discovery Execution** area at the top of the page. This section lists all scan sets that have been defined so far. Figure 80 illustrates this page.

Figure 80 ***Device Setup > Discover > Executing a Scan*** *Illustration*



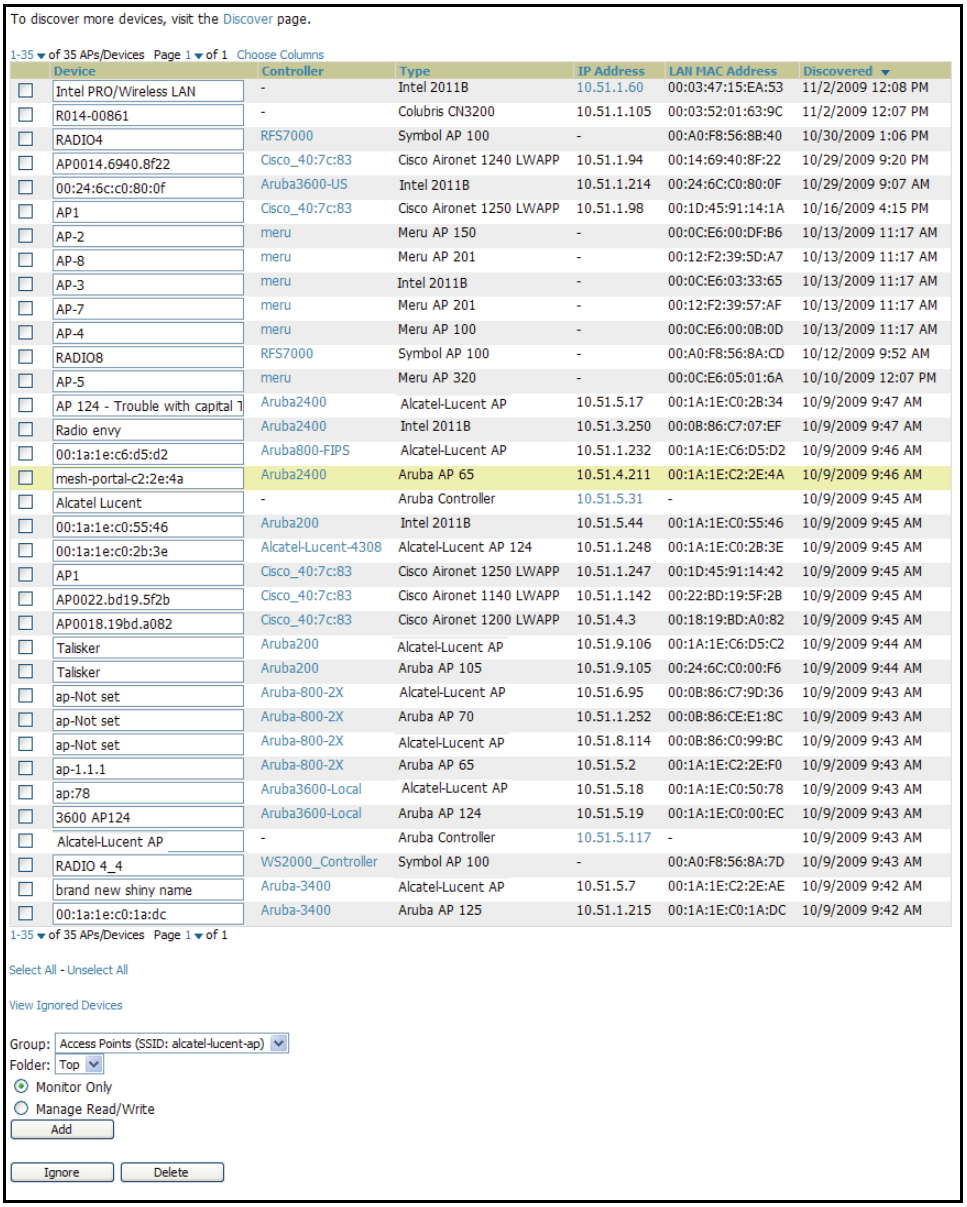
2. Check the box next to the scan(s) that you would like to execute.
3. Click **Scan** to execute the selected scans, and the scan immediately begins. The **Stop** column reads **In Progress**.
4. For future scans, click **Show Scheduling Options** and enter the desired date and time to schedule a future scan.
5. After several minutes have passed, click the **Refresh** button in your browser to refresh the page and view the results of the scan you have just run. When the **Start** and **Stop** columns display date and time information, and no longer display **In progress**, the scan is available to display the results.
6. Click the **Pencil** icon for the scan you have just run to display the results. Table 78 describes the scan results and related information.

Table 78 ***Device Setup > Discover > Discovery Execution*** *Fields*

Column	Description
Network	Displays the network to be scanned.
Credentials	Displays the credentials used in the scan.
Total APs 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 APs Found	Displays the number of newly discovered APs that are not yet being managed by OV3600 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. Navigate to the **APs/Devices > New** page to see a full list of the newly discovered devices that the scan detected. Figure 81 illustrates this page.

Figure 81 ***APs/Devices > New*** *Page Illustration*



What Next?

- To assign one or more devices to a group, see "Assigning Devices to OV3600 from APs/Devices > New Page" on page 142.
- To delete a device altogether from OV3600, select the corresponding check box for each device, and click **Delete**.

Enabling Cisco Discovery Protocol (CDP)

CDP uses the polling interval configured for each individual 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. As OV3600 adds each router or switch, OV3600 pings that device and initiates a connection using SNMP with the specified community string. This verifies that the proper IP address and community string have been provided.

Assigning Devices to OV3600 from APs/Devices > New Page

Once you have discovered devices on your network, you must add these devices to a group. To configure a new group, refer to "Configuring and Using Device Groups in OV3600" on page 81. When you add a device to a group, you must specify whether the device is to be placed in **Manage read/write** or **Monitor only** mode.

If you place the device 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.

If you place the device in **Monitor read only** mode, 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.

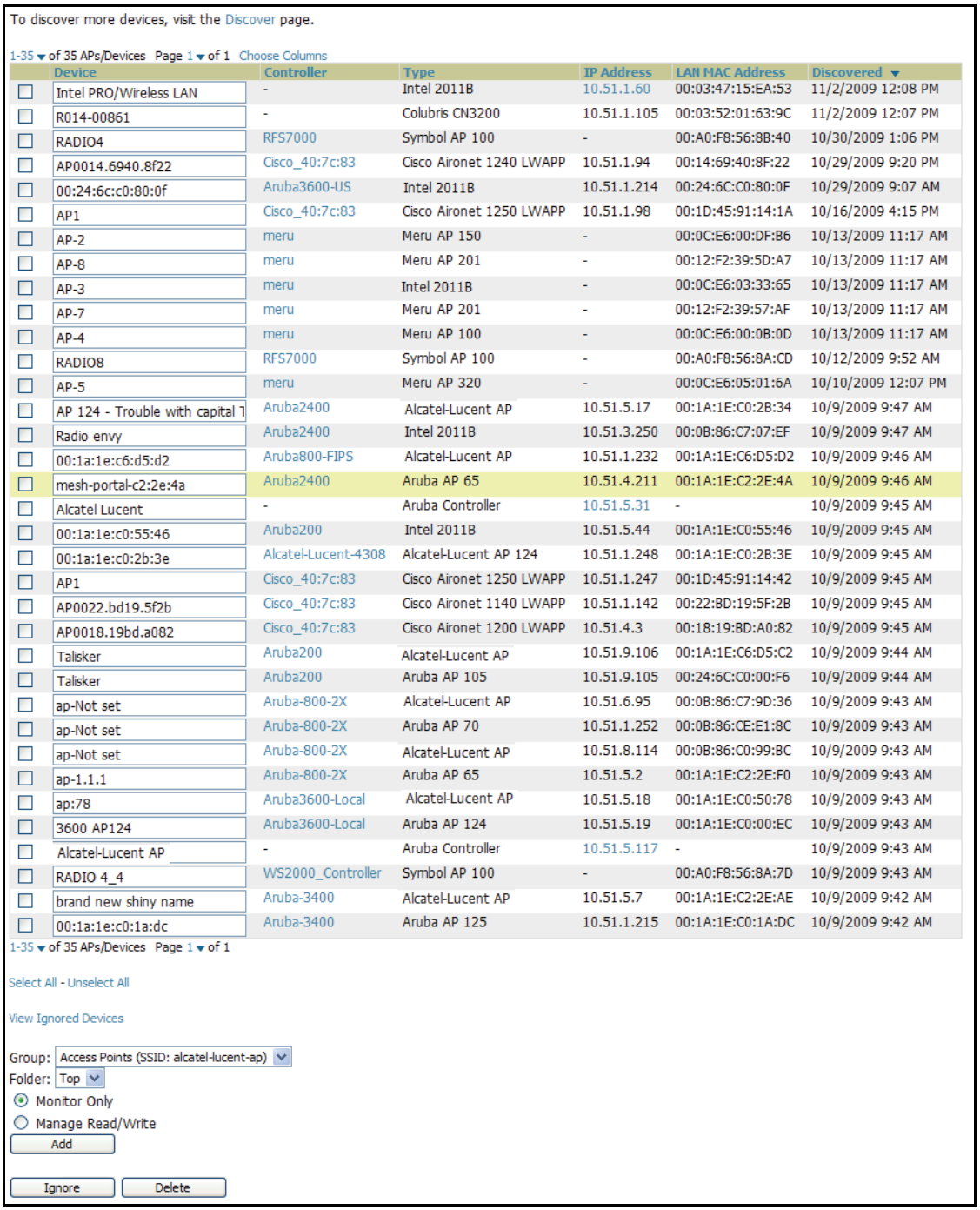
Alcatel Lucent recommends putting devices in **Monitor only** mode when they are added to a newly established Group. This avoids overwriting any important existing configuration settings.

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, and the device vendor, model, MAC Address, IP Address, and the date/time of discovery. Figure 82 illustrates this page.

Figure 82 ***APs/Devices > New***



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). Note that 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 click the **Add** button.

At this point you can navigate 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.

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 click 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.

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

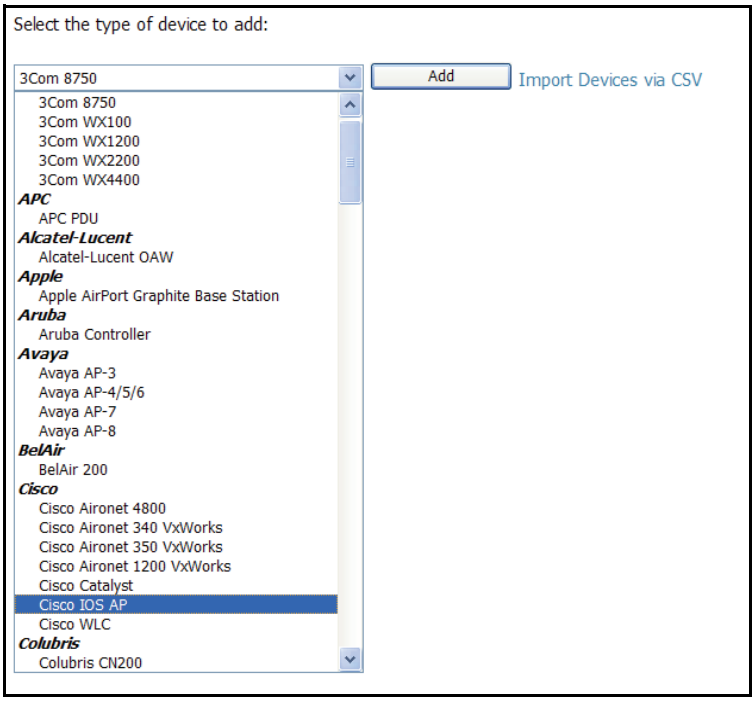
Manually adding devices from the **Device Setup > Add** page to OV3600 is an option for adding all device types. You only need to select device vendor information from a drop down menu for Cisco and Aruba

controllers and/or APs, and OV3600 automatically finds and adds specific make and model information into its database.

Perform these steps to manually add devices to OV3600:

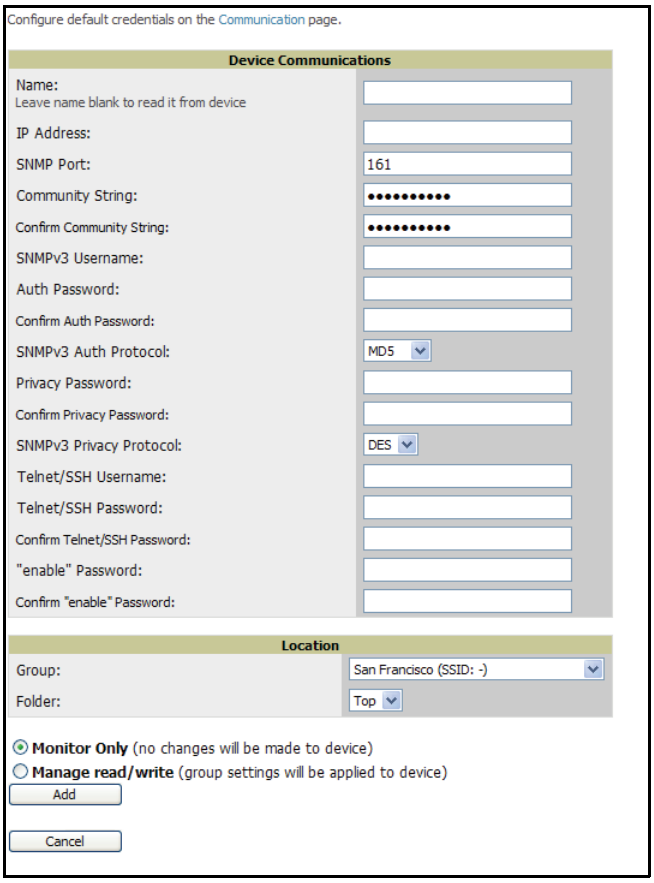
1. The first step to add a device manually is to select the vendor and model. Browse to the **Device Setup > Add** page and select the vendor and model of the device to add. Figure 83 illustrates this page.

Figure 83 ***Device Setup > Add*** *Page Illustration*



2. Click **Add**, and the **Device Communications** and **Location** sections appear, illustrated in Figure 84.

Figure 84 ***Device Setup > Add > Device Communications*** *and* ***Location*** *Page Illustration*



3. Complete these **Communications** and **Location** settings for the new device. Table 79 further describes the contents of this page. Note that 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 79 ***Device Setup > Communications > Add > 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 (Required)	None	IP address of the device Ethernet page. If One-to-One NAT is enabled, OV3600 communicates with the AP on a different address (the IP address defined in the **Device Communication** area).
SNMP Port	161	Port OV3600 uses to communicate with the AP using SNMP.
Community String (Confirm)	Taken from the **Device Setup > Communication** page	Community string used to communicate with the AP. **NOTE:** The **Community String** should have RW (Read-Write) capability.

Table 79 ***Device Setup > Communications > Add > Device Communications*** *and* ***Location*** *Fields and Default Values*

Setting	Default	Description
SNMPv3 Username **Auth Password** (Confirm)	Taken from the **Device Setup > Communication** page	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. **NOTE:** 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.
Privacy Password (Confirm)	Taken from the **Device Setup > Communication** page	SNMPv3 privacy password.
SNMPv3 Auth Protocol	Taken from the **Device Setup > Communication** page	Drop-down menu that allows you to enable the SNMPv3 authentication protocol to the device being added.
SNMPv3 Privacy Protocol	Taken from the **Device Setup > Communication** page	Drop-down menu that allows you to enable SNMPv3 privacy protocol to the device being added.
Telnet/SSH Username & Password (Confirm)	Taken from the **Device Setup > Communication** page	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 the **Device Setup > Communication** page	Password that allows OV3600 to enter **enable** mode on the AP.
HTTP Username & Password	Taken from the **Device Setup > Communication** page	HTTP password used to manage the AP initially, and to enable SNMP if desired. **NOTE:** Enter **Intel** if you are supporting new, out-of-the-box Intel APs.
Auth Password	Taken from the **Device Setup > Communication** page	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 the **Device Setup > Communication** page	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. Refer to Table 80.

Table 80 ***Device Setup > Communications > Add*** *>* ***Location*** *Section Fields and Default Values*

Setting	Default	AP Type	Description
Group	Default Group	All	This is a drop-down menu used to assign the AP to a **Group**.

Table 80 ***Device Setup > Communications > Add*** *>* ***Location*** *Section Fields and Default Values*

Setting	Default	AP Type	Description
Folder	Top	All	This is drop-down menu used to assign the AP to a **Folder**.

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 "Assigning Devices to OV3600 from APs/Devices > New Page" on page 142.

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. Click **Add** to finish adding the devices to the network.

Adding Multiple Devices from a CSV File

Adding devices in bulk from a CSV file to OV3600 is another option for adding all device types. Here you also have the option of specifying vendor name only, and OV3600 will automatically determine the correct type while bringing up the device. Note that 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

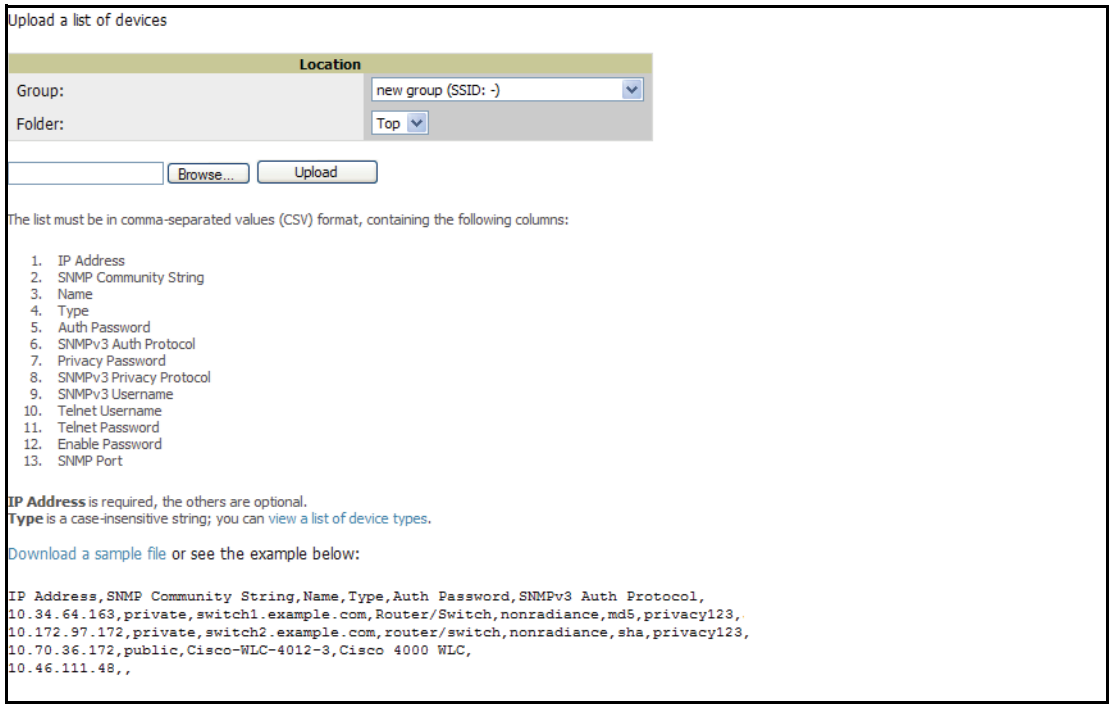
You can download a CSV file and customize it as you like. A sample CSV file is shown in illustrated in Figure 85.

Figure 85 *Sample CSV File*

```
IP Address,SNMP Community String,Name,Type,Auth Password,SNMPv3 Auth Protocol,Privacy Password,SNMPv3 Privacy Protocol,SNMPv3 Username,Telnet 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, navigate to the **Device Setup > Add** page.
2. Click **Import Devices via CSV**. The **CSV Upload** page displays, as illustrated in Figure 86.

Figure 86 ***Device Setup > Add > Import Devices via CSV*** *Page Illustration*



3. Select a group and folder into which to import the list of devices.
4. Click the **Browse...** button and navigate to the CSV list file.
5. Click **Upload** to add the list of devices into OV3600. The OV3600 user interface provides additional instructions, supporting links, and examples of CSV file contents.

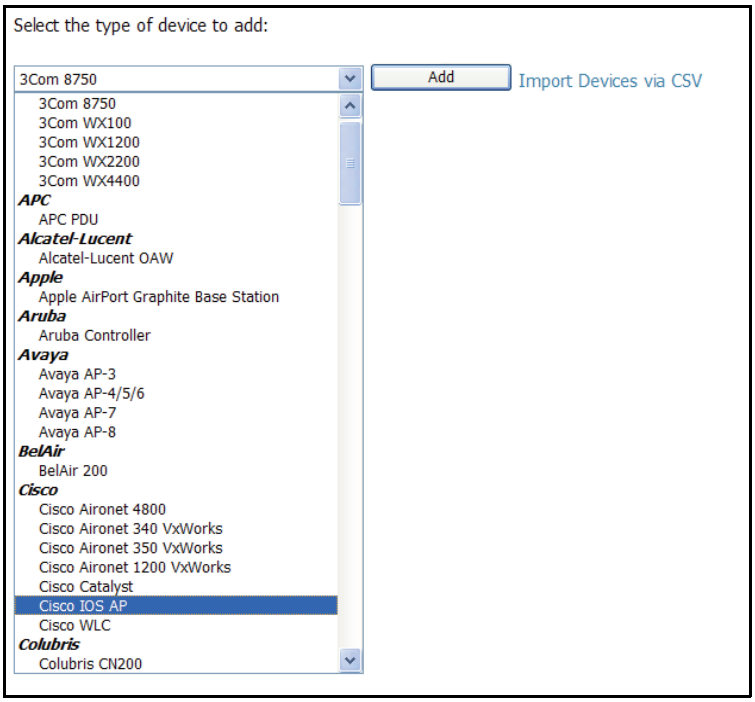
Adding Universal Devices

OV3600 get basic monitoring information from any device including switches, routers and access points 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 these steps to add universal devices to OV3600.

1. Browse to the OV3600 **Device Setup > Add** page and select the device vendor name for the wired or wireless device you are adding. Figure 87 illustrates this page.

Figure 87 ***Device Setup > Add*** *Page Illustration*



2. Click **Add**. Large numbers of Universal Network Devices can be added from a CSV file by clicking the **Import Devices via CSV** link.
3. Enter the name, IP address and read-only SNMP community string for the device.
4. Select the appropriate group and folder.
5. Click **Add**. All universal devices are added in **Monitor Only** mode.

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 clicking 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** interface. 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

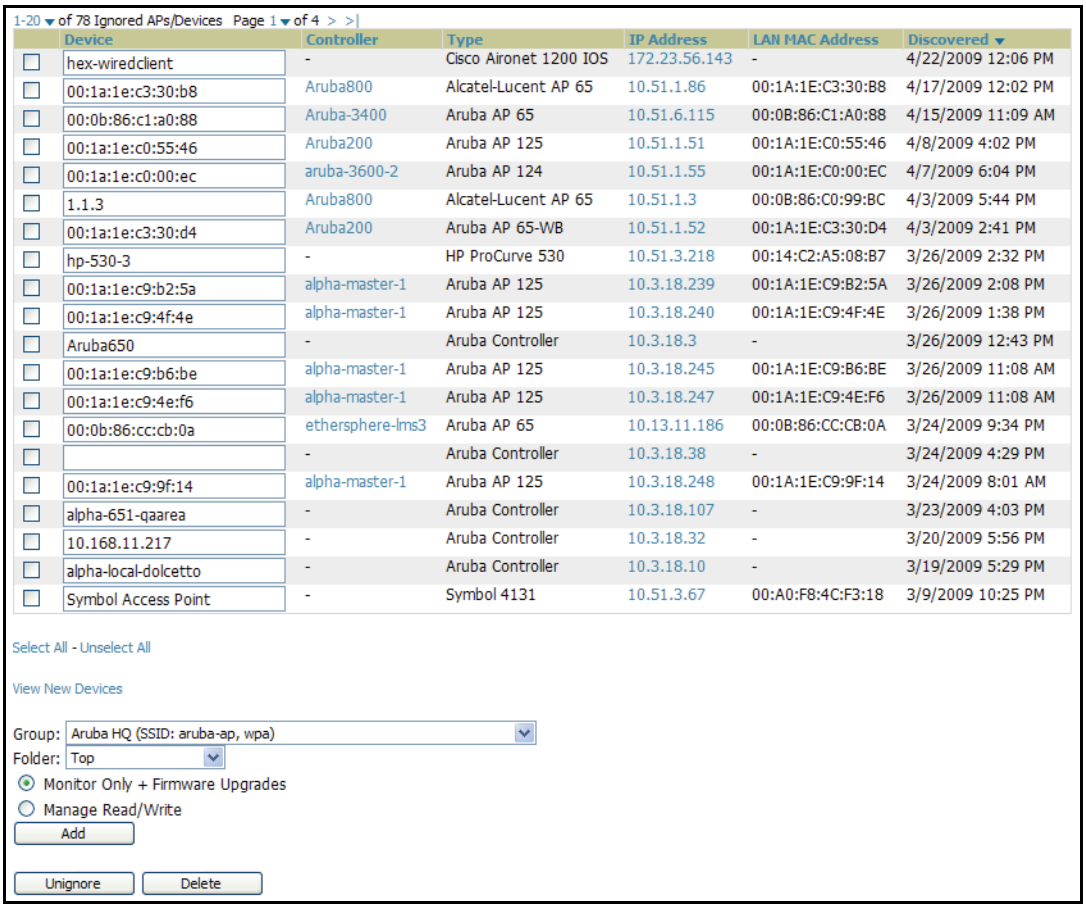
There are two ways a device can be assigned to the **Ignored** page: from the **APs/Devices > New** page, or from the **APs/Devices > Manage** page. The advantage of having the device be designated in this way, as in the case of a device that is temporarily down for a known reason, is that when you take it off the ignored list, it returns immediately to the location in OV3600 where it had resided before it was marked **Ignored**.

- If you choose to ignore devices, they are not be displayed in the **APs/Devices > New** list if they are discovered in subsequent scans.
- 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.

This procedure provides additional guidelines about using the **APs/Devices > Ignored** page. Perform these steps to further process or return an ignored device to a managed status.

1. To view all devices that are ignored, navigate to the **APs/Devices > Ignored** page, illustrated in Figure 88.

Figure 88 ***APs/Devices > Ignored*** *Page Illustration*



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 the device with the corresponding checkbox, and adjust group, folder, monitor, and manage settings as desired.
3. Click **Add** to add the device to OV3600, so that it appears on the APs/Devices New list.

Monitoring Devices

This section discusses various device monitoring options and includes the following sections:

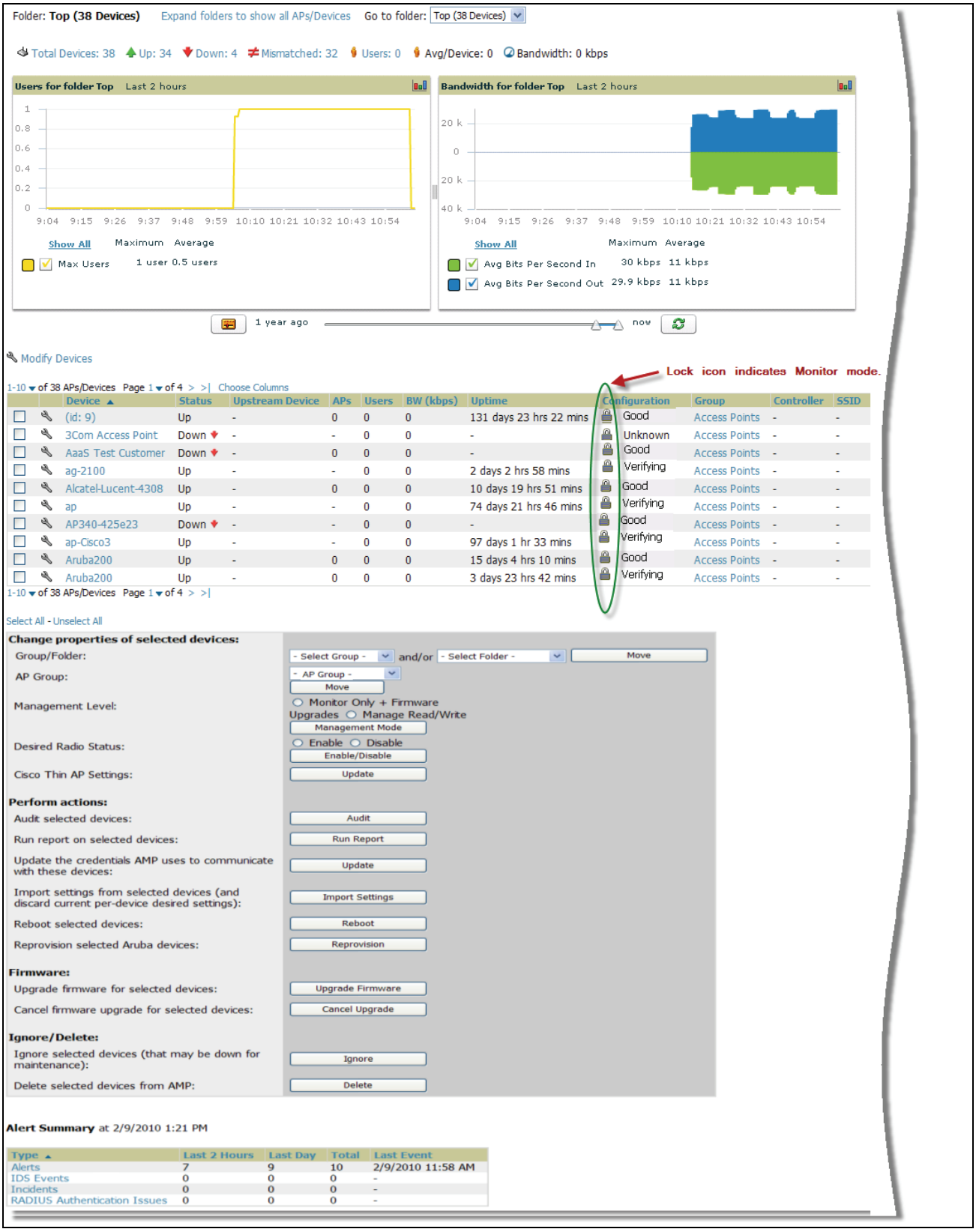
- Viewing Device Monitoring Statistics
- Auditing Device Configuration

Viewing Device Monitoring Statistics

You can view many useful device monitoring statistics as an aggregate, and individual form the **APs/Devices > List** page.

1. Browse to the **APs/Devices > List** page, which lists all devices that are managed or monitored by OV3600. Using the drop-down menu at the top of the **Activity Area**, 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 89 illustrates this page.

Figure 89 ***APs/Devices > List*** *(partial split view accounts for horizontal scrolling)*



2. Verify that the devices you added are now appearing in the devices list with a Status of **Up**.

NOTE

Immediately after you have added the device to a group, notice the device **Status** change to **Down** while OV3600 brings up the device and fetches the configuration from the device to compare it to the group settings. The device **Status** will change to **Up** when verification is complete.

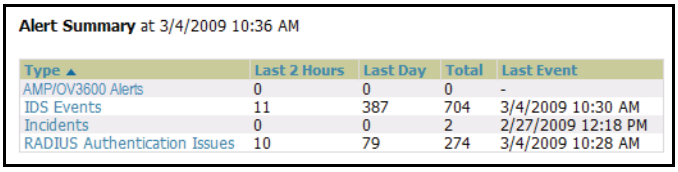
The same section also appears on the **Groups > Monitor** page, and is hyperlinked from a controller's monitoring interface.

3. Navigate to the **Alert Summary** section of the **APs/Devices > List** page. The **Alert Summary** section 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 follows:
   - OV3600 Alerts
   - IDS Events
   - Incidents
   - RADIUS Authentication Issues

NOTE

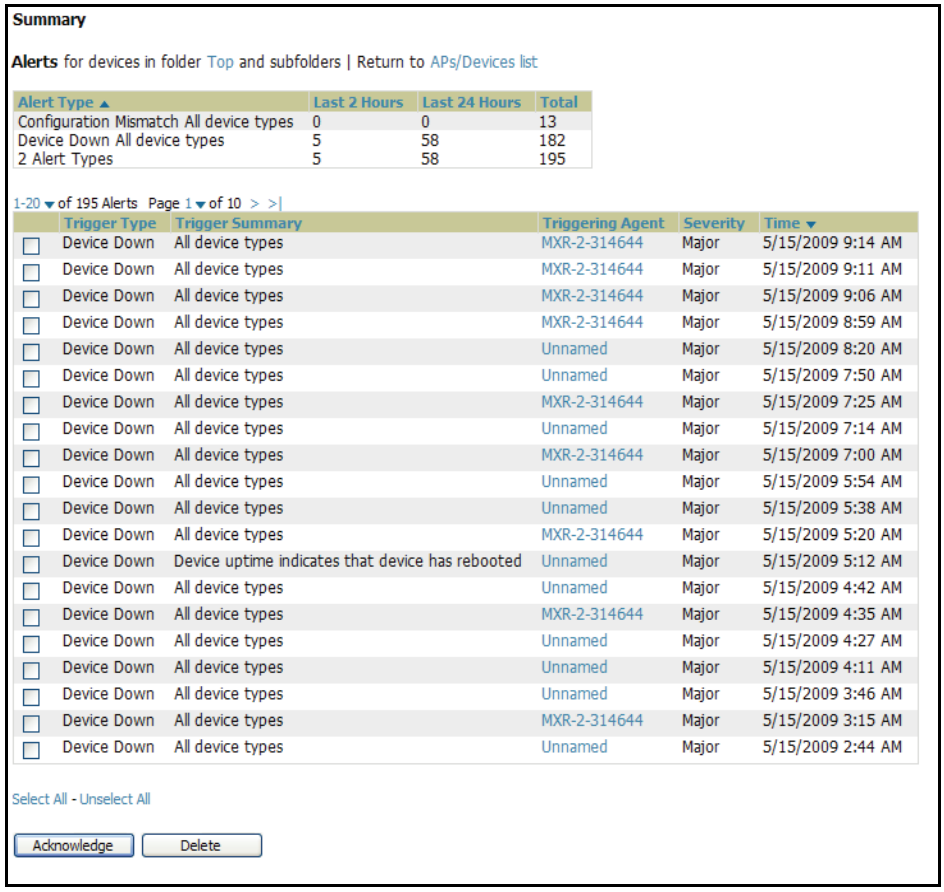
The **Alerts Summary** table is also a feature of the **Home > Overview** page, and has the same links in that location.

Figure 90 ***APs/Devices > List > Alert*** *Summary Section Illustration*



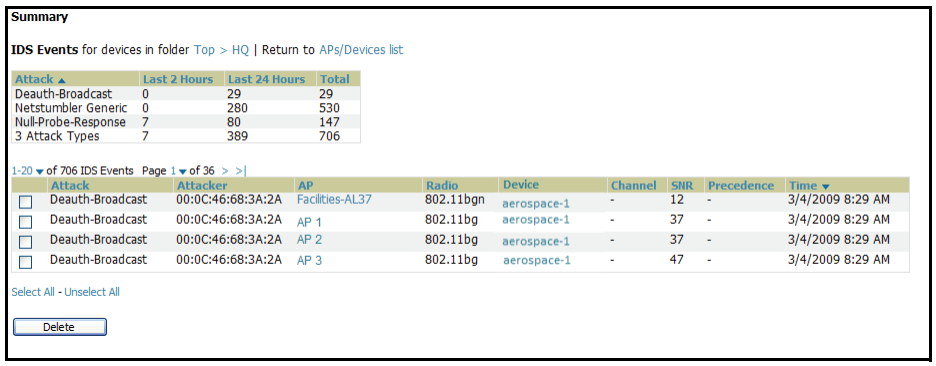
4. You can view details and incidents by clicking the specific **Alert Type**. The alert types and detailed information available for each are as follows:
   - **OV3600 Alerts**—Clicking this link takes you to the **OV3600 Alerts Summary** page, which cites detailed information for the current OV3600 Alerts. Figure 91 illustrates this page.

Figure 91 ***APs/Devices > List > OV3600 Alerts***



- **IDS Events**—Clicking this link takes you to the **IDS Events Summary** page, which cites detailed information according to folder.

Figure 92 ***APs/Devices > List, Alert Summary, IDS Events Summary*** *Page Illustration*

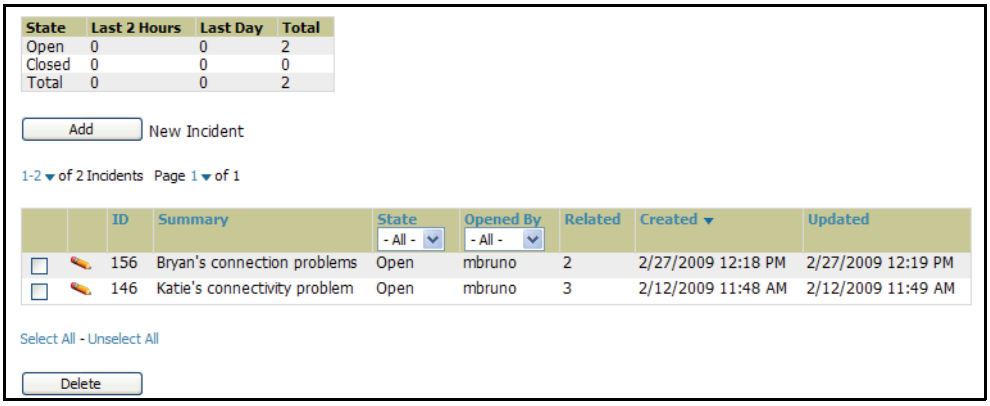


- **Incidents**—Clicking this link takes you to the **Incidents Summary** page, which cites all Helpdesk incidents and provides detailed information. Helpdesk incidents are opened with the **Helpdesk** tab.

NOTE

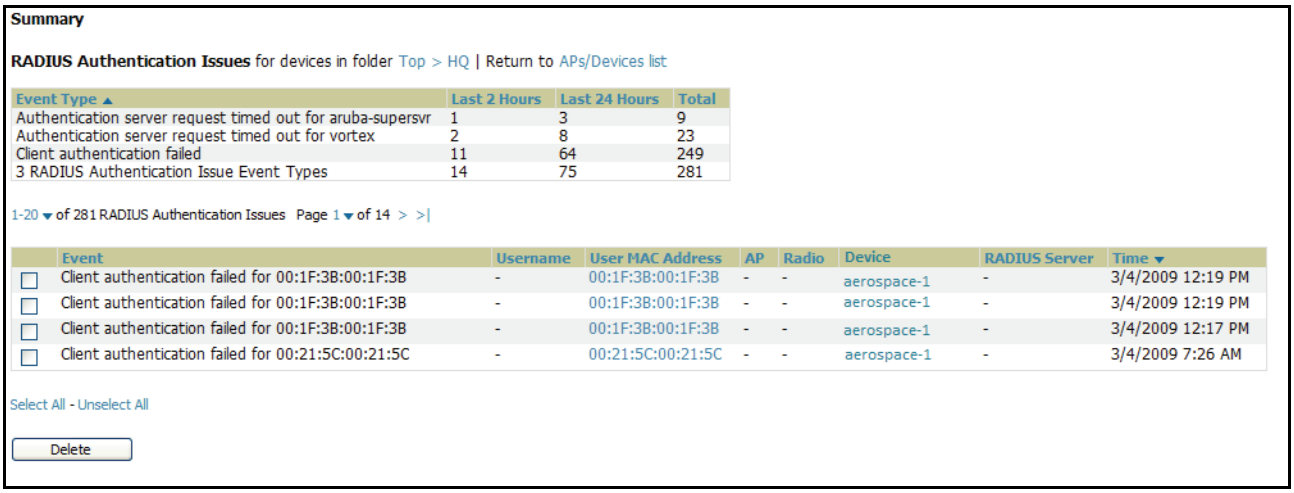
The **Incidents** portion of this **Alert Summary** table only increments the counter for incidents that are open and associated to an AP. The incidents are based on the Top folder on the **Groups > Monitor** page and on the **Home > Overview** page. Incidents that are not related to devices in that folder are not counted in this **Alert Summary**. To view all incidents, including those not associated to an AP, navigate to the **Helpdesk > Incidents** page.

Figure 93 ***APs/Devices > List, Alert Summary, Incidents Summary***



- **RADIUS Authentication Issues**—Click this link to go to the related **Summary** page, to include groupings of RADIUS Authentication issues by type, and all such issues listed in chronological sequence and by folder. Figure 94 illustrates this page.

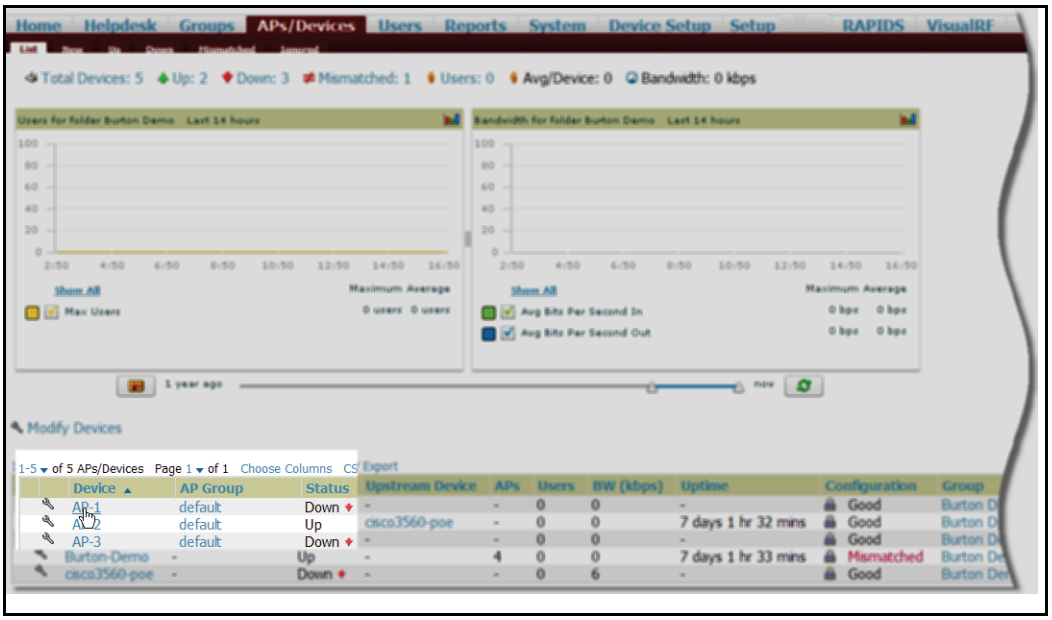
Figure 94 ***RADIUS Authentication Issues*** *Summary*



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

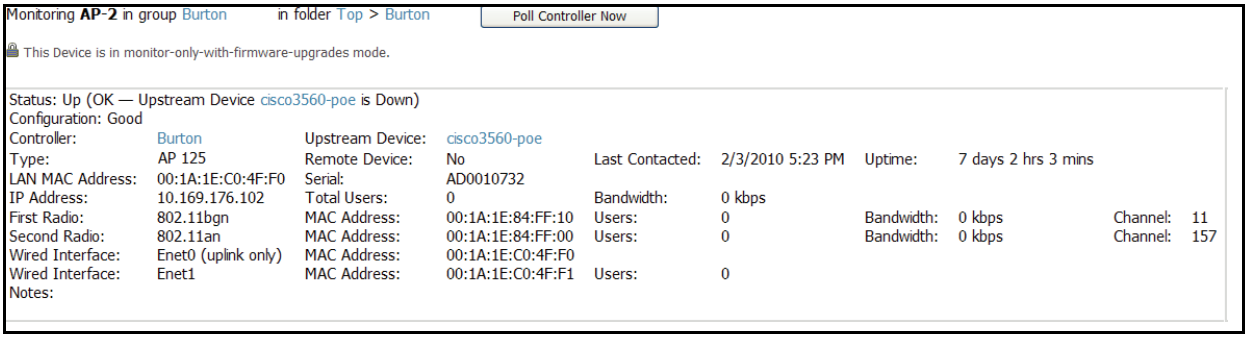
You can quickly go to any device's monitoring page once you navigate to its specific folder or group on the **APs/Devices > List** page, by clicking its hyperlinked name in the **Device** column of the table in which it is listed as shown in Figure 98.

Figure 95 ***APs/Devices > List*** *Page Showing Path to* ***Monitor*** *Page*



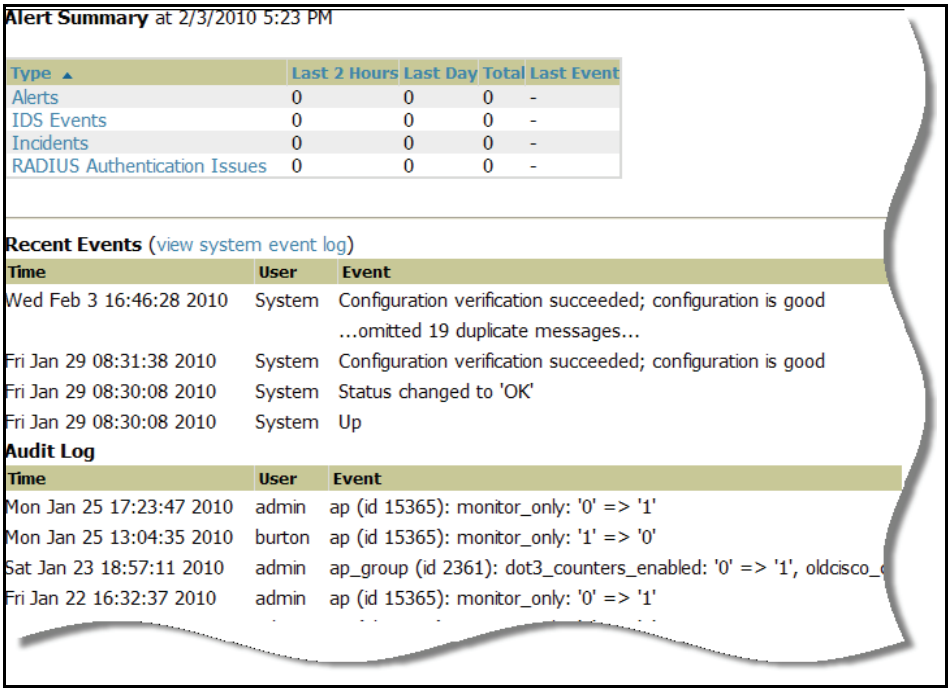
All **Monitor** pages include a section at the top displaying information such as monitoring/configuration status, serial number, firmware version and so on, as shown in Figure 96.

Figure 96 ***Monitoring*** *Page Top Level Data Common to All Device Types*



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 97.

Figure 97 ***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', oldcisco_
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

APs/Devices > Monitor 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, a

list of CDP and RF neighbors are also listed. A sample monitoring page for wireless devices is shown in Figure 98.

Figure 98 ***APs/Devices > Monitor*** *Page for Wireless Devices (partial view)*

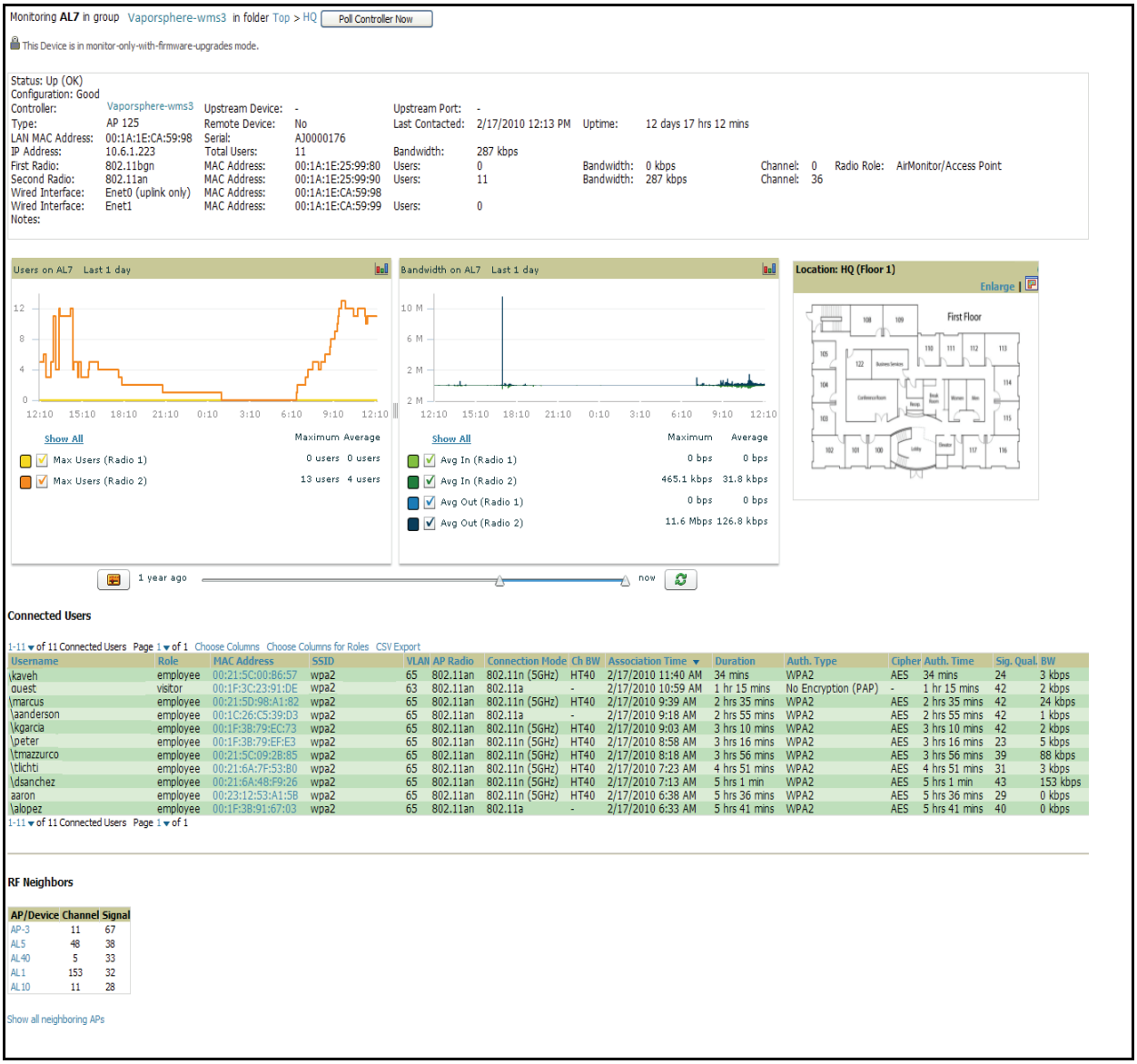


Table 81 describes the fields and information displayed in the **General** field.

Table 81 ***APs/Devices > Monitor > General*** *Fields and Default Values*

Field	Description
Poll Controller 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.

Table 81 ***APs/Devices > Monitor > General*** *Fields and Default Values (Continued)*

Field	Description
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.
Firmware	Displays the firmware version running on the AP.
Controller	Displays the controller for the associated AP device. Click 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**, **Controller Bandwidth by SSID**, **CPU Utilization**, **Memory Utilization**, **APs Managed by this Controller**, **Alerts**, and **Recent Events**. Figure 98 illustrates the **Controller** page.
Portal [a]	Specifies the mesh AP acting as the wired connection to the network for this mesh AP.
Mesh Mode [b]	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 [c]	Displays the number of mesh links between this AP and the portal.
Type	Displays the make and model of the access point.
Last Polled	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	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.
SSID	Displays the SSID of the primary radio.
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.
First Radio	Displays the Radio type of the first radio (802.11a, 802.11b or 802.11g).
Second Radio	Displays the Radio type of the second radio (802.11a, 802.11b or 802.11g.
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.

Table 81 ***APs/Devices > Monitor > General*** *Fields and Default Values (Continued)*

Field	Description
Bridge Links	Displays the number of bridge links for devices that are point-to-multi-point (see the **Groups > PTMP/ WiMAX** page for more details).
Mesh Links [d]	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	Provides 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.

a. Field is only visible for Mesh APs.
b. Field is only visible for Mesh APs.
c. Field is only visible for Mesh APs.
d. Field is only visible for Mesh APs.

Table 82 describes graph information displayed in the **Graphical Data** pane.

Table 82 ***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.

Table 83 describes the fields and information displayed for the **Connected Users** display.

Table 83 ***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, traps from Cisco VxWorks APs and tables on Colubris APs.
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.

Table 83 ***APs/Devices > Monitor > Connected Users*** *Fields and Default Values (Continued)*

Field	Description
Association Time	Displays the first time OV3600 recorded the MAC address as being associated.
Duration	Displays the length of time the MAC address has been associated.
Auth. Type	Displays the type of authentication employed by the user. Supported auth types are as follows: • **EAP**—Extensible Authentication Protocol, only reported by Cisco VxWorks using SNMP traps. • **PPTP**—Point-to-Point Protocol, supported by Colubris APs acting as VPNs. • **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 APs and/or controllers 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 the OV3600 server. 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 association table of Colubris APs or 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.

Table 84 describes the fields of this **QuickView** page.

Table 84 ***QuickView*** *Fields*

Field	Description
AP Name	Displays the name of the AP that is linked with the currently viewed AP.
MAC Address	Displays the radio MAC address of the AP that is linked with the currently viewed AP.
Link Time	Displays date and time the link was initiated.
Duration	Displays length of time the two APs have been linked.

Table 84 ***QuickView*** *Fields*

Field	Description
Link Type	Specifies the type of link, either uplink or downlink, connecting the two APs. An uplink leads to the portal AP. A downlink connects serves the viewed APs connection to the portal AP to other APs.
RSSI	Displays the RSSI observed between the two linked devices.
Hop Count	Displays the number of hops between the device and its portal.

The **Recent Events** area lists the most recent events specific to the AP. This information also appears on the **System > Events Log** page. Table 85 describes the fields in this page display.

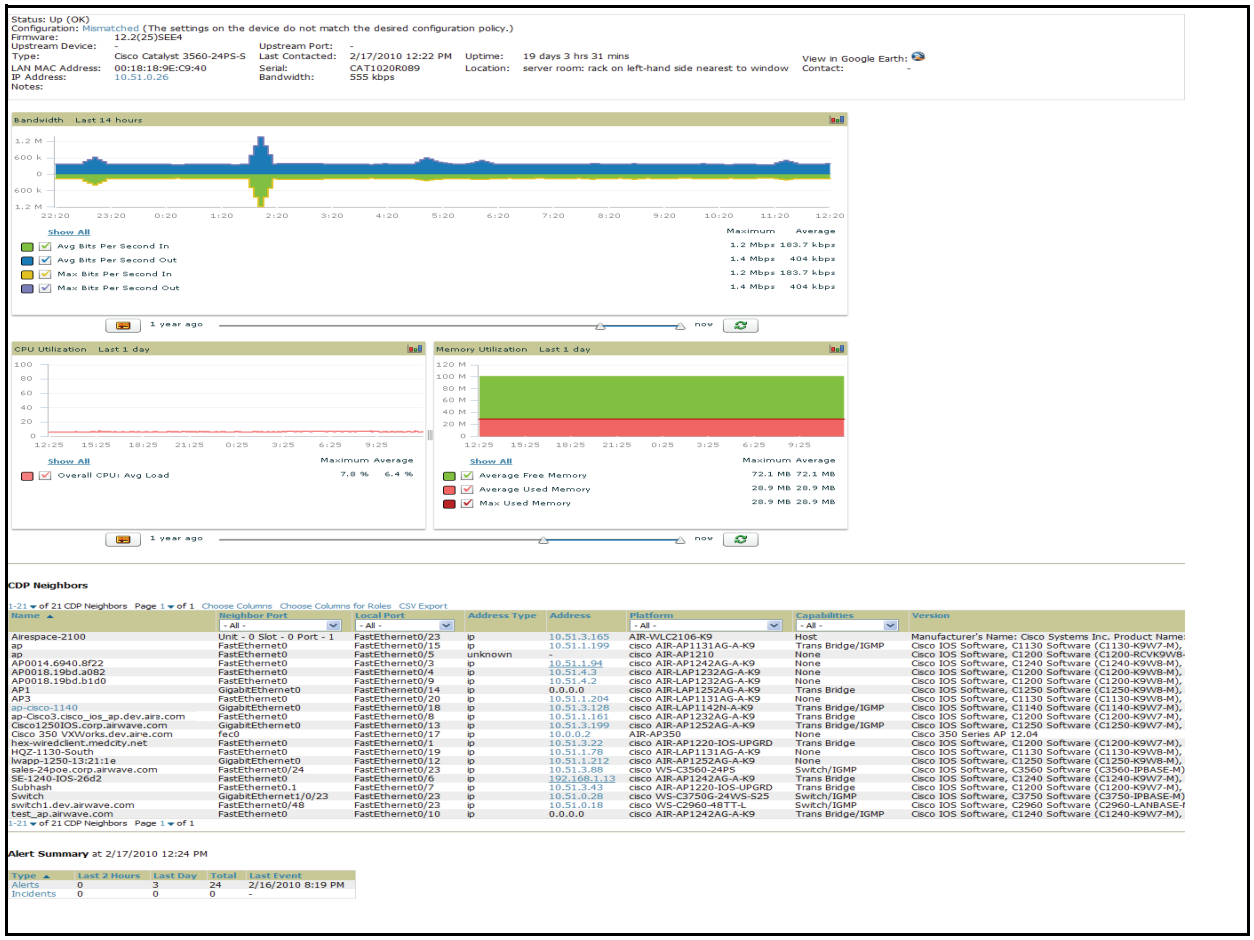
Table 85 ***APs/Devices > Monitor > Recent Events*** *Fields and Default Values*

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.

Monitoring Data Specific to Wired Devices (Routers and Switches)

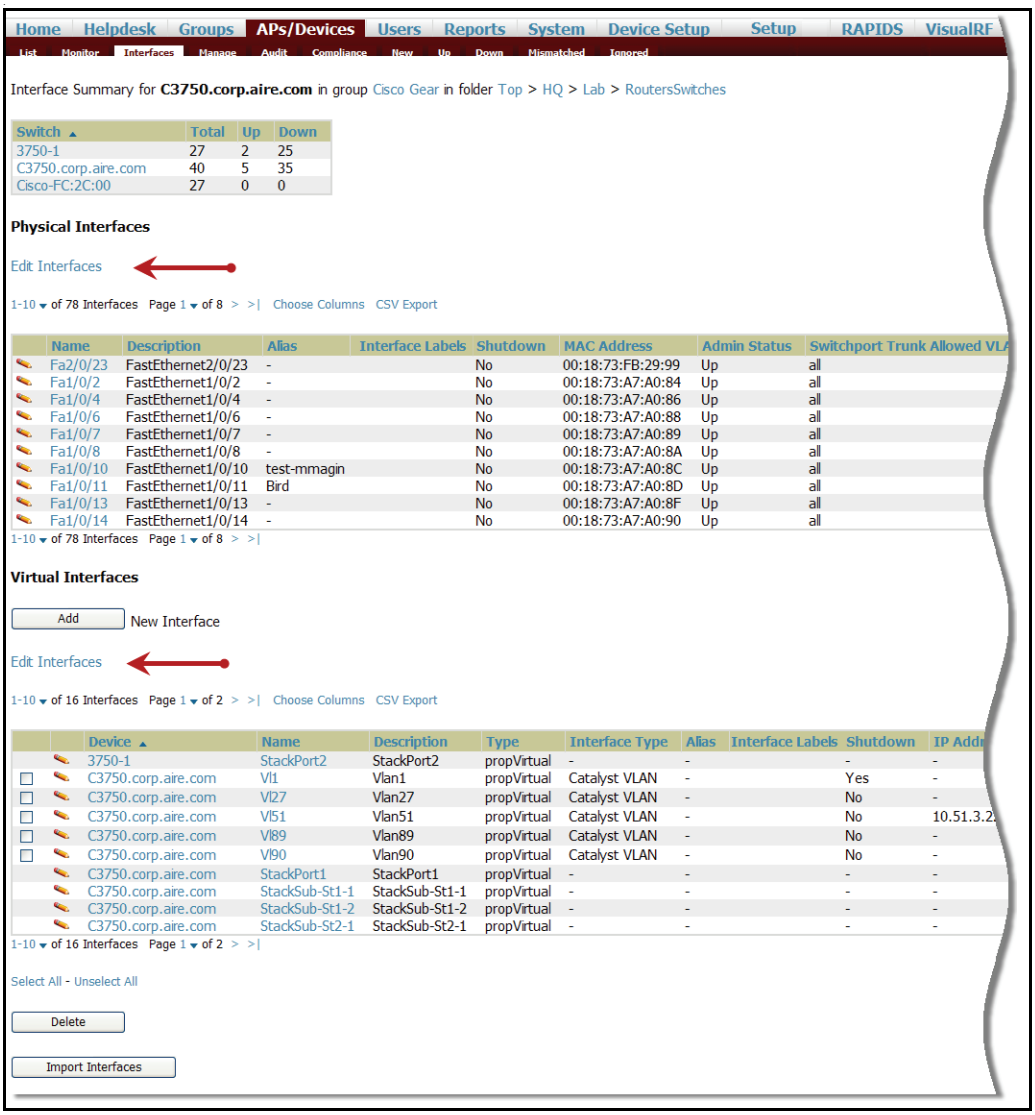
The monitoring page for routers and switches includes basic device information at the top, a bandwidth graph depicting the sum of all the physical interfaces, and beneath that, CPU/Memory usage graphs as shown in Figure 99.

Figure 99 ***APs/Devices > Monitor*** *Page for Wired Devices*



All managed wired devices also include an **Interfaces** tab, as shown in Figure 100.

Figure 100 ***APs/Devices > Interfaces*** *Page for Wired Devices (partial view)*



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, labelled **Physical** and **Virtual**.

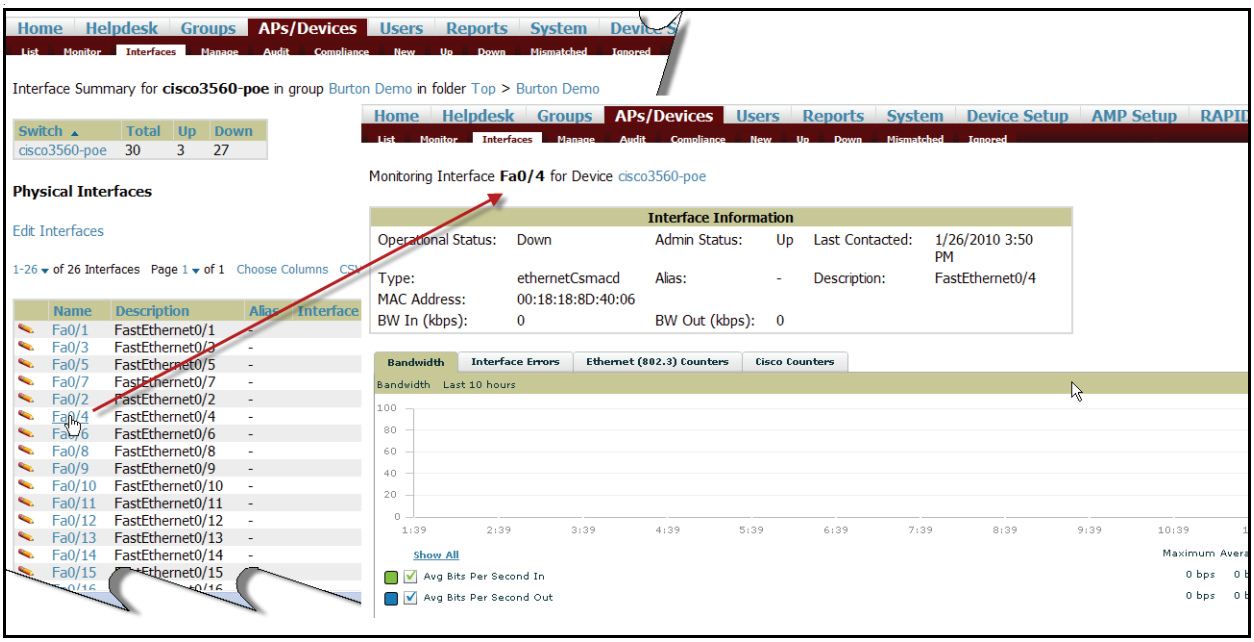
OV3600 now monitors **Up/Down** status and bandwidth information on all interfaces. You can edit multiple interfaces concurrently by clicking one of the two **Edit Interfaces** hyperlinks as shown using red arrows in Figure 100 above. You can edit both monitoring and configuration settings this way.

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 "Creating and Using Triggers and Alerts" on page 224.

Understanding the APs/Devices > Interfaces Page

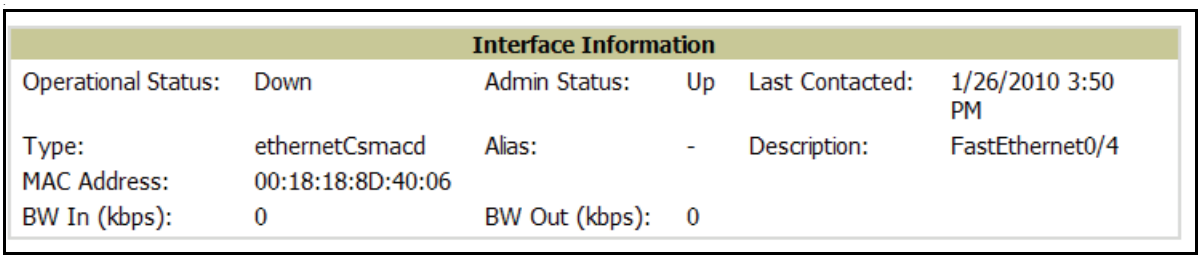
"Monitoring Data Specific to Wired Devices (Routers and Switches)" on page 163 shows you how to view high level interface information for all physical and virtual interfaces on an entire router or switch. Click any interface hotlink in the **Name** column of the Physical or Virtual Interfaces tables on the stacked switches **Interfaces** monitoring page to navigate to an **Interfaces** page displaying data relevant to that specific interface, as shown Figure 101.

Figure 101 ***Individual Interface Monitoring*** *Page*



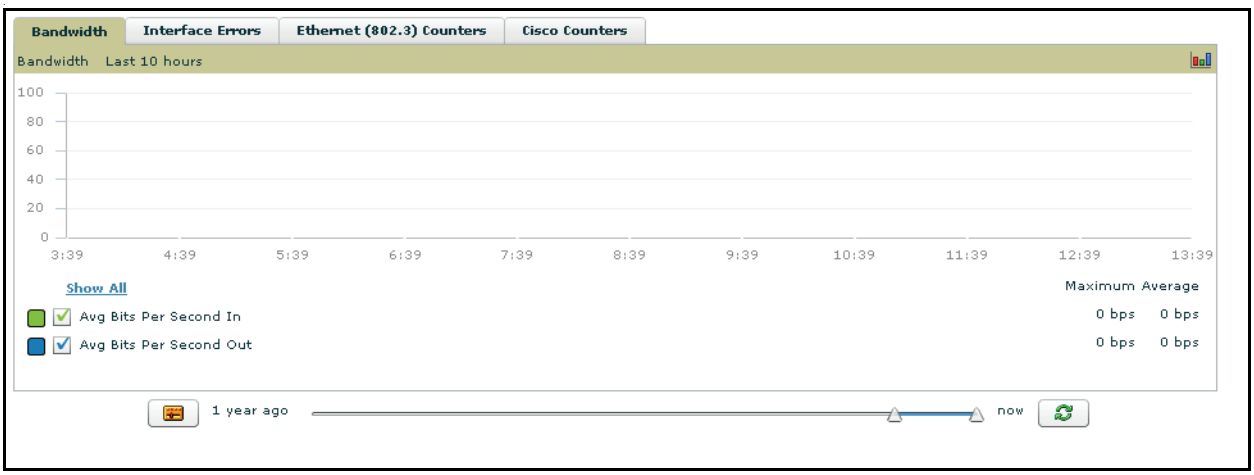
An individual **Interface** monitoring page includes is comprised of 2 panes. Specifics of the interface are in the upper pane, as depicted in Figure 102.

Figure 102 ***Individual Interface Operational Status Information*** *Pane*



Bandwidth, and various standard and enterprise specific error counting information is displayed in the lower pane in a tabbed graph as shown in Figure 103.

Figure 103 ***Individual Interface Bandwidth and Error Counting*** *Graph*



What Next?

All device monitoring pages act as portals to management pages if you have the proper (read/write) privileges. Clicking the wrench or pencil icon next to a device table entry, or clicking **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 168 for more information, and detailed procedures.

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. Aruba devices and wired routers and switches use Telnet/SHH to read device configuration. See "Individual Device Support and Firmware Upgrades" on page 179 for more details.

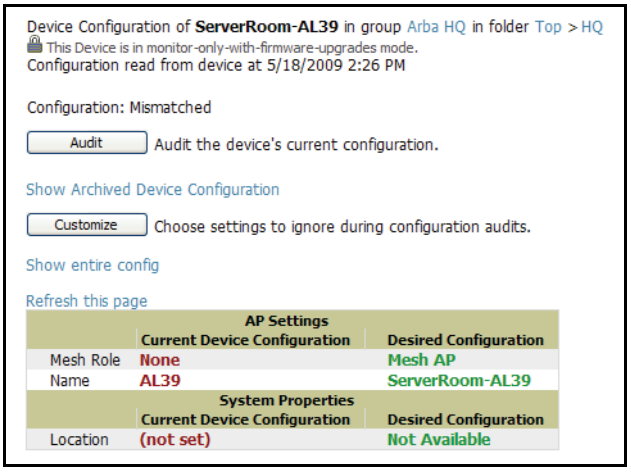
Perform these steps to verify the device configuration status:

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**, click 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.

After upgrade, the **APs/Devices > Audit** page, and certain additional pages, show only **Mismatched** status by default for non-template devices.

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 104 illustrates this page.

Figure 104 ***APs/Devices > Audit*** *Page Illustration*

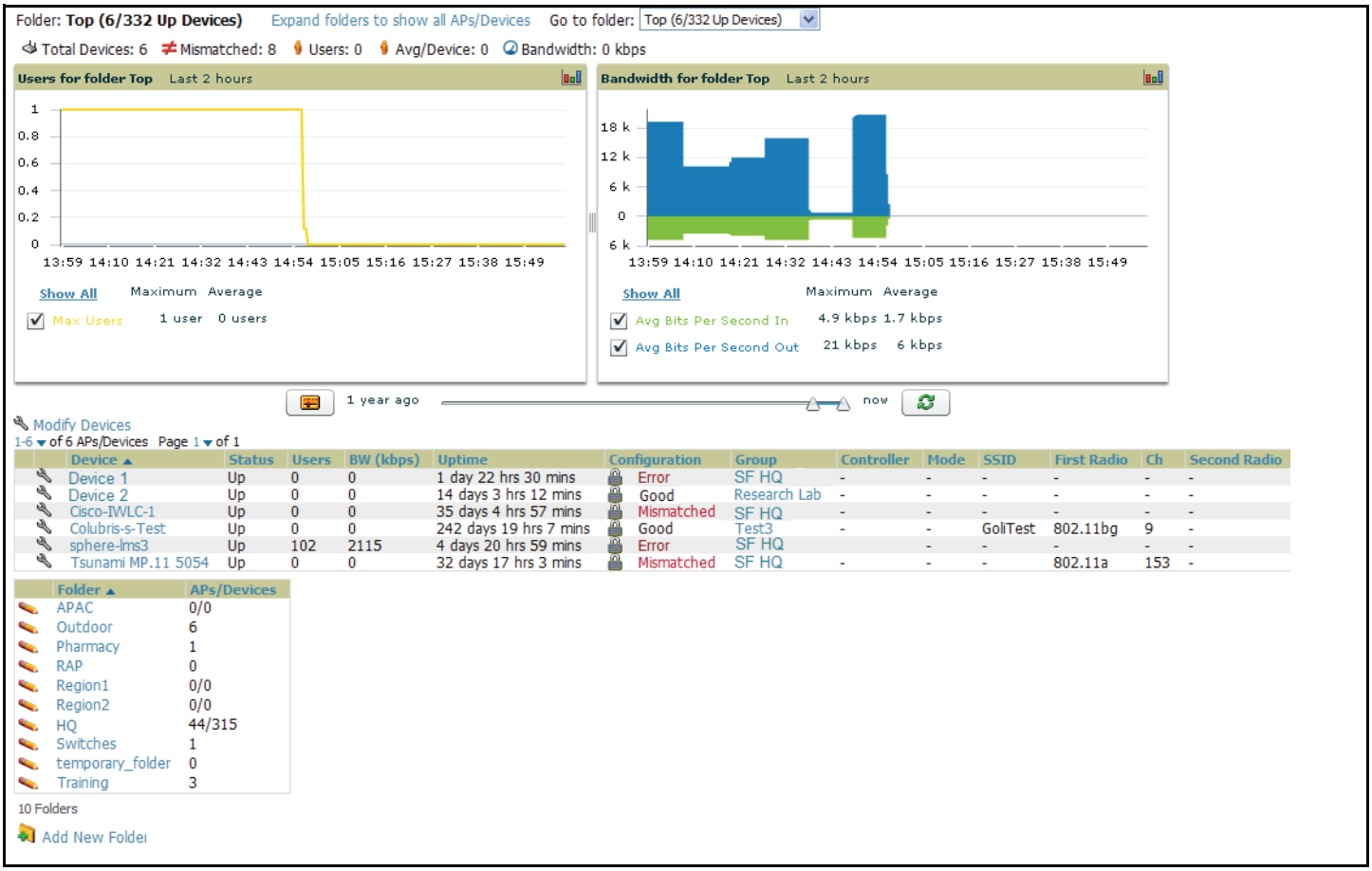


6. Review the list of changes to be applied to the device to determine whether the changes are appropriate. If not, you need to change the Group settings or reassign the device to another Group.

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. Figure 105 and Figure 106 illustrate this component.

Figure 105 ***APs/Devices > Up Page*** *Example*



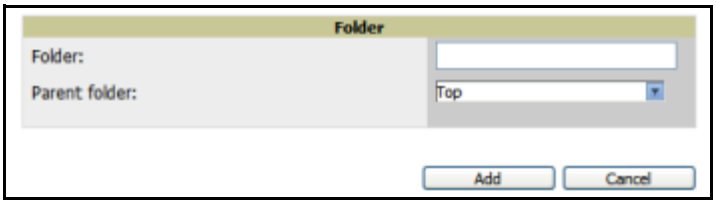
Folder views are persistent in OV3600. If you select the **Top** folder and then click the **Down** link at the top of the page, you are taken to all of the down devices in the folder.

If you want to see every **down** device, click 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, click the **Add New Folder** link. Figure 106 illustrates the page that appears.

Figure 106 ***Folder Creation***



2. Enter the name of the new folder.
3. Select the **Parent** folder.

4. Click **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 168
- "Configuring AP Settings" on page 169
- "Configuring Device Interfaces for Cisco Catalyst Switches" on page 176
- "Individual Device Support and Firmware Upgrades" on page 179

While most device configuration settings are managed by OV3600 at a Group level to enable efficient change management, 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 would not make sense to configure RF channel settings at a Group level. Instead, channel settings are managed at an individual device level to avoid RF interference between two or more devices.

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; devices 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.

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 28.

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.

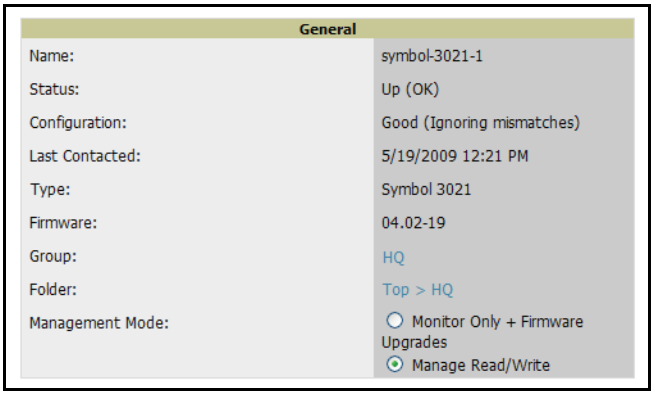
Once a device is in Manage mode, OV3600 will push a new configuration to the device in the event that the actual device configuration does not match the OV3600 configuration for that device.

To move a device from **Monitor** to **Manage Read/Write** mode, perform the following steps.

1. Navigate to the **APs/Devices > List** page and click 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 107.

Figure 107 ***APs/Devices > Manage > General*** *Section Illustration*

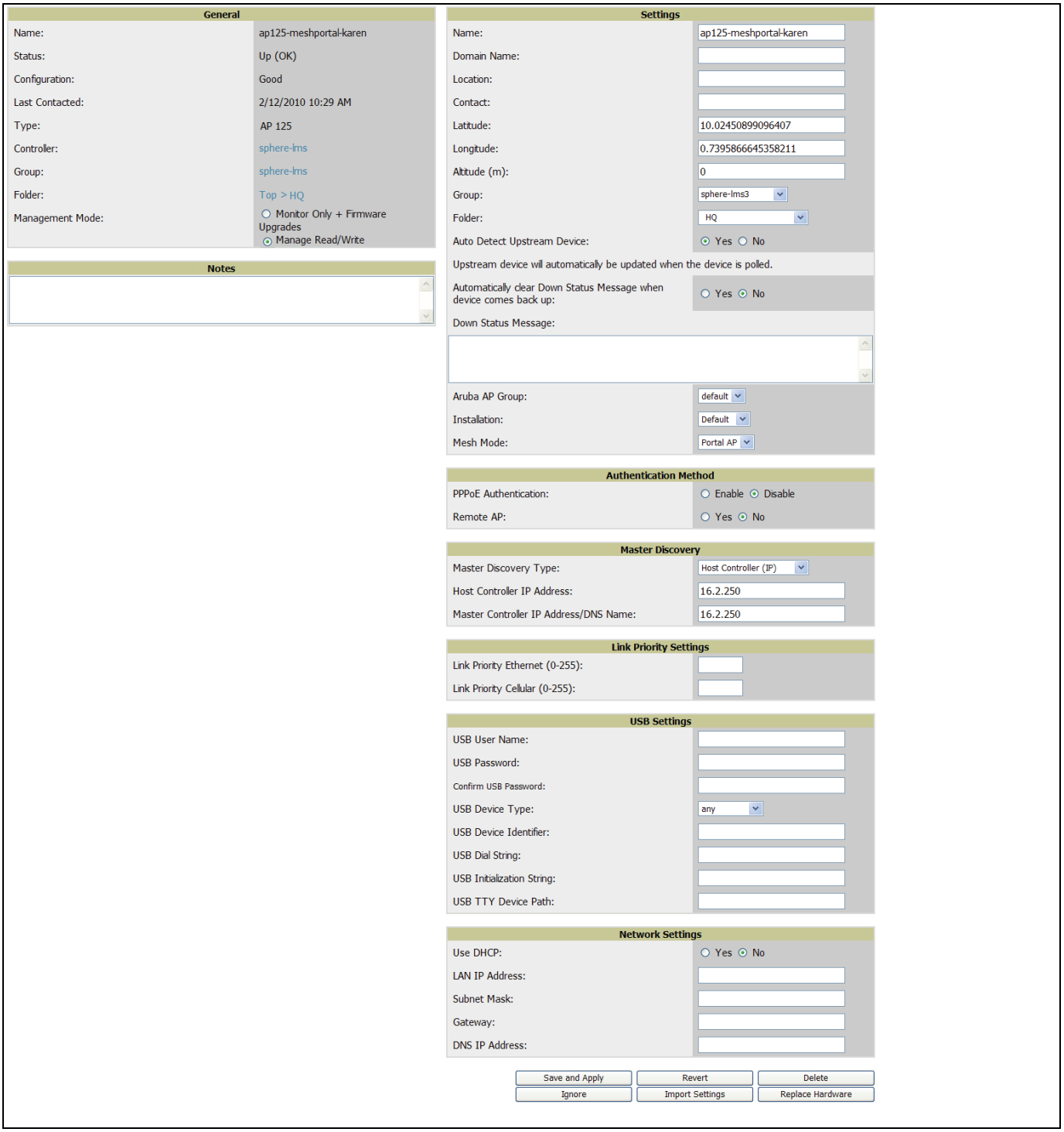


3. Click **Manage Read/Write** on the **Management Mode** radio button to shift the device from **Monitor Only** to **Manage Read/Write** mode.
4. Click **Save and Apply** to retain these settings and to push configuration to the device.
5. OV3600 presents a confirmation window reminding you of all configuration changes that will be applied to the device in **Manage** mode.
6. Click **Confirm Edit** to apply the changes to the device immediately, click **Schedule** to schedule the changes to occur during a specific maintenance window, or click **Cancel** to return to the **APs/Devices > Manage** page.
7. Some device configuration changes may require the device to reboot. Use the **Schedule** function to schedule these changes to occur at a time when WLAN users will not be affected.
8. To move multiple devices into managed mode at once, use the **Modify these devices** link. Refer to "Modifying Multiple Devices" on page 129 for more information.

Configuring AP Settings

1. Browse to the **APs/Devices > List** page and click 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 108 illustrates this page.

Figure 108 ***APs/Devices > Manage*** *Page Illustration*



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 the **System > Configuration Change Job Detail** page for the job.

2. Locate the **General** section—this section provides general information about the APs current status. Table 86 describes the fields, information, and settings.

Table 86 ***APs/Devices > Manage > General*** *Fields and Default Values*

Message	Meaning
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, click **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.
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 being managed using 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.

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 87 describes field settings, default values, and information for the **Sections** area of this page.

Table 87 ***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	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.

Table 87 ***APs/Devices > Manage > Settings*** *Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
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.
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 88 describes many of the possible fields.

For complete listing and discussion of settings applicable only to Aruba/Alcatel-Lucent devices, see the *Aruba/Alcatel-Lucent Configuration Guide, Version 7.0*.

Table 88 ***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.

Table 88 ***APs/Devices > Manage*** *Page Illustration, Additional Settings*

Setting	Default	Device Type	Description
Bridge Role	Base Station	PTMP/WiMAX	Base Station units provide backhaul connections for satellite units, to which wireless users connect.
Mode of Operation	Bridge	PTMP/WiMAX	Units that can operate in bridge or router mode.
Ethernet Interface Configuration	100 Mbps Full Duplex	PTMP/WiMAX	Bandwidth rates for uploading and downloading data.
Dynamic Data Rate Selection	Enabled	PTMP/WiMAX	Allows subscribers to receive the maximum data rate possible.
Subscriber Station Class	G711 VoIP UGS	WiMAX Subscriber Stations	Defines the subscriber station class for the AP. Subscriber station classes are defined on the **Groups > WiMAX** page.
Uplink Modulation	bpsk-1-2	WiMAX Subscriber Stations	Drop-down menu that defines the uplink modulation type for the subscriber station.
Downlink Modulation	bpsk-1-2	WiMAX Subscriber Stations	Drop-down menu that defines the downlink modulation type for the subscriber station.
VLAN Mode	Inherit	WiMAX Subscriber Stations	Drop-down menu that defines the VLAN mode of the AP. Inherit - The AP will inherit the VLAN settings from the subscriber class. Transparent - Tagged and untagged traffic is passed along unless blocked by a PIR restriction.
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	Intel 2011, 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 88 ***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.
Neighboring APs	Blank	All	Represents top five contiguous access points calculated by summing the number of roams to and from the access point and the access point of focus. 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.
Transmit Power Level	Highest power level supported by the radio in the regulatory domain (country)	Cisco, Colubris, Intel, 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) Intel/Symbol (Full or 50mW, 30mW, 15mW, 5mW, 1mW) Colubris (High or 23 dBm, Med. or 17 dBm, Low or 13 dBm)**
Distance Between APs	Large	Colubris	Determines how far a user can roam before roaming to another AP.
Notes (Optional)	Blank	All	Free form text field for entering fixed asset numbers or other device information. This information is printed on the nightly inventory report.
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 (except Colubris)	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 (except Colubris)	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.
BSID	00:00:00: 00:00	WiMAX Base Station	Defines the BSID for the base station. This BSID should match the BSID on the **Groups > WiMAX** page if you want subscriber stations to associate with the base station. Subscriber stations use the BSID defined on the **Groups > WiMAX** page to determine which base stations to associate with.
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 **IOS Template Options** area on the **APs/Devices > Manage** page.

This field only appears for IOS APs in groups with Templates enabled.

Table 89 describes field settings, default values, and additional information for this page.

Table 89 ***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 IOS 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.
switch_command	None	Cisco IOS	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, navigate to the interfaces section of the **AP > Manage** page. Click **Add new interface** to add another controller interface, or click the **pencil** icon to edit an existing controller interface. Figure 109 describes the settings and default values. For detailed descriptions of Cisco WLC devices supported by OV3600, refer to the Cisco WLC product documentation at http://www.cisco.com/en/US/products/ps6366/tsd_products_support_series_home.html.

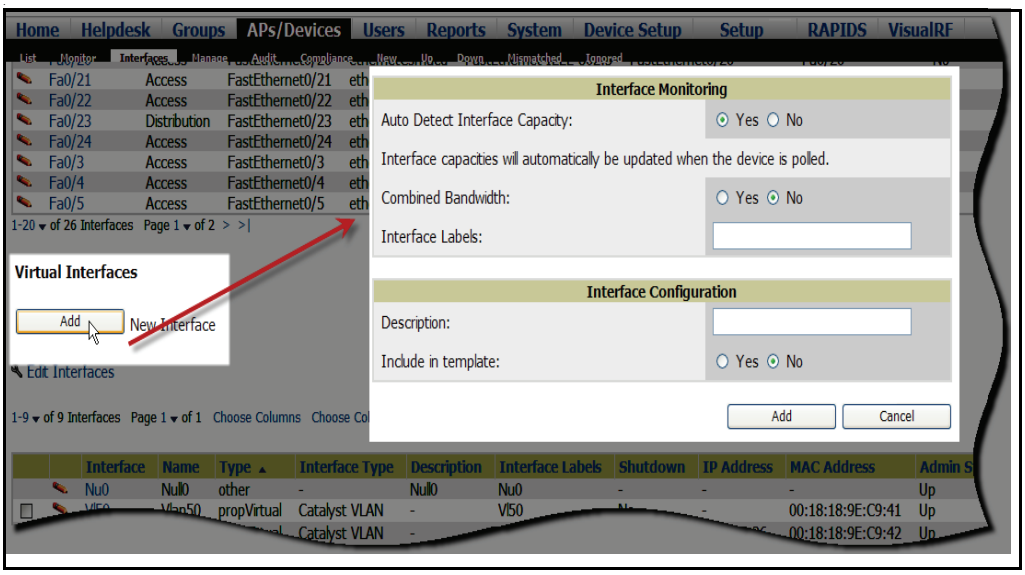
Figure 109 ***APs/Devices > Manage*** *Fields and Default Values*

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	Disabled	Enabled indicates it is a quarantine VLAN; used only for H-REAP-associated clients.

Configuring Device Interfaces for Cisco Catalyst Switches

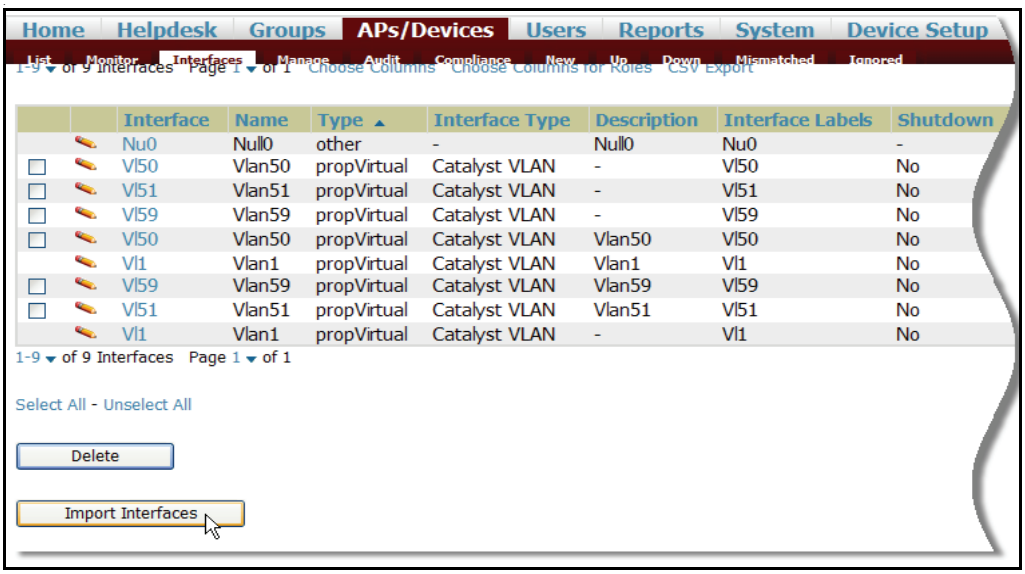
You can add a Virtual interface by clicking **Add** and entering the appropriate information in the Interface and Interface Capacity panes of the page that then appears as shown in Figure 110.

Figure 110 ***Add Virtual Interfaces*** *Page for Wired Devices*



New physical and virtual interfaces are discovered using SNMP polling as described in "SNMP/HTTP Scanning" on page 136. To refresh and reload all current interface information from a device, click **Import Interfaces** on the bottom of the page as shown in Figure 111.

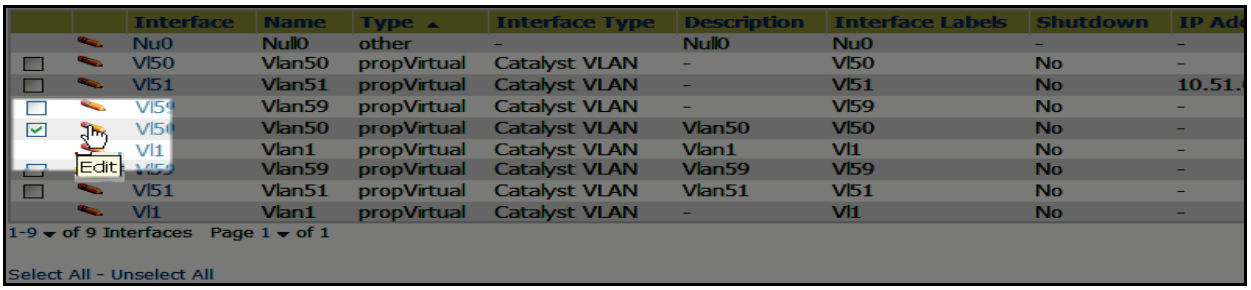
Figure 111 ***Import Interfaces*** *for Refresh and Reload (lower portion of page)*



You can view details for each interface on a wired device, from its individual interface page, as well. For a detailed explanation of the data available on each individual interface monitoring page, see "Understanding the APs/Devices > Interfaces Page" on page 164.

You can configure interface settings individually or in groups. To configure individual interface settings, click the pencil icon to the left of the interface name appearing from the **AP/Devices > Interfaces** page, as shown in Figure 112.

Figure 112 ***Editing Individual Interfaces*** *Page*



This takes you to the **Interfaces Monitoring and Configuration** window, that has a slightly different appearance depending on whether you are configuring a physical or virtual interface, as shown in Figure 113 and Figure 114.

Figure 113 ***Physical Interfaces Monitoring and Configuration*** *Window (***Interfaces Monitoring and Configuration** *Window)*

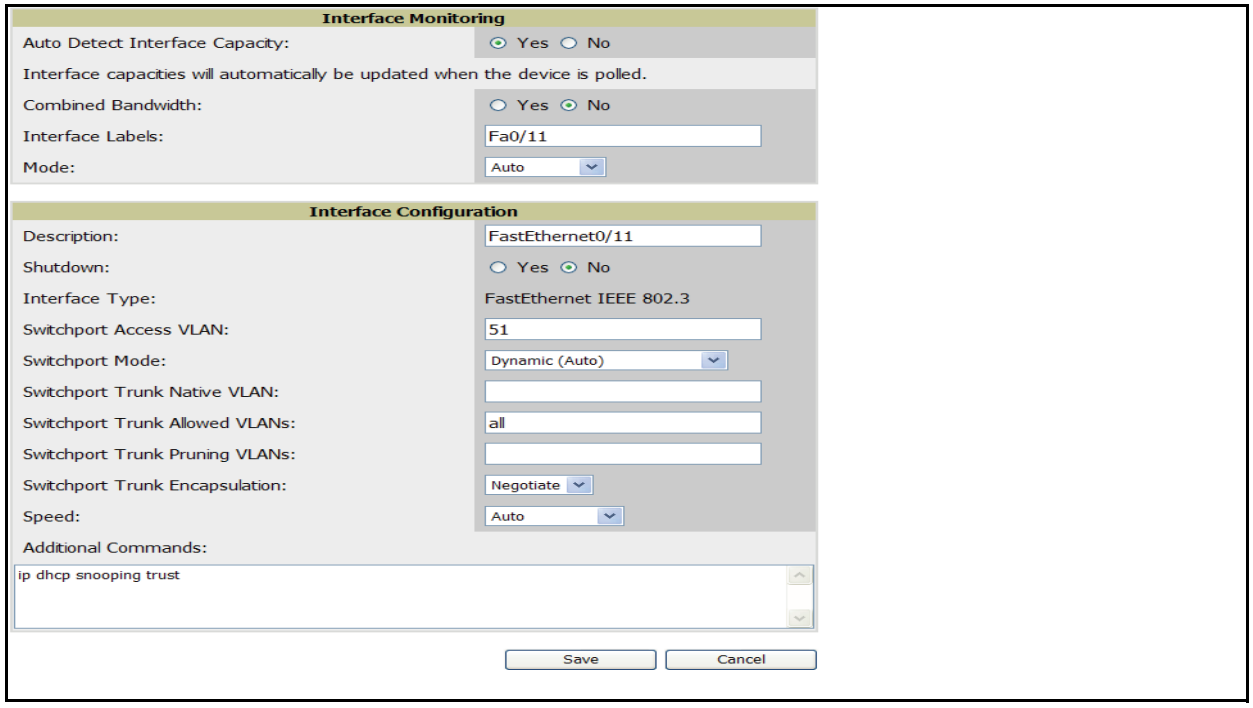
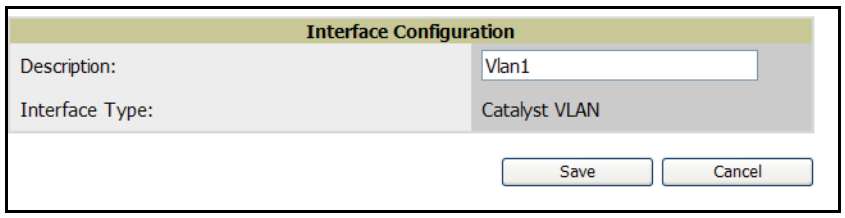
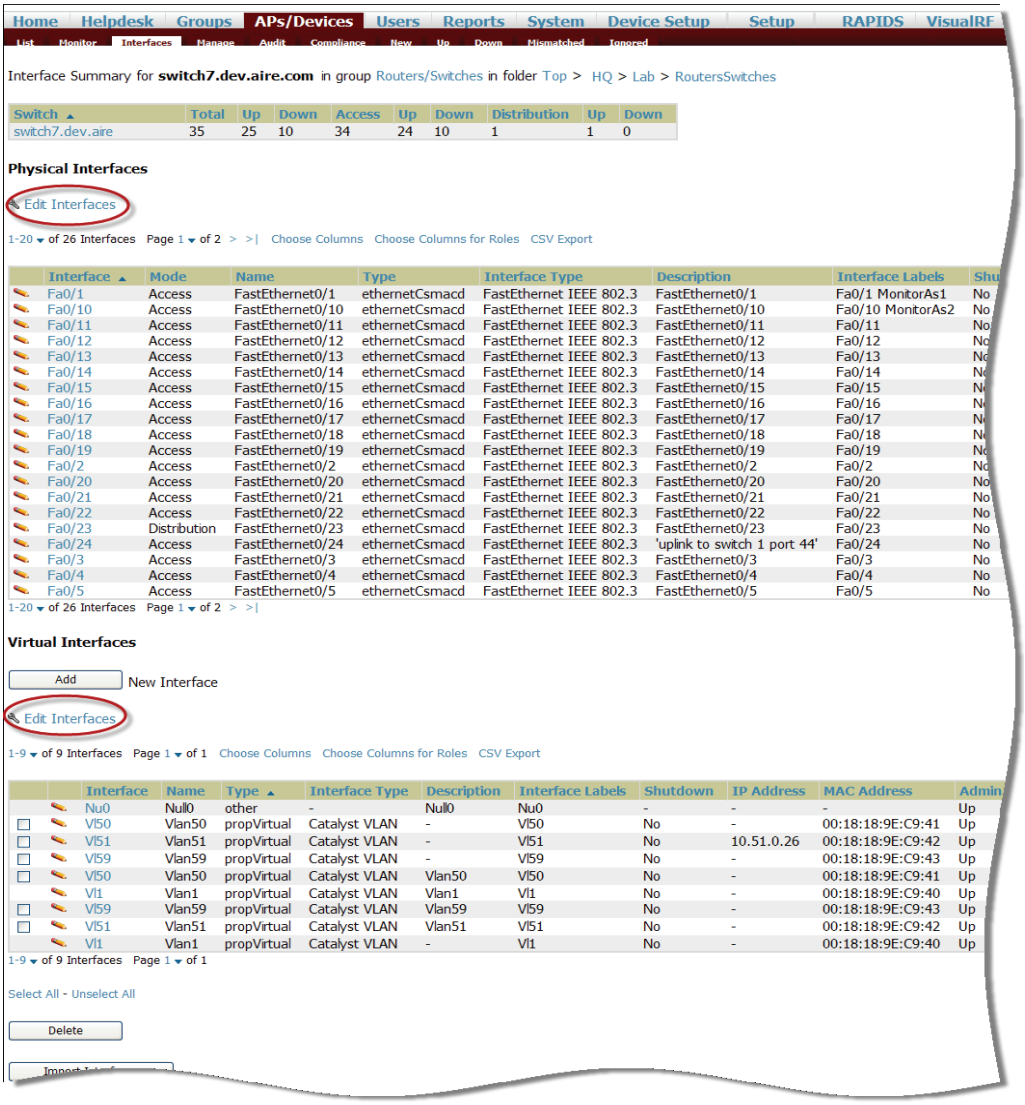


Figure 114 ***Virtual Individual Interfaces Configuration*** *Pane (***Interfaces Monitoring and Configuration** *Window)*



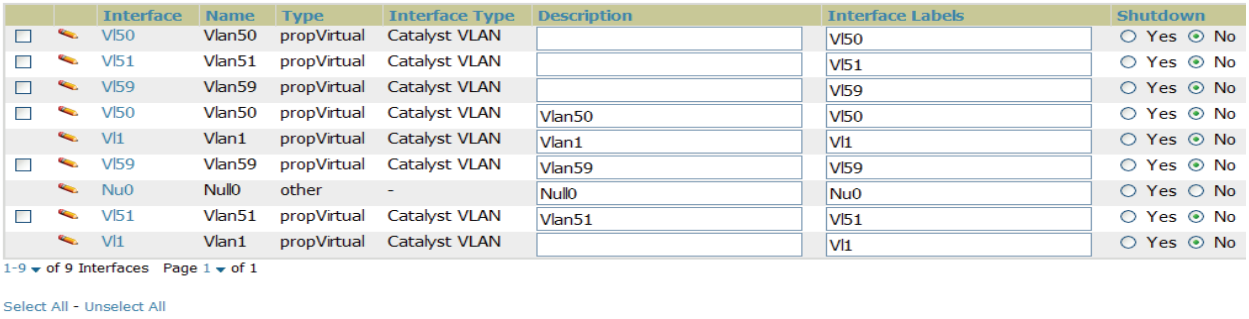
To configure interfaces as a group, click the **Edit Interfaces** button above the Physical or Virtual Interfaces table that includes the interfaces you want to edit collectively as shown in Figure 115.

Figure 115 *Edit Multiple Interfaces*



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 116.

Figure 116 *Multiple Interface Edit UI*

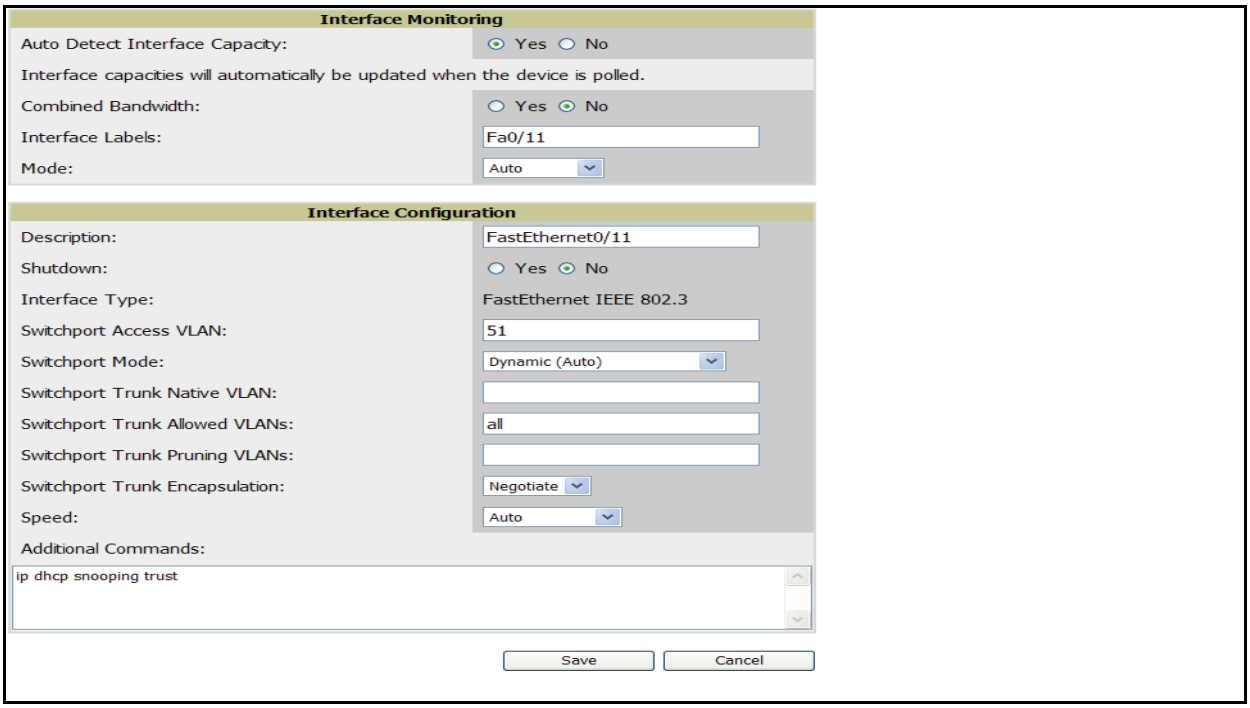


OV3600 assembles the entire running configuration using templates and your modifications to these pages. For a more detailed discussion on the use of templates, see Chapter 6, “Creating and Using Templates” on page 185.

Configuring Cisco Router and Switch Interface Settings

When you select an interface on a Cisco wired device to edit in OV3600, the fields available in the virtual or physical **Interface Configuration** pane will auto-populate according to the existing interface device configuration as shown in Figure 117.

Figure 117 ***Physical Interfaces Configuration*** *Pane (Interfaces Monitoring and Configuration Window)*



Not all interface settings are valid for all switches. You can change or overwrite any of the pre-populated settings as well as revise or add to the Additional Commands fields to tailor the template configuration to the needs of your production environment. For further details and assistance with settings configuration, refer to your Cisco product documentation.

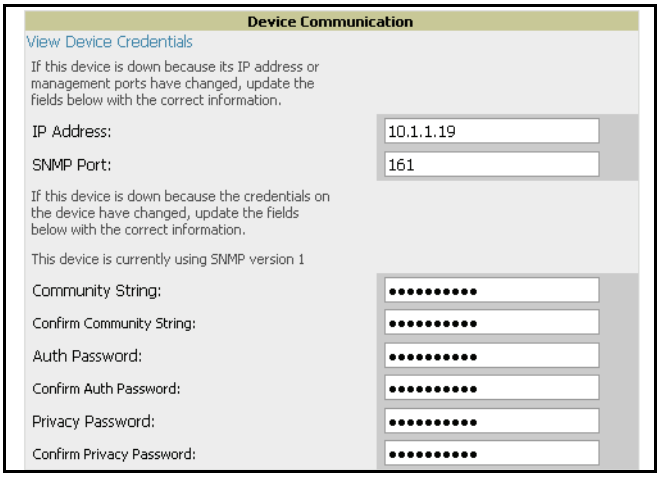
OV3600 assembles the entire running configuration using templates and your modifications to these pages. For a more detailed discussion on the use of templates, see Chapter 6, “Creating and Using Templates” on page 185.

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 118 illustrates this page.

Figure 118 ***APs/Devices > Manage > Device Communication***



NOTE

The **Device Communication** area may appear slightly different depending on the particular vendor and model of the APs being used.

3. Enter the appropriate **Auth Password** and **Privacy Password**.
4. You can disable the **View AP Credentials** link in OV3600 by the root user. Contact Alcatel Lucent support for detailed instructions to disable the link.
5. (Optional-Not pictured.) Enter the appropriate SSH and Telnet credentials if you are configuring Aruba/Alcatel-Lucent or any Cisco device except Cisco wireless LAN controllers.
6. Click **Apply**. OV3600 presents a confirmation window reminding you of all configuration changes that will be applied to the AP. Click **Confirm Edit** to apply the changes to the AP immediately, **Schedule** to schedule the changes to occur during a specific maintenance window, or **Cancel** to return to the **APs/Devices > Manage** page.

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.

Click **Upgrade Firmware** to upgrade the device's firmware. Figure 119 illustrates this page and Table 90 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.

Figure 119 ***APs/Devices > Manage Firmware Upgrades***

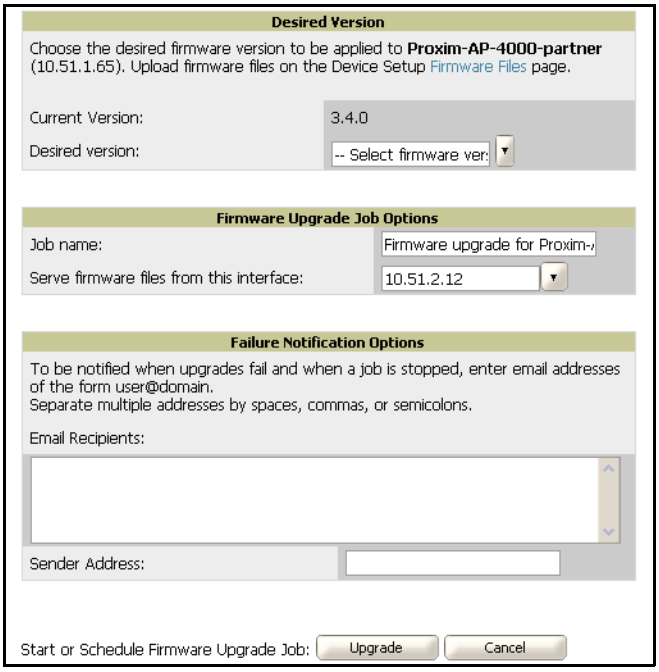


Table 90 ***APs/Devices > Manage Firmware Upgrades*** *Fields and Default Values*

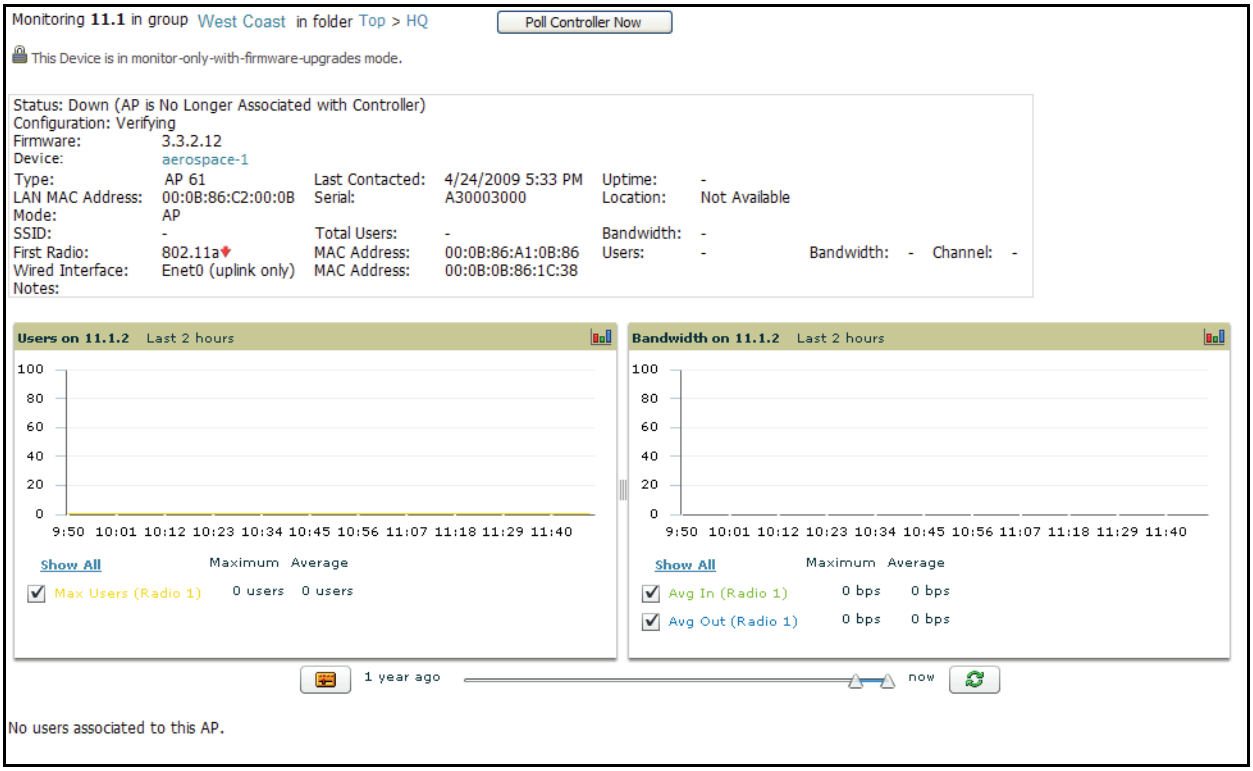
Setting	Default	Description
Desired Version	None	Drop-down menu that specifies the firmware to be used in the upgrade. Firmware can be added to this drop-down menu on the **Device Setup > Firmware Files** page.
Job Name	None	Sets a user-defined name for the upgrade job. Alcatel Lucent recommends using a meaningful and descriptive name.
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.

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. Click 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, shown in Figure 120.

Figure 120 ***APs/Devices > Monitor*** *Page Illustration for a Down Device*



2. Locate the **Status** section. If the Status is **Down**, there is an onscreen error message indicating the cause of the problem. Some of the common system messages are as follows in Table 91:

Table 91 *Common System Messages for Down Status*

Message	Meaning
SNMP Get Failed	SNMP community string specified for that device is incorrect or an incorrect SNMP port is specified. If SNMP is not enabled on the device you will also receive this message. Some factory default APs, including Cisco IOS 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.
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, click the **APs/Devices > Manage** tab to go to the management page for that device.
4. If visible, click the **View device credentials** link in the **Device Communications** area. 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. If you are interested in disabling this feature, please contact Alcatel Lucent support. See "Contacting Alcatel-Lucent" on page 11. Figure 121 illustrates this page.

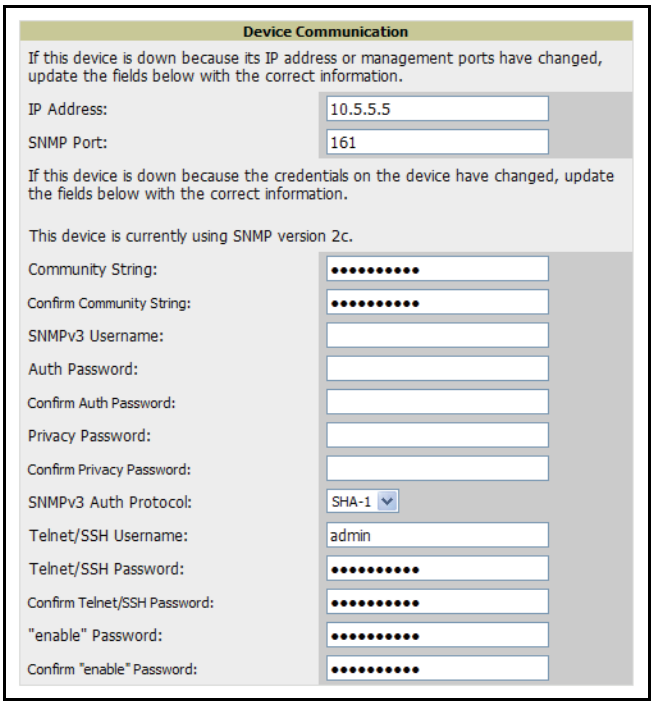
Figure 121 ***View AP Credentials***

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. Figure 122 illustrates this page.

Figure 122 ***APs/Devices > Manage > Device Communication*** *Section Illustration*



NOTE

The **Device Communication** area may appear slightly different depending on the particular vendor and model.

6. Enter the appropriate credentials, and click **Apply**.
7. Return to the **APs/Devices\ List** page to see if the device appears with a Status of **Up**.

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 186
- "Viewing and Adding Templates" on page 187
- "Configuring General Template Files and Variables" on page 191
- "Configuring Cisco IOS Templates" on page 196
- "Configuring Cisco Catalyst Switch Templates" on page 198
- "Configuring Symbol Controller / HP WESM Templates" on page 198
- "Configuring a Global Template" on page 202

For additional information, refer to the *Alcatel Lucent Wireless Knowledge Base*, which requires registration and login.

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:

- Alcatel-Lucent
- Aruba

Alcatel Lucent recommends using the graphical AOS Config feature in support of Aruba and Alcatel-Lucent devices, particularly for AOS 3.3.2.x and AOS 3.4.x. Refer to the Aruba/*Alcatel-Lucent Configuration Guide* for additional information.

- Cisco Aironet IOS and 4800 autonomous APs
- Cisco Catalyst Switches
- HP ProCurve 530 and WeSM controllers
- Hirschmann
- LANCOM
- 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.

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. Navigate 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 clicking 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 81.

2. From the OV3600 navigation pane, click **Templates**. The **Templates** page appears. Figure 123 illustrates the **Groups > Templates** configuration page, and Table 92 describes the information columns.

Figure 123 ***Groups > Templates*** *Page Illustration for a Sample Device Group*

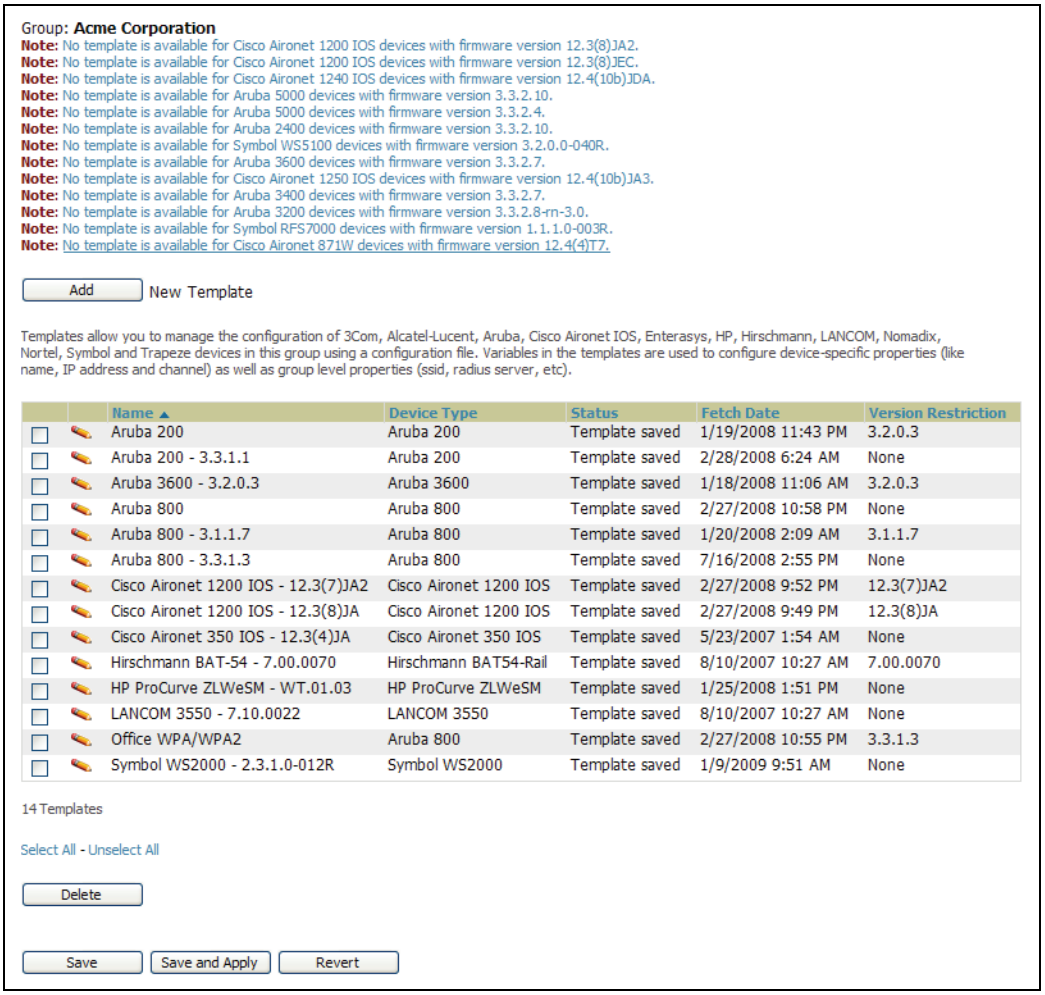


Table 92 ***Groups > Templates*** *Fields and Default Values*

Setting	Description
Notes	When applicable, this section lists devices that are active on the network with no template available for the respective firmware. Click the link from such a note to launch the Add Template configuration page for that device.
Name	Displays the template name.
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.

Table 92 ***Groups > Templates*** *Fields and Default Values (Continued)*

Setting	Description
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, navigate to the **Groups > List** page, and select the group to which you will apply the template. Click the group name and the **Details** page appears. Click **Templates**, then click **Add**.

4. Complete the configurations illustrated in Figure 124, and the settings described in Table 93.

Figure 124 ***Groups > Templates > Add Template*** *Page Illustration*

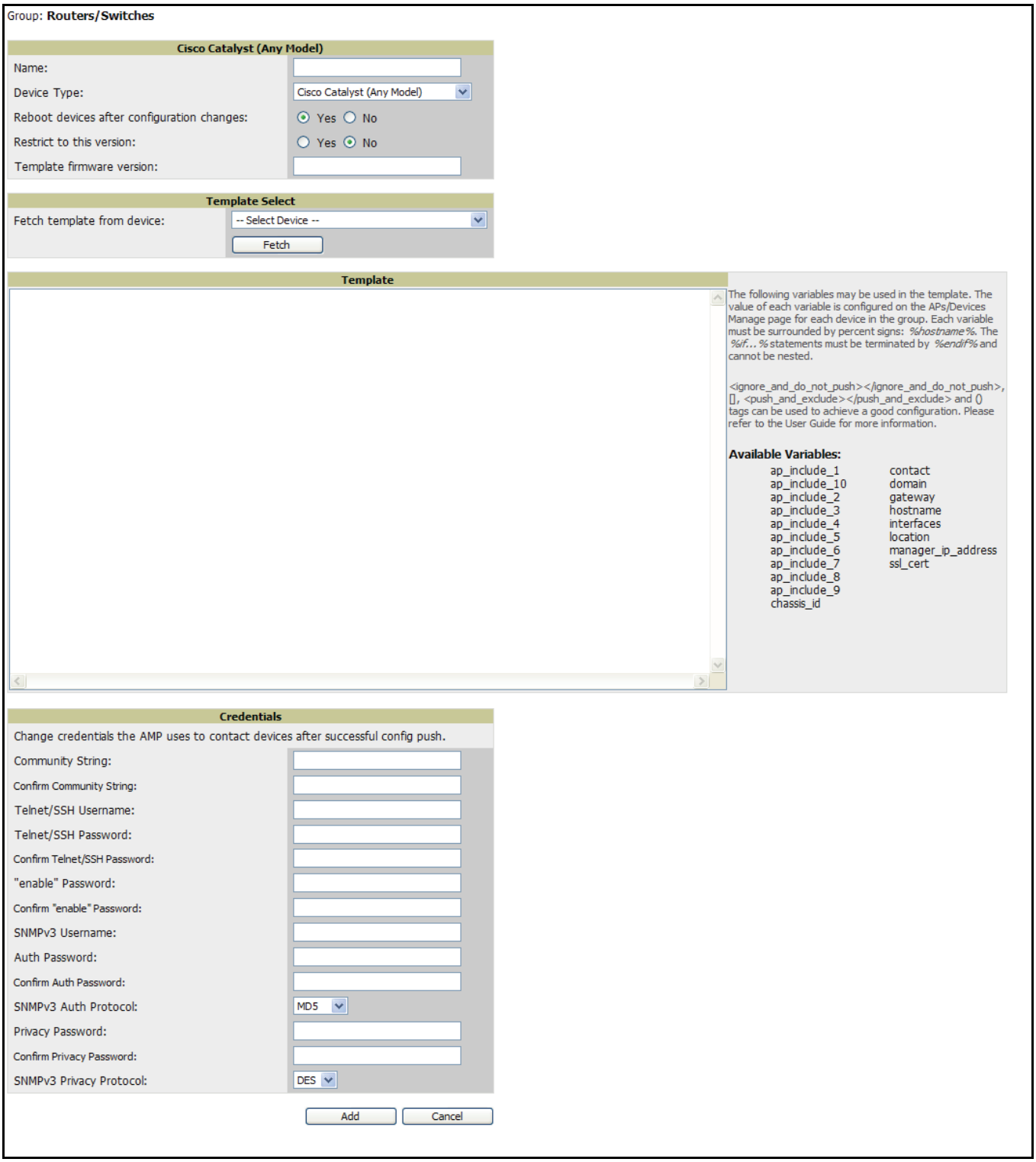


Table 93 ***Groups > Templates > Add Template*** *Fields and Default Values*

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*.
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. **NOTE:** 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.

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 via 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. Navigate to the **Groups > Templates** configuration page. Click **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 click **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 193

   These variables are always encapsulated between % signs. On the right side of the configuration page is the **Additional Variables** section. This section lists all available variables for your template. Variables that are in use in a template are green, while variables that are not yet in use are black. Verify these substitutions to ensure that all of the settings that you believe should be managed on an AP-by-AP basis are labeled as variables in this fashion. If you believe that any AP-level settings are not marked correctly, please contact Alcatel-Lucent Technical Support at Esd.support@alcatel-lucent.com 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. Click the **Save and Apply** button 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.

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>substring</ignore_and_do_not_push>

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.

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</push_and_exclude>

Instead of using the full tags you may use the parenthesis shorthand, (substring). The push and exclude directive is used to push commands to the AP that will not appear in the running-config file. For example, some **no** commands that are used to remove SSIDs or remove configuration parameters do not appear in the running-config file of a device. A command inside the push and exclude directive are included in the

startup-config file pushed to a device, but OV3600 excludes them when calculating and reporting configuration mismatches.

The opening tag may have leading spaces.

Below are some examples of using directives:

```
…
line con 0
 </push_and_exclude>no stopbits</push_and_exclude>
line vty 5 15
!
ntp server 209.172.117.194
<ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push>
end
```

Using Conditional Variables in Templates

Conditional variables allow lines in the template to be applied only to access points where the enclosed commands will be applicable and not to any other access points within the Group. For example, if a group of APs consists of dual-radio Cisco 1200 devices (802.11a/b) and single-radio Cisco 1100 (802.11b) devices, it is necessary to make commands related to the 802.11a device in the 1200 APs conditional. Conditional variables are listed in the table below.

The syntax for conditional variables is as follows, and syntax components are described in Table 94:

```
%if variable=value%
…
%endif%
```

Table 94 *Conditional Variable Syntax Components*

Variable	Values	Meaning
`interface`	Dot11Radio0	2.4GHz radio module is installed
	Dot11Radio1	5GHz external radio module is installed
`radio_type`	a	Installed 5GHz radio module is 802.11a
	b	Installed 2.4GHz radio module is 802.11b only
	g	Installed 2.4GHz radio module is 802.11g capable
`wds_role`	backup	The wds role of the AP is the value selected in the drop down menu on the **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 95 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 95.

Table 95 *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
`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%	-

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 literally hundreds of configurable settings. For simplicity and ease of use, OV3600 enables you to control them via the **Groups > Templates** configuration page. This configuration page defines the startup-config file of the devices rather than utilizing 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 within those groups.

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. Alcatel Lucent recommends using 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 315 for a full Cisco IOS template.

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 be 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 APs 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 certain radio types (that is, 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. You can 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. The below examples illustrate this usage:

```
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 Cisco Router and Switch Interface Settings" on page 179. 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 191.

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 controllers (5100 and 2000) can be configured in OV3600 using templates. OV3600 supports Symbol 5100 firmware upgrades for 3.x.

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 196.

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.

There is an option on the **Group > Templates** page to reboot the device after pushing a configuration to it. Certain settings have integrated variables, including `ap-license` and `adoption-preference-id`. The radio preamble has been template-integrated as well.

```
//
// WS2000 Configuration Command Script
// System Firmware Version: 2.1.0.0-035R
//
/
passwd enc-admin b30e1f81296925
passwd enc-manager a11e00942773
/
system
ws2000
// WS2000 menu
set name %hostname%
set loc %location%
set email %contact%
set cc us
set airbeam mode disable
set airbeam enc-passwd a11e00942773
set applet lan enable
set applet wan enable
set applet slan enable
set applet swan enable
set cli lan enable
set cli wan enable
set snmp lan enable
set snmp wan enable
set workgroup name WORKGROUP
set workgroup mode disable
set ftp lan disable
set ftp wan disable
set ssh lan enable
set ssh wan enable
set timeout 0
/
"templatized-running-config-static" 1309L, 28793C
1,1           Top
set port 8 primary 1812

set server 8 secondary 0.0.0.0
set port 8 secondary 1812

/
// Hotspot Whitelist configuration
network
wlan
hotspot
white-list
clear rule all
// Hotspot Whitelist 1 configuration
// Hotspot Whitelist 2 configuration
// Hotspot Whitelist 3 configuration
// Hotspot Whitelist 4 configuration
// Hotspot Whitelist 5 configuration
// Hotspot Whitelist 6 configuration
```

```
// Hotspot Whitelist 7 configuration
// Hotspot Whitelist 8 configuration
/
/
network
dhcp
// network->dhcp menu
set firmwareupgrade 1
set configupgrade 1
set interface s2
set dhcpvendorclassid
/
Save
```

A sample Symbol thin AP template is provided below for reference and for the formatting of **`if`** statements.

```
set mac %radio_index% %radio_mac%
set ap_type %radio_index% %ap_type%
set radio_type %radio_index% %radio_type%
set beacon intvl %radio_index% 100
set dtim %radio_index% 10
set ch_mode %radio_index% fixed
%if radio_type=802.11a%
set primary %radio_index% 1
%endif%
%if radio_type=802.11b%
set short-pre %radio_index% disable
%endif%
%if radio_type=802.11b/g%
set short-pre %radio_index% disable
%endif%
set div %radio_index% full
set reg %radio_index% in/out %channel% %transmit_power%
set rts %radio_index% 2341
set name %radio_index% %description%
set loc %radio_index%
set detectorap %radio_index% %detector%
%if radio_type=802.11a%
set rate %radio_index% 6,12,24 6,9,12,18,24,36,48,54
%endif%
%if radio_type=802.11b%
set rate %radio_index% 1,2 1,2,5.5,11
%endif%
%if radio_type=802.11b/g%
set rate %radio_index% 1,2,5.5,11 1,2,5.5,6,9,11,12,18,24,36,48,54
%endif%
```

Configuring Clustering and Redundancy

The following redundancy parameters can be considered 'device' parameters, and the %ap_include variables can be used to represent them:

- interface-ip
- mode
- member-ip
- enable

The following redundancy parameters can be considered 'group' parameters, and should not be mad into a variable in the template:

- group-id
- heartbeat-period
- hold-period
- discovery-period
- handle-stp

The following is an example template (redundancy section only):

```
redundancy group-id 5
redundancy interface-ip %ap_include_2%
redundancy mode %ap_include_3%
redundancy heartbeat-period 60
redundancy hold-period 120
redundancy discovery-period 10
redundancy handle-stp enable
%ap_include_1%
%ap_include_4%
```

Put the controller-appropriate values into the relevant fields on the **APs/Devices > Manage** pages.

Changing Redundancy Configuration

This procedure presumes an operable configuration from which you can build additional and redundant templates. To configure an Active/Active as opposed to an Active/Standby template, perform the following steps:

1. On the **APs/Devices > Manage** page of the device that is or will be the Standby device, change the ap_include_4 variable to `no redundancy enable`.
2. Put device in **Manage** mode, then click **Save and Apply**. The configuration is pushed to the device. There should be no mismatches with this approach.
3. On the **APs/Devices > Manage** page for that same device, change the `ap_include_3 variable` to **Primary** or **Standby**. Click **Save and Apply**. The configuration is pushed to the device. There should be no mismatches with this approach.
4. On the **APs/Devices > Manage** page of same device, change the `ap_include_4` variable to redundancy enable. Click Save and Apply. The configuration is pushed to the device. There should be no mismatches with this approach.

Adding Clustering Members

This template configuration changes group-level parameters.

1. On the **APs/Devices > Manage** page of each of the devices in the group, change the `ap_include_4` variable to `no redundancy enable`. Put device in management mode. Click **Save and Apply**.
2. Configuration will be pushed to the devices. There should be no mismatches.
3. Edit one or more of the 'group' redundancy parameters in the template. Click **Save and Apply.**
4. Configuration will be pushed to the device. There should be no mismatches.
5. On the **APs/Devices > Manage** page of the devices, change ap_include_4 to "redundancy enable". Click Save and Apply.

6. Configuration will be pushed to the devices. There should be no mismatches.

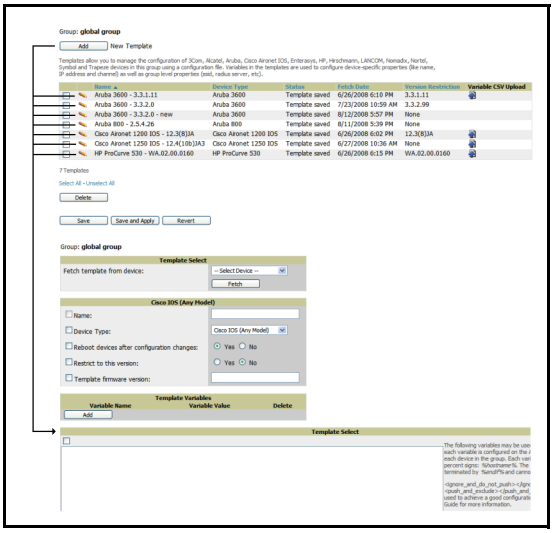
Configuring a Global Template

Global templates allow OV3600 users to define a single template in a global group that can be used to manage access points in subscriber groups. Such a template enables turning 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:

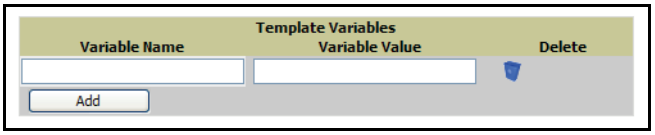
1. Navigate to the **Group > Templates** configuration page for the global group that owns it.
2. Click the **Add** button to add a new template, or click the **pencil** icon next to an existing template to edit that template.
3. Examine the configurations illustrated in Figure 125.

Figure 125 ***Group > Templates > Add*** *Page Illustration*



4. Use the drop-down menu to select a device from which to build the global template and click the **Fetch** button. The drop-down 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 126.

Figure 126 ***Template Variables*** *Illustration*



The variable name cannot have any spaces or non-alphanumeric characters. The initial variable value entered is the default value, but can be changed on a per-group basis later. You can also populate global template variables by uploading a CSV file (see below).

5. Once you have configured your global template, click **Add** at the bottom of the configuration page. You are taken to a confirmation configuration page where you can review your changes.
6. If you want to add the global template, click the **Apply Changes Now** button. If you do not want to add the template, click the **Cancel and Discard Changes** button. 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. Navigate to the **Groups > Templates** configuration page and click the **CSV** upload icon for the template. The CSV file must contain columns for **Group Name** and **Variable Name**. All fields must be completed.

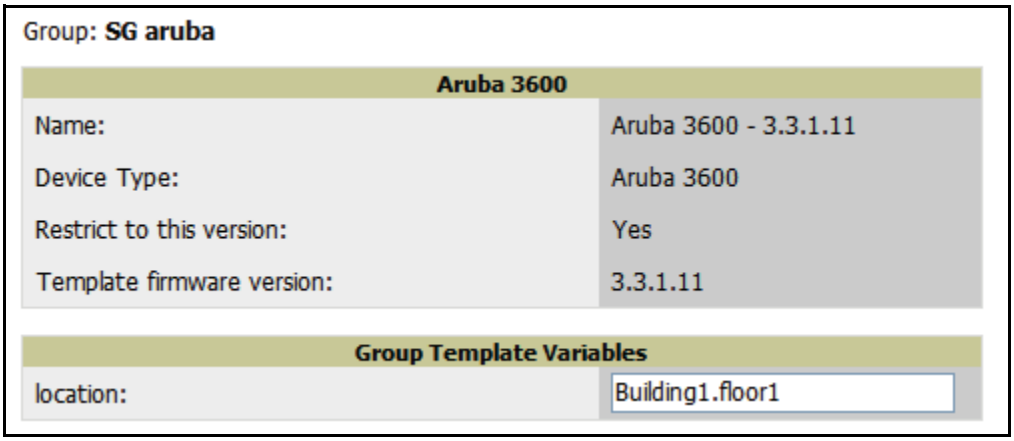
- **Group Name**—the name of the subscriber group that you wish to update.
- **Variable Name**—the name of the group template variable you wish to update.
- **Variable Value**—the value to set.

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. Navigate to the **Groups > Template** configuration page for the local group and click the pencil icon next to the name of the global template in the list. Figure 127 illustrates this page.

Figure 127 ***Groups > Templates Edit****, Topmost Portion*



9. To make template changes, navigate to the **Groups > Template** configuration page for the global group and click 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 detection using RAPIDS, and contains the following sections:

- "Overview Tab" on page 205
- "List" on page 207
- "RAPIDS Setup" on page 211
- "RAPIDS Rules" on page 214
- "Score Override" on page 220
- "Audit Log" on page 221
- "Additional Rogue Device Resources" on page 221

Overview Tab

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 to mitigate 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 eliminate the threat.

RAPIDS discovers unauthorized devices in your WLAN network in the following ways:

- **Over the Air**
  - Using your existing enterprise APs (Alcatel Lucent, Alcatel-Lucent, Cisco WLC, Symbol for example)
  - RF scanning using Alcatel Lucent Management Client (AMC)—Optional
- **On the Wire**
  - Using HTTP and SNMP Scanning
  - Polling routers and switches to identify, classify, and locate unknown APs

Furthermore, RAPIDS integrates with external intrusion detection systems (IDS), as follows:

- **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.

The **Overview** tab displays a page of RAPIDS summary information (see Figure 128).

Figure 128 *RAPIDS Overview tab*

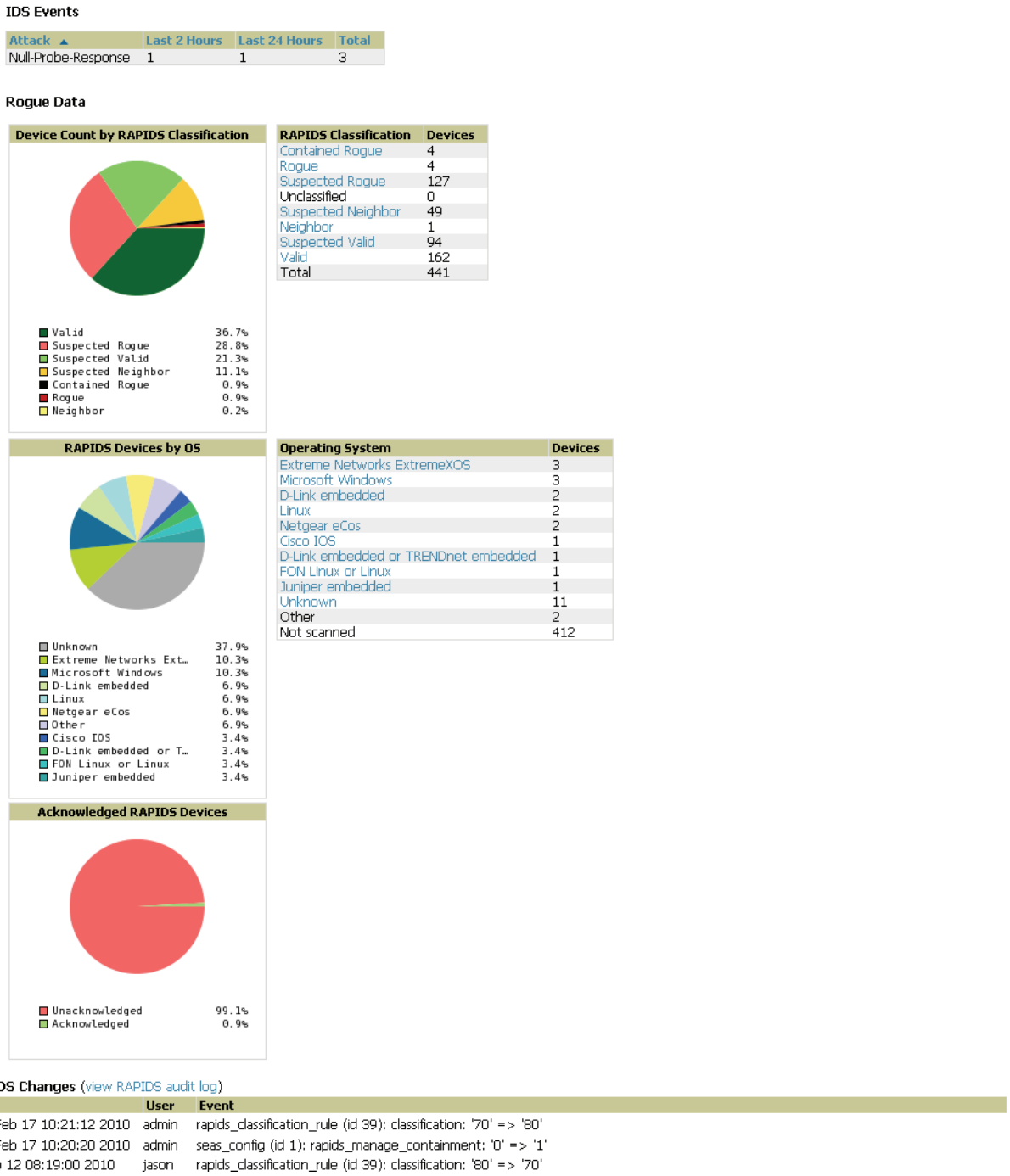


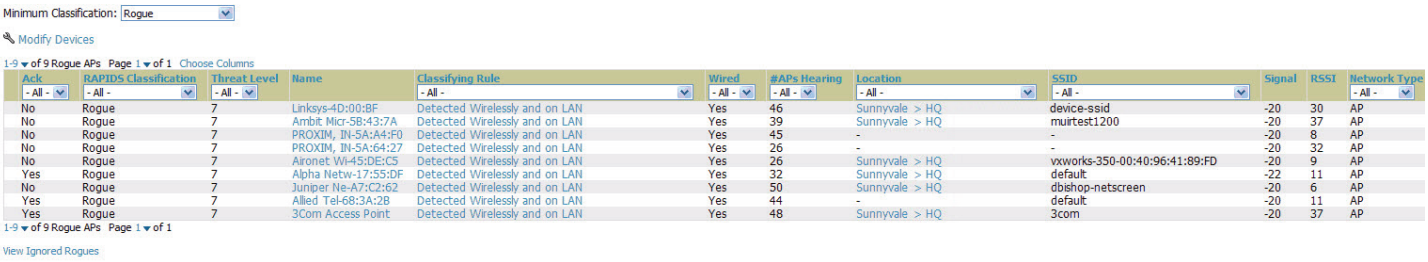
Table 96 ***Overview*** *Fields*

Summary	Description
IDS Events	Displays a list of IDS events for the designated folder (**Top** is the default) and subfolders. Field displays events from the past two hours, the past 24 hours, and total IDS events.
Rogue Data	A summary of rogue device counts by RAPIDS classification in a color coded pie chart format and listed summary. View additional details for rogue devices via the **RAPIDS > List** page.
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.
Acknowledge Devices	A color coded pie chart comparing the number of acknowledged devices to the unacknowledged devices.
RAPIDS Changes	RAPIDS change log tracks every change made to the RAPIDS system including changes to rules, manual classification, and anything on the **RAPIDS > Setup** page.

List

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 129). You can sort the table columns (up/down) by selecting the column head or filter data using the column head drop down menus.

Figure 129 ***Viewing a Rogue AP by Classification***



NOTE

The page displayed in Figure 129 may require a moment to load; no rogues displayed for a given classification means that no such rogue device was discovered on your network.

Table 97 details the column information displayed in Figure 129. For additional information about RAPIDS rules, refer to "RAPIDS Rules" on page 214.

The active links on this page launch additional pages for RAPIDS configuration or device processing.

Table 97 ***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 211).
RAPIDS Classification	Displays the current RAPIDS classification. This classification is determined by the rules defined on the **RAPIDS > Rules** page.

Table 97 ***RAPIDS > List*** *Column Definitions*

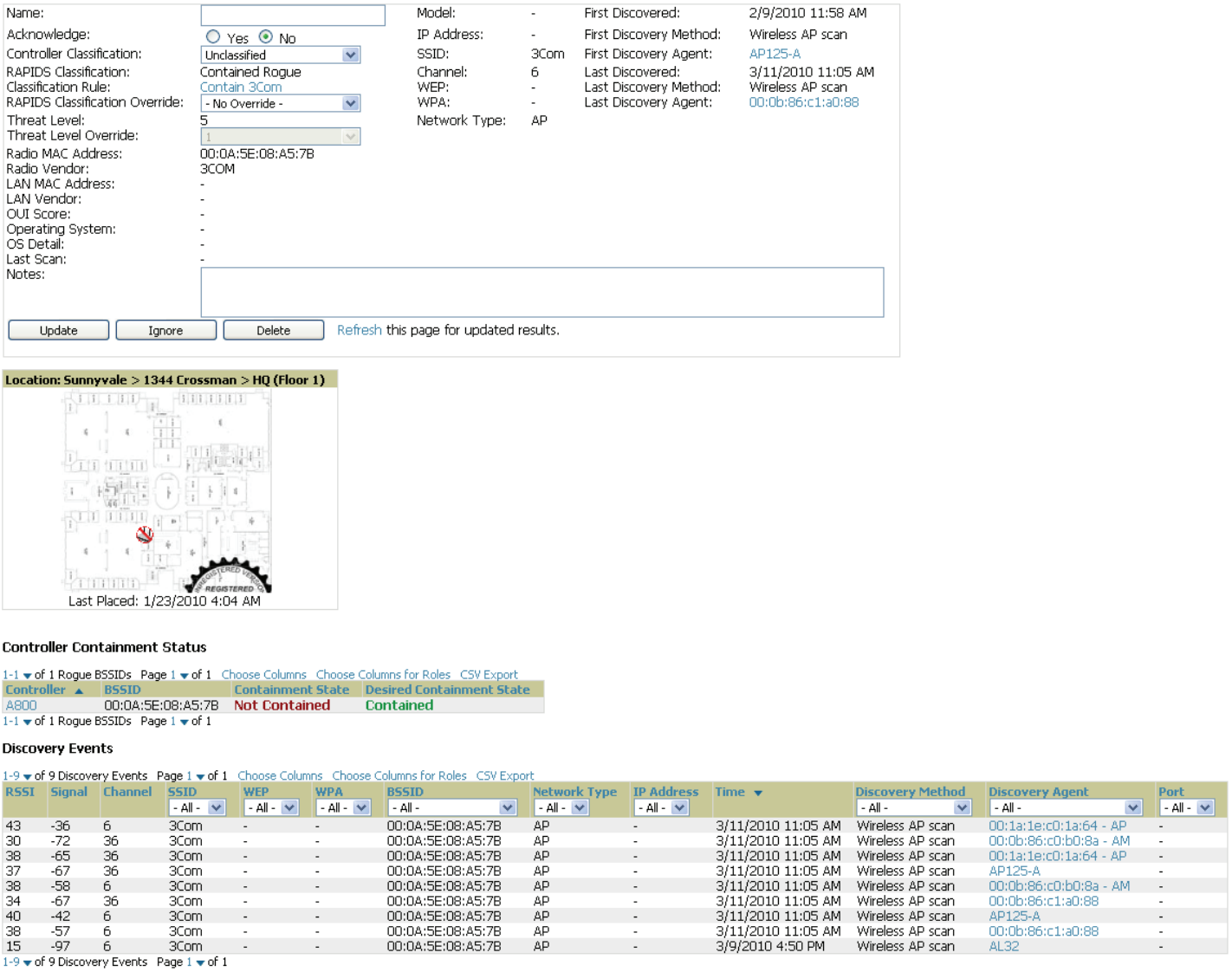
Column	Description
Threat Level	This field displays the numeric threat level of the device, in a range from 1 to 10. The definition of threat level is configurable, as described in "Rogue Device Threat Level" on page 215. The threat level is also supported with Triggers (see "Creating and Using Triggers and Alerts" on page 224).
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 215).
Controller Classification	Displays the classification of the device based on the controller's hard-coded rules. **NOTE:** This column is hidden unless *Offload Aruba/Alcatel-Lucent WMS Database* is enabled by at least one group on the **Groups > Basic** page.
Wired	Displays whether the rogue device has been discovered on the wire. This column displays **Yes** or is blank if wired information was not detected.
#APs Hearing	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 all **List** pages in OV3600 7.0, the **RAPIDS > List** page includes the **Location** column. Click the location associated to the rogue device to view the VisualRF floor plan that includes the specified device. 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.
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 comprised of ceiling-mounted APs, 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 as known. Possible contents of this field include the following encryption types: • **Open**—Definition pending • **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 RF channel on which the rogue device was detected.
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 based on the results of the scan.

Table 97 ***RAPIDS > List*** *Column Definitions*

Column	Description
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 the group.
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.

To view the details for any rogue device, select the device name to launch the device's detail page (Figure 130).

Figure 130 ***Rogue APs*** *Device Detail Page*



NOTE

The historical information displayed on the device detail page indicates the most recent discovery event per discovering device.

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.
- Each rogue device typically 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 from this page. Otherwise, best practices strongly recommends that you extract the device from your building and delete the rogue device from the system.

To update a rogue device:

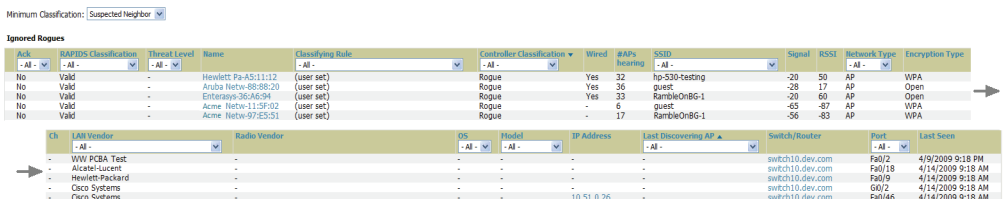
1. Select the device name from the list on the **RAPIDS > List** page to launch the device detail page (see Figure 130).
2. If an IP address is available for a given device, click the **Identify OS for Suspected Rogues** option to obtain operating system information.
3. Select the **Ignore** button if the rogue device is to be ignored.
4. 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.

1. From the **RAPIDS > List** page, click **View Ignored Rogues** (at the bottom left of the page) to launch the **Ignored Rogues** page.
2. From the **Minimum Classification** drop-down menu, select the type of ignored rogue devices to display. Table 97 explains the fields on this page.

Figure 131 ***Ignored Rogue Devices*** *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.
- Click **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 "RAPIDS Setup" on page 211)

  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 mitigate the rogue remove it from the network and delete the rogue record. If you want to allow it on the network, classify the device as valid and update with notes that describe it.

Be aware that 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.

RAPIDS Setup

The **RAPIDS > Setup** page allows you to configure your OV3600 server for RAPIDS. Complete the settings on this page as desired, and click **Save**. Note that 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. Table 98 illustrates this page and Table 98 describes default values.

Table 98 *RAPIDS > Setup*

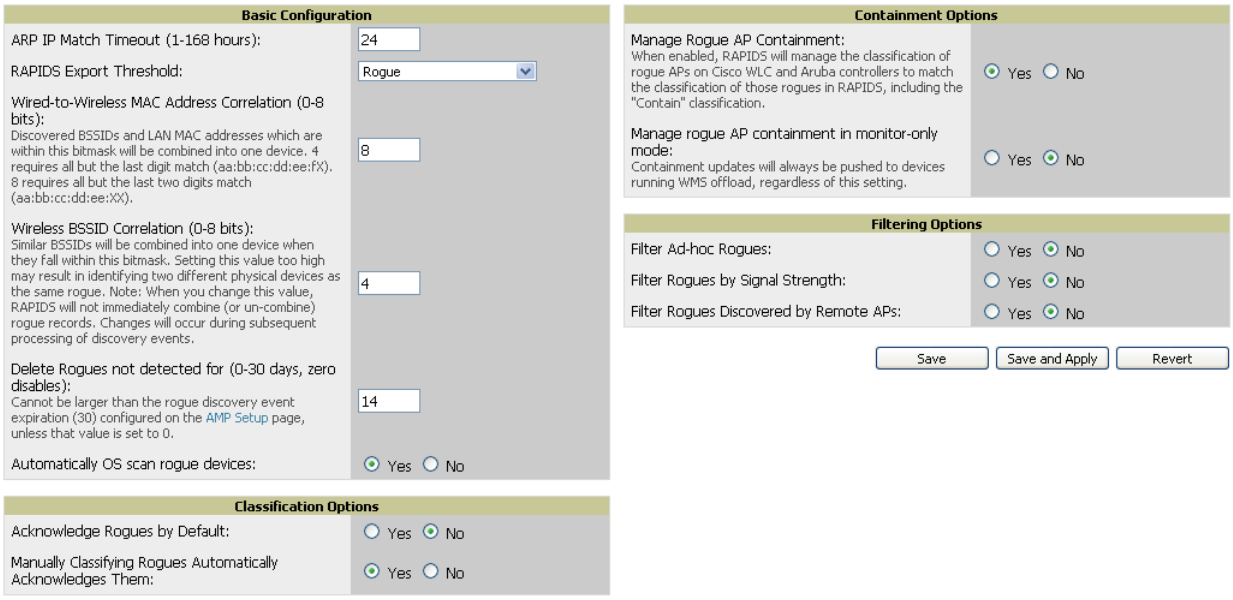


Figure 132

Table 99 *RAPIDS > Setup Page Fields > Classification Options*

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.

Table 100 *RAPIDS > Setup Page Fields > 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 recomment 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.

Containment Options

Using RAPIDS, OV3600 can shield rogue devices from associating to Cisco WLC (versions 4.2.114 and later), and Alcatel Lucent controllers (running AOS versions 3.x and later). OV3600 will alert you to the appearance of the rogue device and identify any mismatch between controller configuration and the desired configuration.

WMS Offload is not required to manage containment in OV3600.

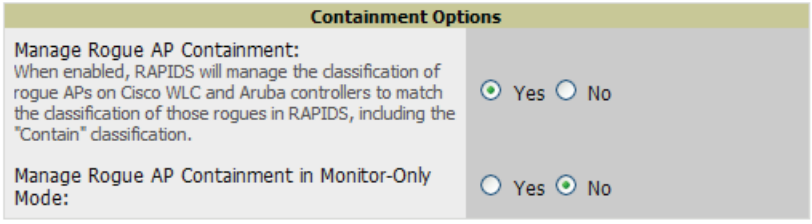
Table 101 shows Containment Options.

Table 101 *RAPIDS > Setup > Containment Options*

Field	Default	Description
Manage Rogue AP Containment	**Yes**	Rogue APs on Cisco WLC and Aruba 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.
Manage Rogue AP Containment in Monitor-Only Mode	**No**	If No is selected, OV3600 will display the desired containment settings but not push them to the 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 Yes is selected, OV3600 will push the desired containment settings to the controllers in Monitor-Only mode, as well as the devices in managed mode.

1. Navigate to the **RAPIDS > SETUP** page to see Containment Options, as shown in Figure 133.

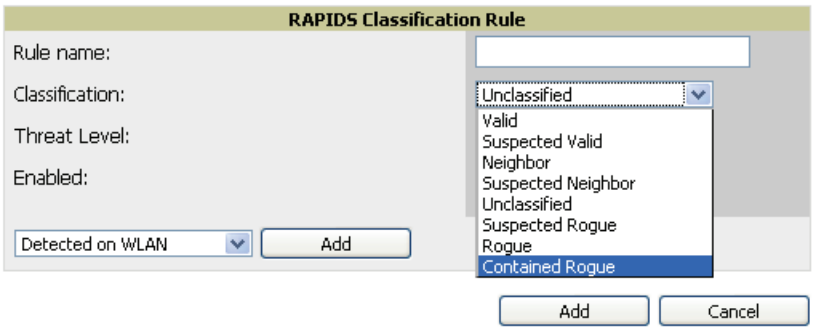
Figure 133 ***RAPIDS > Setup Containment Options Pane***



2. From the **Containment Options** pane, click the Yes radio button 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 134.

   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 134 ***RAPIDS > Rules Classification Options Menu with Containment***



From the **APs/Devices > Rogues Contained** page, you can see the containment status information, as shown in Figure 135.

NOTE

The Rogue Containment device tab is only present for devices that support containment.

Figure 135 ***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 52.
- Use the **OV3600 Setup > General > Performance Tuning** page to define the processing priority of RAPIDS in relation to OV3600 as a whole (see Table 13 on page 46).

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:

- "Controller Classification with WMS Offload" on page 214
- "Device OUI Score" on page 215
- "Rogue Device Threat Level" on page 215
- "Viewing and Configuring RAPIDS Rules" on page 215
- "Recommended RAPIDS Rules" on page 219
- "Using RAPIDS Rules with Additional OV3600 Functions" on page 219

Controller Classification with WMS Offload

This classification method is supported only when WMS offload is enabled on Alcatel Lucent WLAN switches. Controller 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 ArubaOS controllers that are WMS offload enabled.

WMS offload ensures that a particular BSSID has the same classification on all of the controllers. WMS offload removes some load from master controllers and feeds 'connected-to-lan' information to the RAPIDS classification engine. RAPIDS classifications and controller classifications are separate and often are not synchronized.

RAPIDS classification is not pushed to the devices.

The following table compares how default classification may differ between OV3600 and ArubaOS, for scenarios involving WMS Offload.

Table 102 *Rogue Device Classification Matrix*

OV3600	AOS (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 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 103 provides list the OUI scores definitions.

Table 103 *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 SOHO market.
Score of 4	Indicates that the OUI matches a block that belonged to a manufacturer that produces SOHO 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,which is based on the classifying rule, ranging from 1 to 10, with a default value of 5. This classification process can help identify which of two rogues is likely to be a greater threat. Alerts can be defined and based on threat level; this is helpful for sorting rogue devices.

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 a device 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 136). Table 104 defines the content of the **RAPIDS > Rules** page.

Figure 136 ***RAPIDS > Rules*** *Page Illustration*

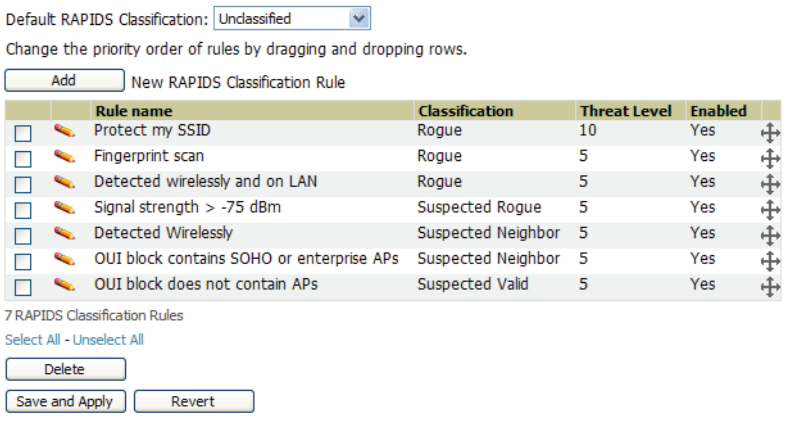
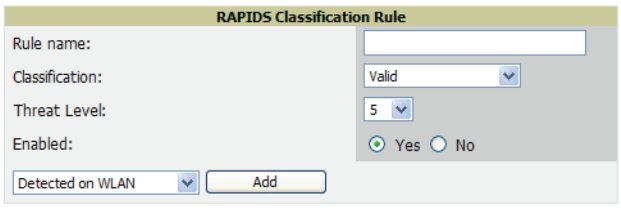


Table 104 *RAPIDS > Rules Page*

Field	Description
Default Classification	Sets the classification that a rogue device receives when it does not match any rules.
Add New RAPIDS Classification Rule	Click 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.
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 215 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. Click, 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 to 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 137).

Figure 137 *Classification Rule Page*



Fill in the settings described in Table 104 then select an option from the drop down menu.

Table 105, Table 106, and Table 107 define the drop down menu options that are at the bottom left of the RAPIDS Classification Rule dialog box (see Figure 137). Once all rule settings are defined, click the **Add** button. The new rule automatically appears in the **RAPIDS > Rules** page.

Table 105 *Wireless Properties Drop Down Menu*

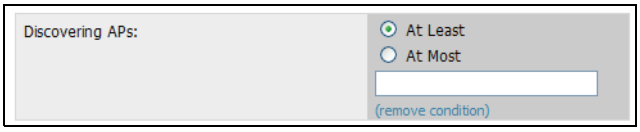
Option	Description
Detected on WLAN	Classifies based on how the rogue is detected on the wireless LAN.
Discovering AP Count	Classifies based on the number of managed devices that can hear the rogue. Enter a numeric value and select **At Least** or **At Most**. 

Table 105 *Wireless Properties Drop Down Menu*

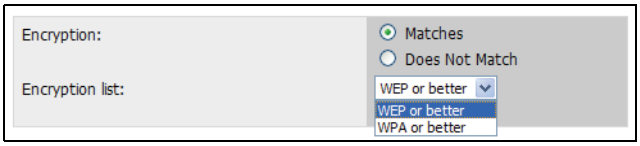
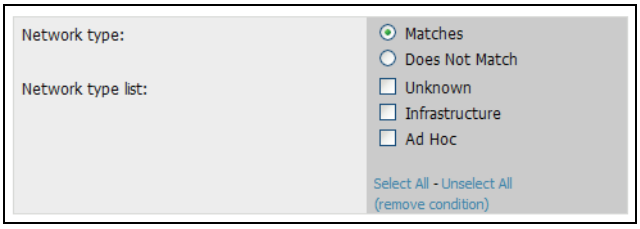
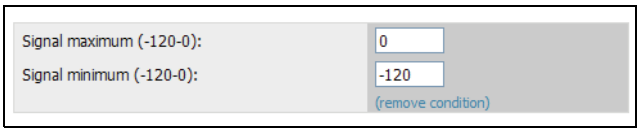
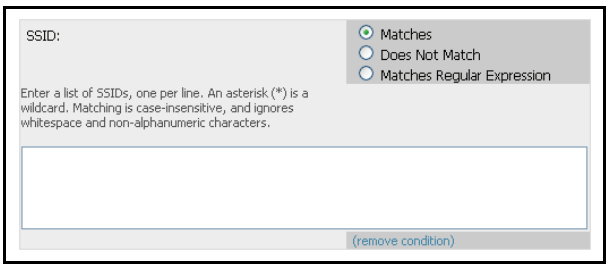
Option	Description
Encryption	Classifies based on the rogue matching a specified encryption method. 
Network type	Rogue is running on the selected network type, either **Ad-hoc** or **Infrastructure.** 
Signal Strength	Rogue matches signal strength parameters. Specify a minimum and maximum value in DBm. 
SSID	Classifies the rogue when it matches or does not match the specified string for the SSID or a specified regular expression.  **Note:** For SSID matching functions, OV3600 processes only alpha-numeric characters and the asterisk wildcard character (*****). OV3600 ignores all other non-alpha-numeric characters. For example, the string of **`ethersphere-*`** matches the SSID of **`ethersphere-wpa2`** but also the SSID of **`ethersphere_this_is_an_example`** (without any dashes).

Table 106 *Wireline Properties Drop Down Menu*

Option	Description
Detected on LAN	Rogue is detected on the wired network. Select **Yes** or **No**.

Table 106 *Wireline Properties Drop Down Menu*

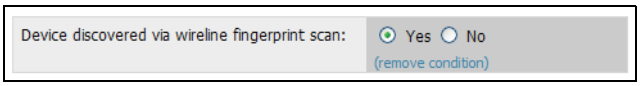
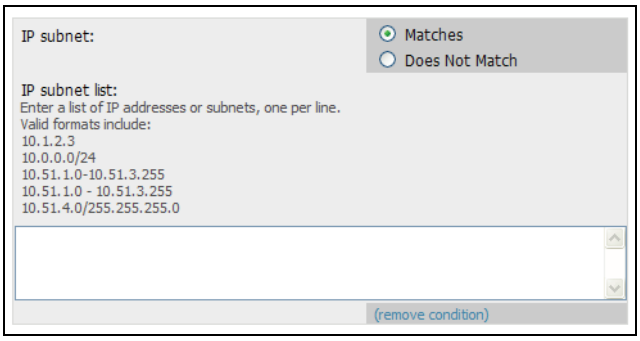
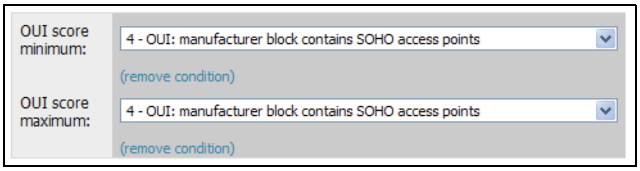
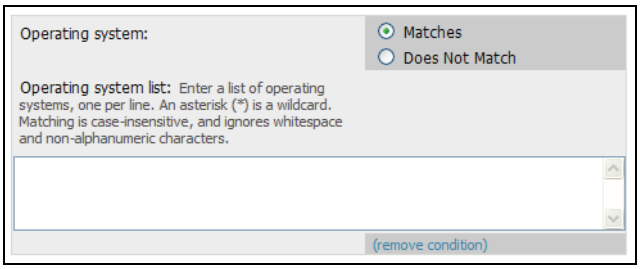
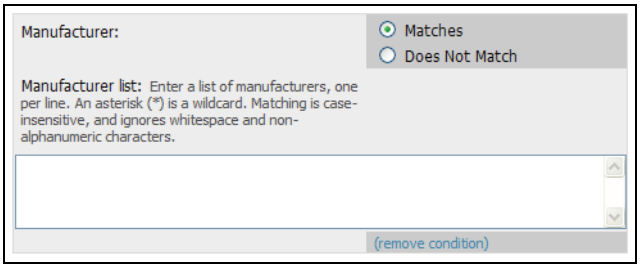
Option	Description
Fingerprint Scan	Rogue matches fingerprint parameters. 
IP Address	Rogue matches a specified IP address or subnet. Enter IP address or subnet information as explained by the fields. 
OUI Score	Rogue matches manufacturer OUI criteria. You can specify minimum and maximum OUI score settings from two drop-down lists. Click **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. 

Table 107 *Wires/Wireline Properties Drop Down Menu*

Option	Description
Manufacturer	Rogue matches the manufacturer information of the rogue device. 

After creating a new rule, click Add. This will return you to the **RAPIDS > Rules** page. Click Save and Apply to have the new rule take effect.

Deleting or Editing a Rules

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 click the **Delete** button. The rule is automatically deleted from the **RAPIDS > Rules** page.

To edit any existing rule, click the pencil icon next to that rule to launch the **RAPIDS Classification Rule** page (see Figure 137). Edit or revise the fields (see Table 106) as necessary then select the Save button.

To change the sequence in which rules apply to any rogue device, drag and drop the rule to a new position in the rules sequence.

Recommended RAPIDS Rules

If Any Device Has Your SSID, Then Classify as Rogue

The only devices broadcasting your corporate SSID should be devices that you are aware of and are managed by OV3600. Rogue devices often broadcast your official SSID in an attempt to get access to your users, or to trick your users into providing their authentication credentials. Devices with your SSID generally pose a severe threat. This rule helps to discover, flag, and emphasize such a device for prompt response on your part.

If Any Device Has Your SSID and is Not an Ad-Hoc Network Type, Then Classify as Rogue

This rule classifies a device as a rogue when the SSID for a given device is your SSID and is not an Ad-Hoc device. Windows XP automatically tries to create an Ad-hoc network if it can not find the SSID for which it is searching. This means that user's laptops on your network may appear as Ad-Hoc devices that are broadcasting your SSID. If this happens too frequently, you can restrict the rule to apply to non-ad-hoc devices.

If More Than Four APs Have Discovered a Device, Then Classify as Rogue

By default, OV3600 tries to use Signal Strength to determine if a device is on your premises. Hearing device count is another metric that can be used.

The important concept in this scenario is that legitimate neighboring devices are only heard by a few APs on the edge of your network. Devices that are heard by a large number of your APs are likely to be in the heart of your campus. This rule works best for scenarios in large campuses or that occupy an entire building. For additional rules that may help you in your specific network scenario, contact Alcatel Lucent Technical Support or see the *Alcatel Lucent Wireless Management Suite Knowledge Base*.

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.

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 138, Figure 139, and Table 108 illustrate and describe RAPIDS Score Override. Perform these steps to create a score override.

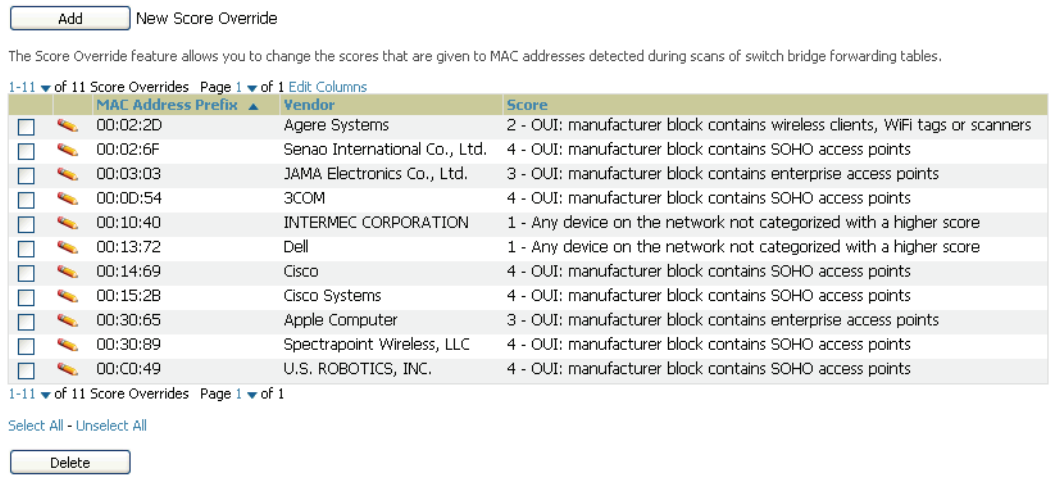
Once a new score is assigned, all devices with the specified MAC address prefix receive the new score.

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 138 ***RAPIDS > Score Override*** *Page*



2. Click **Add** to create a new override or click the pencil icon next to an existing override to edit that override. The **Score Override** add or edit page appears(Figure 139).

Figure 139 ***Add/Edit Score Override*** *Page*

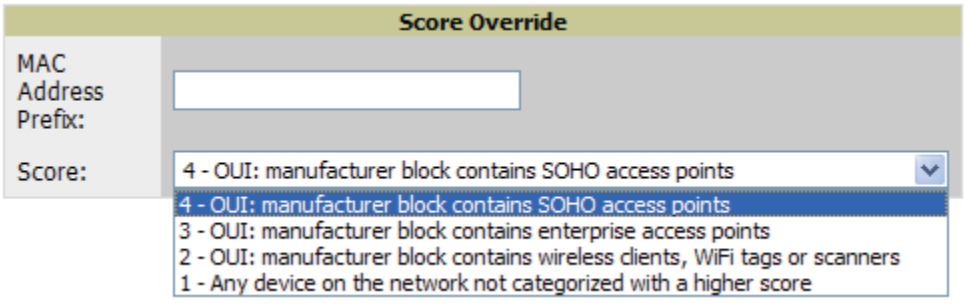


Table 108 ***RAPIDS > Add/Edit Score Override*** *Page Fields*

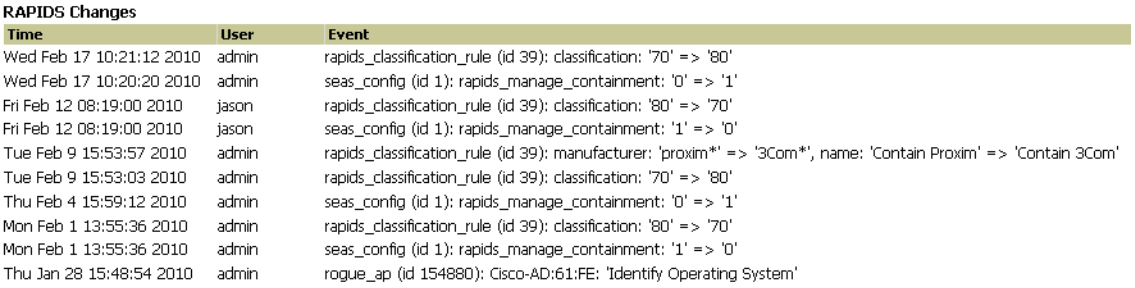
Field	Description
MAC Address Prefix	Use this field to define the OUI prefix to be re-scored.
Score	Use this field to set the score that a device, with the specified MAC address prefix, will receive.

3. Enter in the six-digit MAC prefix for which to define a score, and select the desired score. Once the new score has been saved, all detected devices with that prefix receive the new score.
4. Click **Add** to create the new override, or click **Save** to retain changes to an existing override. The new or revised override appears on the **RAPIDS > Score Override** page.
5. To remove any override, select that override in the checkbox and click **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 140 for more information.

Figure 140 *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 Rogue Device Resources

The following OV3600 tools support RAPIDS:

- **System Triggers and Alerts**—Triggers and Alerts that are associated with rogue devices follow the classification-based system described in this chapter. For additional information about triggers that support rogue device detection, see to "Creating and Using Triggers and Alerts" on page 224.
- **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 296.

Additional Security-Related Topics

For additional security-related features and functions, see the following topics in this guide.

- "Configuring Group Security Settings" on page 96
- "Configuring Group SSIDs and VLANs" on page 99
- "Creating and Using Triggers and Alerts" on page 224

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:

- "Creating and Using Triggers and Alerts" on page 224
- "Monitoring and Supporting WLAN Users" on page 238
- "Evaluating and Diagnosing User Status and Issues" on page 245
- "Supporting OV3600 Stations with the Master Console" on page 250
- "Monitoring and Supporting OV3600 with the Home Pages" on page 252
- "Monitoring and Supporting OV3600 with the System Pages" on page 260
- "Upgrading OV3600" on page 266
- "Backing Up OV3600" on page 267

Creating and Using Triggers and Alerts

This section describes triggers and alerts and contain the following topics:

- Overview of Triggers and Alerts
- Viewing Triggers
- Creating New Triggers
- Delivering Triggered Alerts
- Viewing Alerts
- Responding to Alerts

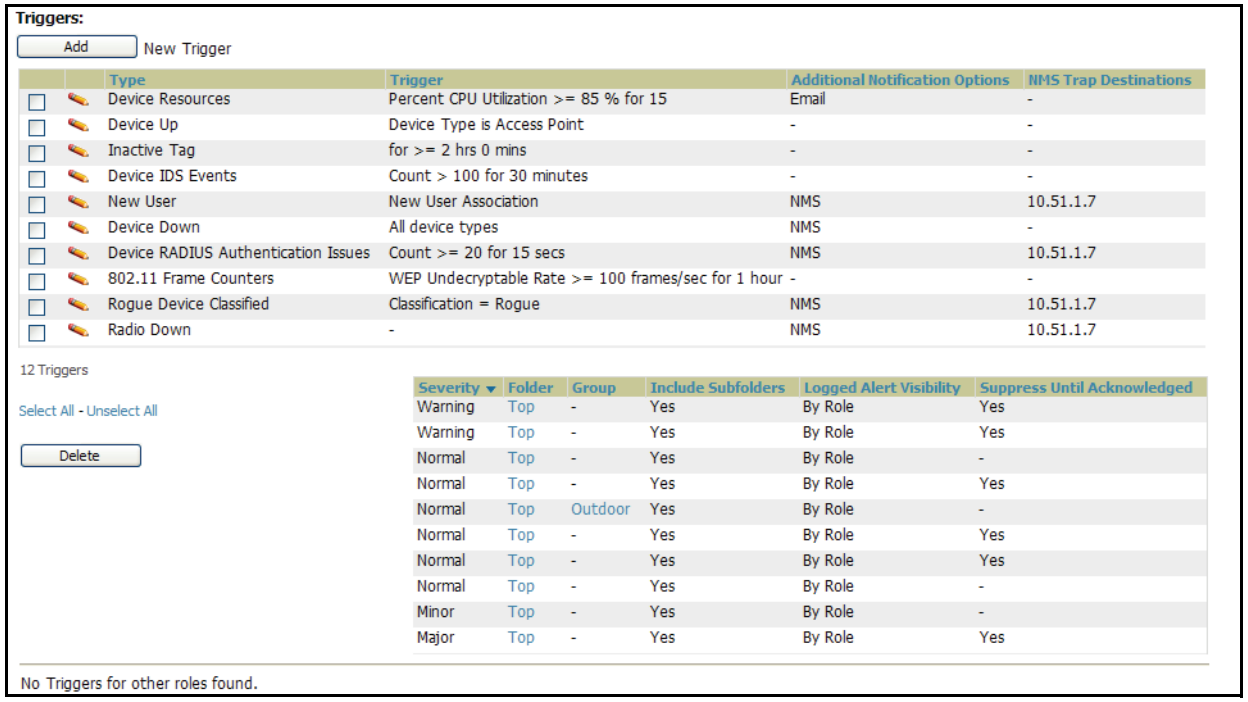
Overview of Triggers and Alerts

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. OV3600 deploys two types of alerts:

Viewing Triggers

To view defined system triggers, navigate to the **System > Triggers** page. Figure 141 illustrates this page.

Figure 141 ***System > Triggers*** *Page Illustration (Split View)*

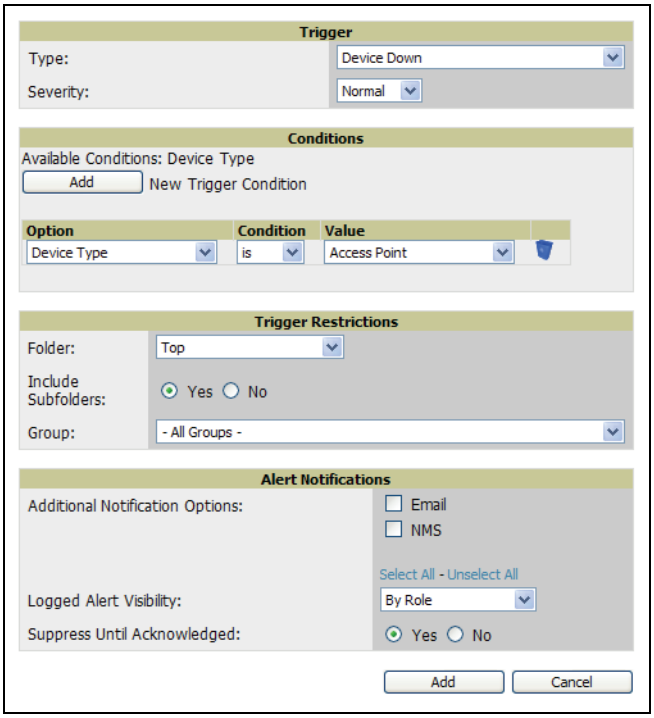


Creating New Triggers

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, click the **Add New Trigger** button from the **System > Triggers** page. OV3600 launches the **Trigger Detail** page, illustrated in Figure 142.

Figure 142 ***System*** > ***Trigger Detail*** *Page Illustration*



2. Configure the **Trigger Restrictions** and **Alert Notifications**. This configuration is consistent regardless of the trigger type to be defined.

   a. Configure the **Trigger Restrictions** settings. This establishes how widely or how narrowly the trigger applies. Define the folder, subfolder, and Group covered by this trigger. Table 109 describes the options for trigger restrictions.

Table 109 ***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. Configure the **Alert Notifications** settings. In addition to appearing on the **System > Triggers** page, triggers 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 provide the IP address of the **NMS Trap Destinations**.
      - 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.

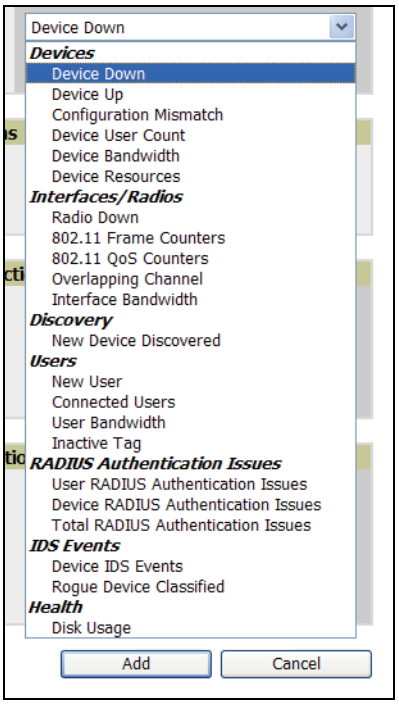
- The **Suppress Until Acknowledged** setting defines whether the trigger requires manual and administrative acknowledgement to gain visibility.

Table 110 ***System > Trigger Condition Detail Alert Notifications for Defined Alerts***

Notification Option	Description
Notification Type	Selects the action OV3600 should take when an alert is triggered. When the NMS checkbox is checked OV3600 sends an SNMP trap to the NMS servers defined for the role. When the **Email** checkbox is selected, OV3600 sends an email to the specified address.
Sender Address	Displays the originator's email address in the **From** field of alert emails. **NOTE:** This field is only visible if the **Email** checkbox is selected.
Recipient Email Addresses	Displays the user, users or distribution lists that receive any email alerts. **NOTE:** This field is only visible if the **Email** checkbox is selected.
Logged Alert Visibility	Defines which users are able to view the alerts. When limited by role only users with the same role as the creator of the alert will be able to view it. When limited by triggering agent, any user who can view the device can view the alert.
Suppress new alerts until current alerts are acknowledged/ deleted	Determines how often a trigger will fire. When No is selected a new alert will be created every time the trigger criteria are met. When Yes is selected an alert will only be received the first time the criteria is met. A new alert for the AP/device is not created until the initial one is acknowledged.

3. In the **Trigger** field, choose the desired trigger **Type** and the desired **Severity**, according to your needs. Figure 143 illustrates the trigger types supported in OV3600. Severity levels are included 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 143 ***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.

Complete the creation of your trigger type using one of the following procedures for each trigger:

- "Setting Triggers for Devices" on page 227

- "Setting Triggers for Radios" on page 228
- "Setting Triggers for Discovery" on page 230
- "Setting Triggers for Users" on page 231
- "Setting Triggers for RADIUS Authentication Issues" on page 233
- "Setting Triggers for IDS Events" on page 234
- "Setting Triggers for OV3600 Health" on page 235

Setting Triggers for Devices

After completing steps 1-3 in "Creating New Triggers" on page 224, perform the following steps to complete the configuration of device-related triggers.

a. If you have not already done so, choose a device type from the **Devices** listed in the **Type** drop-down menu. See Figure 143. Table 111 itemizes and describes device trigger options and condition settings.

Table 111 ***Devices*** *Trigger Types*

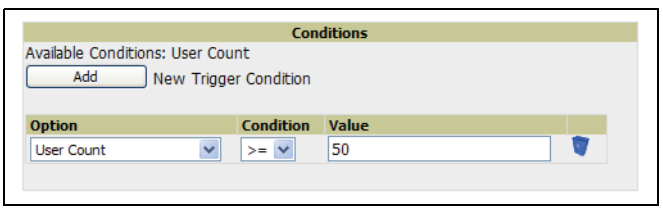
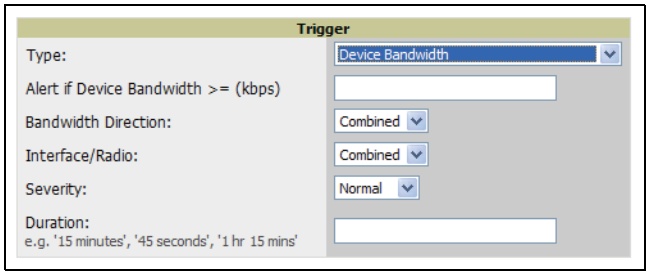
Devices Trigger Options	Description
Device Down	This is the default type whenever configuring a new trigger. This type of trigger activates when an authorized, managed AP has failed to respond to SNMP queries from OV3600. To set the conditions for this trigger type, click **Add** in the **Conditions** 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.
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, click **Add** in the **Conditions** section. Complete the conditions with the **Option**, **Condition**, and **Value** drop-down menus. The conditions establish the type that a device is or is not. Multiple conditions can apply to this type of trigger.
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, click **Add** in the **Conditions** section. Complete the conditions with the **Option**, **Condition**, and **Value** drop-down menus. The conditions establish the type that a device is or is not. The conditions establish the type that a device is or is not. Multiple conditions can apply to this type of trigger.
AP User Count	This trigger type activates when the user count on a given AP device reaches a specific threshold. The number of user devices associated to an AP has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 10 users associated for more than 60 seconds). Selecting **AP User Count** displays an additional **Duration** setting. Define the **Duration**, which can be expressed as hours, minutes, seconds, or a combination of these. Click the **Add New Trigger Condition** button to create one or more conditions for the **User Count** trigger. **Figure 144** *Sample of Trigger Condition for AP Device User Count* 

Table 111 ***Devices*** *Trigger Types*

Devices Trigger Options	Description
Device Bandwidth	This trigger type indicates that the total bandwidth through the AP has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 1500 kbps for more than 120 seconds). You can also select bandwidth direction and page/radio. Selecting **Device Bandwidth** as the trigger type displays the following new fields in the **Type** section. Define these settings. **Figure 145** ***Trigger Type*** *Section for* ***Device Bandwidth*** *Type*  • **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. • **Interface/Radio**—Choose either **First** or **Second**. • **Severity**—The Severity level is likely defined already from an earlier step in this procedure. See "Creating New Triggers" on page 224. • **Duration**—The Duration level is likely defined already from an earlier step in this procedure. See "Creating New Triggers" on page 224.
Device Resources	This type of trigger indicates that the CPU or memory utilization for a device has exceeded a defined a defined percentage for a specified period of time. Selecting the **Device Resources** trigger type displays a new **Duration** setting. Define the **Duration**, which can be expressed as hours, minutes, seconds, or a combination of these.

b. Delete conditions as desired by clicking the trash can icon to the right of the condition to be removed.

c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.

d. You can edit or delete any trigger as desired from the **System > Triggers** page.

   - To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in Table 111.
   - To delete a trigger, check the box next to the trigger to remove, and click **Delete**.

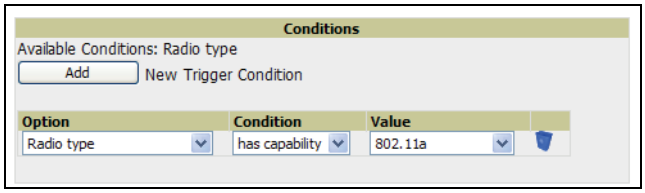
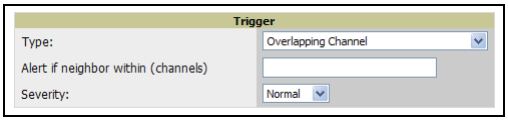
e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 224 to create a new trigger.

Setting Triggers for Radios

After completing steps 1-3 in "Creating New Triggers" on page 224, perform the following steps to complete the configuration of radio-related triggers.

a. If you have not already done so, choose a trigger type from the **Radios** category, listed in the **Type** drop-down menu. Table 112 itemizes and describes the Radios-related trigger types, and condition settings for each.

Table 112 *Radio-Related Trigger Types*

Radio Trigger Options	Description
Radio Down	This trigger indicates when a device's radio is down on the network. Once you choose this trigger type, click **Add New Trigger Condition** to create at least one condition. **The Radio Down** trigger requires that a radio capability be set as a condition. The **Value** drop-down menu supports several condition options. The following example illustrates a **Radio** trigger that has **802.11a** capability: **Figure 146** *Sample of Trigger Condition for Radio Type* 
802.11 Frame Counters	This trigger type enables monitoring of traffic levels. When **802.11 Frame Counters** is the trigger type, there are multiple rate-related parameters for which you define conditions. The rate of different parameters includes ACK Failures, Retry Rate and Rx Fragment Rate. See the drop-down **Field** menu in the Conditions section of the trigger page for a complete list of parameters. Click **Add New Trigger Condition** to access these settings. Define at least one condition for this trigger type. Selecting this trigger type displays a new **Duration** setting. Define the **Duration**, which can be expressed as hours, minutes, seconds, or a combination of these.
802.11 QoS Counters	This trigger type 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. Click **Add New Trigger Condition** to access these settings. Define at least one condition for this trigger type. Selecting this trigger type displays a new **Duration** setting. Define the **Duration**, which can be expressed as hours, minutes, seconds, or a combination of these.
Overlapping Channel	This type of trigger indicates that the neighboring AP is within a specified number of channels. This is calculated based on the AP with the most roams as reflected on the **APs/Devices > Manage** page, the **Neighbors** section. Selecting this trigger type displays a new option which you can enable as desired: **Alert if neighbor within channels**. **Figure 147** ***Trigger Type*** *Section for* ***Overlapping Channel*** *Type*  **NOTE:** There is no **Conditions** configuration for **Radios: Overlapping Channel** triggers.
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**.

b. Delete conditions as desired by clicking the trash can icon to the right of the condition to be removed.

c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.

d. You can edit or delete any trigger as desired from the **System > Triggers** page.

- To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in Table 111.
- To delete a trigger, check the box next to the trigger to remove, and click **Delete**.

e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 224 to create a new trigger.

Setting Triggers for Discovery

After completing steps 1-3 in "Creating New Triggers" on page 224, 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 143. Table 113 itemizes and describes the Discovery-related trigger types, and condition settings for each discovery trigger type.

Table 113 ***Discovery*** *Trigger Types and Condition Settings*

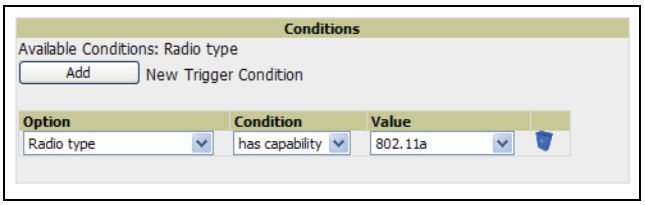
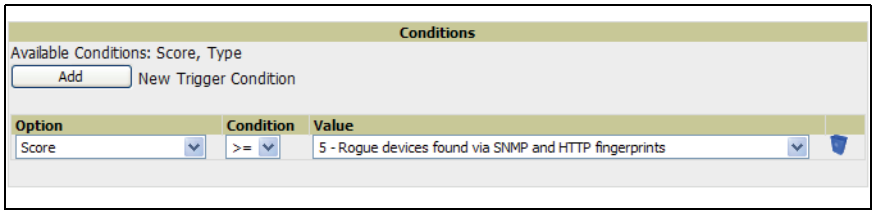
Discovery Trigger Options	Description
New Devices Discovered	This trigger type flags the discovery of a new and manageable AP connected to the network (an AP that OV3600 can monitor and configure). Once you choose this trigger type, click **Add New Trigger Condition** to specify a device type. The following example illustrates the **Add Condition** section for a **New Devices Discovered** trigger. **Figure 148** *Sample of Condition for* ***New Device Discovered*** *Trigger Type* 

Table 113 ***Discovery*** *Trigger Types and Condition Settings (Continued)*

Discovery Trigger Options	Description
New Rogue Device Detected	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 the **Yes** button. See "Using RAPIDS and Rogue Classification" on page 205 for more information on score definitions and discovery methods. Once you choose this trigger type, click **Add New Trigger Condition** to create one or more conditions. A condition for the **Rogue Detected** trigger enables you to specify the nature of the rogue device in multiple ways. • All menus change according to the setting you define in the **Options** drop-down menu. You can define the rogue trigger according to the device type or according to the rogue score, or both if you set two or more conditions. See the **Options** drop-down menu for these choices. • You can define the discovery of a rogue device according to whether it meets certain mathematical parameters, or whether it is or is not a specific device type. See the **Condition** drop-down menu for these options, and note that they change according to your choice in the Options drop-down menu. • You can define either the rogue score or the rogue device type in the **Value** drop-down menu, according to what you chose in the **Options** drop-down menu. **Figure 149** *Sample of Trigger Condition for A Rogue Detected Trigger* 

b. Delete conditions as desired by clicking the trash can icon to the right of the condition to be removed.

c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.

d. You can edit or delete any trigger as desired from the **System > Triggers** page.

   - To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in Table 111.
   - To delete a trigger, check the box next to the trigger to remove, and click **Delete**.

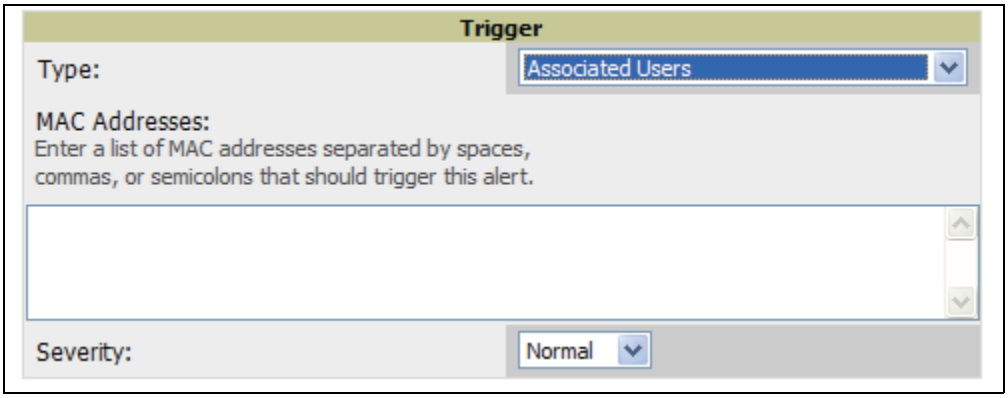
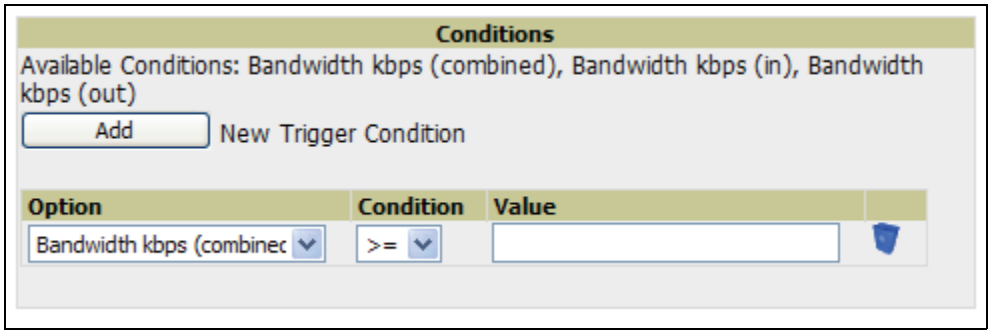
e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 224 to create a new trigger.

Setting Triggers for Users

After completing steps 1-3 in "Creating New Triggers" on page 224, 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 143. Table 114 itemizes and describes the User-related trigger types, and condition settings for each discovery trigger type.

Table 114 ***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.
Associated 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. **Figure 150** *Example of Associated User Configuration Section* 
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 1500 kbps for more than 120 seconds). Once you choose this trigger type, click **Add New Trigger Condition** to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger. The **Option** drop-down menu provides these options: • Bandwidth kbps (Combined) • Bandwidth kbps (in) • Bandwidth kbps (out) The **Condition** drop-down menu provides these options: • **=** — Bandwidth count equals... • **>** — Bandwidth count is greater than... • **<** — Bandwidth count is less than... • **> =** — Bandwidth count is greater than or equal to... • **< =** — Bandwidth count is less than or equal to... The **Value** field requires that you input a numerical figure for kilobits per second (kbps). **Figure 151** *Sample of* ***User Bandwidth*** *Trigger Condition* 
Inactive Tag	This tags flags events in which an RFID tag has not been reported back to OV3600 by a controller for more than a certain number of hours. This trigger can be used to help identify inventory that might be lost or stolen. Set the time duration for this trigger type if not already completed.

b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.

c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.

d. You can edit or delete any trigger as desired from the **System > Triggers** page.

- To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in Table 111.
- To delete a trigger, check the box next to the trigger to remove, and click **Delete**.

e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 224 to create a new trigger.

Setting Triggers for RADIUS Authentication Issues

NOTE

OV3600 first checks its own database prior to checking the RADIUS server database.

After completing steps 1-3 in "Creating New Triggers" on page 224, 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. See Figure 143. Table 115 itemizes and describes the condition settings for each **RADIUS Authentication** trigger type.

Figure 152 ***RADIUS Authentication*** *Trigger Condition Settings*

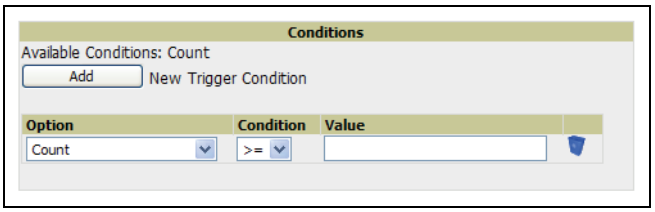


Table 115 ***RADIUS Authentication*** *Trigger Types and Condition Settings*

RADIUS Trigger Options	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. Click **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 device 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. The **Option**, **Condition**, and **Value** fields allow you to define the numeric value of device and user issues combined.

b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.

c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.

d. You can edit or delete any trigger as desired from the **System > Triggers** page.
   - To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in Table 111.
   - To delete a trigger, check the box next to the trigger to remove, and click **Delete**.

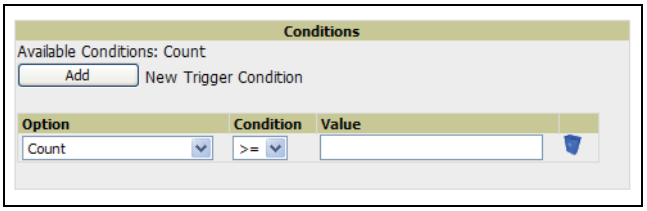
e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 224 to create a new trigger.

Setting Triggers for IDS Events

After completing steps 1-3 in "Creating New Triggers" on page 224, 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 143. Table 116 describes condition settings for this trigger type.

Table 116 ***Device IDS Events Authentication*** *Trigger Types and Condition Settings*

IDS Trigger Options	Description
Device IDS Events	This trigger type is based on twww.www.cnn.com he number of IDS events has exceeded the threshold specified as Count in the Condition within the period of time specified in seconds in Duration. Click **Add New Trigger Condition** to specify the count characteristics that trigger an IDS alert. The **Option**, **Condition**, and **Value** fields allow you to define the numeric count of device IDS thresholds. **Figure 153** ***IDS Events*** *Trigger Condition Settings* 

b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.

c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.

d. You can edit or delete any trigger as desired from the **System > Triggers** page.
   - To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in Table 111.
   - To delete a trigger, check the box next to the trigger to remove, and click **Delete**.

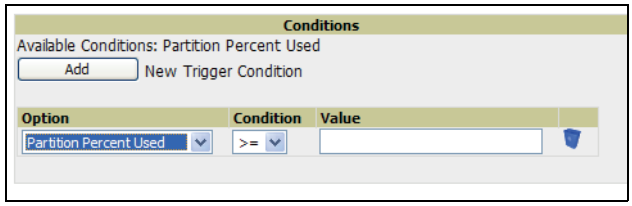
e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 224 to create a new trigger.

Setting Triggers for OV3600 Health

After completing steps 1-3 in "Creating New Triggers" on page 224, 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 143 for trigger types. Table 117 describes the condition settings for this trigger type.

Table 117 ***Disk Usage*** *Trigger and Condition Settings*

OV3600 Health Trigger	Description
Disk Usage	This trigger type is based on the disk usage of the OV3600 (OV3600) system. This type of trigger indicates that disk usage for the OV3600 server has met or surpassed a defined threshold. Click **Add New Trigger Condition** to specify the disk usage characteristics that trigger an alert. The **Option**, **Condition**, and **Value** fields allow you to define the numeric count of partition percent used. **Figure 154** *Condition Settings for* ***Disk Usage*** *Trigger* 

b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.

c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.

d. You can edit or delete any trigger as desired from the **System > Triggers** page.

- To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in Table 111.
- To delete a trigger, check the box next to the trigger to remove, and click **Delete**.

e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 224 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.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: <press enter>
```

4. 4. Check the mail log to ensure mail was sent

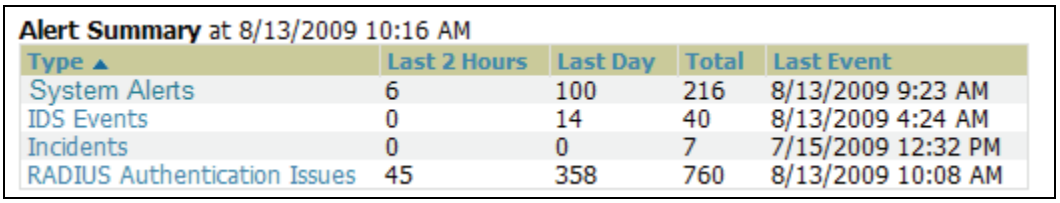
```
tail -f /var/log/maillog
```

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 155:
   - **APs/Devices > List**
   - **Groups > Monitor**
   - **Home > Overview**
   - **Users > Connected**
   - **Users > User Detail**

Figure 155 *Alert Summary Table Illustration*



Alert Summary at 8/13/2009 10:16 AM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
System Alerts	6	100	216	8/13/2009 9:23 AM
IDS Events	0	14	40	8/13/2009 4:24 AM
Incidents	0	0	7	7/15/2009 12:32 PM
RADIUS Authentication Issues	45	358	760	8/13/2009 10:08 AM

This table displays alerts as follows; click 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.
- **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 an AP. The incidents are based on the Top folder on the **Groups > Monitor** page and on the **Home > Overview** page. Incidents that are not related to devices in that folder are not counted in this **Alert Summary**.

To view all incidents, including those not associated to an AP, navigate to the **Helpdesk > Incidents** page.

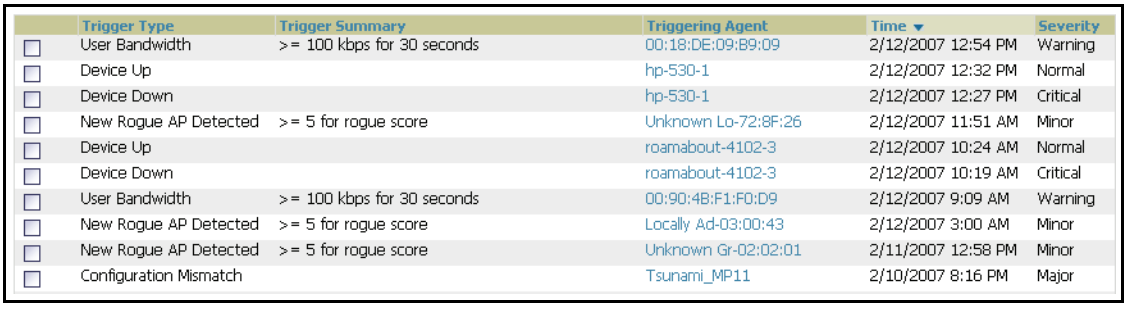
- **RADIUS Authentication Issues**—Displays RADIUS-related alerts for devices in the top viewable folder available to the OV3600 user. The detailed list displays the MAC address, username, AP, radio, controller, RADIUS server, and time of each event. Alerts can be sorted by any column.

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 156.

Figure 156 *Alerts in the OV3600 Status Bar*

Click the **Alerts** or the **Severe Alerts** counter or navigate to the **System > Alerts** page. Figure 157 illustrates this page.

Figure 157 *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
☐	User Bandwidth	>= 100 kbps for 30 seconds	00:90:4B:F1:F0:D9	2/12/2007 9:09 AM	Warning
☐	New Rogue AP Detected	>= 5 for rogue score	Locally Ad-03:00:43	2/12/2007 3:00 AM	Minor
☐	New Rogue AP Detected	>= 5 for rogue score	Unknown Gr-02:02:01	2/11/2007 12:58 PM	Minor
☐	Configuration Mismatch		Tsunami_MP11	2/10/2007 8:16 PM	Major

For each new alert, the **System > Alerts** page displays the items listed in Table 118.

Table 118 *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. Clicking the AP name to display the **APs/Devices > Manage** page for that AP.
Time	Displays the date and time the trigger was generated.
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. For example, if device AP 7 exceeds a maximum bandwidth trigger, that trigger does not create another alert for AP 7 until the first alert is recognized.
- Move the alert to the Alert Log by selecting the alert and clicking the **Acknowledge** button at the bottom of the page.
- You may see all logged alerts by clicking the **View logged alerts** link at the top of the **System > Alerts** page. Click the **New Alerts** link to return to the list of new alerts.
- Delete the alert by selecting the alert from the list and clicking the **Delete** button at the bottom of the **System > Alerts** page.

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 Users on Thin AP Networks 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 the following sections in this guide:

- 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 241.

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. For additional information, refer to "Monitoring WLAN Users With the Users > Connected and Users > All Pages" on page 239.
- **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 239.
- **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 241.
- **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 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 245.
- **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 245.
- **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. OV3600 displays the information it receives from the controller in a table on this page. "Supporting Users on Thin AP Networks With the Users > Tags Page" on page 244.

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 158 and described in Table 119. The information displayed on this page can be adjusted in the following ways:

- You can expand or customize the graphics to show maximum users, maximum average users, and additional custom view options.
- You can expand bandwidth to include custom view options.
- You can display all users, a specific number of users per page, or another custom setting.
- The Alerts section displays custom configured alerts that were defined in the **System > Alerts** page.

OV3600 enhances the **Users > Connection** page to include SSID information for users. This enhancement applies to additional graph-based pages in OV3600. Furthermore, the **Users > Connected** page can display wired users using remote Access Point (RAP) devices in tunnel and split-tunnel mode.

Data that was gathered prior to an upgrade may be reported under an **unknown** SSID.

Figure 158 ***Users > Connected*** *Page Illustration*

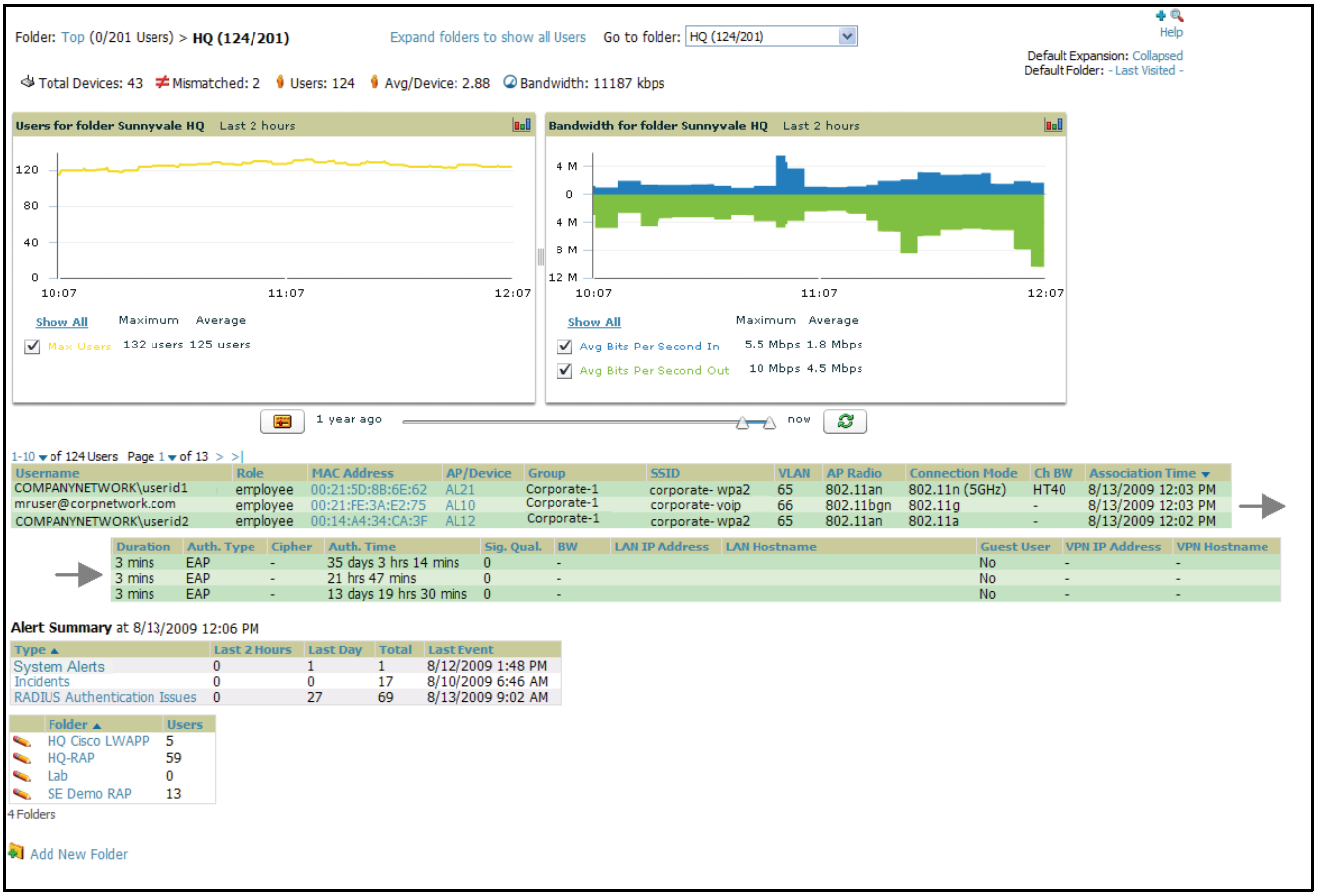


Table 119 ***Users > Connected*** *Fields and Default Values*

Field	Description
Username	Displays 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, traps from Cisco VxWorks APs and tables on Colubris APs. 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 (as indicated if you mouse over the username) 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 radio MAC address of the user associated to the AP. Also displays a link that redirects to the **Users > Detail** page.
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 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.
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.

Table 119 ***Users > Connected*** *Fields and Default Values (Continued)*

Field	Description
Ch BW	Displays the channel bandwidth that currently supports the user.
User Radio Mode	Displays the Radio mode used by the user to associate to the AP. It will display 802.11a/b/g/bg. 802.11bg is reported when the AP does not provide OV3600 with enough information to determine the exact radio type.
Association Time	Displays the first time OV3600 recorded the MAC address as being associated.
Duration	Displays the length of time the MAC address has been associated.
Auth. Type	Displays the type of authentication employed by the user: EAP, PPTP, RADIUS accounting, or not authenticated. • EAP is only reported by Cisco VxWorks via SNMP traps. • PPTP is supported by Colubris APs acting as VPNs. • RADIUS accounting servers integrated with OV3600 will provide the RADIUS Accounting Auth type. • All others are considered to be not authenticated.
Cipher	Displays WEP with keys. Cipher options are as follows: • WEP with 802.11x • WPA PSK (TKIP) • WPA with 802.11x • WPA2 PSK (AES) • WPA2 with 802.11x (AES) This data is also displayed in the **User Session** report.
Auth. Time	Displays the how long ago the user authenticated.
Signal Quality	Displays the average signal quality the user enjoyed.
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 association table of Colubris APs or from the ARP cache of switches set up in OV3600.
LAN Hostname	Displays the LAN hostname of the user MAC.
Guest User	Specifies whether the user is a guest or not.
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.
VPN Hostname	Displays the VPN hostname of the user MAC.

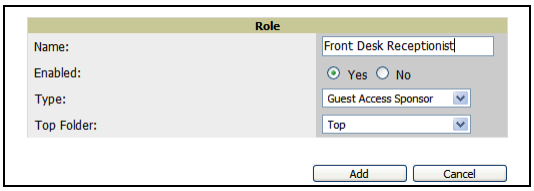
Supporting Guest WLAN Users With the Users > Guest Users Page

OV3600 supports guest user provisioning for Aruba/Alcatel-Lucent and Cisco WLC devices. This allows frontline staff, such as receptionists or help desk technicians, to grant wireless access to WLAN visitors or other temporary personnel.

The first step in creating a guest access user on the WLAN is to define a role for the OV3600 users who will be responsible for associated tasks, if those users are to have a role other than Admin. Perform the following steps in the pages described to configure these settings.

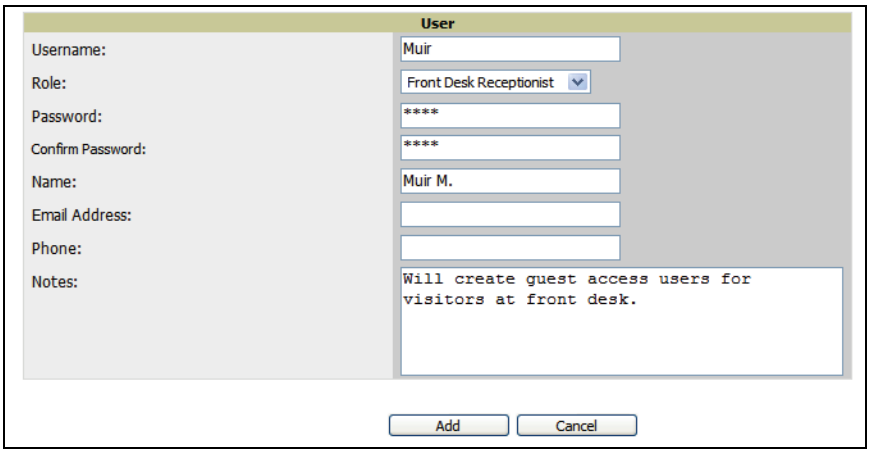
1. Navigate to the **OV3600 Setup > Roles** page and create a new role of the type **Guest Access Sponsor**. Click **Add New Role**, select this role type, and enter a role name. Also, select the top folder for which this role should have access. Figure 159 illustrates this page.

Figure 159 ***OV3600 Setup > Roles*** *Page Illustration*



2. Next, navigate to the **OV3600 Setup > Users** page and create a new user with the role that was just created for **Guest Access Sponsors**. Figure 160 illustrates this page.

Figure 160 ***OV3600 Setup > Users*** *Page Illustration*



3. The newly created login information should be provided to the person or people who will be responsible for creating guest access users. Anyone with an Admin role can also create 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 161 illustrates this page and Table 120 describes the fields and information displayed.

Figure 161 ***Users > Guest Users*** *Page Illustration*

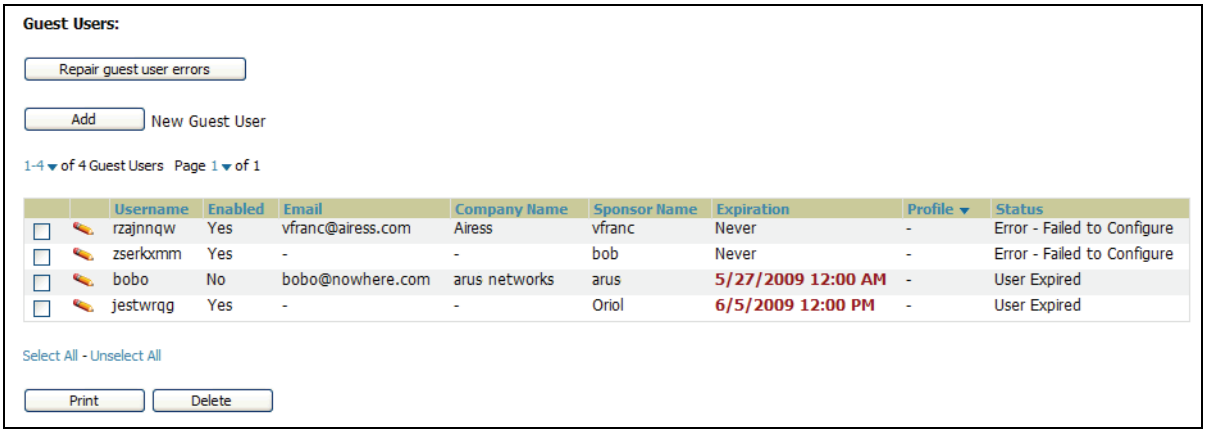


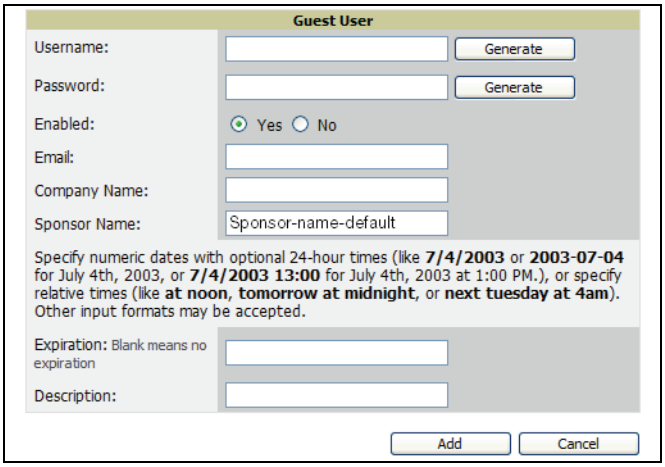
Table 120 ***Users > Guest Users*** *Fields*

Field	Description
Repair Guest User Errors button	Sets OV3600 to attempt to push the guest user again in an attempt to repair any errors in the **Status** column.
Add New Guest Users button	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). Configure the user on the **Guest User** edit page by clicking the pencil icon.
Email	Displays the optional email address of the user. Set the email address with the **Guest User** edit page by clicking the pencil icon.
Company Name	Displays the optional company name for the user. Set the company name with the **Guest User** edit page by clicking the pencil icon.
Sponsor Name	Displays the name of the sponsor for the guest user. This setting is optional. Set the sponsor with the **Guest User** edit page by clicking the pencil icon.
Expiration	Displays the date the guest user's access is to expire. Set the expiration with the **Guest User** edit page by clicking the pencil icon.
Profile/SSID	Sets the SSID that the guest user can access. This setting applies to Cisco WLC only. Set the SSID with the **Guest User** edit page by clicking the pencil icon.
Status	Reports current status by the controller. If error messages appear in this column, select the user with the checkbox at left, and click the **Repair guest user errors** button.
Print button (for checked users)	Sends the selected guest user's information to an external printer.
Delete button (for checked users)	Removes the selected guest user from OV3600 and from the controller.

Guest users associated to the wireless network appear on the same list as other wireless users, but are identified as guest users in the **SSID** column, when this column is present for Cisco WLC. 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, click **Add**, and complete the required and optional fields in the **User Detail** page, illustrated in Figure 162. Table 120 describes most fields. The first three fields are required, and the remaining fields are optional.

Figure 162 ***Users > Guest Users > Add New Guest User*** *Page Illustration*



To make the **Username** or **Password** anonymous and to increase security, complete these fields then click **Generate**. The anonymous and secure **Username** and **Password** appear in the respective fields.

6. Click **Add** to complete the new guest user, or click **Cancel** to back out of new user creation. The **Users > Guest Users** page appears and displays results, as applicable.

Supporting Users on Thin AP Networks 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 163 illustrates this page, and Table 121 describes fields and information displayed.

Figure 163 ***Users > Tags*** *Page Illustration*

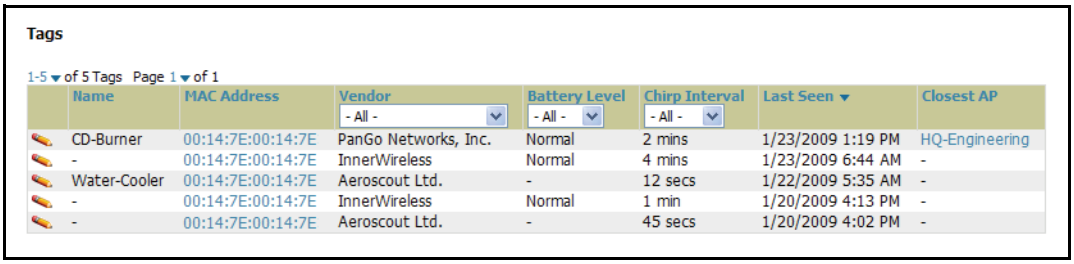


Table 121 ***Users > Tags*** *Fields*

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.

Table 121 ***Users > Tags*** *Fields*

Field	Description
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, click 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 "Creating and Using Triggers and Alerts" on page 224.

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 sub-menu that becomes visible when you select a specific user. Access the **Users > User Detail** page in one of the following ways:

- Click the MAC Address for a specific user from one of the following pages:
  - **Users > Connected**
  - **Users > All**
- Search for a user and click the associated MAC address in the search results, then select the **User Detail** page from the navigation pane.

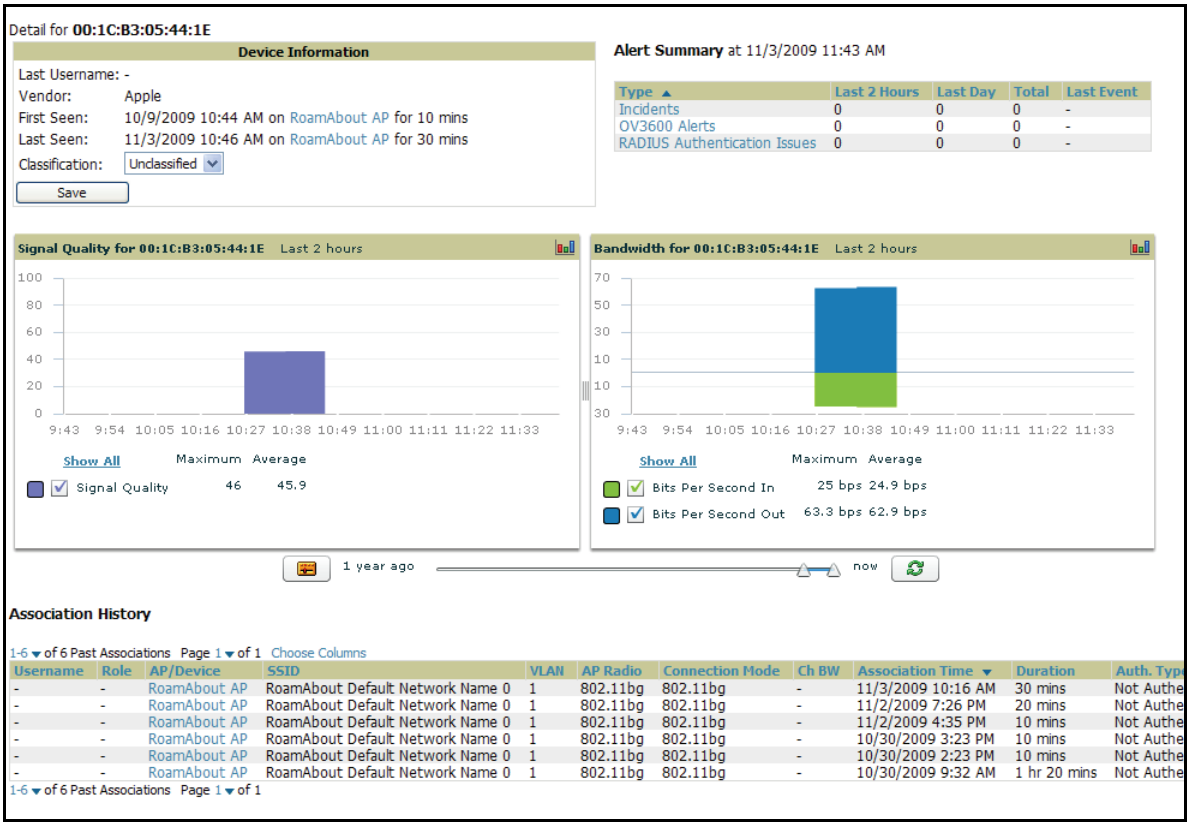
Figure 164 illustrates the contents of **Users > User Details** page.

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 WLAN 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 WLAN switches that govern the devices. The classifications are as follows:

- **Unclassified**—Devices are unclassified by default.
- **Valid**—Designates the device as a legitimate network device. Once this **Valid** setting is pushed to the WLAN switch, and if the **Protect Valid Stations** option is also enabled on the switch, then this setting prevents valid stations from connecting to a non-valid AP.
- **Contained**—Controls the user on the device, as defined with containment configurations set with WMS Offload in AOS.

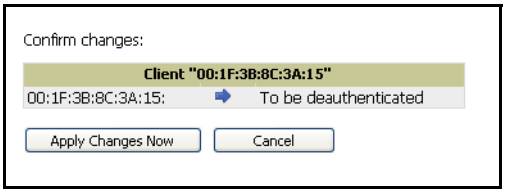
Figure 164 *Users > User Detail Page Illustration*



Using the Deauthenticate User Feature

Some displays of the **User > User Detail** page includes the **Deauthenticate User** feature in the **Current Association** field. Click the **Deauthenticate User** button to use this feature. Refer to Figure 165 as an illustration:

Figure 165 *Users > User Detail > Deauthenticate User Page:*



Evaluating User Status with the Users > Diagnostics Page

Introduction and Overview of the Diagnostics Page

The **Users > Diagnostics** page is a focused sub-menu that becomes visible when you select user-specific information. Access the **Users > Diagnostics** page in one of the following ways:

- Click the MAC Address for a specific user from one of the following pages:
  - **Users > Connected**
  - **Users > All**
- You can search for a user and click 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 122 for explanation and illustration of page components.

Table 122 ***Users > Diagnostics*** *Page Sections*

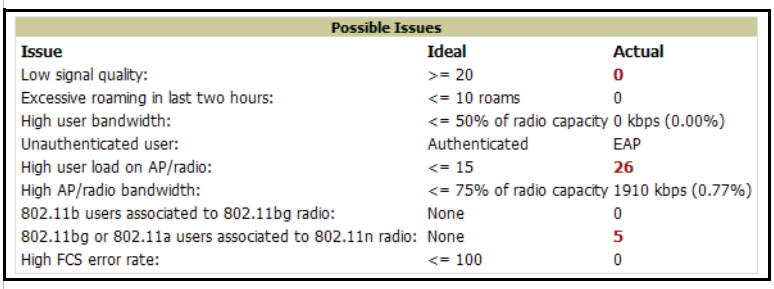
Section	Description
Possible Issues	This section summarizes the most likely items to create issues for a user on the network. Figure 166 illustrates this section. **Figure 166** ***Groups > Diagnostics > Possible Issues*** *Illustration*  • **Low signal quality**—If signal quality falls outside of ideal range, then possible resolution might be installation of 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. • **Excessive roaming in last 2 hours**—Roaming means that a user's connection moves from one AP to another. Excessive roaming is generally classified as 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. In this case, adjusting the signal strength for one of those APs may resolve the issue. • **High User Bandwidth**—If a user reports issues with network performance, the issue could derive from excessive bandwidth consumption. Additionally, another user on the same AP might be consuming excessive bandwidth. In that latter case, investigate user bandwidth consumption for all users on a given AP, not strictly the user who reports an issue. • **Unauthenticated User**—This section conveys the user's current authentication status and the actual authentication type. If a network deploys RADIUS authentication, then the RADIUS server could be experiencing issues even if a user attempts to log in with valid authentication credentials but shows as **Unauthenticated** on this page. • **High user load on AP/radio**—This field indicates if 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. Some users will start to experience performance issues, may start to drop off, You may need to add an additional AP in that area, or take other steps to distribute the user load more evenly across multiple APs. Refer to the **Current User Counts** section on this page for additional details. • **High AP radio bandwidth**—This figure derives from how groups of users share radio bandwidth on a shared AP. You may get a high figure in this category if nearby APs have gone down. 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. • **802.11** radio parameters—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.

Table 122 ***Users > Diagnostics*** *Page Sections*

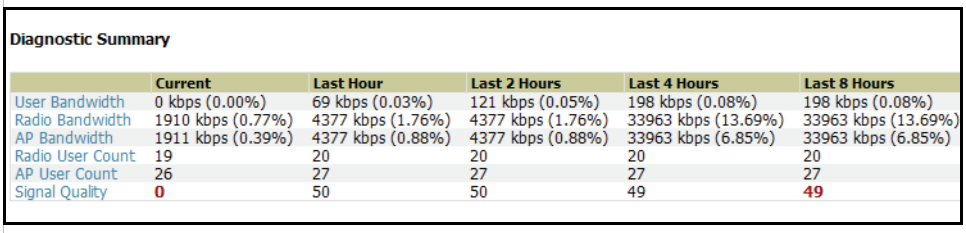
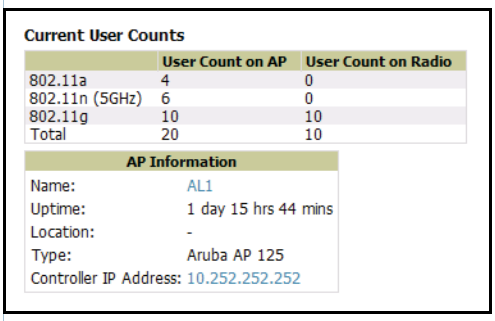
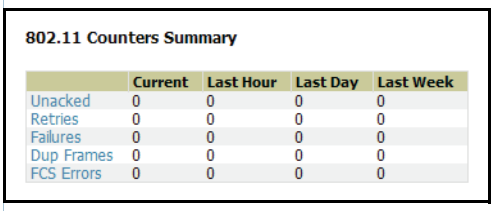
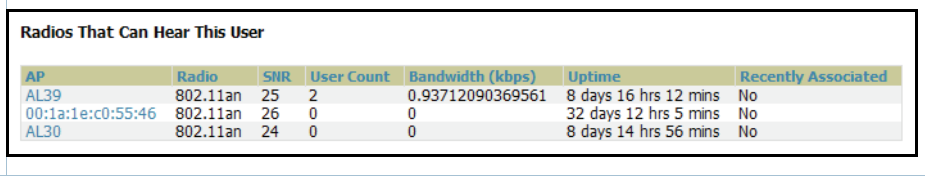
Section	Description
Possible Issues (Cont'd)	• **High FCS error rates**—Frame Check Sequence (FCS) errors indicate that frames of data that transmit across the network are experiencing corruption. A high FCS error rate indicates wireless link interference in the area. Frames that are transmitted by APs managed in OV3600 are susceptible to interference from other devices with radios operating in the same frequencies range (same channel), or electromagnetic interference from electronic devices such as power cables in the office. The 802.11 MAC layer uses the Frame Check Sequence (FCS) field to determine if errors have occurred during the transmission. Each MAC layer frame has a FCS field that is used to store a checksum. The checksum is added at the source AP, and verified at the destination. If the FCS checksum included in the frame does not match the recalculated number, then an error has occurred during the transmission, the frame is discarded, and the destination host requests it to be resent. This can effectively reduce the bandwidth and throughput in the network. A high FCS error rate in this field could indicate that the APs are experiencing a high level of link interference and the clients are getting less bandwidth and throughput due to MAC layer frame retransmissions. One response is to assign a different channel to the AP to improve the performance from your OV3600 server. Use the Optimize feature to assign the best available channel to the AP. 1. Log in to your OV3600. 2. From the **AP/Devices > List** page, click the **Modify Devices** link. 3. Select the APs that are running into channel interference problems by checking the corresponding box for each. Several new settings appear below the device list by which to configure these devices. 4. Toward the bottom of this section, click **Optimize** for the **Optimize channel assignment to reduce overlap** setting. A **confirm changes** page appears by which to apply and schedule this change, or to cancel out of this setting. **NOTE:** This explanation derived from the following location: • *Airheads Online Forum*, explanation by bjacobs: http://airheads.arubanetworks.com/vBulletin/showthread.php?p=1266#post1266
Diagnostics Summary	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 167 illustrates this section. **Figure 167** ***Users > Diagnostics > Diagnostics Summary*** *Illustration (Partial Display)*  Diagnostic Summary Current / Last Hour / Last 2 Hours / Last 4 Hours / Last 8 Hours User Bandwidth: 0 kbps (0.00%) / 69 kbps (0.03%) / 121 kbps (0.05%) / 198 kbps (0.08%) / 198 kbps (0.08%) Radio Bandwidth: 1910 kbps (0.77%) / 4377 kbps (1.76%) / 4377 kbps (1.76%) / 33963 kbps (13.69%) / 33963 kbps (13.69%) AP Bandwidth: 1911 kbps (0.39%) / 4377 kbps (0.88%) / 4377 kbps (0.88%) / 33963 kbps (6.85%) / 33963 kbps (6.85%) Radio User Count: 19 / 20 / 20 / 20 / 20 AP User Count: 26 / 27 / 27 / 27 / 27 Signal Quality: 0 / 50 / 50 / 49 / 49 The following categories link to additional details pages: • **User Bandwidth**—click this link to display flash graphs for user bandwidth metrics. • **Radio Bandwidth**—click this link to display flash graphs for radio bandwidth consumption. • **AP Bandwidth**—click this link to display flash graphs for AP bandwidth consumption. • **Radio User Count**—click this link to display flash graphs for user count metrics. • **AP User Count**—click this link to display flash graphs for user count metrics. • **Signal Quality**—click this link to display flash graphs for signal quality.

Table 122 ***Users > Diagnostics*** *Page Sections*

Section	Description
Current User Counts	The **Current User Counts** section displays user counts for APs and radios, and includes additional summary information for APs. Figure 168 illustrates this section: **Figure 168** ***Users > Diagnostics > Current User Counts*** *Illustration*  Current User Counts User Count on AP / User Count on Radio 802.11a 4 0 802.11n (5GHz) 6 0 802.11g 10 10 Total 20 10 AP Information Name: AL1 Uptime: 1 day 15 hrs 44 mins Location: - Type: Aruba AP 125 Controller IP Address: 10.252.252.252 Use this section in combination with the **Possible Issues** section.
802.11 Counters Summary	The **802.11 Counters Summary** section conveys the same information that is available from the **Radio Statistics** link from the **APs/Devices > Monitor** page. Figure 169 illustrates this section. **Figure 169** ***Users > Diagnostics > 802.1 Counters Summary*** *Illustration*  802.11 Counters Summary Current / Last Hour / Last Day / Last Week Unacked 0 0 0 0 Retries 0 0 0 0 Failures 0 0 0 0 Dup Frames 0 0 0 0 FCS Errors 0 0 0 0 **NOTE:** This section is supported for Cisco devices. OV3600 does not gather device counter information from certain other device vendors. For additional information, click a Cisco device from the **APs/Devices > List** page, and on the **Monitor** page for that device, click **Statistics**. The ensuing page displays the **802.11 Counters Summary** table, which summarizes counters on the AP level. Scroll down on this page to convey additional information from which the counters summary on the **Diagnostics** page is derived. Some of the sections on the **Statistics** page only populate when there is a user when an associated user is generating traffic on the network. Other sections convey information if there is no user associated and the device is strictly listening for traffic.
Radios That Can Hear This User	The **Radios That Can Hear This User** section summarizes the AP correspondence to Radios, with SNR values, user count metrics, bandwidth consumption and additional information that collectively describe the user's device-level activity on the network. Figure 170 illustrates this section. **Figure 170** ***Users > Diagnostics > Radios That Can Hear This User*** *Illustration*  Radios That Can Hear This User AP / Radio / SNR / User Count / Bandwidth (kbps) / Uptime / Recently Associated AL39 802.11an 25 2 0.93712090369561 8 days 16 hrs 12 mins No 00:1a:1e:c0:55:46 802.11an 26 0 0 32 days 12 hrs 5 mins No AL30 802.11an 24 0 0 8 days 14 hrs 56 mins No

Supporting OV3600 Stations 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.

- Reports can be run from the **Master Console** to display information from multiple OV3600 stations; because such reports can be extremely large, reports can also be run as **summary only** so that they generate more quickly and finish as a manageable file size.
- The **Master Console** can also be used to populate group-level configuration on managed OV3600 installations using the **Global Groups** feature.
- The **Master Console** supports:
  - 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, to include **Home > Overview**, **APs Devices > List**, **RAPIDS > Rogue APs**, and additional such pages.
  - The **Public Portal** of the **Master Console** supports configuration of the iPhone interface. This can be configured using the **Master Console OV3600** page. See "Defining General OV3600 Server Settings" on page 38.
  - The **Master Console** and **Failover** servers can be configured with a **Device Down** trigger that generates an alert if communication is lost to a managed or watched OV3600 station. In addition to generating an alert, the **Master Console** or **Failover** server can also send email or NMS notifications about the event. See "Creating and Using Triggers and Alerts" on page 224.

The license key determines if the server will behave as a **Master Console** or as a standard OV3600 server.

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. It can be enabled by navigating to the **OV3600 Setup > General** and then to the **Master Console** section. Once enabled, a new Portal tab will appear to the right of the **Groups** tab. The URL of the public portal will be https://your.OV3600.name/public. When you upgrade to OV3600 7.0, the public portal is disabled by default, regardless of the type of license.

Much like the normal **Home > Overview** page, the **Master Console Home > Overview** page provides summary statistics for the entire network at a glance.

Adding a Managed OV3600 with the Master Console

Perform the following steps to add a managed OV3600 console.

1. Navigate to the **Home > Managed OV3600** page.
2. Click the **Pencil Icon** to edit or reconfigure an existing OV3600 console.
3. Click the **Add New Managed OV3600** button to create a new OV3600 console. The **Managed OV3600** page appears. Complete the settings on this page as described in Table 123.

Table 123 ***Master Console > Manage OV3600 > IP/Hostname*** *Fields and Default Values*

Field	Default	Description
Hostname / IP Address	N/A	Enter the IP address or Hostname of the OV3600 server that will be managed.
Polling Enabled	Yes	Enables or disables the Master Console polling of managed OV3600 server.
Polling Period	5 minutes	Determines how frequently the Master Console polls the managed OV3600 server.

Table 123 ***Master Console > Manage OV3600 > IP/Hostname*** *Fields and Default Values (Continued)*

Field	Default	Description
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.

4. To push configurations to managed groups using OV3600' global groups feature, first navigate to the Master Console's **Groups > List** page.
5. Click the **Add** button to add a new group, or click the name of the group to edit settings for an existing group.
6. Click 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).
7. Clicking the name of an existing group on the **Master Console** loads the subtabs for **Basic, Security, SSIDs, AAA Servers, Radio, WLC Radio, LWAPP APs, PTMP/WiMAX, 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 copied and pasted into the Master Console global group.

When a global group is pushed from the **Master Console** to subscriber groups on managed OV3600s, all settings will be static except for settings with the 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** page, override options are available only on the **Add** page (navigate to the **Groups > SSIDs** page and click the **Add** button).

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. 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.

To configure subscriber groups, navigate to the **Group > Basic** page of a group on a managed OV3600 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 click **Save** and **Apply** for the configuration from the global group to be pushed to the subscriber group on the managed OV3600.

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.

In the example below, the field **Name** was overridden with the checkbox in the global group on the Master Console, so it can be configured for each subscriber group on the managed OV3600. The other four fields in

the Basic section were not overridden, so they are static fields that will be the same for each subscriber group. These fields can only be altered on the global group on the Master Console.

The global groups feature can also be used without the Master Console. For more information about how this feature works, refer to the chapter "Configuring and Using Device Groups in OV3600" on page 81.

Monitoring and Supporting OV3600 with the Home Pages

The **Home** section 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 in the **Home** section of the OV3600 graphical user interface (GUI):

- The **Home > Overview** and the **Home > License** pages condense a large amount of information about your OV3600. From these two pages you can view the health and usage of your network as well as click common links and shortcuts to view system information. Refer to "Monitoring OV3600 with the Home > Overview Page" on page 252.
- The **Home > Search** page provides a simple way to find users and managed devices. OV3600 enhances searching by adding an ability to search for rogue devices by multiple criteria. Refer to "Searching OV3600 with the Home > Search Page" on page 257.
- The **Home > Documentation** page provides easy access to all relevant OV3600 documentation. See "Accessing OV3600 Documentation with the Home > Documentation Page" on page 258.
- The **Home > License** page provides product licensing information. See "Viewing and Updating License Information with the Home > License Page" on page 255.
- The **Home > User Info** page displays information about the users logged in to OV3600, including the role, authentication type (local user or TACACS+) and access level. See "Configuring Your Own User Information with the Home > User Info Page" on page 259.
- The **Home > Customize Dashboard** allows you to customize the **Home > Overview** page. See "Customizing the Overview Subtab Display Using Home > Customize Dashboard" on page 36.

Monitoring OV3600 with the Home > Overview Page

Navigate to **Home > Overview** page with the standard OV3600 menus. Figure 171 illustrates this page, and Table 124 describes the contents. For information on customizing the dashboard display on the Home >

Overview tab, see "Customizing the Overview Subtab Display Using Home > Customize Dashboard" on page 36.

Figure 171 ***Home > Overview*** *Page Illustration*

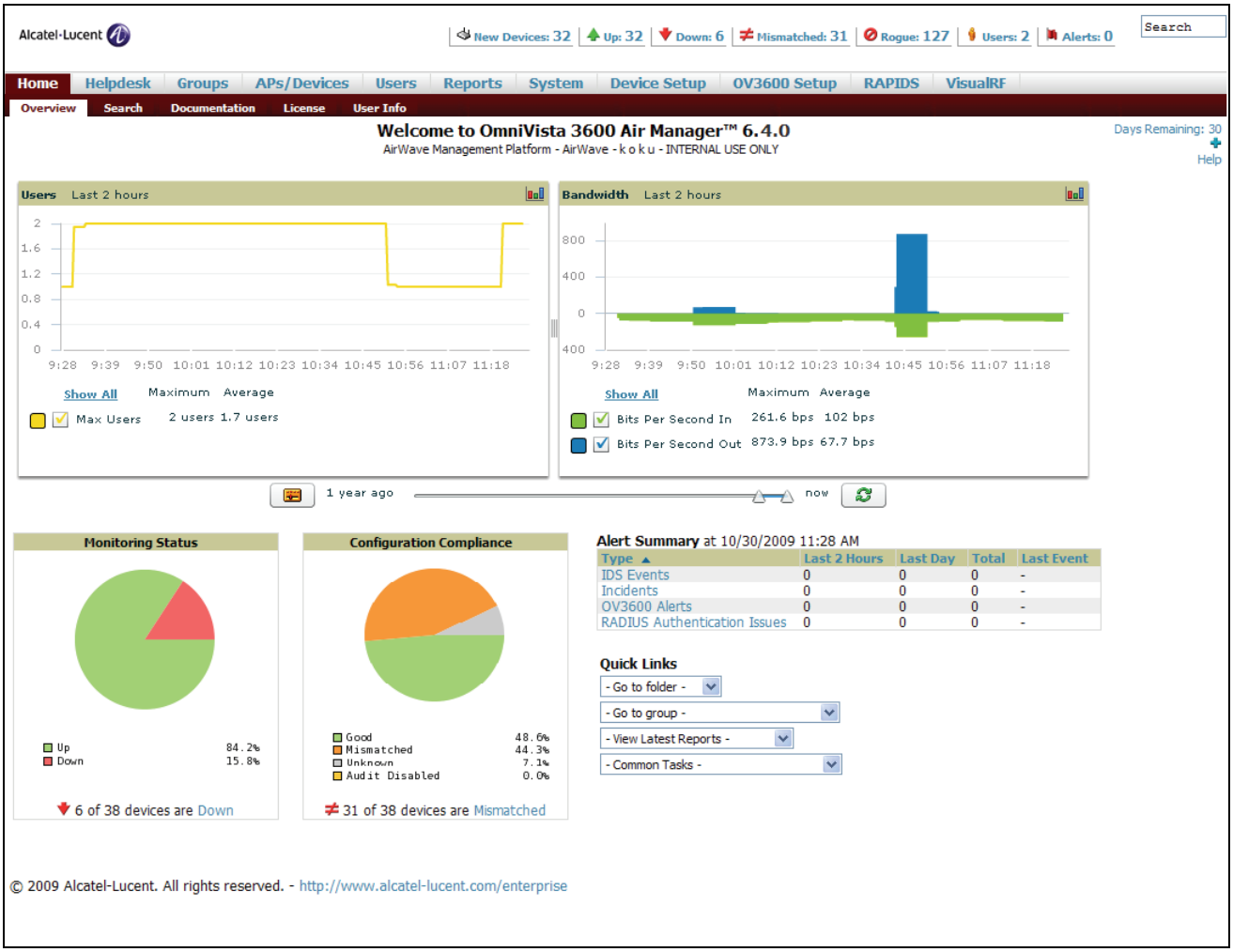


Table 124 ***Home > Overview*** *Sections and Descriptions*

Section	Description
Users	The **Users** section displays a graphical summary of the number of users on the network during a period of time. The time can be adjusted. Click **Show All** to display a complete list of users. Remove the check in the **Max Users** option to change the display of the graph. The graph displays the maximum number of users by default.
Bandwidth	The **Bandwidth** section displays bandwidth data, and this display can be adjusted. To remove bandwidth in or out from the graphical display, clear the check box for **In** or **Out**. To display details for specific devices, click **Show All** and select the devices to be included in the graphical bandwidth summary chart.
Monitoring Status	This **Monitoring Status** chart displays the percentage of devices that are up and down on the network. This chart covers 100% of the known devices on the network. To review devices that are down, click **Down**, and the **APs/Devices > Down** page displays.
Configuration Compliance	The **Configuration Compliance** chart displays all known device configuration status on the network. Devices are classified as Good, Unknown, or Mismatched. Click the Mismatched link to obtain additional information, and the **APs/Devices > Mismatched** page displays.

Table 124 ***Home > Overview*** *Sections and Descriptions*

Section	Description
Alert Summary	The **Alert Summary** section displays all known and current alerts, as previously 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** Click any alert type, and the **Alert Summary** page appears for that alert type, enabling further analysis and investigation. **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 click **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 of the **Home > Overview** page 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, and enables you to display information for any or all of them. See "Using Device Folders (Optional)" on page 167. • **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 81. • **View latest reports**—OV3600 supports 13 reports, enabling you to generate custom reports, or to display the latest daily version of any report. Click any report type to display the daily version. See "Creating, Running, and Emailing Reports" on page 269. • **Common tasks**—This menu provides an inventory of and 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 "Creating and Using Triggers and Alerts" on page 224. ▪ **Configure Default Credentials**—This link takes you to the **Device Setup > Communication** page. See "Configuring Communication Settings for Discovered Devices" on page 55. ▪ **Discover New Devices on Your Network**—This link takes you to the **Device Setup > Discover** page. See "Discovering, Adding, and Managing Devices" on page 135. ▪ **Supported Devices and Features**—This link launches and displays a PDF file that summarizes all supported devices and features in chart format for OV3600. Adobe Reader is required. ▪ **Upload Device Firmware**—This link launches and displays the **Device Setup > Upload Files** page. See "Overview of the Device Setup > Upload Files Page" on page 59. ▪ **View Event Log**—This link launches and displays the **System > Event Log** page. See "Using the System > Event Logs Page" on page 262.

Viewing and Updating License Information with the Home > License Page

Navigate to the **Home > License** page using the standard OV3600 menu. Figure 172 illustrates this page, and Table 125 describes the contents.

Please be aware that you cannot enter multiple licenses. To combine multiple license entitlements into one new license, contact Alcatel-Lucent Technical support at Esd.support@alcatel-lucent.com.

Figure 172 ***Home > License*** *Page Illustration*

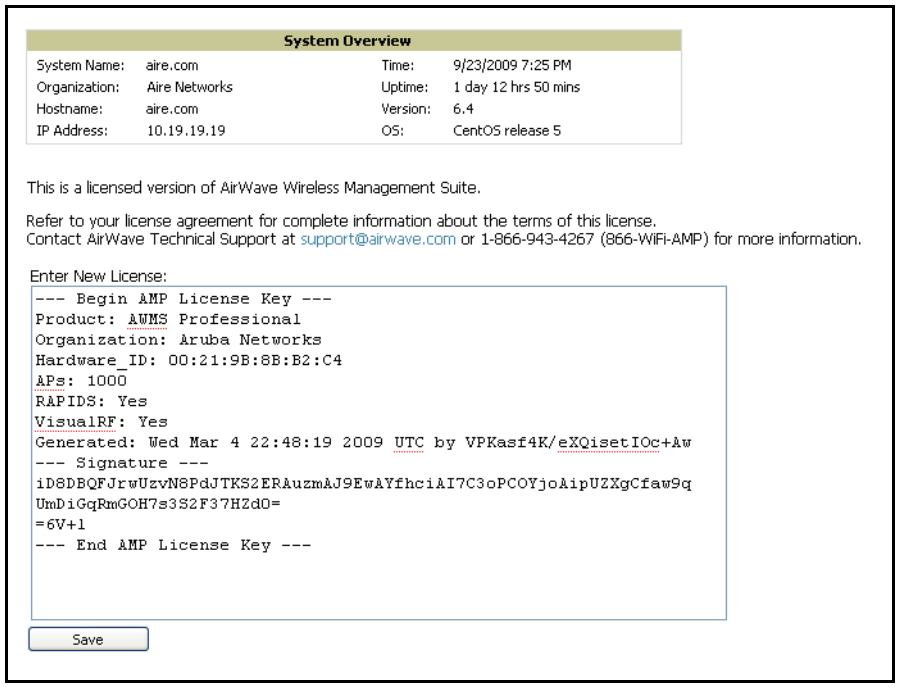


Table 125 ***Home > License*** *Fields*

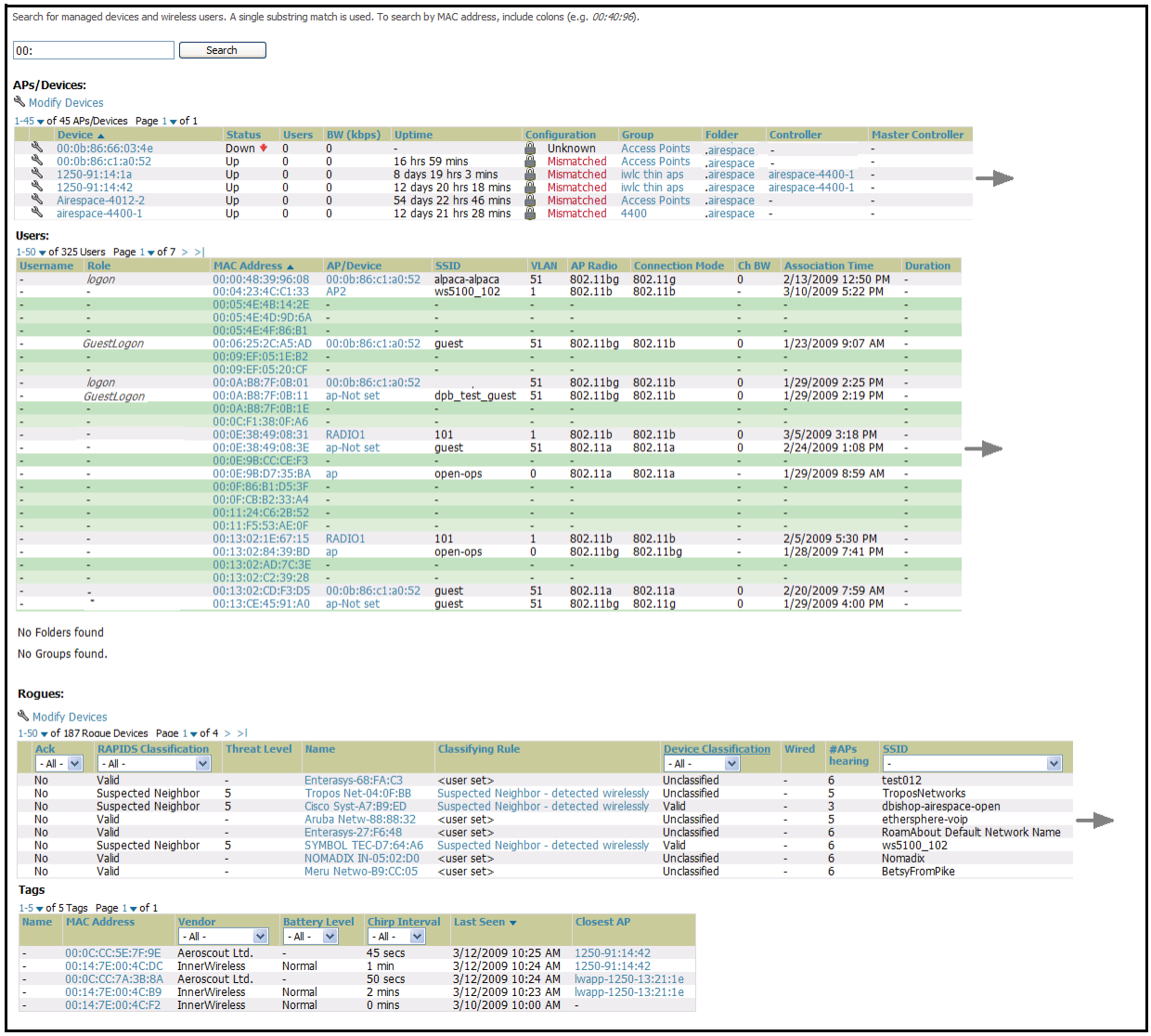
Field	Description
System Name	Displays a user-definable name for OV3600 (maximum 20 characters). The System Name can be configured from the **OV3600 Setup > General** page.
Organization	Displays the organization listed on your license key.
Hostname	Displays the DNS name assigned to OV3600.
IP Address	Displays the static IP address assigned to OV3600. The IP Address can be configured from the **OV3600 Setup > Networking** page.
Current Time	Displays the current date and time set on OV3600.
Uptime	Displays the amount of time since the operating system was last booted. OV3600 processes get restarted daily as part of the nightly maintenance.
Software Version	Displays the version number of OV3600 code currently running.
Operating system	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 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 173 illustrates this page.

Figure 173 ***Home > Search*** *Page Illustration with Sample Hits on "00:"*



1. Enter the keyword or text with which to search. If searching for a MAC address, enter it in colon-delimited format.

The OV3600 Search utility is case-insensitive.

2. Click **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. Not all categories below may offer returns for a given search:

   - **APs/Devices**

- **Users**
- **Rogues**
- **Tags**
- **Folder**
- **Group**

Accessing OV3600 Documentation with the Home > Documentation Page

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 174 illustrates this page.

Figure 174 ***Home > Documentation*** *Page Illustration*

If you have any questions that are not answered by the documentation please contact Alcatel-Lucent Technical Support at Esd.support@alcatel-lucent.com.

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 or TACACS+) and access level. This page also provides the user with the ability to customize some of the information displayed in OV3600 and change their password.

To create new users, navigate to the **OV3600 Setup > Users** page, and refer to "Creating OV3600 Users" on page 50. Users can customize the information displayed in the OV3600 header.

Figure 175 ***Home > User Info*** *Page Illustration*

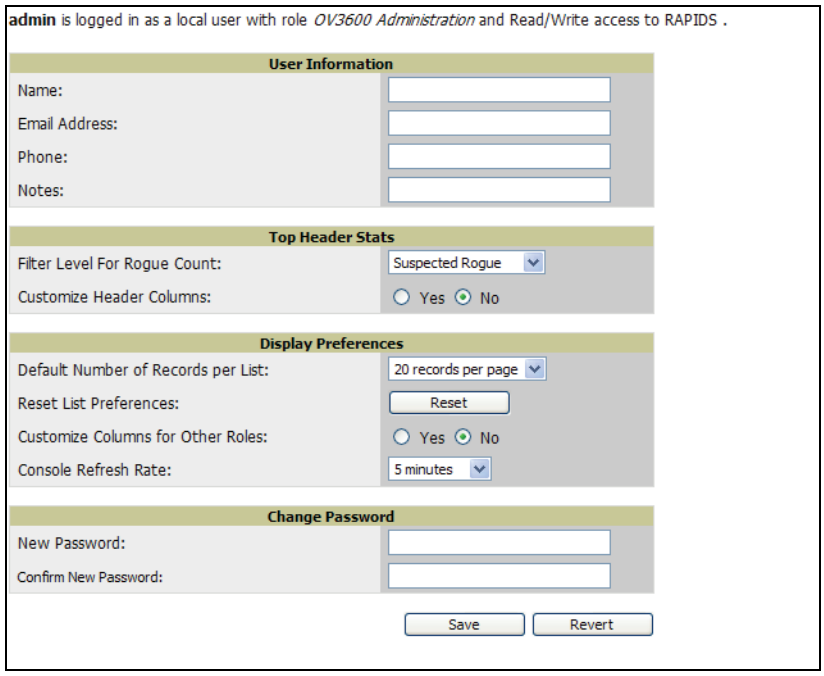


Table 126 ***Home > User Info*** *Fields*

Field	Description
Customize Header columns	Enables/disables the ability to control which statistics hyperlinks are displayed at the top of every OV3600 screen.
Stats	Select the specific data you would like to see in the header.
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.
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.
Default Number of Records per list	Defines the number of rows to appear in any list that has not had a row count manually set. 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 click the Choose Columns for roles link above the list. Make the desired column changes; select the roles to update and click save.
Filter Level For Rouge Count	Specifies the minimum classification that will cause a device to be included in the Rogue count header information.

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 a you logs 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

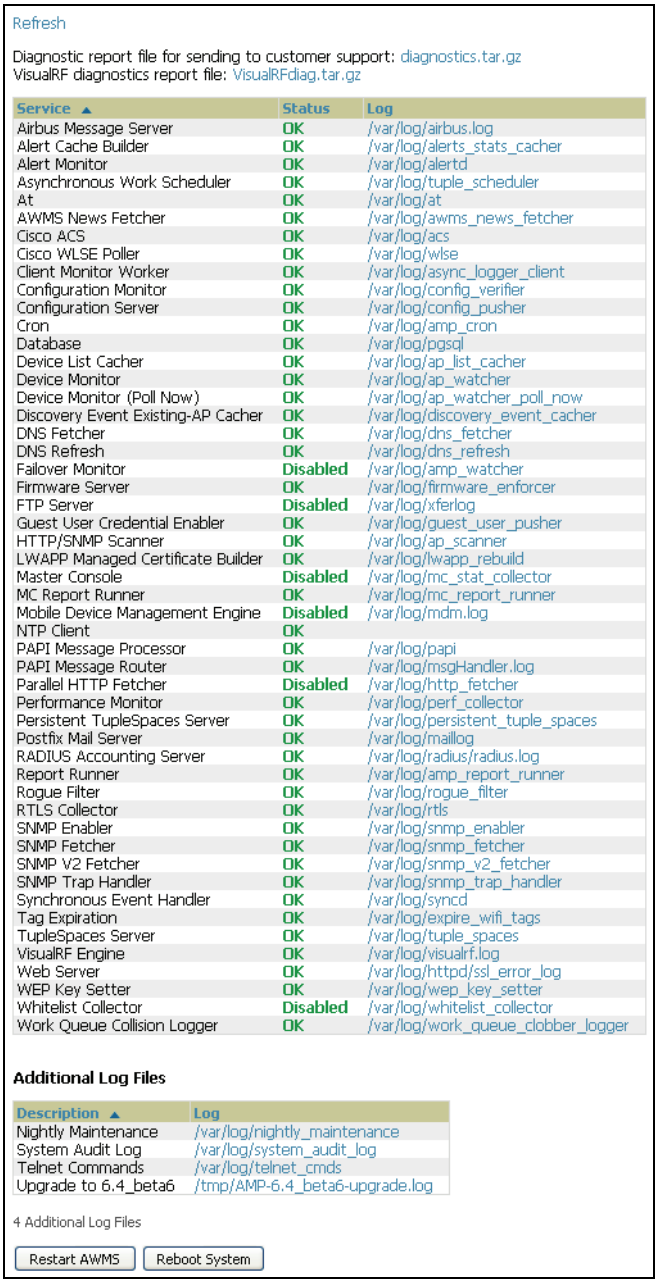
The **System** pages provide a centralized location for system-wide OV3600 data and settings. Apart from **Triggers**, **Alerts**, and **Backups** pages that are described elsewhere in this chapter, the remaining pages of the **System** section are as follows:

- **System > Status**—Displays status of all OV3600 services. Refer to "Using the System > Status Page" on page 261.
- **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 Logs Page" on page 262.
- **System > Configuration Change Jobs**—Manages configuration changes in OV3600. Refer to "Using the System > Configuration Change Jobs Page" on page 263.
- **System > Performance**—Displays basic OV3600 hardware information as well as resource usage over time. Refer to "Using the System > Performance Page" on page 264.
- **System > Firmware Upgrade Jobs**—Displays information about current and scheduled firmware upgrades.

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**. **OK** and **Disabled**, displayed in green, are the expected states of the services. If any service is **Down**, displayed in red, please contact Alcatel Lucent support. The **Reboot** 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 176 illustrates this page.

Figure 176 ***System > Status*** *Page Illustration*



- The link **diagnostics.tar.gz** downloads a tar file that contains reports and logs that are helpful to Alcatel Lucent support in troubleshooting and solving problems. Alcatel Lucent support may request that you submit this file along with other logs that are linked on this page. Logs that are contained in diagnostics.tar.gz include cron_stopped_maintenance, OV3600_events, OV3600_watcher, async_logger, ssl_error and pgsql.

- Similarly, the **VisualRFDiag.tar.gz** link downloads a diagnostic file containing VisualRF 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 127 describes the log information.

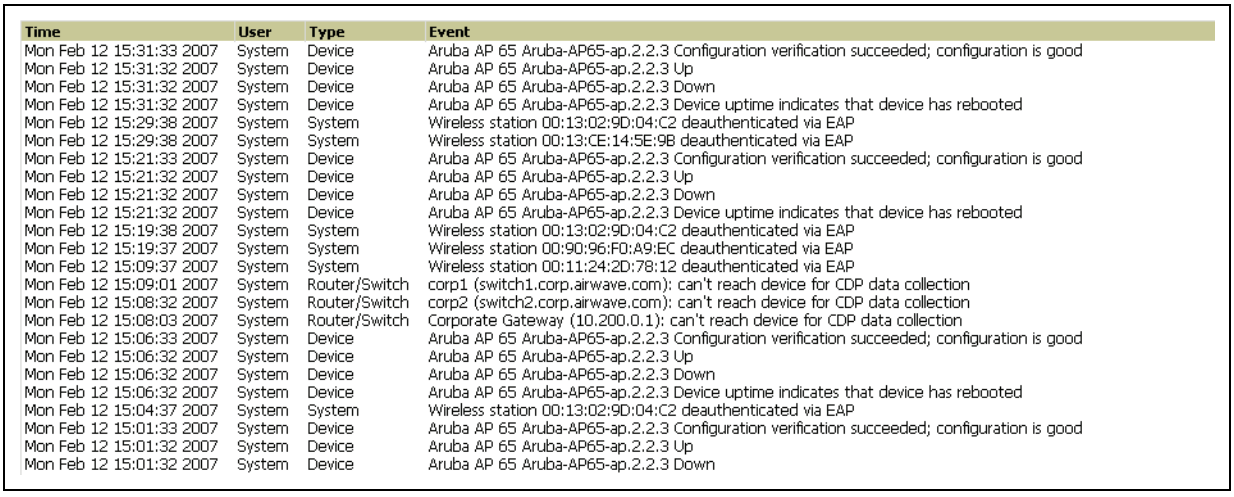
Table 127 ***System > Status Log***

Log	Description
pgsql	Logs database activity.
ssl_error_log	Reports problems with the web server. This report is 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 processes, including user-AP association.
config_verifier	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 Logs Page

The **System > Event** Logs page is a very useful debugging tool. The event log 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. Figure 177 illustrates this page, and Table 128 describes the page components.

Figure 177 ***System > Event Logs*** *Page Illustration*



Time	User	Type	Event
Mon Feb 12 15:31:33 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good
Mon Feb 12 15:31:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Up
Mon Feb 12 15:31:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Down
Mon Feb 12 15:31:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Device uptime indicates that device has rebooted
Mon Feb 12 15:29:38 2007	System	System	Wireless station 00:13:02:9D:04:C2 deauthenticated via EAP
Mon Feb 12 15:29:38 2007	System	System	Wireless station 00:13:CE:14:5E:9B deauthenticated via EAP
Mon Feb 12 15:21:33 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good
Mon Feb 12 15:21:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Up
Mon Feb 12 15:21:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Down
Mon Feb 12 15:21:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Device uptime indicates that device has rebooted
Mon Feb 12 15:19:38 2007	System	System	Wireless station 00:13:02:9D:04:C2 deauthenticated via EAP
Mon Feb 12 15:19:37 2007	System	System	Wireless station 00:90:96:F0:A9:EC deauthenticated via EAP
Mon Feb 12 15:09:37 2007	System	System	Wireless station 00:11:24:2D:78:12 deauthenticated via EAP
Mon Feb 12 15:09:01 2007	System	Router/Switch	corp1 (switch1.corp.airwave.com): can't reach device for CDP data collection
Mon Feb 12 15:08:32 2007	System	Router/Switch	corp2 (switch2.corp.airwave.com): can't reach device for CDP data collection
Mon Feb 12 15:08:03 2007	System	Router/Switch	Corporate Gateway (10.200.0.1): can't reach device for CDP data collection
Mon Feb 12 15:06:33 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good
Mon Feb 12 15:06:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Up
Mon Feb 12 15:06:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Down
Mon Feb 12 15:06:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Device uptime indicates that device has rebooted
Mon Feb 12 15:04:37 2007	System	System	Wireless station 00:13:02:9D:04:C2 deauthenticated via EAP
Mon Feb 12 15:01:33 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good
Mon Feb 12 15:01:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Up
Mon Feb 12 15:01:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Down

Table 128 ***System > Event Logs*** *Fields*

Field	Description
Time	Date and time of the event.
User	The OV3600 user that triggered the event. When OV3600 itself is responsible for the event, System is displayed as the user.

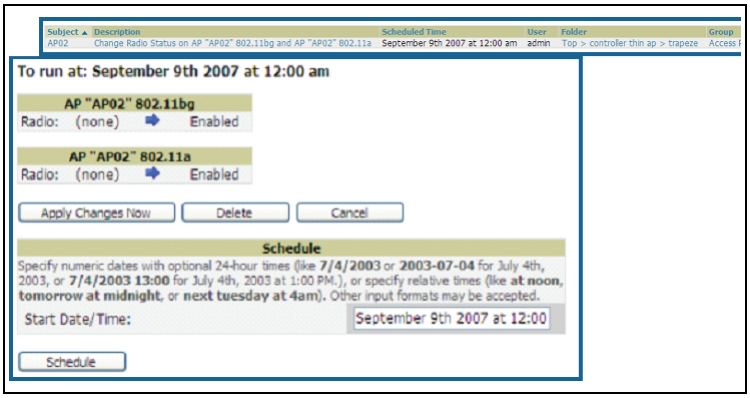
Table 128 ***System > Event Logs*** *Fields*

Field	Description
Type	Displays the Type of event recorded, which is one of four types, as follows: • **AP**—An event localized to one specific AP. • **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 178.

Figure 178 ***System > Configuration Change Jobs*** *Page Illustration*



1. To edit an existing configuration change job click on the linked description name. On the subsequent edit page you can choose to run the job immediately by clicking the **Apply Changes Now** button, reschedule the job using the **Schedule** box, delete the job using the **Delete** button, or cancel the job edit by clicking the **Cancel** button.
2. Click the linked AP or group name under the **Subject** column to go to the monitoring page of the AP or group.
3. Click 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. Figure 179 illustrates this page and Table 129 describes fields and information displayed.

Figure 179 ***System > Performance*** *Page Illustration (Partial Screen Shown)*

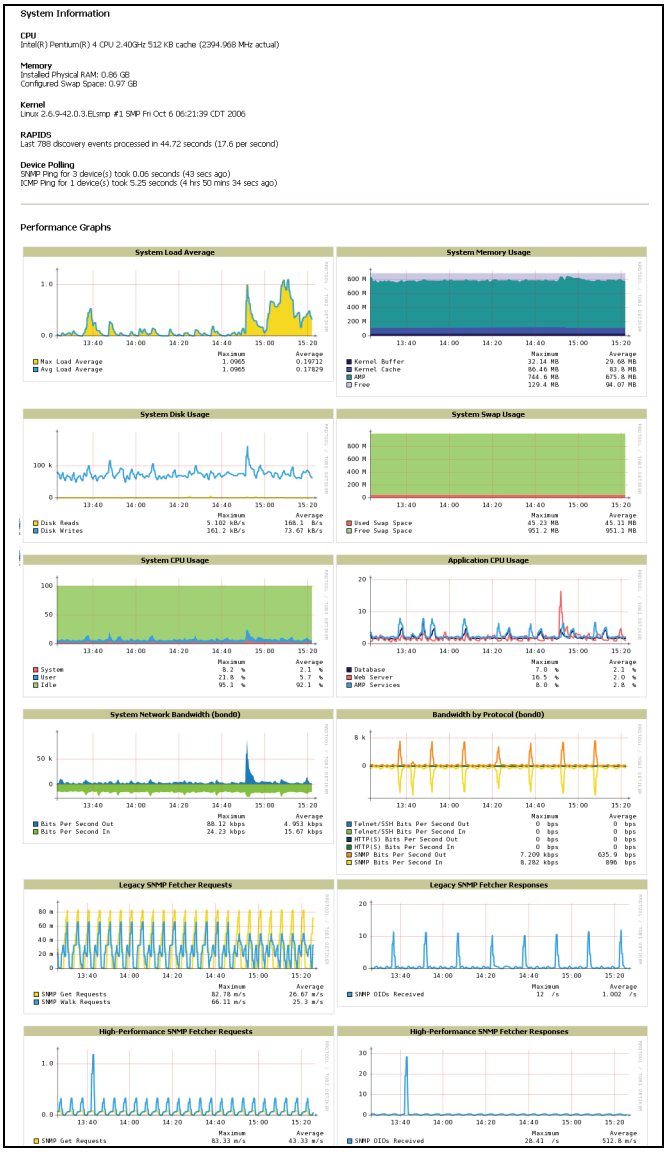


Table 129 ***System > Performance*** *Page Fields*

Field	Description
CPU(s)	Basic CPU information as reported by Linux.
Memory	The amount of physical RAM and Swap space seen by the operating system. OV3600 requires a minimum of 1 gigabyte of physical RAM
Kernel	The version of Linux kernel running on the box.
RAPIDS	Displays how long it took to process the last payload of MAC address.
Device Polling	Displays some AP/Device polling statistics.

Table 129 ***System > Performance*** *Page Fields (Continued)*

Field	Description
System Load Average	The System Load average is 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 3. A constant load of 5 to 7 is cause for concern. A load above 10 is a serious issue and will probably result in OV3600 becoming unusable. To lower the load average try increasing a few polling periods. Increasing the polling period for APs, routers/switches, WLSE, ACS, and so on, will decrease the amount of work OV3600 needs to perform and lower the load average. If you have a load that is consistently below 3 you might consider shortening your polling period and observing. **NOTE:** If the load is less than one the y scale will be 1 to 1000 m standing for milliseconds or 1/1000ths of 1.
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.
Swap Usage	The amount of Swap memory used by OV3600. Swap is used when the 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 for the box.
System CPU Usage	The percentage of CPU that has been used by the user and the system as well as the amount that was idle.
Application CPU Usage	CPU usage broken down by application. OV3600 services includes all OV3600 processes except the database and the webserver.
System Network Bandwidth (Eth0)	All traffic in and out of Eth0 measured in bits per second.
Bandwidth by Protocol (Eth0)	Displays the amount of traffic used by Telnet, HTTPS and SNMP on Eth0.
Legacy SNMP Fetcher (SNMP Get/walk Requests)	The number of SNMP get and walk requests per second performed by the legacy (v1 and v3) SNMP fetcher.
Legacy SNMP Fetcher (SNMP OIDs Received)	The number of SNMP OIDs received per second performed by the legacy (v1 and v3) SNMP fetcher.
High Performance SNMP Fetcher (SNMP Get/walk Requests)	The number of SNMP get and walk requests per second performed by the high performance SNMP (v2c) fetcher.
High Performance SNMP Fetcher (SNMP OIDs Received)	The number of SNMP OIDs received per second performed by the high performance SNMP (v2c) fetcher.
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.

Table 129 ***System > Performance*** *Page Fields (Continued)*

Field	Description
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 Usage	Pie charts that display the amount of used and free hard drive space for each partition. If a drive reaches over 80% full you may want to lower the Historical Data Retention settings on the OV3600 page or consider installing 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 User Guide* or contact Alcatel-Lucent Technical Support at Esd.support@alcatel-lucent.com for the latest recommendations.

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 announcement email:

Upgrading OV3600

1. Download OV3600 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.
The script will then extract the version specific upgrade script.
The version specific script will deploy all needed files, update the database and perform any data migrations and restart the OV3600 services

Backing Up OV3600

Overview of Backups

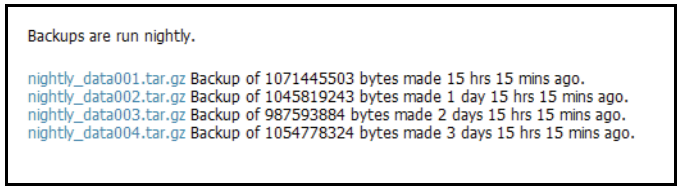
OV3600 creates nightly archives of all relational data, statistical data, and log files. This occurs by default at 4:15 AM, but is configurable on the **OV3600 Setup > General** page under the **Nightly Maintenance Time** setting.

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 180 illustrates this page.

Figure 180 ***System > Backups*** *Page Illustration*



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.

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 an appropriate destination.

   A good open source Windows file transfer client that supports SFTP and SCP for is WinSCP which is available from 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. Run the restore script by typing **ov3600_restore -d /tmp/nightly_data00[1-4].tar.gz**.

OV3600 Failover

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 will enter failover mode. When OV3600 enters failover mode it 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 bar is a static navigation bar containing tabs for the main components of OV3600, while the lower bar is context-sensitive and displays the sub-menus for the highlighted tab. Table 130 describes the contents of this page.

Table 130 *Contents of the **Navigation Section of Failover***

Main Tab	Description	Sub-Menus
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** • **Watched** • **OV3600** • **License** (viewable only by demo versions)
System	The **System** page provides information related to OV3600 operation and administration (including overall system status, performance monitoring and backups).	• **Status** • **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 OV3600** 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 OV3600 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/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 1000 APs it might take up to 10 minutes. For an **OV3600** with 2500 APs it might take as long as 20 minutes. The Failover OV3600 will retain its original IP address.

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 267.

Table 131 ***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 report access, creation, scheduling, and distribution via email and XML processing.

This chapter includes the following sections:

- "Overview of OV3600 Reports" on page 269
- "Using Daily Reports" on page 272
- "Defining Reports" on page 296
- "Emailing and Exporting Reports" on page 299

NOTE

OV3600 ships with several reports as enabled by default. Default reports may run each night or weekly, depending on the OV3600 release. Alcatel Lucent recommends that you 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 report.

NOTE

OV3600 supports additional and more 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, allowing you to act upon information in the reports. You can generate an export a wide variety of reports in OV3600.

OV3600 reports have the following general parameters:

- OV3600 runs daily versions of all reports during predefined windows of time. All reports can be scheduled so that they run in the background.
- The daily version of any report is available instantly using the **Reports > Generated** page and scrolling to the report links at the bottom of the page.
- The **Inventory** and the **Configuration Audit** reports are the only reports that do not span a period of time. Instead, these two reports provide a detailed 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 to take inventory of reports already defined.

The **Definitions** page includes these sections:

- **Report definitions** pane—The **Add** button allows you to define a custom report using the **Custom Options** drag and drop UI or any of the report types from a 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 right then.
- **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** pane—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 Reports** table 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 custom report from the **Definition** page, it appears on the **Generated** page. The **Report > Definition** page is shown in Figure 181, and Table 132 describes the fields available when you select a specific report definition.

Figure 181 ***Report > Definitions*** *Page Illustration (Split View)*

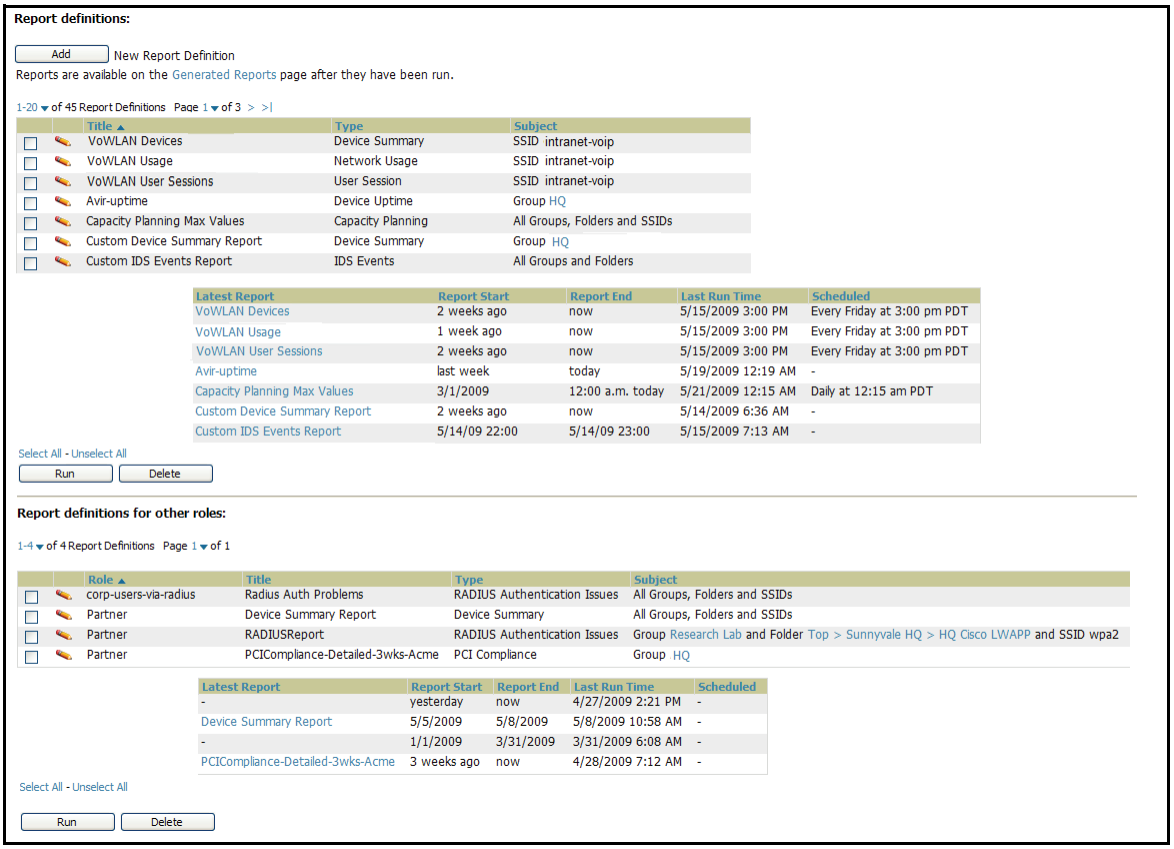
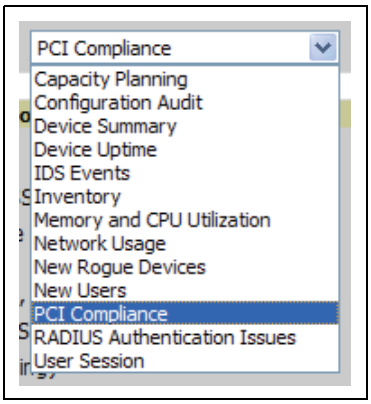


Table 132 ***Report > Definition*** *Page Fields and Descriptions*

Field	Description
Report Definition	Displays a field for entering report title and dropdown menu, shown in Figure 182, 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 the **Yes** radio button. 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 the **Yes** radio button.
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.
Cancel	Returns you to **Reports > Definitions** page.

Figure 182 ***Report Type*** *Drop-down Menu in* ***Reports > Definitions > Add*** *Illustration*



NOTE

Only **admin** users have complete access to complete 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 defined in the **Reports > Definitions** page. This page also enables you to display the most recent daily version of any report. Reports comply with the access permissions defined for OV3600 users. 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 four primary sections, as follows:

- Generated reports configured for the current role and for additional roles
- Generated reports for other roles
- The option to view the latest daily reports with a single click for immediate online viewing

Figure 183 ***Reports > Generated*** *Page Example*

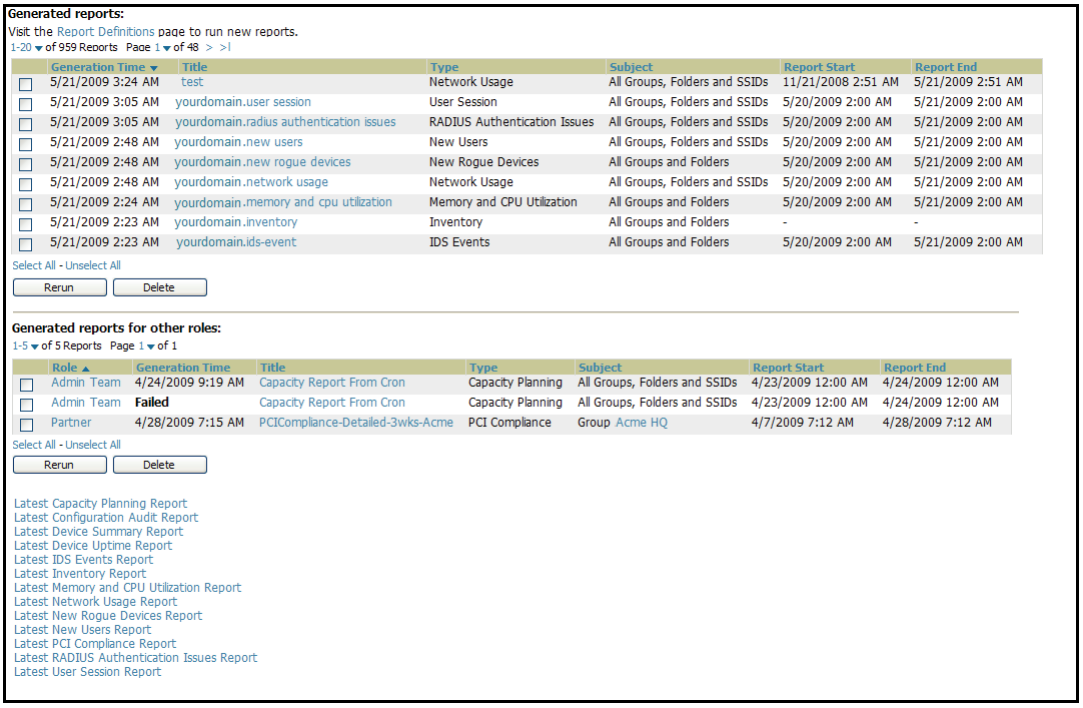


Figure 184 ***Reports > Generated*** *Page with Single-click Report Viewing Options*

NOTE

Clicking any report from the list shown in Figure 184 displays the **Detail** page for the most recent version of that report.

Using Daily Reports

This section describes the reports supported in OV3600. These reports can be accessed from the bottom of the **Reports > Generated** page, and are presented in alphabetical order as follows in Table 133:

Viewing Generated Reports

To display all generated reports that are currently scheduled on OV3600, navigate to the **Reports > Generated** page. Figure 183 and Figure 184 illustrate this page. This 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 category (column header) in sequential or reverse sequential order.
- Click a report title to view details for each scheduled report. Click **Add** to create new generated reports. Generated reports are scheduled and custom configurable.
- Scroll to the bottom of the **Reports > Generated** page, and click any of the 13 report types to view the most recent version of any report. This function is independent of scheduled reports.
- The **Reports > Detail** page launches when you click any report title from this page. The content of the **Reports > Detail** page varies significantly according to the report type.

The **Generated Reports** page contains less columns and information than the **Definitions** page. Table 133 describes each column for the **Reports > Generated** page.

Table 133 ***Report > Definition*** *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. Clicking 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 clicking **Run**.
Title	Displays title of the report. This is a user-configured field when creating the report.
Type	Displays the type of the report. This can be one of 13 report types in OV3600.
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.
Report End	Displays the end of the time period covered in the report.
Role	Added to the **Reports definitions for other roles** section, this column cites the roles for which additional reports are defined.

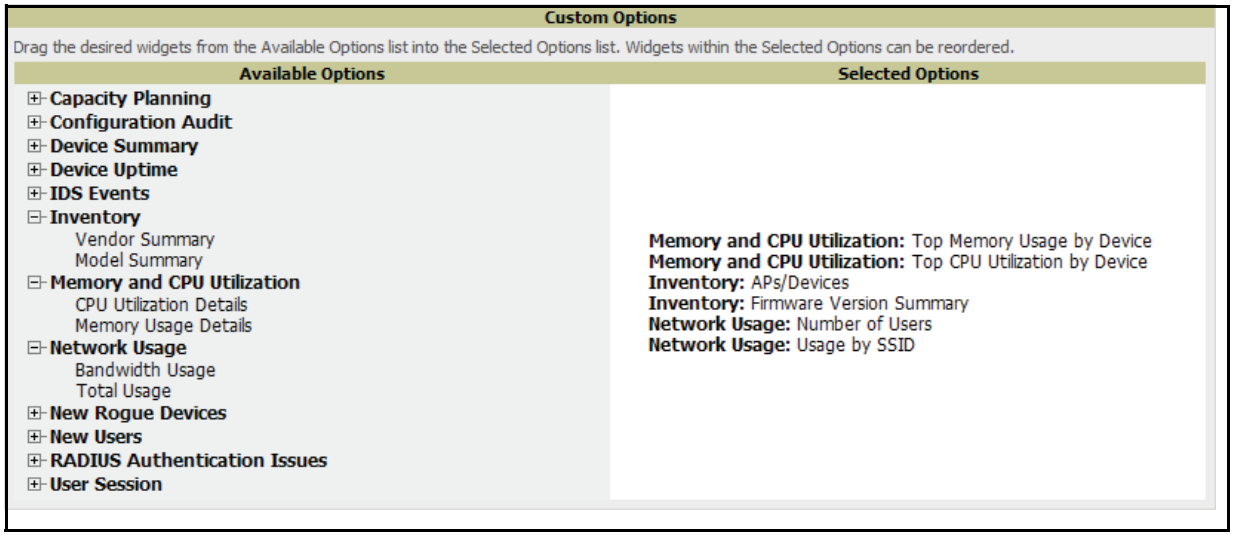
Using Custom Reports

Custom reports allow users to specify the data that should be included in a report and how it should be displayed.

Perform these steps to create a **Custom Report**.

1. Navigate to the **Reports > Definitions** page.
2. Click the **Add** button.
3. Select **Custom** in the type dropdown. The **Custom Options** section will open up as shown in Figure 185.

Figure 185 ***OV3600 Custom Options*** *Page*



The left pane of the **Custom Options** window lists all available data that can be included in the report. The data is broken down by report. If for example, the data you want to include is in the Inventory report, click **Inventory** to view a list of all available inventory 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.

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 clicking the column heading.

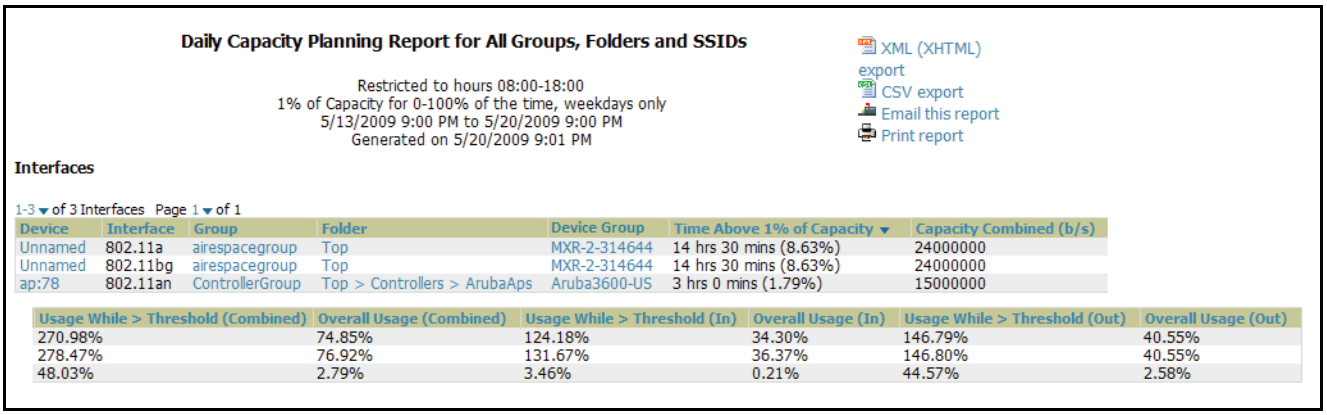
Refer also to the "Using the Network Usage Report" on page 284 for additional bandwidth information.

Perform these steps to view the most recent **Capacity Planning Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Latest Capacity Planning Report** to display **Detail** device capacity information for all devices. The report provides multiple links to additional device configuration, folders, and additional OV3600 pages.

The following figures and Table 134 illustrate and describe the contents of the **Capacity Planning Report**.

Figure 186 ***OV3600 Capacity Planning Report*** *Page (split view)*



Daily Capacity Planning Report for All Groups, Folders and SSIDs

Restricted to hours 08:00-18:00
1% of Capacity for 0-100% of the time, weekdays only
5/13/2009 9:00 PM to 5/20/2009 9:00 PM
Generated on 5/20/2009 9:01 PM

XML (XHTML) export
CSV export
Email this report
Print report

Interfaces

1-3 of 3 Interfaces Page 1 of 1

Device	Interface	Group	Folder	Device Group	Time Above 1% of Capacity	Capacity Combined (b/s)
Unnamed	802.11a	airespacegroup	Top	MXR-2-314644	14 hrs 30 mins (8.63%)	24000000
Unnamed	802.11bg	airespacegroup	Top	MXR-2-314644	14 hrs 30 mins (8.63%)	24000000
ap:78	802.11an	ControllerGroup	Top > Controllers > ArubaAps	Aruba3600-US	3 hrs 0 mins (1.79%)	15000000

Usage While > Threshold (Combined)	Overall Usage (Combined)	Usage While > Threshold (In)	Overall Usage (In)	Usage While > Threshold (Out)	Overall Usage (Out)
270.98%	74.85%	124.18%	34.30%	146.79%	40.55%
278.47%	76.92%	131.67%	36.37%	146.80%	40.55%
48.03%	2.79%	3.46%	0.21%	44.57%	2.58%

Table 134 ***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.
Usage While > Threshold (Combined)	Displays the time in which a device has functioned above defined threshold capacity, both in and out.
Overall Usage (Combined)	Displays the overall usage of the device, both combined in and out traffic.

Table 134 ***Capacity Planning Report*** *Fields and Contents, Top Portion (Continued)*

Field	Description
Usage While > Threshold (in)	Displays device usage that exceeds the defined and incoming threshold capacity.
Overall Usage (In)	Displays overall device usage for incoming data.
Usage While > Threshold (Out)	Displays device usage for outgoing data that exceeds defined thresholds.
Overall Usage (Out)	Displays device usage for outgoing data.

Using the 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 click **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, click 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. Click **Add a Template** when viewing device-specific configuration information.
5. You can audit the current device configuration from the **Detail** page. Click **Audit** when viewing device-specific information.
6. You can display archived configuration about a given device from the **Detail** page. Click **Show Archived Device Configuration**.

Figure 187 and Table 135 illustrate and describe the general **Configuration Audit** report and related contents.

Figure 187 ***Reports > Generated > Daily Configuration Audit*** *Report Page, abbreviated example*

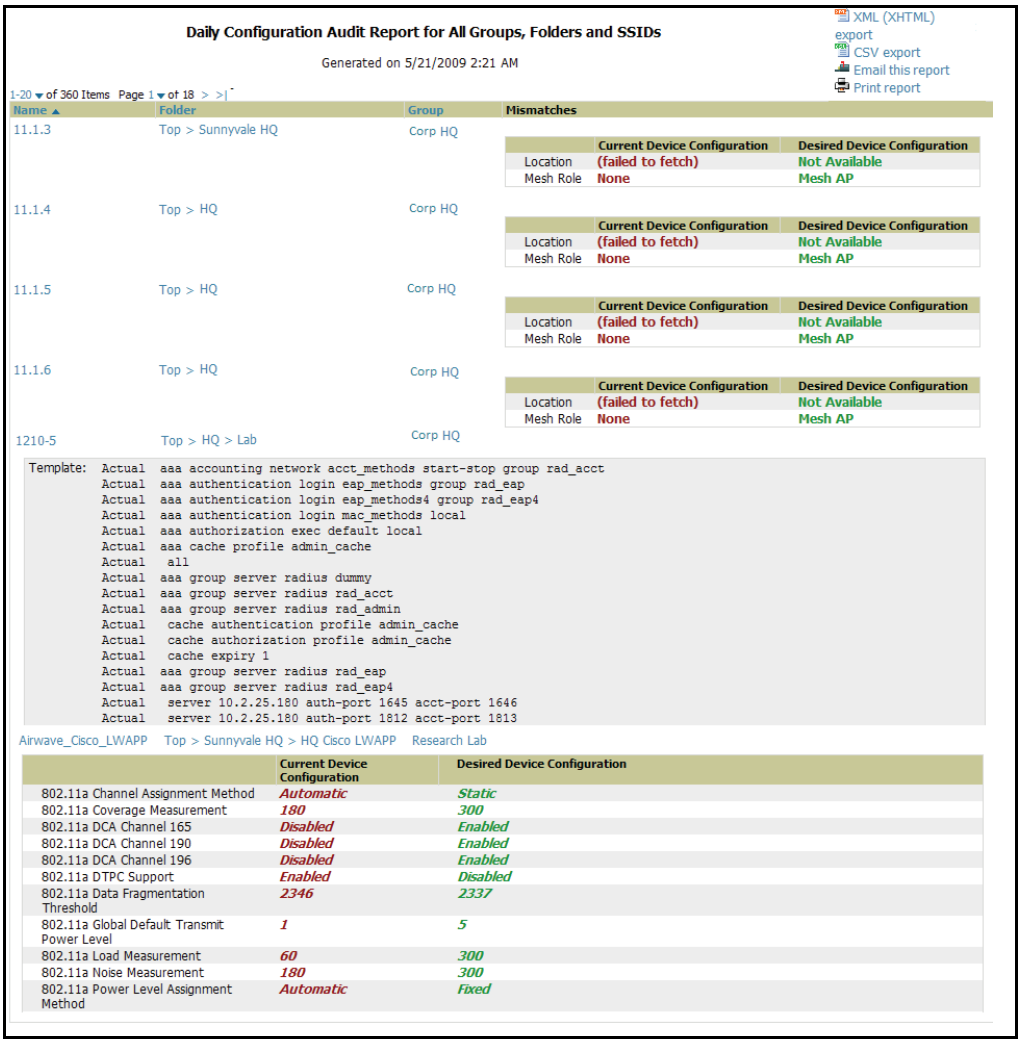


Table 135 *Information Categories in* ***Reports > Generated > Daily Configuration Audit Report***

Field	Description
Name	Displays the device name for every device on the network. Clicking 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. Clicking 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. Clicking 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 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.

You can specify the number of devices that appear in each of the first four categories in the Reports > Definitions > Add page.

- **Devices**—This list displays all devices in OV3600. By default is sorted alphabetically by device name.

Any section of this report can be sorted by any of the columns:

- **Rank**
- **AP/Device**
- **Number of Users**
- **Max Simultaneous Users**
- **Total Bandwidth (MB)**
- **Average Bandwidth (kbps)**
- **Location**
- **Controller**
- **Folder**
- **Group**

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.

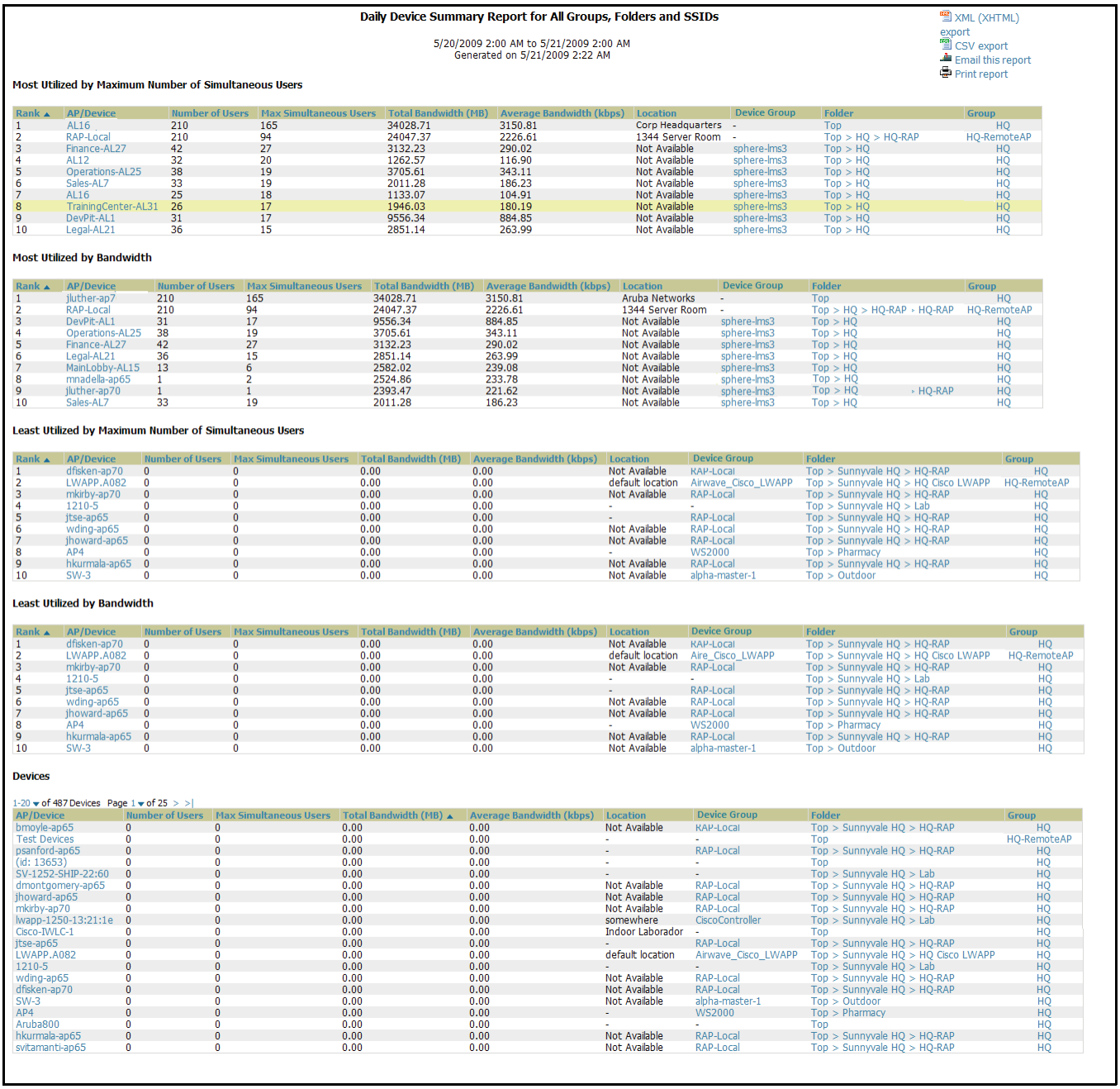
If sorting the **Devices** list does not provide you with sufficient detail, you can specify a **Group** or **Folder** in the report **Definition** of a custom report. If you create a separate Group or Folder for each set of master and local controllers, you can generate a separate report for each Group or Folder. With this method, the summary sections of each report contain only devices from that Group or Folder.

Perform these steps to view the most recent version of this report, and to adjust configurations for over-used or under-used devices.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Device Summary Report** to display **Detail** device information. You can use this report as the central starting point to reconfigure over-used or under-used devices.
3. To generate more reports that cover a greater span of time, refer to "Viewing Generated Reports" on page 272.

Figure 188 and Table 136 illustrate and describe the **Reports > Generated > Device Summary Detail** page.

Figure 188 ***Reports > Generated > Daily Device Summary*** *Report Illustration*



Daily Device Summary 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 2:22 AM

XML (XHTML) export
CSV export
Email this report
Print report

Most Utilized by Maximum Number of Simultaneous Users

Rank	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Device Group	Folder	Group
1	AL16	210	165	34028.71	3150.81	Corp Headquarters	-	Top	HQ
2	RAP-Local	210	94	24047.37	2226.61	1344 Server Room	-	Top > HQ > HQ-RAP	HQ-RemoteAP
3	Finance-AL27	42	27	3132.23	290.02	Not Available	sphere-lms3	Top > HQ	HQ
4	AL12	32	20	1262.57	116.90	Not Available	sphere-lms3	Top > HQ	HQ
5	Operations-AL25	38	19	3705.61	343.11	Not Available	sphere-lms3	Top > HQ	HQ
6	Sales-AL7	33	19	2011.28	186.23	Not Available	sphere-lms3	Top > HQ	HQ
7	AL16	25	18	1133.07	104.91	Not Available	sphere-lms3	Top > HQ	HQ
8	TrainingCenter-AL31	26	17	1946.03	180.19	Not Available	sphere-lms3	Top > HQ	HQ
9	DevPit-AL1	31	17	9556.34	884.85	Not Available	sphere-lms3	Top > HQ	HQ
10	Legal-AL21	36	15	2851.14	263.99	Not Available	sphere-lms3	Top > HQ	HQ

Most Utilized by Bandwidth

Rank	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Device Group	Folder	Group
1	jluther-ap7	210	165	34028.71	3150.81	Aruba Networks	-	Top	HQ
2	RAP-Local	210	94	24047.37	2226.61	1344 Server Room	-	Top > HQ > HQ-RAP ▸ HQ-RAP	HQ-RemoteAP
3	DevPit-AL1	31	17	9556.34	884.85	Not Available	sphere-lms3	Top > HQ	HQ
4	Operations-AL25	38	19	3705.61	343.11	Not Available	sphere-lms3	Top > HQ	HQ
5	Finance-AL27	42	27	3132.23	290.02	Not Available	sphere-lms3	Top > HQ	HQ
6	Legal-AL21	36	15	2851.14	263.99	Not Available	sphere-lms3	Top > HQ	HQ
7	MainLobby-AL15	13	6	2582.02	239.08	Not Available	sphere-lms3	Top > HQ	HQ
8	mnadella-ap65	1	2	2524.86	233.78	Not Available	sphere-lms3	Top > HQ	HQ
9	jluther-ap70	1	1	2393.47	221.62	Not Available	sphere-lms3	Top > HQ ▸ HQ-RAP	HQ
10	Sales-AL7	33	19	2011.28	186.23	Not Available	sphere-lms3	Top > HQ	HQ

Least Utilized by Maximum Number of Simultaneous Users

Rank	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Device Group	Folder	Group
1	dfisken-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
2	LWAPP.A082	0	0	0.00	0.00	default location	Airwave_Cisco_LWAPP	Top > Sunnyvale HQ > HQ Cisco LWAPP	HQ-RemoteAP
3	mkirby-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
4	1210-5	0	0	0.00	0.00	-	-	Top > Sunnyvale HQ > Lab	HQ
5	jtse-ap65	0	0	0.00	0.00	-	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
6	wding-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
7	jhoward-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
8	AP4	0	0	0.00	0.00	-	WS2000	Top > Pharmacy	HQ
9	hkurmala-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
10	SW-3	0	0	0.00	0.00	Not Available	alpha-master-1	Top > Outdoor	HQ

Least Utilized by Bandwidth

Rank	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Device Group	Folder	Group
1	dfisken-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
2	LWAPP.A082	0	0	0.00	0.00	default location	Aire_Cisco_LWAPP	Top > Sunnyvale HQ > HQ Cisco LWAPP	HQ-RemoteAP
3	mkirby-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
4	1210-5	0	0	0.00	0.00	-	-	Top > Sunnyvale HQ > Lab	HQ
5	jtse-ap65	0	0	0.00	0.00	-	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
6	wding-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
7	jhoward-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
8	AP4	0	0	0.00	0.00	-	WS2000	Top > Pharmacy	HQ
9	hkurmala-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
10	SW-3	0	0	0.00	0.00	Not Available	alpha-master-1	Top > Outdoor	HQ

Devices

1-20 of 487 Devices Page 1 of 25 > >|

AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Device Group	Folder	Group
bmoyle-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
Test Devices	0	0	0.00	0.00	-	-	Top	HQ-RemoteAP
psanford-ap65	0	0	0.00	0.00	-	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
(id: 13653)	0	0	0.00	0.00	-	-	Top	HQ
SV-1252-SHIP-22:60	0	0	0.00	0.00	-	-	Top > Sunnyvale HQ > Lab	HQ
dmontgomery-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
jhoward-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
mkirby-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
lwapp-1250-13:21:1e	0	0	0.00	0.00	somewhere	CiscoController	Top > Sunnyvale HQ > Lab	HQ
Cisco-IWLC-1	0	0	0.00	0.00	Indoor Laborador	-	Top	HQ
jtse-ap65	0	0	0.00	0.00	-	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
LWAPP.A082	0	0	0.00	0.00	default location	Airwave_Cisco_LWAPP	Top > Sunnyvale HQ > HQ Cisco LWAPP	HQ
1210-5	0	0	0.00	0.00	-	-	Top > Sunnyvale HQ > Lab	HQ
wding-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
dfisken-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
SW-3	0	0	0.00	0.00	Not Available	alpha-master-1	Top > Outdoor	HQ
AP4	0	0	0.00	0.00	-	WS2000	Top > Pharmacy	HQ
Aruba800	0	0	0.00	0.00	-	-	Top	HQ
hkurmala-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ
svitamanti-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ

Table 136 ***Reports > Generated > Daily Device Summary*** *Report Fields and Descriptions*

Field	Description
Rank	The rank column for any section of this report establishes the top 10 devices for any category, and these are listed in sequential or reverse-sequential order.
AP/Device	Displays the name of the device, which can be a MAC address or other identifier.
Number of Users	Displays the number of users associated with each device.
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.

Table 136 ***Reports > Generated > Daily Device Summary*** *Report Fields and Descriptions*

Field	Description
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.
Location	Displays the location of the device that is included in any category of the report.
Controller	Displays the controller to which any included device is associated.
Folder	Displays the folder with which a device is associated.
Group	Displays the device group with which a device is associated.

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

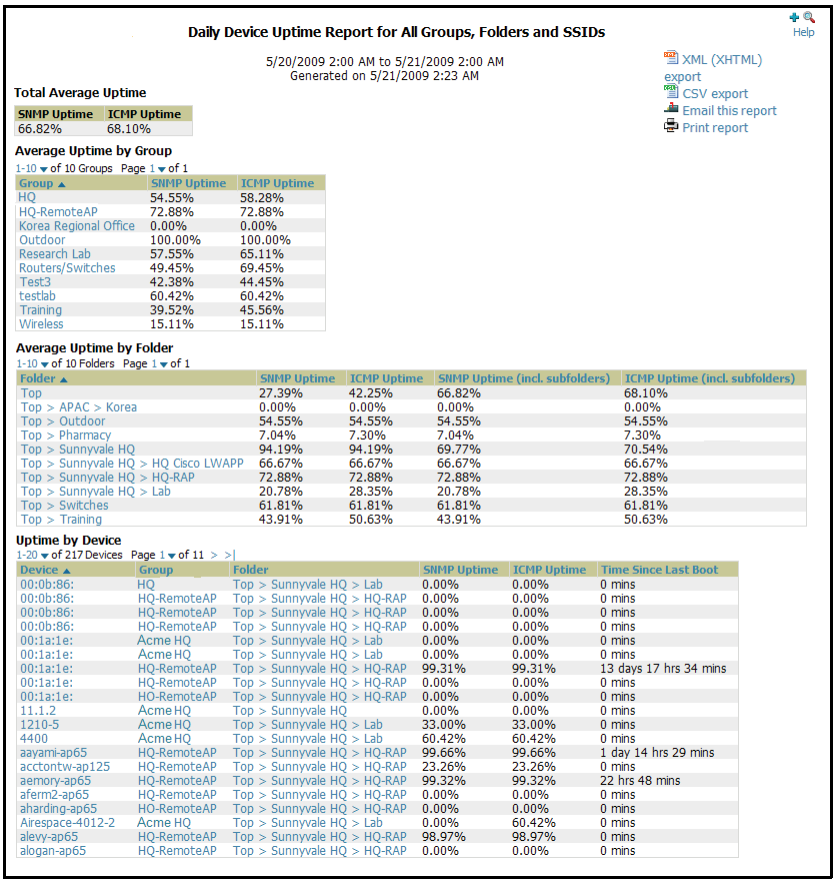
You can use this report as the central starting point to improve uptime by multiple criteria. This report covers protocol-oriented, device-oriented, or SSID-oriented information. This report can help to monitor and optimize the network in multiple ways. This report can demonstrate service parameters, 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.

Perform these steps to view the most recent version of the **Device Uptime** report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Device Uptime Report** to display report **Detail** information.
3. To generate more reports of this type that cover a greater span of time, refer to "Reports > Definitions Page Overview" on page 269.

Figure 189 and Table 136 illustrate and describe the **Reports > Generated > Device Uptime Detail** report.

Figure 189 ***Reports > Generated > 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

Help

XML (XHTML) export
CSV export
Email this report
Print report

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
00:0b:86:	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	0.00%	0.00%	0 mins
00:1a:1e:	Acme HQ	Top > Sunnyvale HQ > Lab	0.00%	0.00%	0 mins
00:1a:1e:	Acme HQ	Top > Sunnyvale HQ > Lab	0.00%	0.00%	0 mins
00:1a:1e:	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	99.31%	99.31%	13 days 17 hrs 34 mins
00:1a:1e:	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	0.00%	0.00%	0 mins
00:1a:1e:	HO-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	0.00%	0.00%	0 mins
11.1.2	Acme HQ	Top > Sunnyvale HQ	0.00%	0.00%	0 mins
1210-5	Acme HQ	Top > Sunnyvale HQ > Lab	33.00%	33.00%	0 mins
4400	Acme HQ	Top > Sunnyvale HQ > Lab	60.42%	60.42%	0 mins
aayami-ap65	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	99.66%	99.66%	1 day 14 hrs 29 mins
acctontw-ap125	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	23.26%	23.26%	0 mins
aemory-ap65	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	99.32%	99.32%	22 hrs 48 mins
aferm2-ap65	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	0.00%	0.00%	0 mins
aharding-ap65	HO-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	0.00%	0.00%	0 mins
Airespace-4012-2	Acme HQ	Top > Sunnyvale HQ > Lab	0.00%	60.42%	0 mins
alevy-ap65	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	98.97%	98.97%	0 mins
alogan-ap65	HQ-RemoteAP	Top > Sunnyvale HQ > HQ-RAP	0.00%	0.00%	0 mins

Table 137 ***Reports > Generated > Device Uptime Report*** *Fields and Descriptions*

Field	Description
Device	Displays the name of the device.
Group	Displays the name of the device's group.
Folder	Displays the folder to which the device belongs.
SSID	Displays the Service Set Identifier (SSID) set on the device.
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 Access Points (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.

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 234 for additional information.

Perform these steps to view the most recent version of the **IDS Events** report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **IDS Events Report** to display report **Detail** information.
3. Clicking the AP device or controller name takes you to the **APs/Devices > List** page.

Figure 190 and Table 138 illustrate and describe the **Reports > Generated > IDS Events Detail** page.

Figure 190 ***Reports > Generated > IDS Events*** *Report Illustration*

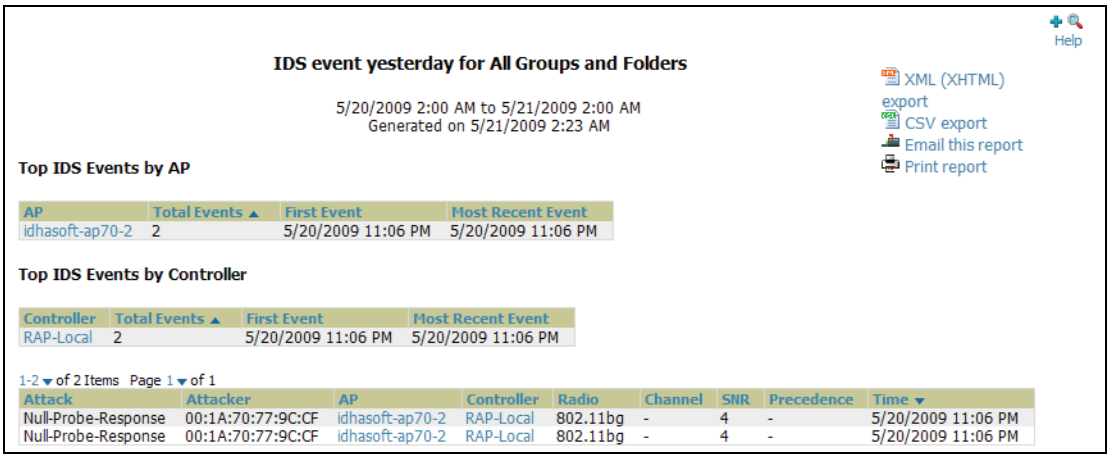


Table 138 ***Reports > Generated > IDS Events Detail*** *Fields*

Field	Description
AP	This column lists the AP devices for which IDS events have occurred in the prior 24 hours, and provides a link to the **APs/Devices > Monitor** page for each.
Total Events	This column cites the total number of IDS events for each device that has experienced them during the prior 24-hour period.
First Event	This column cites the first IDS event in the prior 24-hour period.
Most Recent Event	This column cites the most recent or latest IDS event in the prior 24-hour period.
Attack	Displays the name or label for the IDS event.
Controller	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:

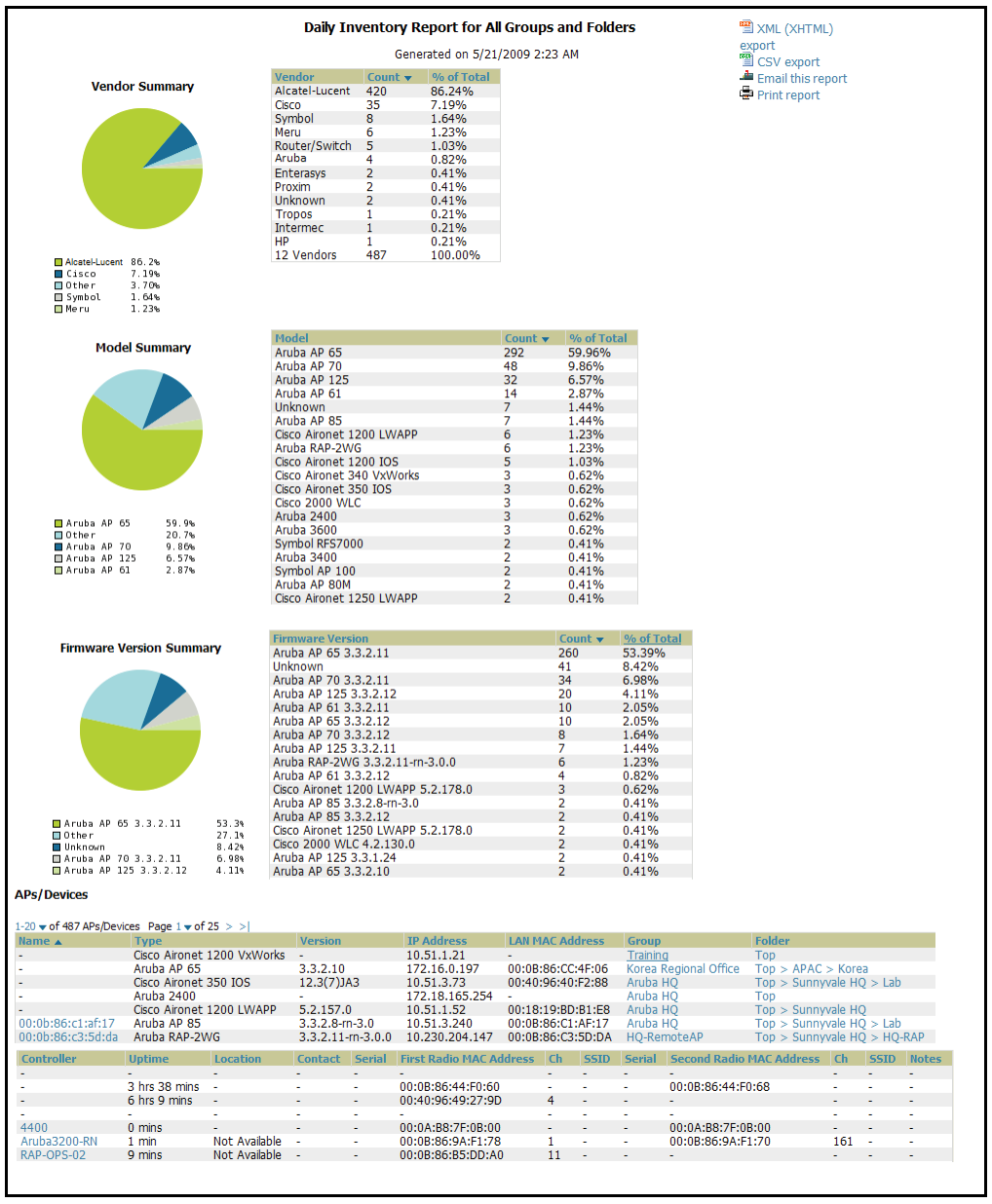
- **Vendor Summary**—Lists the vendors for all devices or firmware on the network.

- **Model Summary**—Lists the model numbers for all devices or firmware on the network.
- **Firmware Version Summary**—Lists the firmware version for all firmware used on the network.
- **APs/Devices**—Lists all devices on the network.

Perform these steps to view the most recent version of the **Inventory** report, illustrated in Figure 191

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Daily Inventory Report** to display report **Detail** information.
3. The **Detail** page allows you to view device or other information by clicking the device name, IP address, MAC Address, Group, Folder, or associated controller links.

Figure 191 ***Reports > Generated > Inventory*** *Report Illustration (Split View)*



Using the Memory and CPU Usage Report

The **Memory and CPU Usage Report** displays the top memory usage by device, and CPU usage on the network by device. The usage for any given resource, whether CPU or RAM usage, is listed as a percentage.

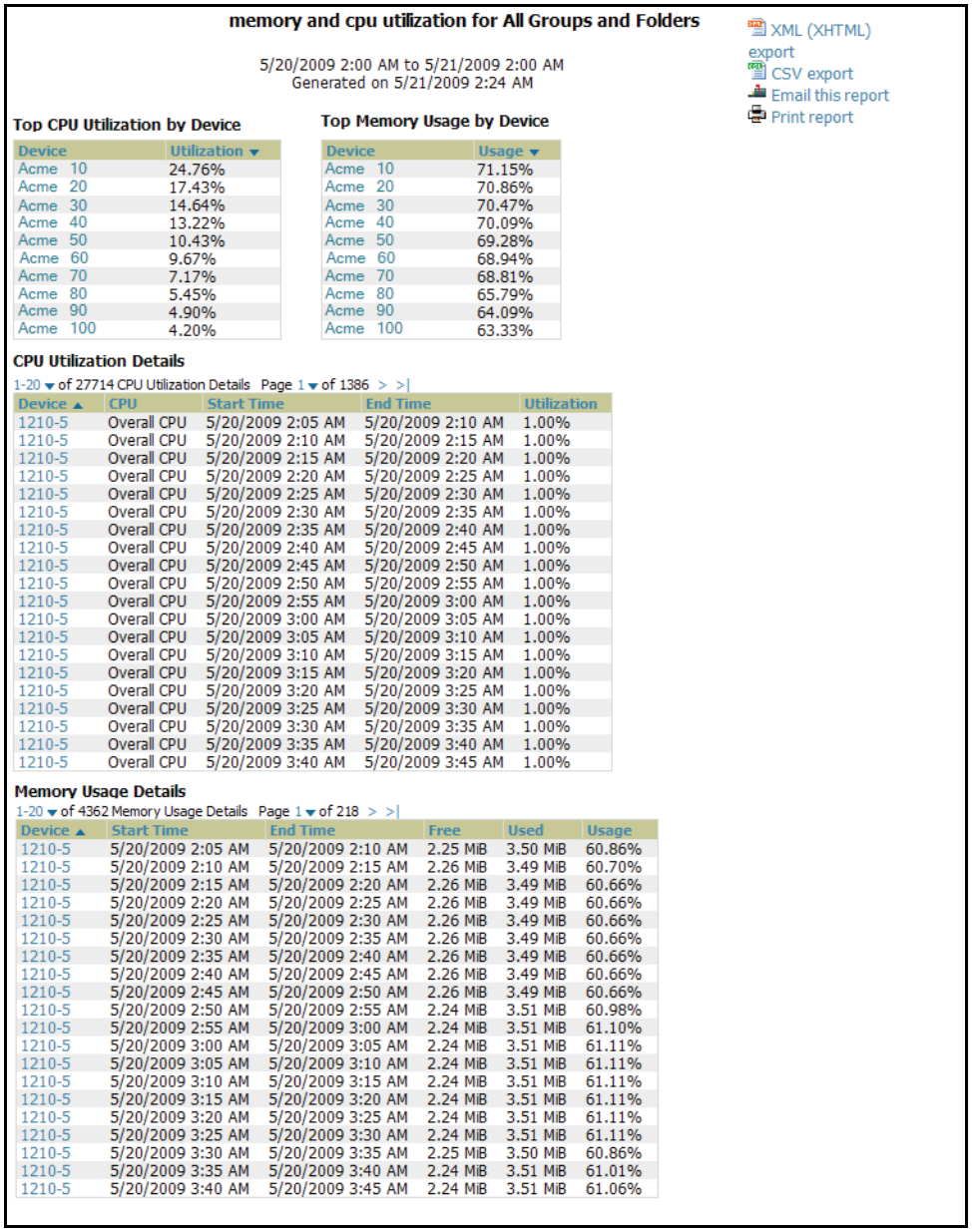
To create a scheduled and generated report of this type, refer to "Using Daily Reports" on page 272.

Perform these steps to view the most recent version of the **Memory and CPU Usage Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Daily Memory and CPU Usage** to display report **Detail** information.
3. The **Detail** page allows you to view device or other information by clicking the device name, IP address, MAC Address, Group, Folder, or associated controller links.

Figure 192 illustrates the **Reports > Generated > Daily Memory and CPU Usage Detail** page.

Figure 192 ***Reports > Generated > Daily Memory and CPU Usage*** *Report Illustration (Contents Rearranged for Space)*



memory and cpu utilization for All Groups and Folders

5/20/2009 2:00 AM to 5/21/2009 2:00 AM
Generated on 5/21/2009 2:24 AM

XML (XHTML) export
CSV export
Email this report
Print report

Top CPU Utilization by Device

Device	Utilization
Acme 10	24.76%
Acme 20	17.43%
Acme 30	14.64%
Acme 40	13.22%
Acme 50	10.43%
Acme 60	9.67%
Acme 70	7.17%
Acme 80	5.45%
Acme 90	4.90%
Acme 100	4.20%

Top Memory Usage by Device

Device	Usage
Acme 10	71.15%
Acme 20	70.86%
Acme 30	70.47%
Acme 40	70.09%
Acme 50	69.28%
Acme 60	68.94%
Acme 70	68.81%
Acme 80	65.79%
Acme 90	64.09%
Acme 100	63.33%

CPU Utilization Details

1-20 of 27714 CPU Utilization Details Page 1 of 1386 > >|

Device	CPU	Start Time	End Time	Utilization
1210-5	Overall CPU	5/20/2009 2:05 AM	5/20/2009 2:10 AM	1.00%
1210-5	Overall CPU	5/20/2009 2:10 AM	5/20/2009 2:15 AM	1.00%
1210-5	Overall CPU	5/20/2009 2:15 AM	5/20/2009 2:20 AM	1.00%
1210-5	Overall CPU	5/20/2009 2:20 AM	5/20/2009 2:25 AM	1.00%
1210-5	Overall CPU	5/20/2009 2:25 AM	5/20/2009 2:30 AM	1.00%
1210-5	Overall CPU	5/20/2009 2:30 AM	5/20/2009 2:35 AM	1.00%
1210-5	Overall CPU	5/20/2009 2:35 AM	5/20/2009 2:40 AM	1.00%
1210-5	Overall CPU	5/20/2009 2:40 AM	5/20/2009 2:45 AM	1.00%
1210-5	Overall CPU	5/20/2009 2:45 AM	5/20/2009 2:50 AM	1.00%
1210-5	Overall CPU	5/20/2009 2:50 AM	5/20/2009 2:55 AM	1.00%
1210-5	Overall CPU	5/20/2009 2:55 AM	5/20/2009 3:00 AM	1.00%
1210-5	Overall CPU	5/20/2009 3:00 AM	5/20/2009 3:05 AM	1.00%
1210-5	Overall CPU	5/20/2009 3:05 AM	5/20/2009 3:10 AM	1.00%
1210-5	Overall CPU	5/20/2009 3:10 AM	5/20/2009 3:15 AM	1.00%
1210-5	Overall CPU	5/20/2009 3:15 AM	5/20/2009 3:20 AM	1.00%
1210-5	Overall CPU	5/20/2009 3:20 AM	5/20/2009 3:25 AM	1.00%
1210-5	Overall CPU	5/20/2009 3:25 AM	5/20/2009 3:30 AM	1.00%
1210-5	Overall CPU	5/20/2009 3:30 AM	5/20/2009 3:35 AM	1.00%
1210-5	Overall CPU	5/20/2009 3:35 AM	5/20/2009 3:40 AM	1.00%
1210-5	Overall CPU	5/20/2009 3:40 AM	5/20/2009 3:45 AM	1.00%

Memory Usage Details

1-20 of 4362 Memory Usage Details Page 1 of 218 > >|

Device	Start Time	End Time	Free	Used	Usage
1210-5	5/20/2009 2:05 AM	5/20/2009 2:10 AM	2.25 MiB	3.50 MiB	60.86%
1210-5	5/20/2009 2:10 AM	5/20/2009 2:15 AM	2.26 MiB	3.49 MiB	60.70%
1210-5	5/20/2009 2:15 AM	5/20/2009 2:20 AM	2.26 MiB	3.49 MiB	60.66%
1210-5	5/20/2009 2:20 AM	5/20/2009 2:25 AM	2.26 MiB	3.49 MiB	60.66%
1210-5	5/20/2009 2:25 AM	5/20/2009 2:30 AM	2.26 MiB	3.49 MiB	60.66%
1210-5	5/20/2009 2:30 AM	5/20/2009 2:35 AM	2.26 MiB	3.49 MiB	60.66%
1210-5	5/20/2009 2:35 AM	5/20/2009 2:40 AM	2.26 MiB	3.49 MiB	60.66%
1210-5	5/20/2009 2:40 AM	5/20/2009 2:45 AM	2.26 MiB	3.49 MiB	60.66%
1210-5	5/20/2009 2:45 AM	5/20/2009 2:50 AM	2.26 MiB	3.49 MiB	60.66%
1210-5	5/20/2009 2:50 AM	5/20/2009 2:55 AM	2.24 MiB	3.51 MiB	60.98%
1210-5	5/20/2009 2:55 AM	5/20/2009 3:00 AM	2.24 MiB	3.51 MiB	61.10%
1210-5	5/20/2009 3:00 AM	5/20/2009 3:05 AM	2.24 MiB	3.51 MiB	61.11%
1210-5	5/20/2009 3:05 AM	5/20/2009 3:10 AM	2.24 MiB	3.51 MiB	61.11%
1210-5	5/20/2009 3:10 AM	5/20/2009 3:15 AM	2.24 MiB	3.51 MiB	61.11%
1210-5	5/20/2009 3:15 AM	5/20/2009 3:20 AM	2.24 MiB	3.51 MiB	61.11%
1210-5	5/20/2009 3:20 AM	5/20/2009 3:25 AM	2.24 MiB	3.51 MiB	61.11%
1210-5	5/20/2009 3:25 AM	5/20/2009 3:30 AM	2.24 MiB	3.51 MiB	61.11%
1210-5	5/20/2009 3:30 AM	5/20/2009 3:35 AM	2.25 MiB	3.50 MiB	60.86%
1210-5	5/20/2009 3:35 AM	5/20/2009 3:40 AM	2.24 MiB	3.51 MiB	61.01%
1210-5	5/20/2009 3:40 AM	5/20/2009 3:45 AM	2.24 MiB	3.51 MiB	61.06%

Using the Network Usage Report

The **Network Usage Report** contains network-wide information in three categories:

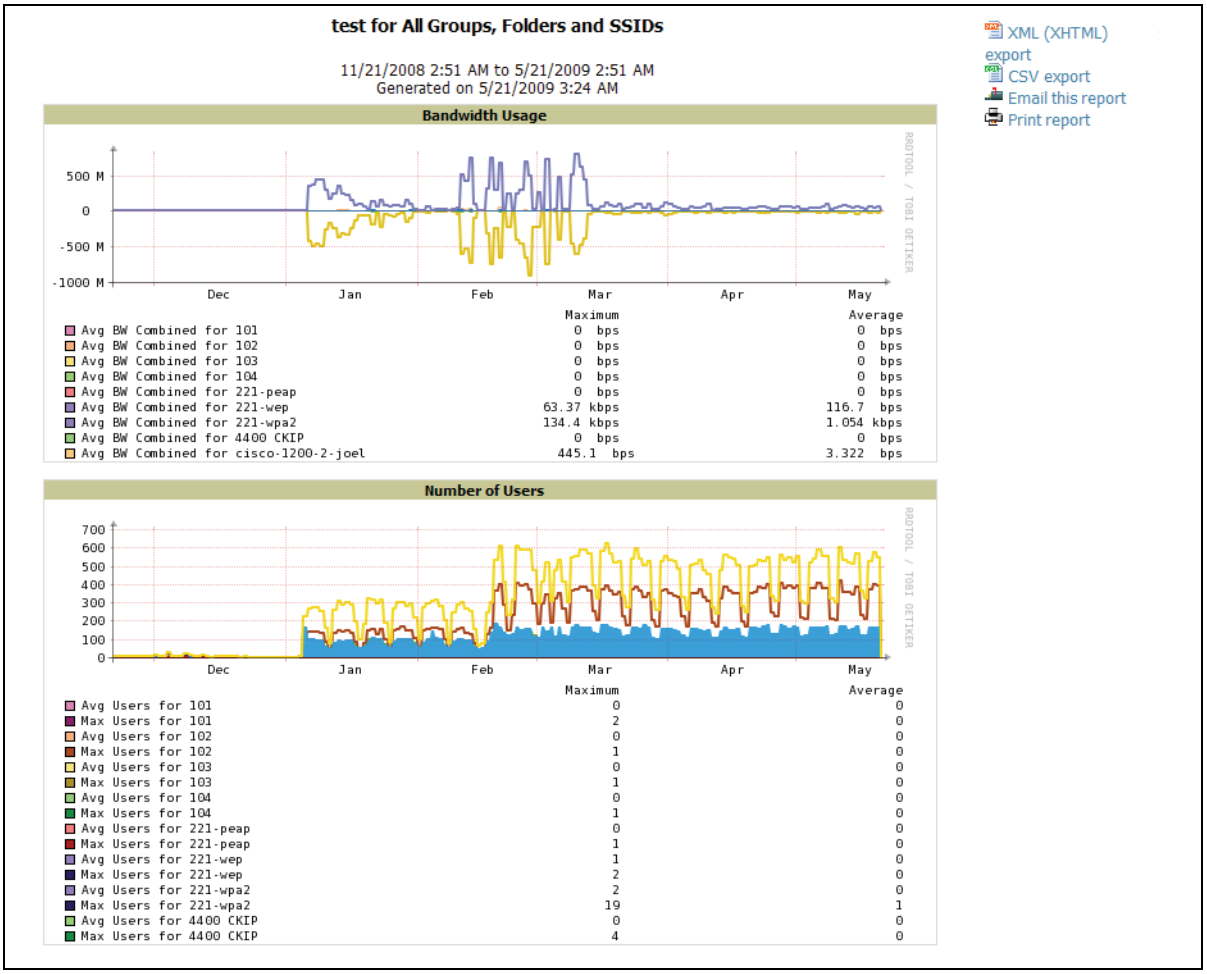
- **Bandwidth usage by device**—maximum and average bandwidth in kbps
- **Number of users by device**—maximum and average by connection instances
- **Number of users by time period**—average bandwidth in and out

Perform these steps to view the most recent version of the **Network Usage Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Network Usage** to display report **Detail** information.
3. The **Detail** page allows you to view bandwidth and device usage in three sections, illustrated below.

Figure 193 illustrates the **Reports > Generated > Daily Memory and CPU Usage Detail** page.

Figure 193 ***Reports > Generated > Network Usage*** *Report Illustration (Partial Example)*



Using the New Rogue Devices Report

The **New Rogue Devices Report** summarizes rogue device information in a number of ways, to include the following categories of information:

- Rogue devices by RAPIDS classification—described in "Using RAPIDS and Rogue Classification" on page 205
- 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

Perform these steps to view the most recent version of the **New Rogue Devices Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **New Rogue Devices** to display report **Detail** information.
3. The **Detail** page allows you to view bandwidth and device usage in multiple sections, illustrated below. Several figures below illustrate the multiple fields and information in the **New Rogue Devices Report**.

Figure 194 ***Reports > Generated > New Rogue Devices*** *Report Illustration, Top Half of Report*

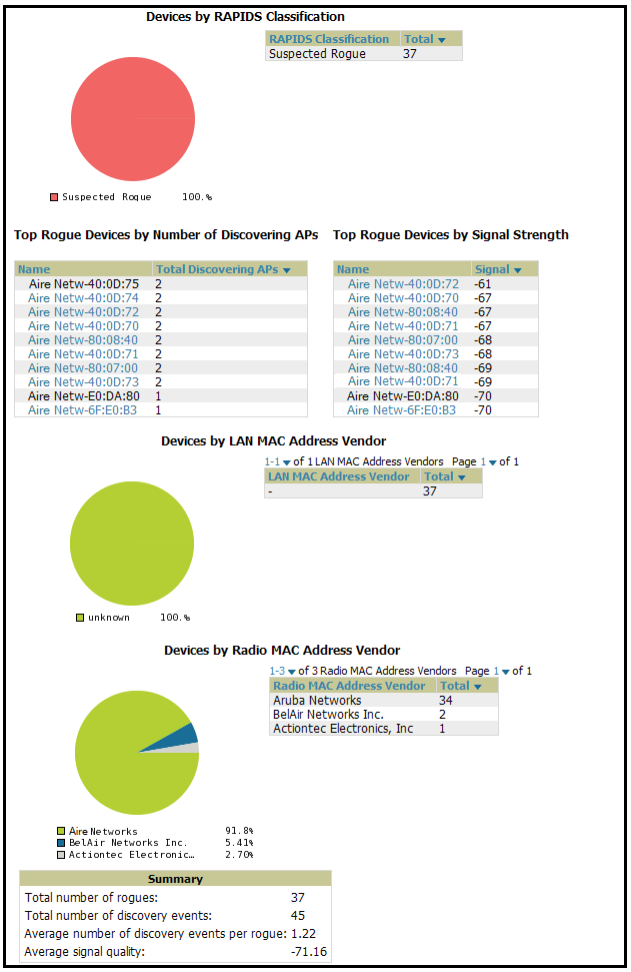
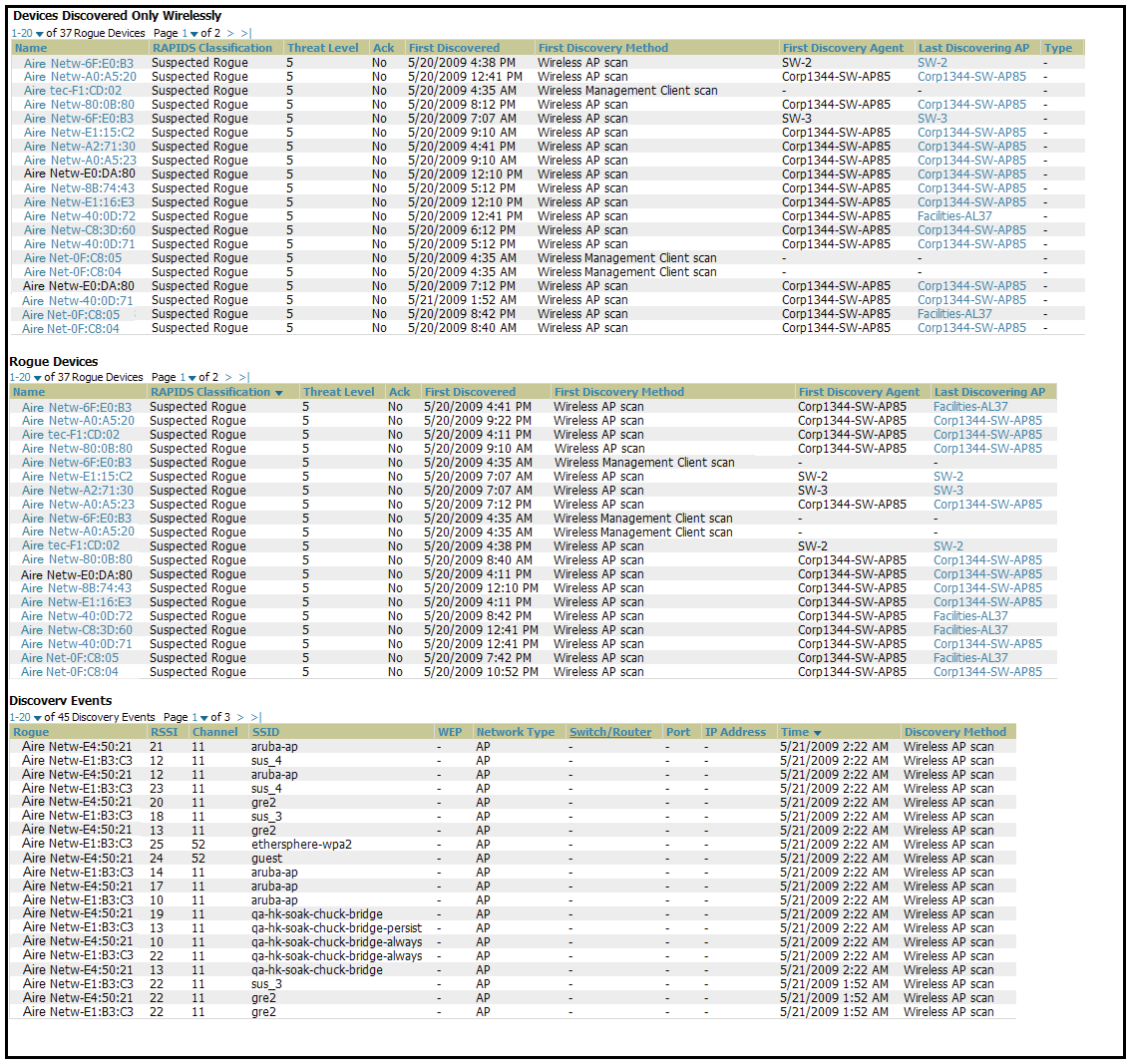


Figure 195 ***Reports > Generated > New Rogue Devices*** *Report Illustration, Bottom Half of Report (Partial View)*



Devices Discovered Only Wirelessly

1-20 of 37 Rogue Devices Page 1 of 2 > >|

Name	RAPIDS Classification	Threat Level	Ack	First Discovered	First Discovery Method	First Discovery Agent	Last Discovering AP	Type
Aire Netw-6F:E0:B3	Suspected Rogue	5	No	5/20/2009 4:38 PM	Wireless AP scan	SW-2	SW-2	-
Aire Netw-A0:A5:20	Suspected Rogue	5	No	5/20/2009 12:41 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire tec-F1:CD:02	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-	-
Aire Netw-80:0B:80	Suspected Rogue	5	No	5/20/2009 8:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Netw-6F:E0:B3	Suspected Rogue	5	No	5/20/2009 7:07 AM	Wireless AP scan	SW-3	SW-3	-
Aire Netw-E1:15:C2	Suspected Rogue	5	No	5/20/2009 9:10 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Netw-A2:71:30	Suspected Rogue	5	No	5/20/2009 4:41 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Netw-A0:A5:23	Suspected Rogue	5	No	5/20/2009 9:10 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Netw-E0:DA:80	Suspected Rogue	5	No	5/20/2009 12:10 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Netw-8B:74:43	Suspected Rogue	5	No	5/20/2009 5:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Netw-E1:16:E3	Suspected Rogue	5	No	5/20/2009 12:10 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Netw-40:0D:72	Suspected Rogue	5	No	5/20/2009 12:41 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37	-
Aire Netw-C8:3D:60	Suspected Rogue	5	No	5/20/2009 6:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Netw-40:0D:71	Suspected Rogue	5	No	5/20/2009 5:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Net-0F:C8:05	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-	-
Aire Net-0F:C8:04	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-	-
Aire Netw-E0:DA:80	Suspected Rogue	5	No	5/20/2009 7:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Netw-40:0D:71	Suspected Rogue	5	No	5/21/2009 1:52 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-
Aire Net-0F:C8:05	Suspected Rogue	5	No	5/20/2009 8:42 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37	-
Aire Net-0F:C8:04	Suspected Rogue	5	No	5/20/2009 8:40 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-

Rogue Devices

1-20 of 37 Rogue Devices Page 1 of 2 > >|

Name	RAPIDS Classification	Threat Level	Ack	First Discovered	First Discovery Method	First Discovery Agent	Last Discovering AP
Aire Netw-6F:E0:B3	Suspected Rogue	5	No	5/20/2009 4:41 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37
Aire Netw-A0:A5:20	Suspected Rogue	5	No	5/20/2009 9:22 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85
Aire tec-F1:CD:02	Suspected Rogue	5	No	5/20/2009 4:11 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85
Aire Netw-80:0B:80	Suspected Rogue	5	No	5/20/2009 9:10 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85
Aire Netw-6F:E0:B3	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-
Aire Netw-E1:15:C2	Suspected Rogue	5	No	5/20/2009 7:07 AM	Wireless AP scan	SW-2	SW-2
Aire Netw-A2:71:30	Suspected Rogue	5	No	5/20/2009 7:07 AM	Wireless AP scan	SW-3	SW-3
Aire Netw-A0:A5:23	Suspected Rogue	5	No	5/20/2009 7:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85
Aire Netw-6F:E0:B3	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-
Aire Netw-A0:A5:20	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-
Aire tec-F1:CD:02	Suspected Rogue	5	No	5/20/2009 4:38 PM	Wireless AP scan	SW-2	SW-2
Aire Netw-80:0B:80	Suspected Rogue	5	No	5/20/2009 8:40 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85
Aire Netw-E0:DA:80	Suspected Rogue	5	No	5/20/2009 4:11 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85
Aire Netw-8B:74:43	Suspected Rogue	5	No	5/20/2009 12:10 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85
Aire Netw-E1:16:E3	Suspected Rogue	5	No	5/20/2009 4:11 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85
Aire Netw-40:0D:72	Suspected Rogue	5	No	5/20/2009 8:42 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37
Aire Netw-C8:3D:60	Suspected Rogue	5	No	5/20/2009 12:41 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37
Aire Netw-40:0D:71	Suspected Rogue	5	No	5/20/2009 12:41 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85
Aire Net-0F:C8:05	Suspected Rogue	5	No	5/20/2009 7:42 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37
Aire Net-0F:C8:04	Suspected Rogue	5	No	5/20/2009 10:52 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85

Discovery Events

1-20 of 45 Discovery Events Page 1 of 3 > >|

Rogue	RSSI	Channel	SSID	WEP	Network Type	Switch/Router	Port	IP Address	Time	Discovery Method
Aire Netw-E4:50:21	21	11	aruba-ap	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	12	11	sus_4	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	12	11	aruba-ap	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	23	11	sus_4	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	20	11	gre2	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	18	11	sus_3	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	13	11	gre2	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	25	52	ethersphere-wpa2	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	24	52	guest	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	14	11	aruba-ap	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	17	11	aruba-ap	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	10	11	aruba-ap	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	19	11	qa-hk-soak-chuck-bridge	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	13	11	qa-hk-soak-chuck-bridge-persist	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	10	11	qa-hk-soak-chuck-bridge-always	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	22	11	qa-hk-soak-chuck-bridge-always	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	13	11	qa-hk-soak-chuck-bridge	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	22	11	sus_3	-	AP	-	-	-	5/21/2009 1:52 AM	Wireless AP scan
Aire Netw-E4:50:21	22	11	gre2	-	AP	-	-	-	5/21/2009 1:52 AM	Wireless AP scan
Aire Netw-E1:B3:C3	22	11	gre2	-	AP	-	-	-	5/21/2009 1:52 AM	Wireless AP scan

The rogue device inventories that comprise this report contain many fields, described in Table 139.

Table 139 ***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 205 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 205 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.

Table 139 ***New Rogue Devices*** *Report Fields (Continued)*

Field	Description
Last Discovering AP	Displays the network device that most recently discovered the rogue device.
Type	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 Wired Equivalent Privacy (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

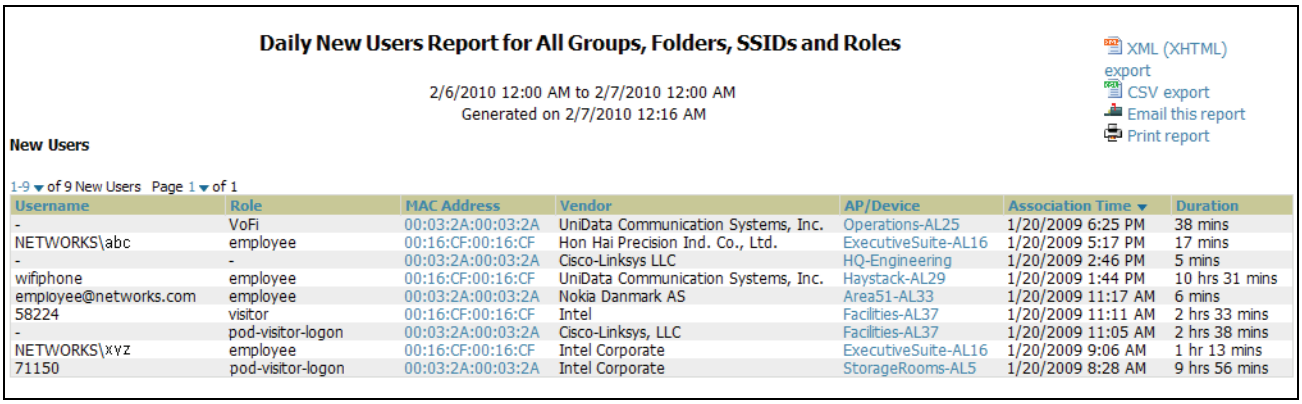
The **New Users Report** lists all new users that have appeared on the network during the time duration defined for the report. This report covers the user identifier, the associated role when known, device information and more.

Perform these steps to view the most recent version of the **New Users Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **New Users** to display report **Detail** information.
3. The **Detail** page allows you to view information for new users that have appeared on the network during the time period defined for the report.

Figure 196 illustrates the fields and information in the **New Users Report**.

Figure 196 ***Reports > Generated > New Users Report*** *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

XML (XHTML) export
CSV export
Email this report
Print report

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 mins
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 mins
-	pod-visitor-logon	00:03:2A:00:03:2A	Cisco-Linksys, LLC	Facilities-AL37	1/20/2009 11:05 AM	2 hrs 38 mins
NETWORKS\xyz	employee	00:16:CF:00:16:CF	Intel Corporate	ExecutiveSuite-AL16	1/20/2009 9:06 AM	1 hr 13 mins
71150	pod-visitor-logon	00:03:2A:00:03:2A	Intel Corporate	StorageRooms-AL5	1/20/2009 8:28 AM	9 hrs 56 mins

Table 140 ***Reports > Generated > New Users*** *Report Fields*

Field	Description
Username	Displays the username when known.
Role	Displays the role with which the user is associated.
MAC Address	Displays the MAC address of the AP device by which the user connected.
Vendor	Displays vendor information for the AP device by which the user connected.
AP/Device	Displays the device type by which the user connected.
Association Time	Displays the time in which the AP device associated with the controller.
Duration	Displays the duration of the user's connection.

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.

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.

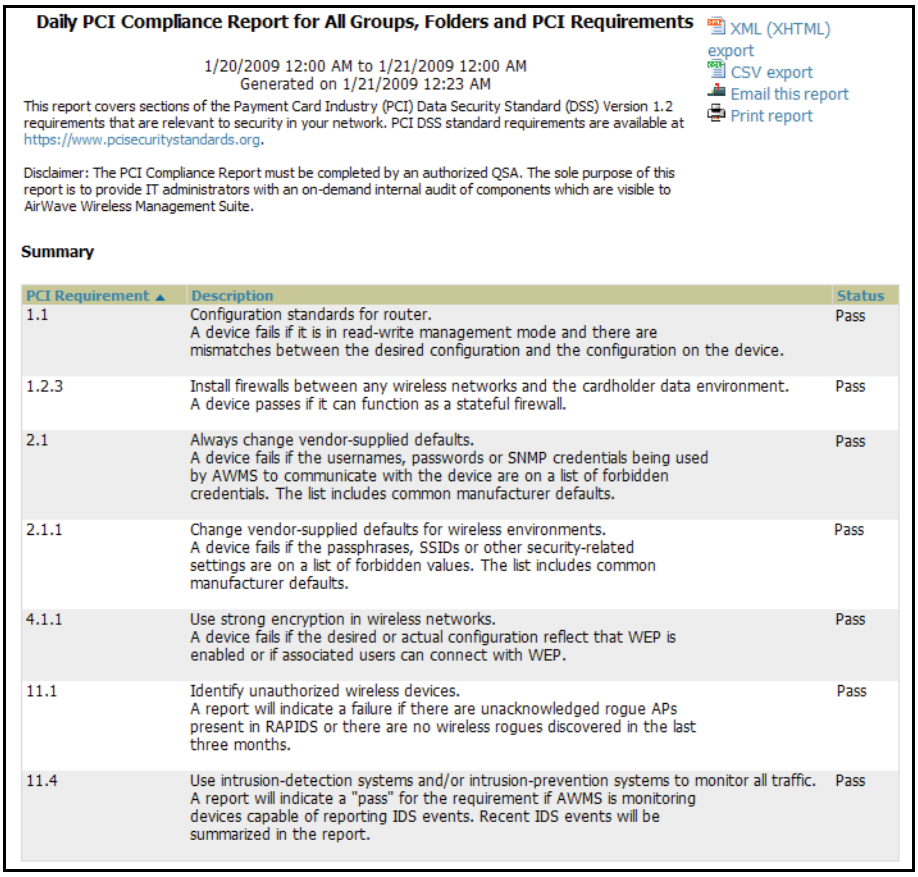
Refer to the "Auditing PCI Compliance on the Network" on page 76 for information about enabling PCI on the network. The configurations in that section enable or disable the contents of the PCI Compliance Report that is viewable on the **Reports > Generated** page.

Perform these steps to view the most recent version of the **PCI Compliance Report**.

1. Verify that OV3600 is enabled to monitor compliance with PCI requirements, as described in the "Enabling or Disabling PCI Auditing" on page 78.
2. Navigate to the **Reports > Generated** page.
3. Scroll to the bottom, and click **PCI Compliance** to display **Detail** information.

Figure 197 illustrates the fields and information in the most recent **PCI Compliance Report**.

Figure 197 ***Reports > Generated > PCI Compliance Report*** *Illustration, Pass or Fail Example*



Daily PCI Compliance Report for All Groups, Folders and PCI Requirements

XML (XHTML) export
CSV export
Email this report
Print report

1/20/2009 12:00 AM to 1/21/2009 12:00 AM
Generated on 1/21/2009 12:23 AM

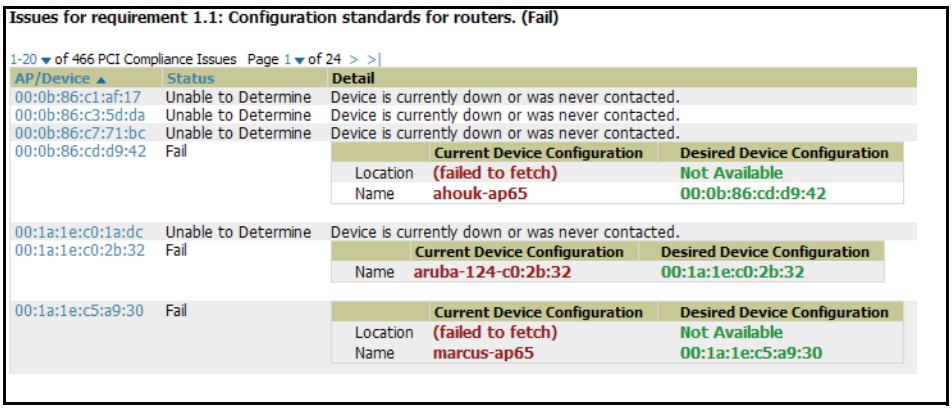
This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.2 requirements that are relevant to security in your network. PCI DSS standard requirements are available at https://www.pcisecuritystandards.org.

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

Figure 198 ***Reports > Generated > PCI Compliance Report*** *Illustration, Diagnostics Example*



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

1-20 ▾ of 466 PCI Compliance Issues Page 1 ▾ of 24 > >|

AP/Device ▲	Status	Detail
00:0b:86:c1:af:17	Unable to Determine	Device is currently down or was never contacted.
00:0b:86:c3:5d:da	Unable to Determine	Device is currently down or was never contacted.
00:0b:86:c7:71:bc	Unable to Determine	Device is currently down or was never contacted.
00:0b:86:cd:d9:42	Fail	Current Device Configuration / Desired Device Configuration Location: (failed to fetch) / Not Available Name: ahouk-ap65 / 00:0b:86:cd:d9:42
00:1a:1e:c0:1a:dc	Unable to Determine	Device is currently down or was never contacted.
00:1a:1e:c0:2b:32	Fail	Current Device Configuration / Desired Device Configuration Name: aruba-124-c0:2b:32 / 00:1a:1e:c0:2b:32
00:1a:1e:c5:a9:30	Fail	Current Device Configuration / Desired Device Configuration Location: (failed to fetch) / Not Available Name: marcus-ap65 / 00:1a:1e:c5:a9:30

Using the Port Usage Report

You can generate a wide array of port usage statistics from the **Port Usage Report** feature, including each of the following:

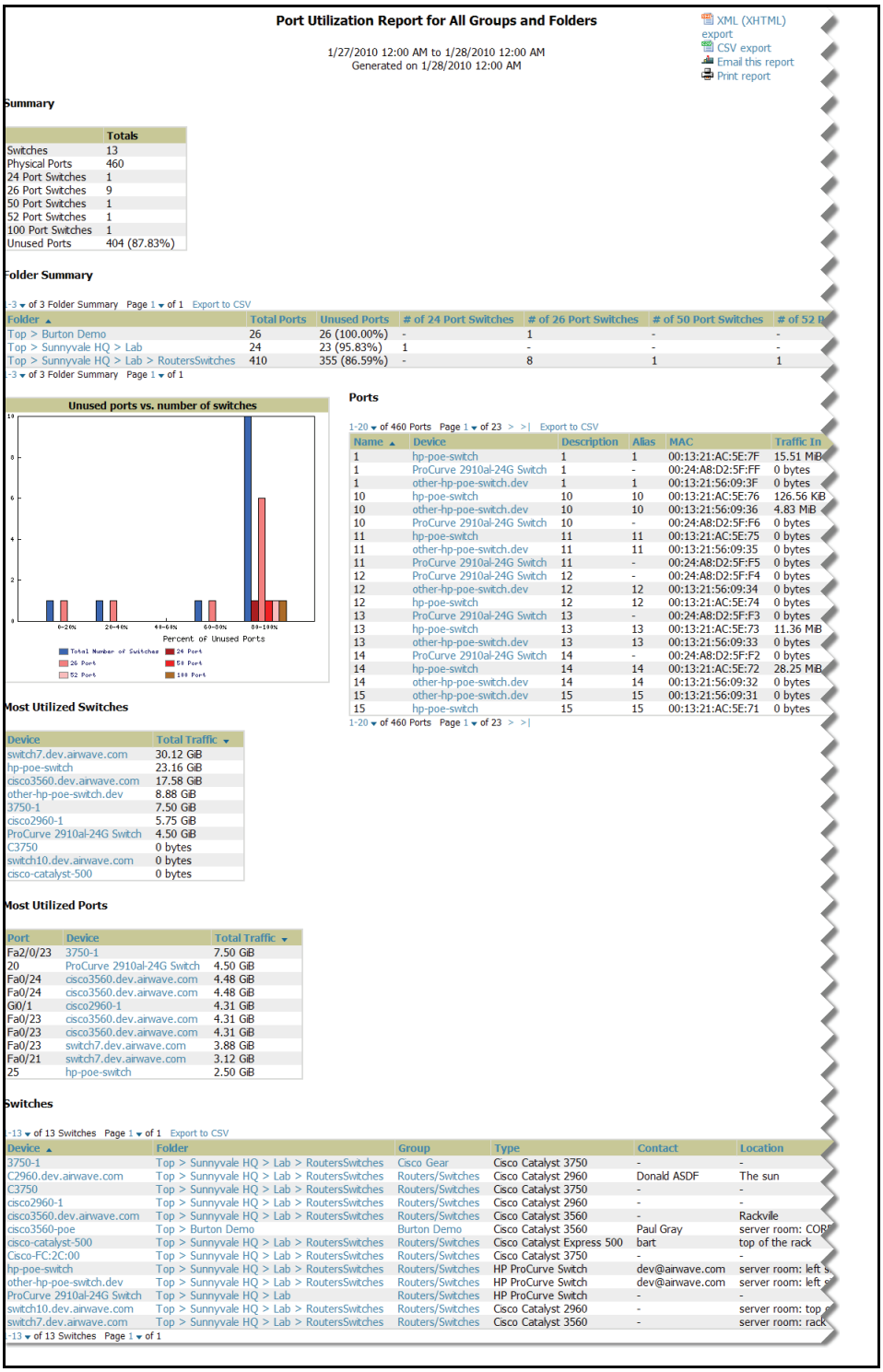
- list of all the switches and ports in your network by folder
- list of unused ports
- list of access and distribution ports
- histogram displaying unused ports vs. unused switches by type (access or distribution)
- list of most used switches
- list of most used ports

Perform these steps to view the most recent version of the **Port Usage Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Port Usage Report** to display report **Detail** information.
3. The **Detail** page allows you to view all the information you selected from the **Port Usage** area of the **Reports > Definitions** page.

A sample of the types of information you might choose to generate in a **Port Usage Report** Figure 199.

Figure 199 ***Reports > Generated > Port Usage Report*** *Detail Page (partial view)*



Port Utilization Report for All Groups and Folders

1/27/2010 12:00 AM to 1/28/2010 12:00 AM
Generated on 1/28/2010 12:00 AM

XML (XHTML) export
CSV export
Email this report
Print report

Summary

	Totals
Switches	13
Physical Ports	460
24 Port Switches	1
26 Port Switches	9
50 Port Switches	1
52 Port Switches	1
100 Port Switches	1
Unused Ports	404 (87.83%)

Folder Summary

-3 of 3 Folder Summary Page 1 of 1 Export to CSV

Folder	Total Ports	Unused Ports	# of 24 Port Switches	# of 26 Port Switches	# of 50 Port Switches	# of 52 P
Top > Burton Demo	26	26 (100.00%)	-	1	-	-
Top > Sunnyvale HQ > Lab	24	23 (95.83%)	1	-	-	-
Top > Sunnyvale HQ > Lab > RoutersSwitches	410	355 (86.59%)	-	8	1	1

-3 of 3 Folder Summary Page 1 of 1

Unused ports vs. number of switches

Ports

1-20 of 460 Ports Page 1 of 23 > >| Export to CSV

Name	Device	Description	Alias	MAC	Traffic In
1	hp-poe-switch	1	1	00:13:21:AC:5E:7F	15.51 MiB
1	ProCurve 2910al-24G Switch	1	-	00:24:A8:D2:5F:FF	0 bytes
1	other-hp-poe-switch.dev	1	1	00:13:21:56:09:3F	0 bytes
10	hp-poe-switch	10	10	00:13:21:AC:5E:76	126.56 KiB
10	other-hp-poe-switch.dev	10	10	00:13:21:56:09:36	4.83 MiB
10	ProCurve 2910al-24G Switch	10	-	00:24:A8:D2:5F:F6	0 bytes
11	hp-poe-switch	11	11	00:13:21:AC:5E:75	0 bytes
11	other-hp-poe-switch.dev	11	11	00:13:21:56:09:35	0 bytes
11	ProCurve 2910al-24G Switch	11	-	00:24:A8:D2:5F:F5	0 bytes
12	ProCurve 2910al-24G Switch	12	-	00:24:A8:D2:5F:F4	0 bytes
12	other-hp-poe-switch.dev	12	12	00:13:21:56:09:34	0 bytes
12	hp-poe-switch	12	12	00:13:21:AC:5E:74	0 bytes
13	ProCurve 2910al-24G Switch	13	-	00:24:A8:D2:5F:F3	0 bytes
13	hp-poe-switch	13	13	00:13:21:AC:5E:73	11.36 MiB
13	other-hp-poe-switch.dev	13	13	00:13:21:56:09:33	0 bytes
14	ProCurve 2910al-24G Switch	14	-	00:24:A8:D2:5F:F2	0 bytes
14	hp-poe-switch	14	14	00:13:21:AC:5E:72	28.25 MiB
14	other-hp-poe-switch.dev	14	14	00:13:21:56:09:32	0 bytes
15	other-hp-poe-switch.dev	15	15	00:13:21:56:09:31	0 bytes
15	hp-poe-switch	15	15	00:13:21:AC:5E:71	0 bytes

1-20 of 460 Ports Page 1 of 23 > >|

Most Utilized Switches

Device	Total Traffic
switch7.dev.airwave.com	30.12 GiB
hp-poe-switch	23.16 GiB
cisco3560.dev.airwave.com	17.58 GiB
other-hp-poe-switch.dev	8.88 GiB
3750-1	7.50 GiB
cisco2960-1	5.75 GiB
ProCurve 2910al-24G Switch	4.50 GiB
C3750	0 bytes
switch10.dev.airwave.com	0 bytes
cisco-catalyst-500	0 bytes

Most Utilized Ports

Port	Device	Total Traffic
Fa2/0/23	3750-1	7.50 GiB
20	ProCurve 2910al-24G Switch	4.50 GiB
Fa0/24	cisco3560.dev.airwave.com	4.48 GiB
Fa0/24	cisco3560.dev.airwave.com	4.48 GiB
Gi0/1	cisco2960-1	4.31 GiB
Fa0/23	cisco3560.dev.airwave.com	4.31 GiB
Fa0/23	cisco3560.dev.airwave.com	4.31 GiB
Fa0/23	switch7.dev.airwave.com	3.88 GiB
Fa0/21	switch7.dev.airwave.com	3.12 GiB
25	hp-poe-switch	2.50 GiB

Switches

-13 of 13 Switches Page 1 of 1 Export to CSV

Device	Folder	Group	Type	Contact	Location
3750-1	Top > Sunnyvale HQ > Lab > RoutersSwitches	Cisco Gear	Cisco Catalyst 3750	-	-
C2960.dev.airwave.com	Top > Sunnyvale HQ > Lab > RoutersSwitches	Routers/Switches	Cisco Catalyst 2960	Donald ASDF	The sun
C3750	Top > Sunnyvale HQ > Lab > RoutersSwitches	Routers/Switches	Cisco Catalyst 3750	-	-
cisco2960-1	Top > Sunnyvale HQ > Lab > RoutersSwitches	Routers/Switches	Cisco Catalyst 2960	-	-
cisco3560.dev.airwave.com	Top > Sunnyvale HQ > Lab > RoutersSwitches	Routers/Switches	Cisco Catalyst 3560	-	Rackville
cisco3560-poe	Top > Burton Demo	Burton Demo	Cisco Catalyst 3560	Paul Gray	server room: COR
cisco-catalyst-500	Top > Sunnyvale HQ > Lab > RoutersSwitches	Routers/Switches	Cisco Catalyst Express 500	bart	top of the rack
Cisco-FC:2C:00	Top > Sunnyvale HQ > Lab > RoutersSwitches	Routers/Switches	Cisco Catalyst 3750	-	-
hp-poe-switch	Top > Sunnyvale HQ > Lab > RoutersSwitches	Routers/Switches	HP ProCurve Switch	dev@airwave.com	server room: left s
other-hp-poe-switch.dev	Top > Sunnyvale HQ > Lab > RoutersSwitches	Routers/Switches	HP ProCurve Switch	dev@airwave.com	server room: left s
ProCurve 2910al-24G Switch	Top > Sunnyvale HQ > Lab	Routers/Switches	HP ProCurve Switch	-	-
switch10.dev.airwave.com	Top > Sunnyvale HQ > Lab > RoutersSwitches	Routers/Switches	Cisco Catalyst 2960	-	server room: top
switch7.dev.airwave.com	Top > Sunnyvale HQ > Lab > RoutersSwitches	Routers/Switches	Cisco Catalyst 3560	-	server room: rack

-13 of 13 Switches Page 1 of 1

Using the RADIUS Authentication Issues Report

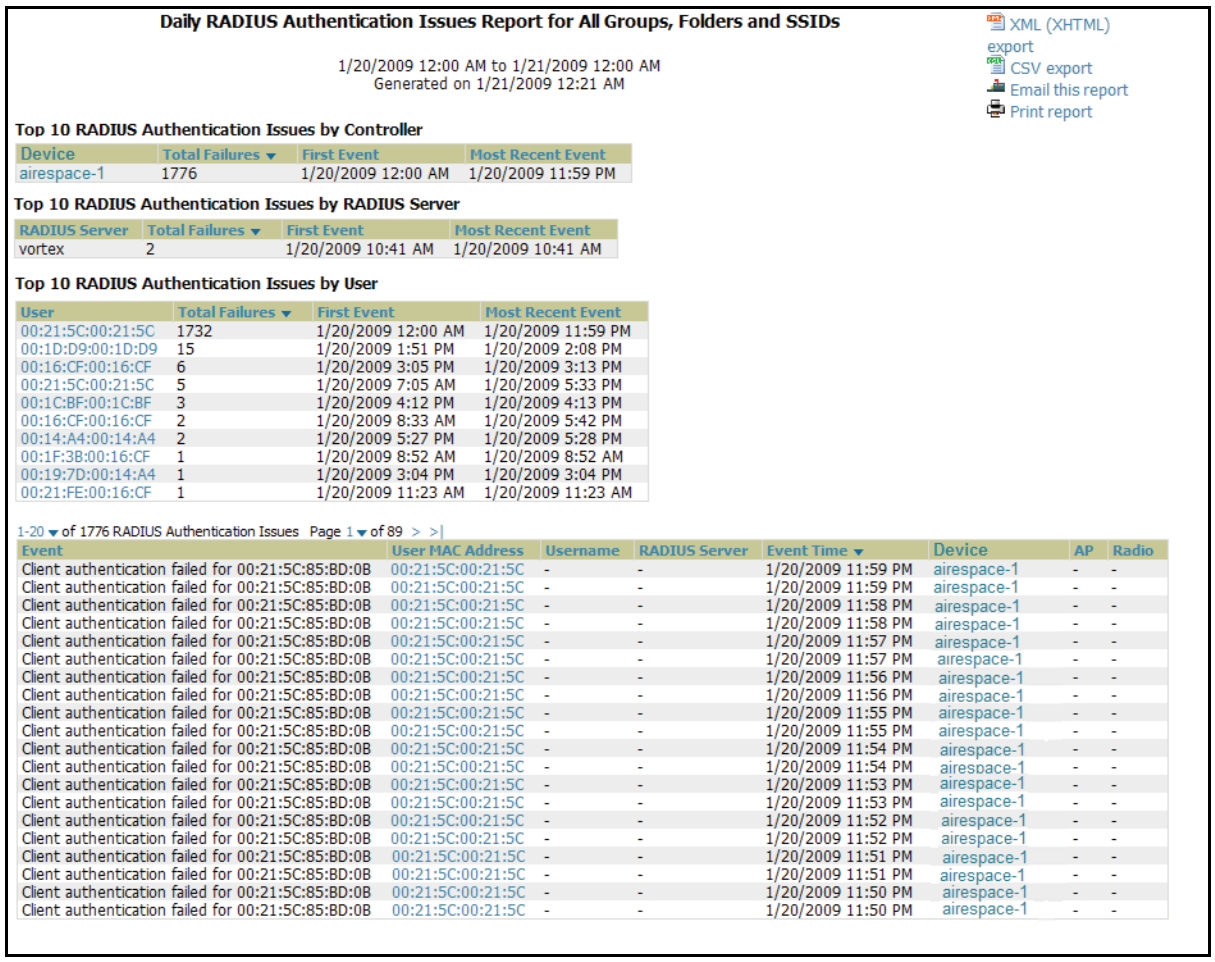
The **RADIUS Authentication Issues Report** contains issues that may appear with AP controllers, RADIUS Servers, and users.

Perform these steps to view the most recent version of the **RADIUS Authentication Issues Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **RADIUS Authentication Issues Report** to display report **Detail** information.
3. The **Detail** page allows you to view information for RADIUS issues that have appeared on the network during the time period defined for the report.

Figure 200 illustrates the fields and information in the **RADIUS Authentication Issues Report.**

Figure 200 ***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

XML (XHTML) export
CSV export
Email this report
Print report

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

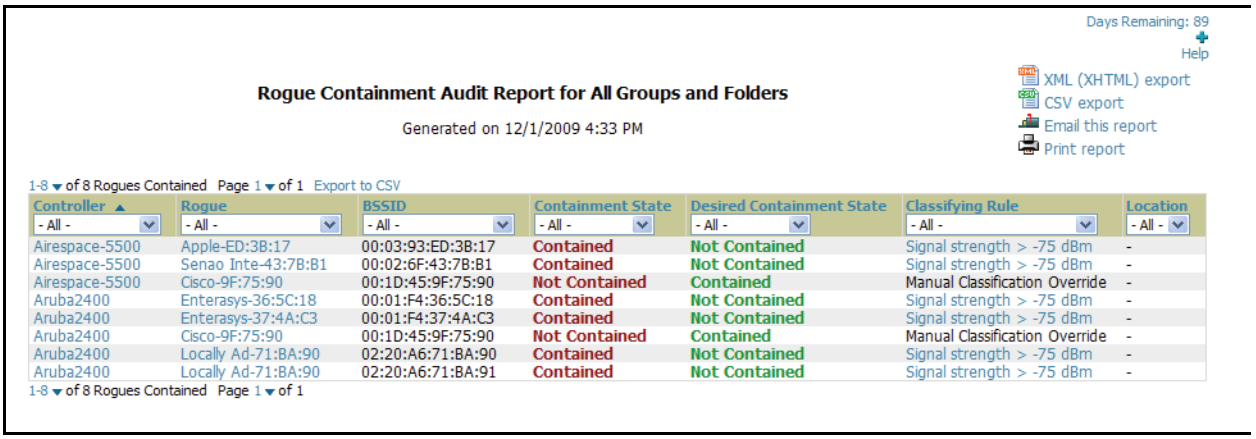
1-20 of 1776 RADIUS Authentication Issues Page 1 of 89 > >|

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	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:56 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:56 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:55 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:55 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:54 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:54 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:53 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:53 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:52 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:52 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:51 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:51 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:50 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:50 PM	airespace-1	-	-

Using the Rogue Containment Audit Report

The rogue containment audit report that lets you know if any containment is failing. Figure 201 illustrates the fields and information in this report type.

Figure 201 ***Reports > Generated > Rogue Containment Audit*** *Detail Page Illustration*



Days Remaining: 89
Help
XML (XHTML) export
CSV export
Email this report
Print report

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** 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:

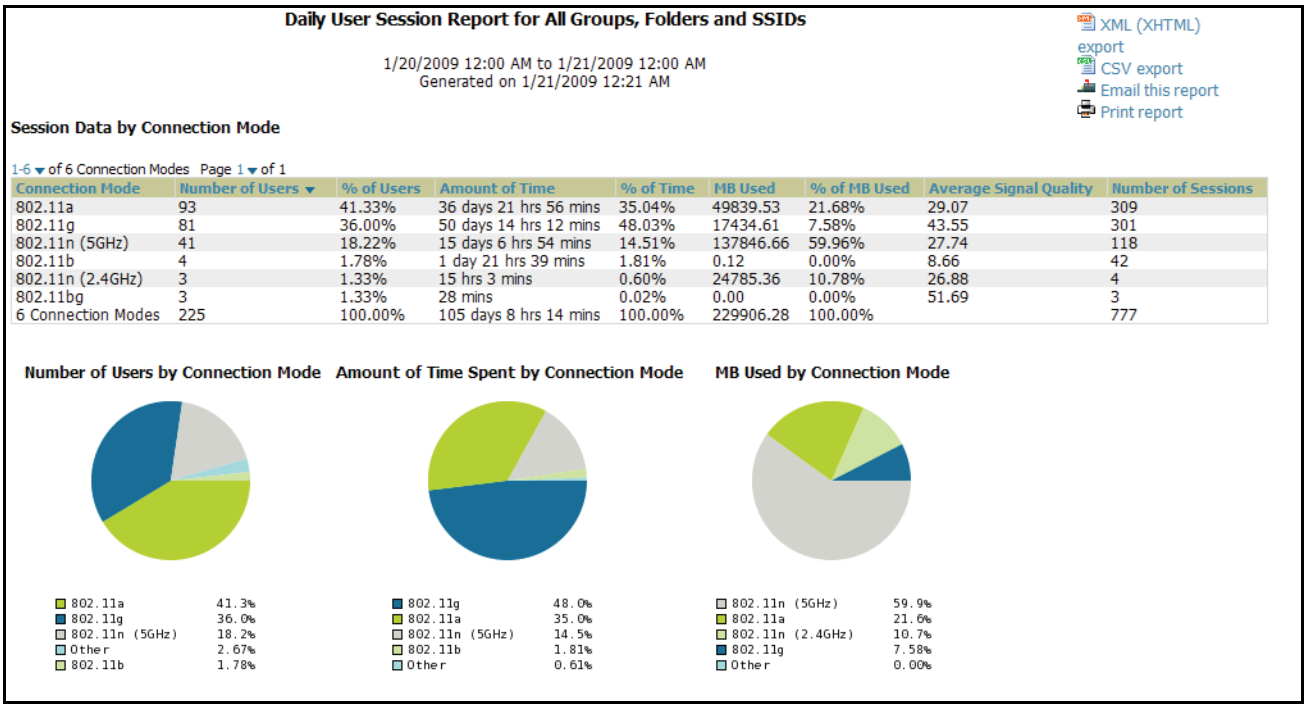
- Connection Mode
- SSID
- Role
- VLAN
- Cipher (\Summary
- Summary
- Sessions
- User

Perform these steps to view the most recent version of the **User Session Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **User Session Report** to display report **Detail** information.
3. The **Detail** page allows you to view multifaceted information for user sessions during the time period defined for the report.

The figures that follow illustrate the fields and information in the **User Session Report.**

Figure 202 ***Reports > Generated > 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

XML (XHTML) export
CSV export
Email this report
Print report

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

802.11a 41.3%
802.11g 36.0%
802.11n (5GHz) 18.2%
Other 2.67%
802.11b 1.78%

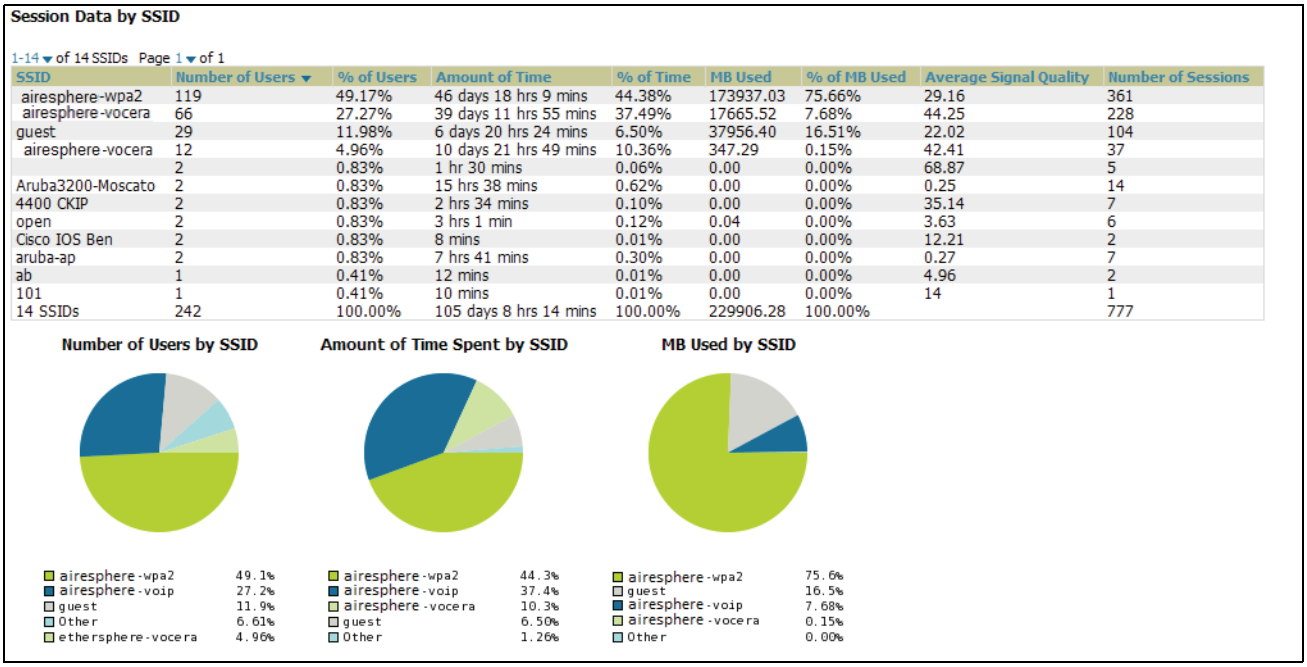
Amount of Time Spent by Connection Mode

802.11g 48.0%
802.11a 35.0%
802.11n (5GHz) 14.5%
802.11b 1.81%
Other 0.61%

MB Used by Connection Mode

802.11n (5GHz) 59.9%
802.11a 21.6%
802.11n (2.4GHz) 10.7%
802.11g 7.58%
Other 0.00%

Figure 203 ***Reports > Generated > 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

airesphere-wpa2 49.1%
airesphere-voip 27.2%
guest 11.9%
Other 6.61%
ethersphere-vocera 4.96%

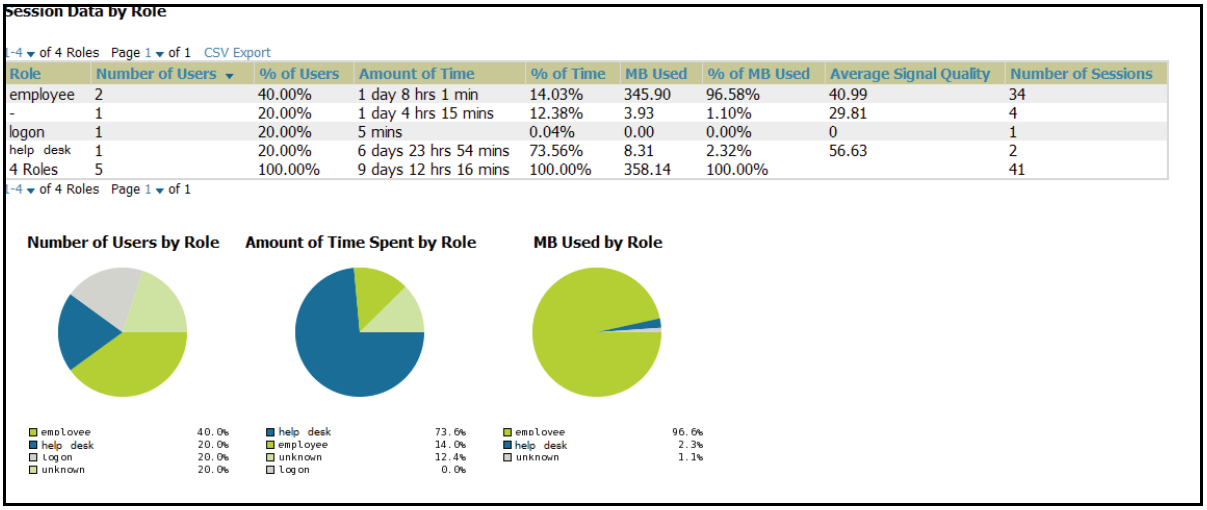
Amount of Time Spent by SSID

airesphere-wpa2 44.3%
airesphere-voip 37.4%
airesphere-vocera 10.3%
guest 6.50%
Other 1.26%

MB Used by SSID

airesphere-wpa2 75.6%
guest 16.5%
airesphere-voip 7.68%
airesphere-vocera 0.15%
Other 0.00%

Figure 204 ***Reports > Generated > User Session Detail > Role*** *Information*



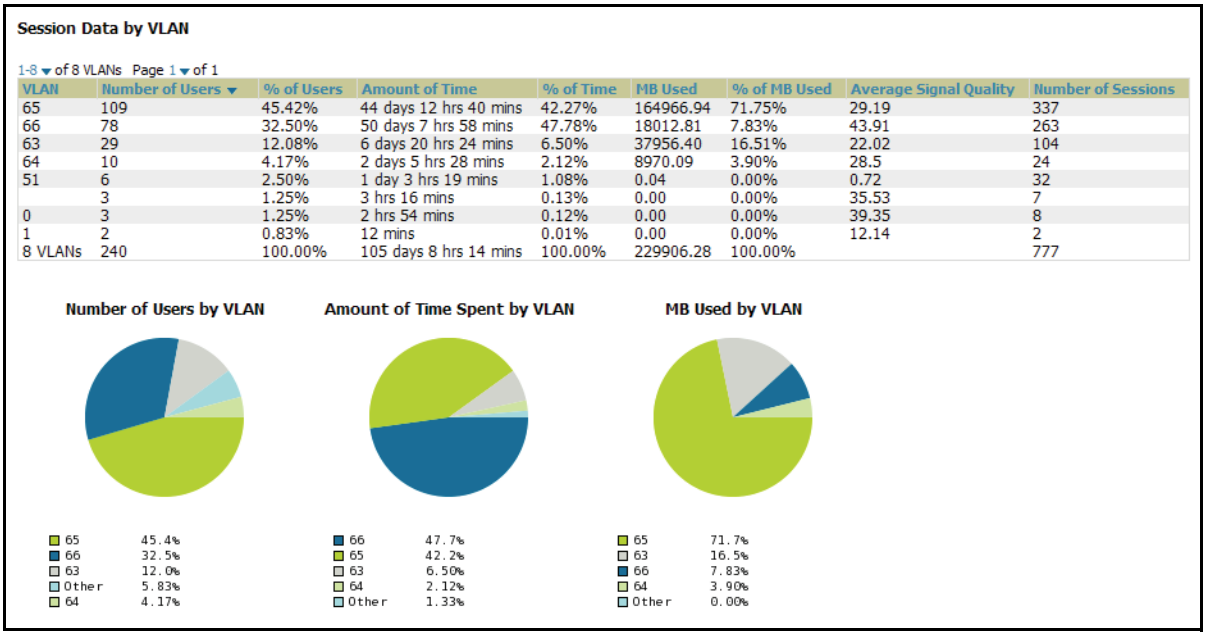
Session Data by Role

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 205 ***Reports > Generated > User Session Detail > VLAN*** *Information*

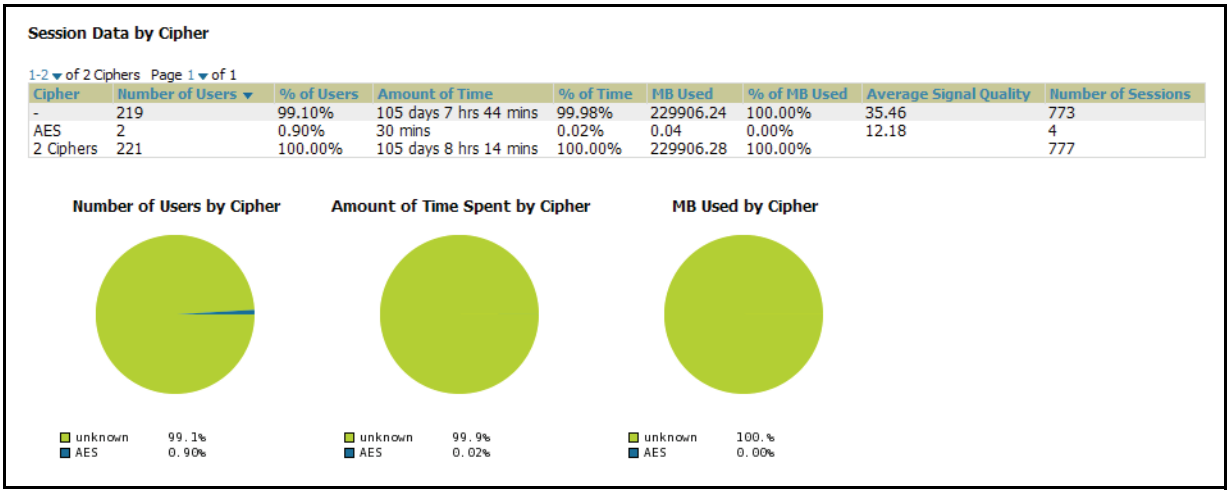


Session Data by VLAN

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 206 ***Reports > Generated > User Session Detail > Cipher*** *Information*

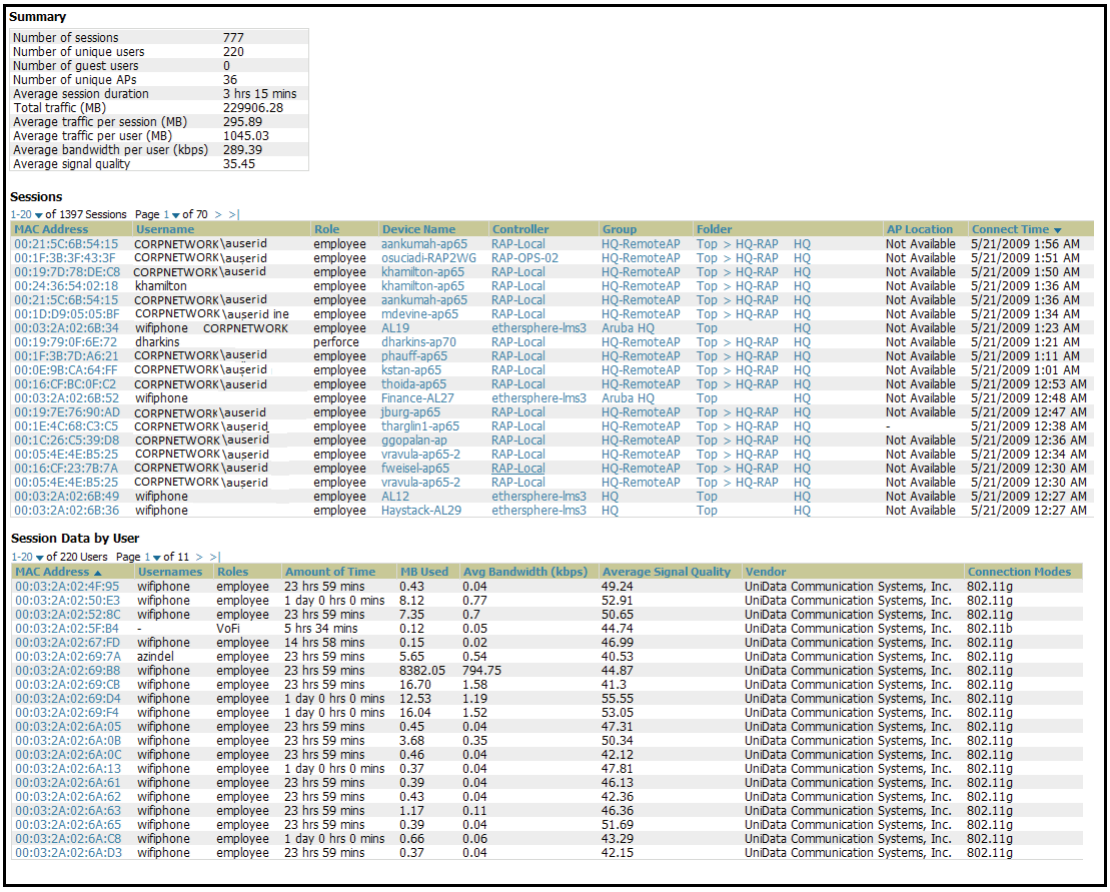


Session Data by Cipher

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 207 ***Reports > Generated > User Session Detail > Summary and User*** *Information (partial view)*



Summary

Number of sessions	777
Number of unique users	220
Number of guest users	0
Number of unique APs	36
Average session duration	3 hrs 15 mins
Total traffic (MB)	229906.28
Average traffic per session (MB)	295.89
Average traffic per user (MB)	1045.03
Average bandwidth per user (kbps)	289.39
Average signal quality	35.45

Sessions

1-20 of 1397 Sessions Page 1 of 70 > >|

MAC Address	Username	Role	Device Name	Controller	Group	Folder		AP Location	Connect Time
00:21:5C:6B:54:15	CORPNETWORK\auserid	employee	aankumah-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:56 AM
00:1F:3B:3F:43:3F	CORPNETWORK\auserid	employee	osuciadi-RAP2WG	RAP-OPS-02	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:51 AM
00:19:7D:78:DE:C8	CORPNETWORK\auserid	employee	khamilton-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:50 AM
00:24:36:54:02:18	khamilton	employee	khamilton-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:36 AM
00:21:5C:6B:54:15	CORPNETWORK\auserid	employee	aankumah-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:36 AM
00:1D:D9:05:05:BF	CORPNETWORK\auserid ine	employee	mdevine-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:34 AM
00:03:2A:02:6B:34	wifiphone CORPNETWORK	employee	AL19	ethersphere-lms3	Aruba HQ	Top	HQ	Not Available	5/21/2009 1:23 AM
00:19:79:0F:6E:72	dharkins	perforce	dharkins-ap70	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:21 AM
00:1F:3B:7D:A6:21	CORPNETWORK\auserid	employee	phauff-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:11 AM
00:0E:9B:CA:64:FF	CORPNETWORK\auserid	employee	kstan-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:01 AM
00:16:CF:BC:0F:C2	CORPNETWORK\auserid	employee	thoida-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:53 AM
00:03:2A:02:6B:52	wifiphone	employee	Finance-AL27	ethersphere-lms3	Aruba HQ	Top	HQ	Not Available	5/21/2009 12:48 AM
00:19:7E:76:90:AD	CORPNETWORK\auserid	employee	jburg-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:47 AM
00:1E:4C:68:C3:C5	CORPNETWORK\auserid	employee	tharglin1-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	-	5/21/2009 12:38 AM
00:1C:26:C5:39:D8	CORPNETWORK\auserid	employee	ggopalan-ap	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:36 AM
00:05:4E:4E:B5:25	CORPNETWORK\auserid	employee	vravula-ap65-2	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:34 AM
00:16:CF:23:7B:7A	CORPNETWORK\auserid	employee	fweisel-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:30 AM
00:05:4E:4E:B5:25	CORPNETWORK\auserid	employee	vravula-ap65-2	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:30 AM
00:03:2A:02:6B:49	wifiphone	employee	AL12	ethersphere-lms3	HQ	Top	HQ	Not Available	5/21/2009 12:27 AM
00:03:2A:02:6B:36	wifiphone	employee	Haystack-AL29	ethersphere-lms3	HQ	Top	HQ	Not Available	5/21/2009 12:27 AM

Session Data by User

1-20 of 220 Users Page 1 of 11 > >|

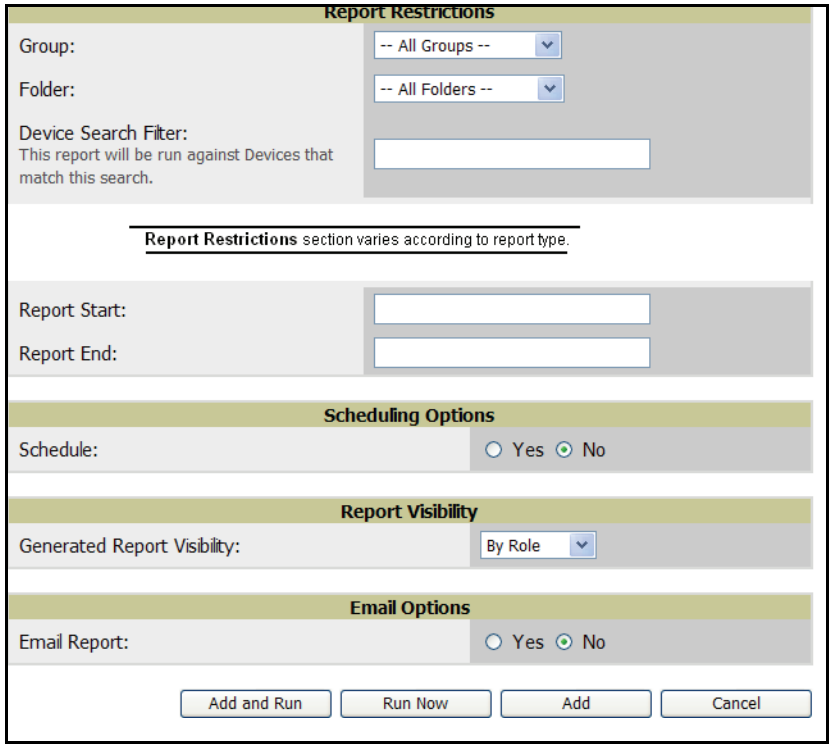
MAC Address	Usernames	Roles	Amount of Time	MB Used	Avg Bandwidth (kbps)	Average Signal Quality	Vendor	Connection Modes
00:03:2A:02:4F:95	wifiphone	employee	23 hrs 59 mins	0.43	0.04	49.24	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:50:E3	wifiphone	employee	1 day 0 hrs 0 mins	8.12	0.77	52.91	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:52:8C	wifiphone	employee	23 hrs 59 mins	7.35	0.7	50.65	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:5F:B4	-	VoFi	5 hrs 34 mins	0.12	0.05	44.74	UniData Communication Systems, Inc.	802.11b
00:03:2A:02:67:FD	wifiphone	employee	14 hrs 58 mins	0.15	0.02	46.99	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:69:7A	azindel	employee	23 hrs 59 mins	5.65	0.54	40.53	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:69:B8	wifiphone	employee	23 hrs 59 mins	8382.05	794.75	44.87	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:69:CB	wifiphone	employee	23 hrs 59 mins	16.70	1.58	41.3	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:69:D4	wifiphone	employee	1 day 0 hrs 0 mins	12.53	1.19	55.55	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:69:F4	wifiphone	employee	1 day 0 hrs 0 mins	16.04	1.52	53.05	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:6A:05	wifiphone	employee	23 hrs 59 mins	0.45	0.04	47.31	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:6A:0B	wifiphone	employee	23 hrs 59 mins	3.68	0.35	50.34	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:6A:0C	wifiphone	employee	23 hrs 59 mins	0.46	0.04	42.12	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:6A:13	wifiphone	employee	1 day 0 hrs 0 mins	0.37	0.04	47.81	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:6A:61	wifiphone	employee	23 hrs 59 mins	0.39	0.04	46.13	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:6A:62	wifiphone	employee	23 hrs 59 mins	0.43	0.04	42.36	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:6A:63	wifiphone	employee	23 hrs 59 mins	1.17	0.11	46.36	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:6A:65	wifiphone	employee	23 hrs 59 mins	0.39	0.04	51.69	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:6A:C8	wifiphone	employee	1 day 0 hrs 0 mins	0.66	0.06	43.29	UniData Communication Systems, Inc.	802.11g
00:03:2A:02:6A:D3	wifiphone	employee	23 hrs 59 mins	0.37	0.04	42.15	UniData Communication Systems, Inc.	802.11g

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 click the **Add** button, or click the **pencil** icon to edit an existing report definition. Figure 208 illustrates one view of the **Reports > Definitions** page.

Figure 208 *Defining a Report with **Reports > Definitions > Add** Button*



2. Complete the fields described in Table 141 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 272.

Table 141 ***Report > Definitions > Add** Page Fields*

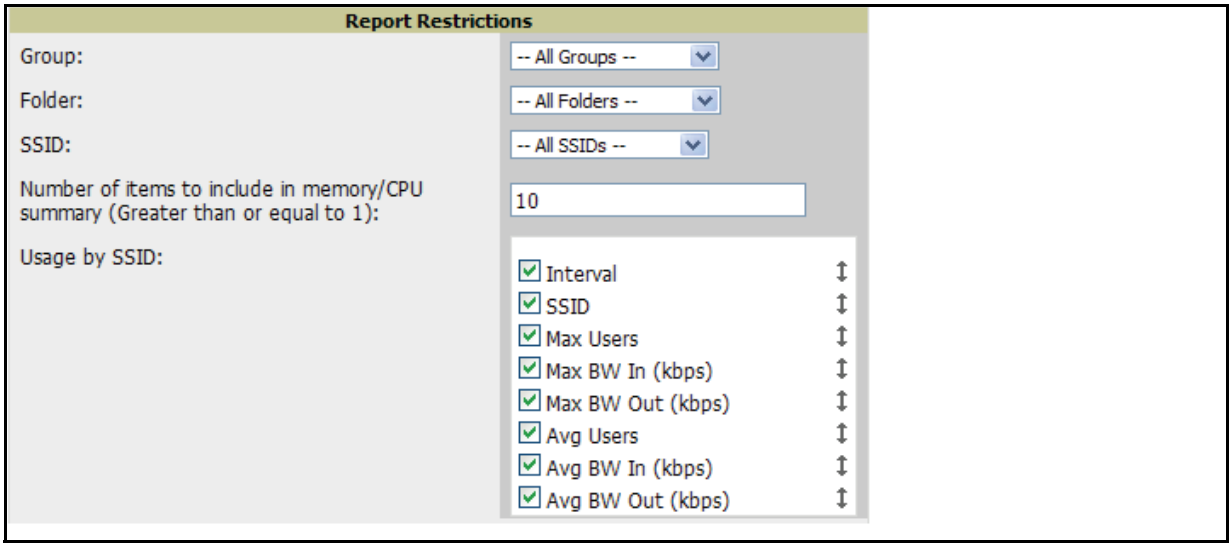
Field	Default	Description
Title	Empty	Enter a **Report Title**. Alcatel Lucent recommends using a title that is a meaningful and descriptive, so it may be found easily on the lists of reports that appear on either **Generated** or **Definitions** pages.
Type	Capacity	Choose the type of report you wish to create in the Report Type drop-down menu.
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	

Table 141 ***Report > Definitions > Add*** *Page Fields (Continued)*

Field	Default	Description
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 209 shows a sample **Report Restrictions** page.

Figure 209 ***Report Restrictions*** *Illustration*



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:
   - Click **Add and Run** to generate the report immediately, in addition to saving report settings.
   - Click **Run Now** to generate the report immediately without creating a new report definition or saving the report settings.
   - Click **Add (**only) to complete the report creation, to be run at the time scheduled.
   - Click **Cancel** to exit from the **Add** page.

Table 142 describes the configurable settings for the custom report to be created.

Table 142 *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.

Table 142 *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 Memory and CPU Usage 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.
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 Rogue Containment Audit 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.
- Click **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 296, and in "Emailing Reports to Smarthost" on page 300.

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: <press Enter>
   ```
4. 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.

Perform the following steps to export reports to XML, MS Excel, and CSV:

1. Navigate to the **Reports > Generated** page and click the name of the report you wish to export. You can also click on the link at the bottom of the page for the latest version of a report. The corresponding **Detail** page displays.
2. On the top right of the page, click **XML (XHTML) export** or **CSV export**. After a moment the XML page appears in your browser or, if you chose **CSV export**, a File Download window appears prompting you for a location on which it can save the .zip CSV files.
3. In your browser, click **File > Save As….** Define the filename and location, select **Web Page Complete** as the file type**,** then click **Save**. A brief **Save Webpage** status box appears to display the saving process. Allow the process sufficient time, particularly for reports that contain many links or large graphics. If you are downloading a .zip file, you only need to navigate to the desired location, and click **Save**.
4. Open the resulting file in MS Excel. You may need to display files of all type to access the file.
5. From Excel you can save the report as a single file using the **Save As > Excel Workbook** option (Excel 2007). You can also save it as an .xls file for compatibility with older versions of Excel though some formatting in the report might not be supported.

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 located in the /var/airwave/custom directory. Contact Alcatel Lucent support, for more information. See "Contacting Alcatel-Lucent" on page 11.

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 301
- "Monitoring Incidents with Helpdesk" on page 302
- "Creating a New Incident with Helpdesk" on page 303
- "Creating New Snapshots or Incident Relationships" on page 304
- "Using the Helpdesk Tab with an Existing Remedy Server" on page 305

OV3600 Helpdesk Overview

The Helpdesk module of the OmniVista Air Manager allows front-line technical support staff to take full advantage of the data available in the OmniVista Air Manager. The OV3600 Helpdesk includes the following features and functions, with additional features described in this chapter:

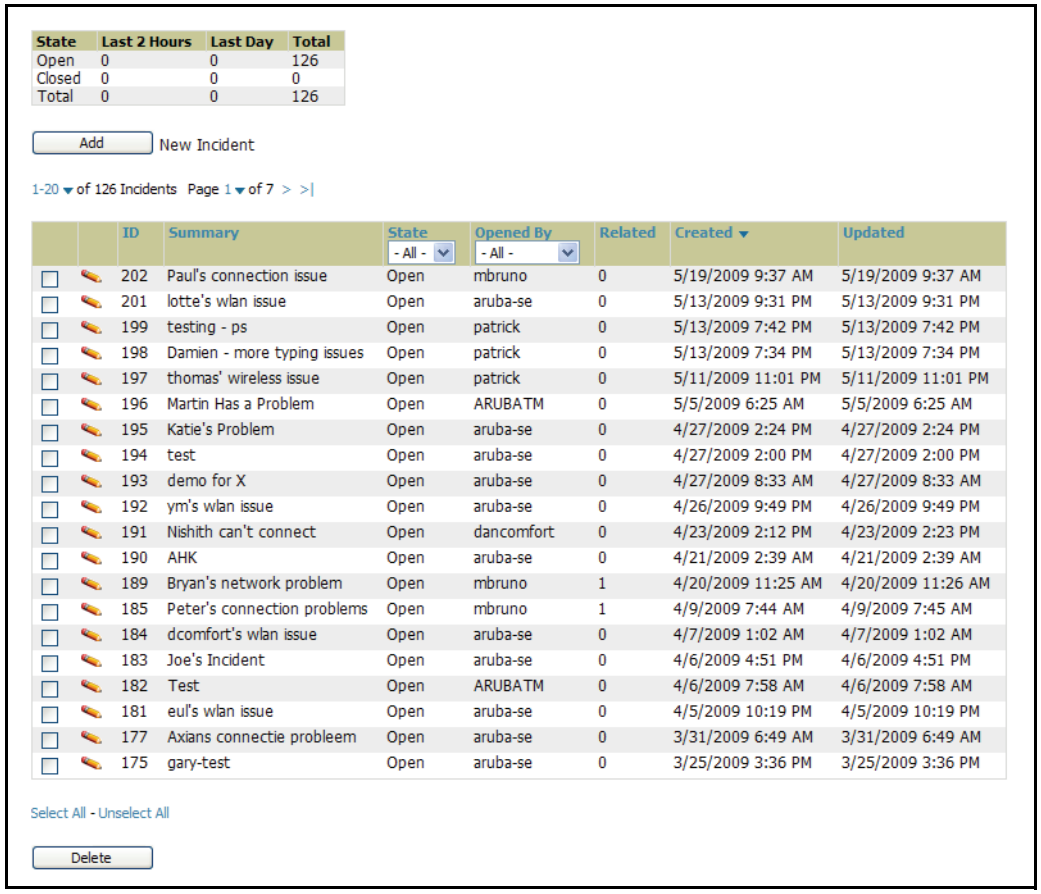
- The **Helpdesk** tab appears to the right of the **Home** tab.
- Users with an **Admin** role have the **Helpdesk** option enabled by default.
- **Admin** users can make the Helpdesk available to users of any role by selecting the **enabled** radio button on the **role detail** page. To edit existing roles, click 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 305 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 210 illustrates the components of the OV3600 **Helpdesk Incidents** page.

Figure 210 ***Helpdesk > Incidents*** *Page Illustration*



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 143 ***Helpdesk > Incidents >*** *Topmost 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 144 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.

Clicking 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 clicking the **Delete** button at the bottom of the table.

Table 144 *OV3600* ***Helpdesk > Incidents >*** *Bottommost 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. Click 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, click the **Add New Incident** button underneath the top table. This launches and displays an incident edit page, as illustrated in Figure 211. The contents of this page are described in Table 145.

Figure 211 ***Add Incident*** *Page Illustration*

Table 145 ***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 212.

Figure 212 *Helpdesk Icons on Additional Pages*

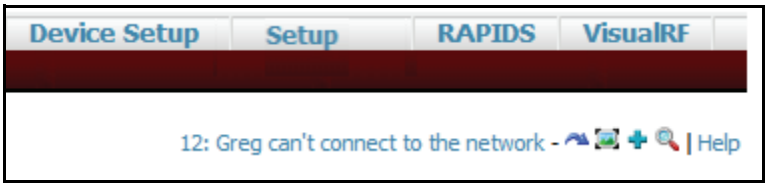


Table 146 describes the Helpdesk icon components.

Table 146 ***Helpdesk*** *Icon Components*

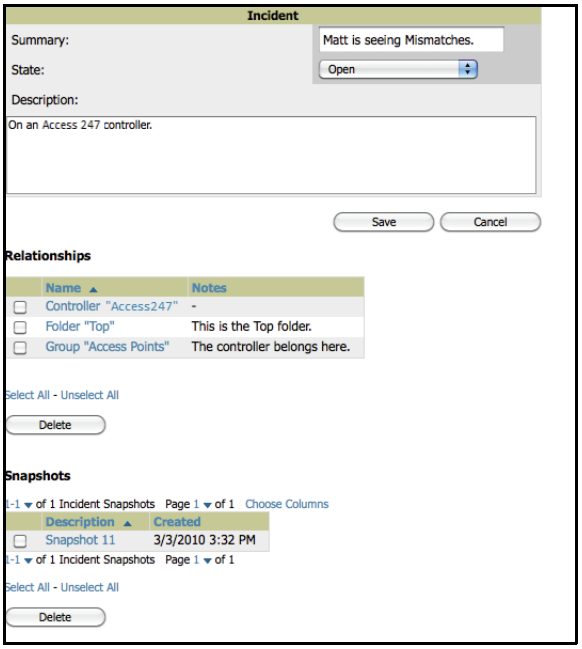
Icon	Description
Current Incident	(ID number and description) Identifies the current incident of focus in the Helpdesk header. Clicking the link brings up the **Incident Edit** page (see above). Mousing over the incident brings up a summary popup of the incident.
	Relates the device, group or client 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 clicking the Helpdesk header icon (see Table 146) 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, click 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. Clicking the snapshot description opens a popup window to display the screenshot. Figure 213 illustrates these GUI tools.

Figure 213 *Relationships and Snapshots on the **Incident Edit** Page*



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, click the **Yes** button 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 214 illustrates this appearance, and Table 147 describes the components. For more details, see "Creating New Snapshots or Incident Relationships" on page 304.

Figure 214 ***Helpdesk > Setup** with Remedy Enabled*

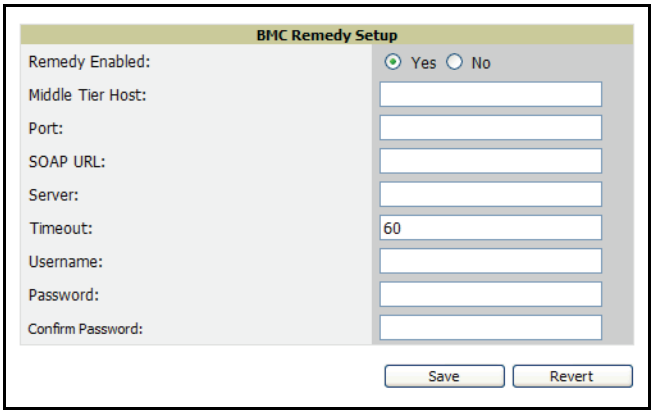


Table 147 *Components of **Helpdesk > Setup** with Remedy Enabled*

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 147 *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 215 illustrates the appearance and Table 148 describes the components of this page.

Figure 215 ***Helpdesk > Incidents** with Remedy Enabled*

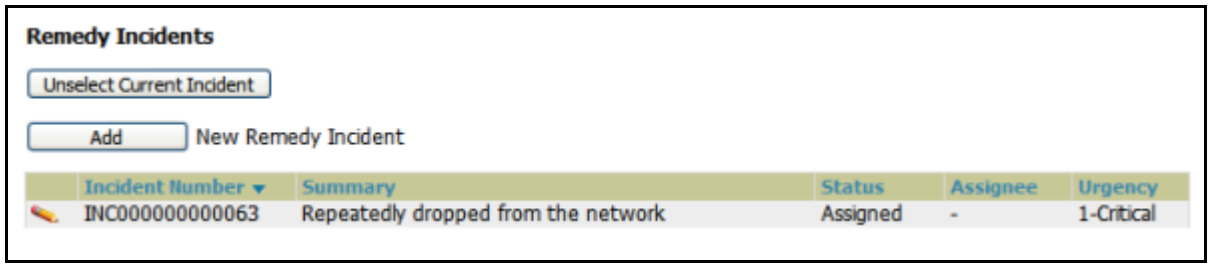


Table 148 *Components of **Helpdesk > Incidents** with Remedy Enabled*

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.

Table 148 *Components of **Helpdesk > Incidents** with Remedy Enabled*

Field	Description
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, click the **Unselect Current Incident** button. To add a new Remedy incident, click the **Add** button. To edit an existing Remedy incident, click the **pencil** icon next to the incident you wish to edit. Refer to Figure 216 and Table 149 for additional illustration and explanation.

Figure 216 ***Helpdesk > Incidents > Add a New Remedy Incident*** *Page Illustration*

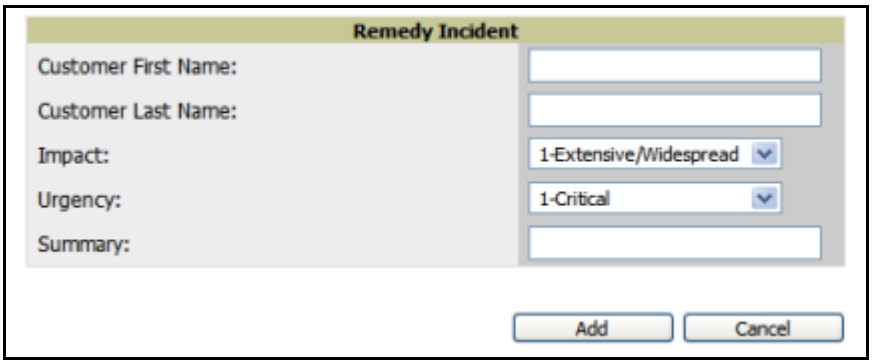


Table 149 *Components of **Helpdesk > Incidents > Add a New Remedy Incident** Fields*

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.

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, click 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

This appendix describes the Yum packaging management system, provides advisories on alternative methods that may cause issues with OV3600, and includes the following sections:

- "Yum for OV3600" on page 309
- "Package Management System Advisories for OV3600" on page 309

Yum for OV3600

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 4/5 or CentOS 4/5.

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 as current as possible to close any known security holes in the OS as quickly as possible.

Check the **Operating System** field on the **Home > Overview** page to determine if OV3600 can safely run Yum. Perform the following steps to run Yum with OV3600.

To run Yum on a CentOS 4 machine, use the steps below; for a CentOS 5 machine, yum-cron is also required.

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.
2. To install the GPG key, type **`rpm --import /usr/share/doc/fedora-release-3/RPM-GPG-KEY-fedora`**.
3. 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.
4. To configure Yum to run nightly, type **`chkconfig yum on`** and press **Enter**. The **`chkconfig`** command instructs yum to run nightly at 4:02 AM when the yum service is running, but **chkconfig** does not start yum.
5. Type **`service yum start`** and press **Enter** to start Yum, or restart the server and Yum automatically starts.
6. 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 Technical Support at Esd.support@alcatel-lucent.comfor further assistance.

Package Management System Advisories for OV3600

Alcatel Lucent does not support Yum or Up2date on Red Hat 8 or 9. Running Yum on RH8 or RH9 will cause serious problems.

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 311
- "ReefEdge Integration" on page 311
- "HP ProCurve 700wl Series Secure Access Controllers Integration" on page 312

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. Click **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. Click the **Save** button.
11. If you are you 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. Click the **Save** button.
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 66.

ReefEdge Configuration

Perform these steps to configure a ReefEdge security scheme:

1. Login into the ReefEdge ConnectServer via HTTP with the proper user credentials.
2. Navigate to the **Connect System > Accounting** page.
3. Click **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 Controllers 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 66.

Example Network Configuration

In this example, the APs are connected to the Access Controller. The Access Controller 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 Controller 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. Login 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** page.

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 315
- "Cisco IOS Dual Radio Template" on page 317
- "Speed Issues Related to Cisco IOS Firmware Upgrades" on page 318

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.

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 click **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 click **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), click **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), click **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.

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 access points. 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 321
- "Procedure" on page 321

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.

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 Alcatel Lucent Support, type **`service support_connection stop`** at the command line interface.

If you have any questions, please contact Alcatel-Lucent Technical Support at Esd.support@alcatel-lucent.com.

Appendix E

Cisco Clean Access Integration (Perfigo)

This appendix includes the following sections:

- "Prerequisites for Integrating OV3600 with Cisco Clean Access:" on page 323
- "Adding OV3600 as RADIUS Accounting Server" on page 323
- "Configuring Data in Accounting Packets" on page 323

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 of 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** button to save.

Configuring Data in Accounting Packets

1. Navigate to **User Management > Accounting > Shared Events**.
2. Map the following attributes to corresponding data elements as seen in the graphic:

```
Framed_IP_Address = "User IP"
User_Name = "LocalUser"
Calling_Station_ID = "User MAC"
```

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 <- This is the actual HP agents
   hpsmh-2.1.9-178.linux.i386.rpm <- This is the HP web portal to the agents
   ```

2. Type **`rpm -i hpasm-7.8.0-88.rhel4.i386.rpm`** at the command line interface.
3. Type **`hpasm activate`** at the command line interface.

   Take the default values. You will need the SNMP RW and RO strings at this point.

4. Type **`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. Type **`perl /usr/local/hp/hpSMHSetup.pl`** at the command line interface.

   This configures the web server.

   Configure the **Add Group > Administrator** page with a name '**`0`**'.

   Enable IP Binding—type **`1`** at the command line interface.

   At the next interface enter the IP address and mask of the server.

6. Type **`/etc/init.d/hpasm reconfigure`** at the command line interface.

   When going through this menu this time, select '**`y`**' to use the existing snmpd.conf.

7. Type **`vi /etc/snmp/snmpd.conf`** at the command line interface.

   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. Type **`service snmpd restart`** at the command line interface.
9. Type **`user add xxusernamexx`** at the command line interface.
10. Type **`passwd xxusernamexx`** at the command line interface and enter a password for the user.
11. Type **`vi /etc/passwd`** at the command line interface.

    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 327
- "Installing OV3600 on the Virtual Machine" on page 327
- "OV3600 Post-Installation Issues on VMware" on page 328

Creating a New Virtual Machine to Run OV3600

1) Click **Create a new virtual machine** from the VMware Infrastructure Client.

2) Click **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. Click **Next**.

5) Click 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). Click **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 best practice guide *Choosing the Right Server Hardware* for suggested disk space allocations for typical wireless network deployments). Click **Next**.

10) 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 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 **`cd /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.

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

OmniVista Air Manager 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:

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.

Net-SNMP:

--- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

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 appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND

FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE 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.

---- 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 POSS

Index

A

AAA servers 103
access control lists 125
access points
  adding with CSV file 148
ACLs 125
ACS
  integrating 73
  servers 73
Alcatel 186
alerts
  viewing 236
  warning behavior, setting 37

B

backups 266

C

CDP, enabling for device discovery 141
Cisco
  configuring IOS templates 192, 196
Cisco Catalyst Switches 186
Cisco Discovery Protocol
  see CDP 141
Cisco IOS 186
Cisco WLC 92
Cisco WLSE
  configuring 68
Colubris 57
CSV File 148

D

dashboard
  customizing display 36
date and time
  configuring 18
devices 135
  adding discovered devices to groups 142
  adding manually 144
  communication settings 55
  discovering, managing, and troubleshooting ... 135
  modifying 129
  troubleshooting a newly discovered device 182
  verifying 151, 166

F

firewall
  configuring 22
firmware
  loading device firmware 59
  specifying minimum firmware 126

G

global templates 202
groups
  assigning newly discovered devices to groups 142
  changing multiple group configurations 128
  configuring and using 81
  configuring basic group settings 87
  configuring group AAA servers 103
  configuring group SSIDs and VLANS 99
  configuring group templates 186
  configuring PTMP/WiMAX settings 118
  configuring radio settings 105
  configuring security settings 96
  deleting a group 128
  global groups 132
  MAC access control lists 125
  overview 83
  viewing 83

H

Helpdesk 301
  creating a new incident 303
  creating snapshots and incident relationships . 304
  monitoring incidents 302
  using with remedy server 305
Hirschmann 186
host name
  assigning host name 21
HP ProCurve 93, 107, 186

I

incidents
  creating 303

installation
checking....20
IP address
adding and assigning....20
iPhone....250

L

Lancom....186
Linux CentOS 5
installing....17

M

MAC access control lists....125
Master Console....250

N

navigation
understanding the UI....31
Network integration....14
network settings
defining....48
NMS....75
Nomdix....186
NTP....91

O

OV3600 interface
sections....23
System > Backups....266

P

pagination records
setting, resetting....33
pagination widget, using....34
password
changing default root....21
PCI Compliance
Default Credential Compliance....79
PCI Requirements....77
product overview
additional interfaces and tools....223
changing default root password....21
checking installation....20
configuring date and time....18
configuring mesh radio settings....123
defining a scan....138
executing a scan....140
getting started with....30
hardware requirements....17
initial login....30
installing....17, 21
naming the network administration system....21
Package Management....309
protocol and port diagram....22
Proxim 4900....110
Proxim/Avaya....92
PTMP....118

R

radio settings
configuring for groups....105
RADIUS....103
adding a server....103
authentication....63
configuring authentication and authorization....65
integrating....66
RAPIDS....26, 205
RAPIDs....13
reports....269
creating, running, and emailing....269
defining custom reports....296
rogue classification....205
rogue devices
configuring WLSE scanning....68
WLSE rogue scanning....68
root password....21
routers and switches
adding with a CSV file....148

S

scanning
defining credentials....137
security
auditing PCI compliance....76
configuring ACS servers....73
configuring group security settings....96
configuring group SSIDs and VLANs....99
configuring RADIUS....63
configuring TACACS+....63
integrating NMS....75
RAPIDS and rogue classification....205
using triggers and alerts....224
servers
specifying general settings....38
Smarthost....300
SNMP
polling period....89

SSIDs 99
Symbol 111, 186
Symbol/Intel 93

T

TACACS+ 103
adding a server 103
configuring authentication 63
integrating 63
templates 187
adding 189, 202
configuring a global template 202
configuring Cisco IOS templates 196
configuring for groups 186
global template variables 202
variables 202
Trapeze 186

U

UI
understanding the navigation bar 31
user interface
APs/Devices 25
APs/Devices > Audit 166
APs/Devices > Ignored 151
APs/Devices > List 152
APs/Devices > Manage 183
APs/Devices > New 143
Authentication Dialog Box 30
Buttons and Icons 28
Configuration Change Confirmation 128
Device Setup > Add 149
Device Setup > Communication 55, 56, 57, 58
Device Setup > Discover 137, 140
Device Setup > Firmware Files 59
flash graphs 35, 36, 37, 38
Group SNMP Polling Period 89
Groups 25
Groups > Basic 88, 89, 90, 91, 92, 93, 132
Groups > Firmware 126
Groups > List 83, 84
Groups > MAC ACL 125
Groups > PTMP/WiMAX 118, 119, 121
Groups > Radio 105
Groups > Templates 187, 189, 202, 203
GRUB screen 18
Help 27
Helpdesk > Incident 305
Helpdesk > Incidents 302, 306
Helpdesk > Setup 305
Home 25, 252
Home > Documentation 257
Home > License 255
Home > Overview 253
Home > Search 256
Home > User Info 258
Home Overview 35, 36, 37, 38
Master Console 250
Master Console > Groups > Basic 251, 252
Master Console > Groups > Basic, Managed .. 251
Master Console > Manage, IP/Hostname 250
RAPIDS 26
RAPIDS > Rogue APs (Detail), Score Override 220
Reports 26
Reports > Definitions 272, 296
Reports > Generated > Port Utilization Report 290
sections
Activity section 27
Navigation section 25
Status section 24
Setup > General 39
Setup > NMS 75
Setup > Users 50
Setup tab 26
System 26, 259
System > Alerts 236
System > Configuration Change Jobs 262
System > Event Logs 261
System > Performance 263
System > Status 260
System > Status Log 261
System > Trigger Detail 225
System > Triggers 224
Triggers and Alerts 224
Users 26, 238
Users > Connected 239
Users > Guest Users 242
Users > Tags 244
View AP Credentials 183
VisualRF 26
user roles
creating 52
users
creating 50

V

VisualRF 13, 26
VLANs 99

W

WiMAX 118
Wireless LAN
components 14
WLSE
configuring 68
WLSE rogue scanning 68

Y

Yum 309