

OmniVista 3600 Air Manager (OV3600)

Version 6.2



www.alcatel-lucent.com/enterprise

Part Number: 0510589-01

Copyright

© 2009 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.

User Guide

Document Revisions and Enhancements

Table 1 summarizes OV3600 product features, graphical user interface (GUI) enhancements, and related document changes.

Table 1 *User Guide Document Revisions, OV3600*

Enhancement	Document Section	Description
Content Reorganization and Document Features	<ul style="list-style-type: none"> "Preface" on page 11 "Creating and Using Templates" on page 127 "Using the OV3600 Helpdesk" on page 263 "Index" on page 303 	Rearranged existing chapters or created new document components. One such change is the consolidation of template procedures and guidelines into a newly dedicated chapter.
Device Support: <ul style="list-style-type: none"> Cisco 871w Router Monitoring Additional Devices 	See the <i>OV3600 6.2 Release Notes</i> , and the Home > Overview, Quick Links page, Supported Devices and Features .	OV3600 Version 6.2 adds support for several new devices and their related functions, to include the devices cited at left and additional new devices available in the OV3600 GUI.
Cisco WLC Radio Settings	<ul style="list-style-type: none"> "Configuring Cisco WLC Radio Settings" on page 95 	The GUI graphics, procedures, and configuration instructions are updated for OV3600 6.2 support of Cisco WLC Radio devices. This changes frequent citation of Airespace to WLC in the OV3600 6.2 interface and documentation.
PCI Compliance	<ul style="list-style-type: none"> "Configuring and Using Security in OV3600" on page 173 "PCI Compliance Report" on page 257 	OV3600 6.2 greatly enhances compliance with PCI requirements, in accordance with the PCI DSS standard.
Port Consumption	<ul style="list-style-type: none"> "Configuring and Mapping Port Usage for OV3600 Version 6.2" on page 24 	Document updates the protocols and port consumption information in Table 2, now searchable in PDF documents.
RADIUS Authentication	<ul style="list-style-type: none"> "Configuring Group Security Settings" on page 74 "Supporting RADIUS Server Accounting in OV3600" on page 53 	<p>RADIUS Authentication for Administrative Users</p> <ul style="list-style-type: none"> OV3600 6.2 expands RADIUS options. You can configure RADIUS authentication either by using the OV3600 database for RADIUS authentication, or by using one or more separate RADIUS servers, primary and secondary. The role that governs a RADIUS client derives from the authentication method that is chosen. OV3600 6.2 uses RADIUS management servers, as defined in the Group > AAA page, and pushes such configurations to controller devices. Therefore, the RADIUS Management Section in the Group > Security page is no longer required, and is removed from the GUI for Version 6.2.
Reports	<ul style="list-style-type: none"> "Creating, Running, and Emailing Reports" on page 229 	<ul style="list-style-type: none"> The OV3600 module in OV3600 Version 6.2 supports 13 specific reports and related enhancements: <ul style="list-style-type: none"> Each report can be generated to run at pre-set times and by specific criteria. Each report can be displayed in real-time fashion to show data from the most recent 24-hour period. All reports can be exported to email and migrated to XML format, supporting graphics. Many reports display the latest of OV3600 6.2 features, to include new levels of SSID classification, PCI compliance, and device support not available in prior versions.
Bill of Materials Report Improvements	<ul style="list-style-type: none"> <i>Visual RF User Guide</i>, Version 6.2 	<ul style="list-style-type: none"> Bill of Materials Report improvements are supported.

Table 1 *User Guide Document Revisions, OV3600 (Continued)*

Enhancement	Document Section	Description
Rogue Device Classification Improvements	<ul style="list-style-type: none"> "Monitoring Rogue AP Devices with RAPIDS > Rogue APs Pages" on page 175 "Using the RAPIDS > Setup Page" on page 179 	<p>OV3600 improves the classification of rogue devices. Newly supported rogue device classifications include Neighbor, Unmanaged, and Rogue. This enhancement propagates throughout several reports and pages in the OV3600 6.2 interface.</p> <p>The Rogue APs pages, both Basic and Detail, add a new Classification column, allowing users to sort rogue AP devices by type.</p> <p>The RAPIDS > Setup page supports this classification for rogue AP devices, and enables additional default settings and OV3600 actions for rogue device discovery.</p>
Search Functions	<ul style="list-style-type: none"> "Searching OV3600 with the Home > Search Page" on page 199 	<p>Searching for an IP address, operationally unique identifier (OUI), LAN address, radio MAC address, or name now brings up matching rogue devices and tags.</p>
SNMP "Down AP" traps from Cisco Controllers supported	<ul style="list-style-type: none"> See the <i>OV3600 6.2 Release Notes and multiple device pages in the OV3600 GUI</i>. 	<p>OV3600 6.2 enhances SNMP support for Cisco controllers, to include SNMP Down AP traps for enhanced network monitoring and device status information. This information propagates throughout the OV3600 6.2 interface, enhancing reports and device information available on multiple pages.</p>
SSID-based Statistics Collection and Reporting	<ul style="list-style-type: none"> "Monitoring APs with the Monitoring and Controller Pages" on page 166 "User Session Report" on page 260 	<p>OV3600 6.2 newly reports users and statistics based on SSID, and continues to support such user data by radio and other criteria, as in prior versions.</p>
User Roles have access to multiple branches in folder hierarchy	<ul style="list-style-type: none"> "Creating OV3600 User Roles" on page 42 	<p>Commencing with OV3600 Version 6.2, User Roles can be created with access to folders within multiple branches of the overall hierarchy.</p>
WMS Offload Support	<ul style="list-style-type: none"> "Deploying WMS Offload in OV3600" on page 54 	<p>OV3600 Version 6.2 enhances support for WSM Offload in scenarios that combine Alcatel-Lucent network topology with advanced OV3600 6.2 network monitoring and control.</p>
VisualRF	<ul style="list-style-type: none"> "Creating OV3600 User Roles" on page 42 <i>VisualRF User Guide, Version 6.2</i> 	<p>Corrected information about access to VisualRF. Clarified how user access and administrator access differ in their rights to modify VisualRF.</p> <p>Suggested Placement of Sensors and Visualized WLAN Coverage</p>
Triggers and Alerts	<ul style="list-style-type: none"> "Using Triggers and Alerts" on page 207 Chapter 1, "Introduction to the OmniVista 3600 Air Manager" on page 17 	<p>Enhanced the procedure and graphic illustrations for creating Triggers.</p> <p>The Master Console and Failover servers can now 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.</p>
Complete Chapter Update	<p>Chapter 4, "Enabling OV3600 to Manage Your Devices" on page 57</p>	<p>Updated OV3600 6.2 content, graphics, and procedures for the Device > Setup > Upload Files and Device > Setup > Communication pages.</p>

Preface		11
	Document Organization	11
	Text Conventions	12
	Contacting Alcatel-Lucent	13
Chapter 1	Introduction to the OmniVista 3600 Air Manager	15
	OV3600—A Unified Wireless Network Command Center	15
	OmniVista Air Manager 3600	16
	VisualIRF™	16
	RAPIDs™	17
	Master Console and Failover	17
	Integrating OV3600 into the Network and Organizational Hierarchy	17
	OV3600 Hardware Requirements and Installation Media	18
Chapter 2	Installing The OmniVista 3600 Air Manager	19
	Introduction	19
	Installing Linux CentOS 5 (Phase 1)	19
	Installing OV3600 Software (Phase 2)	20
	Getting Started	20
	Step 1: Configuring Date and Time, Checking for Prior Installations	20
	Date and Time	20
	Previous OV3600 Installations	21
	Step 2: Installing OV3600 Software	21
	Step 3: Checking the OV3600 Installation	21
	Step 4: Assigning an IP Address to the OV3600 System	22
	Step 5: Naming the OV3600 Network Administration System	22
	Step 6: Assigning a Host Name to the OV3600	22
	Step 7: Changing the Default Root Password	23
	Completing the Installation	23
	Configuring and Mapping Port Usage for OV3600 Version 6.2	24
	OV3600 Navigation Basics	25
	Status Section	26
	Navigation Section	27
	Activity Section	29
	Help Links in the GUI	29
	Buttons and Icons	29
	Getting Started with OV3600	32
	Initial Login	32
	OV3600 Version 6.2 Interface Overview	32
Chapter 3	Configuring the OmniVista 3600 Air Manager	33
	Introduction	33
	Specifying General OV3600 Server Settings	33
	Defining OV3600 Network Settings	40
	Creating OV3600 User Roles	42
	Creating OV3600 Users	44

	Configuring TACACS+ Integration (Optional)	47
	Integrating with WLSE Rogue Scanning (Optional)	48
	Integrating ACS (Optional)	50
	Integrating with an Existing Network Management Solution (Optional)	51
	Integrating OV3600 with a RADIUS Accounting Server (Optional)	53
	Supporting RADIUS Server Accounting in OV3600	53
	Deploying WMS Offload in OV3600	54
	Overview of WMS Offload in OV3600	54
	General Configuration Tasks Supporting WMS Offload in OV3600	55
	Additional Information Supporting WMS Offload	55
Chapter 4	Enabling OV3600 to Manage Your Devices	57
	Introduction	57
	Configuring Communication Settings for Discovered Devices	57
	Loading Device Firmware onto OV3600 (Optional)	60
	Overview of the Device Setup > Upload Files Page	60
	Loading Firmware Files to OV3600 6.2	62
Chapter 5	Configuring and Using Groups in OV3600	65
	Introduction	65
	OV3600 Group Overview	65
	Group Configuration Overview	66
	Viewing All Defined Device Groups	66
	Configuring Basic Group Settings	68
	Configuring Group Security Settings	74
	Configuring Group SSIDs and VLANS (Optional)	80
	Configuring Group AAA Servers	86
	Configuring Group Radio Settings	88
	Configuring Cisco WLC Radio Settings	95
	Configuring Global Controller Settings	95
	Configuring LWAPP AP Settings	110
	Configuring Group PTMP/WiMAX Settings	111
	Configuring Mesh Radio Settings	115
	Configuring Colubris Advanced Settings (Optional)	117
	Configuring Group MAC Access Control Lists (Optional)	119
	Specifying Minimum Firmware Versions for APs in a Group (Optional)	120
	Creating New Groups	121
	Deleting a Group	121
	Changing Multiple Group Configurations	121
	Modifying Multiple Devices	123
	Using Global Groups for Group Configuration	124
Chapter 6	Creating and Using Templates	127
	Introduction	127
	Overview of Group Templates	128
	Adding Templates	130
	Configuring General Template Files and Variables	132
	Configuring General Templates	132
	Using Template Syntax	134
	Using Directives to Eliminate Reporting of Configuration Mismatches	134
	<ignore_and_do_not_push>substring</ignore_and_do_not_push>	134

	<push_and_exclude>command</push_and_exclude>	134
	Using Conditional Variables in Templates	135
	Using Substitution Variables in Templates	135
	Using AP-Specific Variables	136
	Configuring Cisco IOS Templates	137
	Applying Startup-config Files	137
	WDS Settings in Templates	137
	SCP Required Settings in Templates	138
	Supporting Multiple Radio Types via a Single IOS Template	138
	Configuring Single and Dual-Radio APs via a Single IOS Template	138
	Configuring a Global Template	139
Chapter 7	Discovering and Managing Devices	141
	Introduction	141
	Discovery of Devices Overview	142
	Enabling AP Automatic Discovery	142
	Defining Networks for SNMP/HTTP Scanning	143
	Defining Credentials for Scanning	143
	Defining a Scan	144
	Executing a Scan	145
	Manually Adding Individual Devices	146
	Adding Access Points, Routers and Switches with a CSV File	148
	Adding Universal Devices	149
	Assigning Newly Discovered Devices to Groups	150
	Overview	150
	Adding a Newly Discovered Device to a Group	150
	Verifying That Devices Are Successfully Added to a Group	151
	Troubleshooting a Newly Discovered Device with Down Status	153
	Replacing a Broken Device	154
	Verifying the Device Configuration Status	155
	Moving a Device from Monitor Only to Manage Read/Write Mode	156
	Configuring Individual Device Settings	157
	Overview of Individual Device Configuration	157
	Configuring AP Settings	157
	Configuring AP Communication Settings	163
	Using the OV3600 APs/Devices Pages	165
	Using Device Folders (Optional)	165
	Monitoring APs with the Monitoring and Controller Pages	166
Chapter 8	Configuring and Using Security in OV3600	173
	Introduction	173
	Deploying RAPIDS in OV3600 6.2	173
	RAPIDS Overview	173
	Monitoring Rogue AP Devices with RAPIDS > Rogue APs Pages	175
	Classifying Rogue AP Devices in RAPIDS	175
	Using the RAPIDS > Rogue APs Pages	175
	Modifying Rogue Devices with the RAPIDS > Rogue APs > Modify Devices Page	178
	Viewing Ignored Rogue Devices	178
	Using the RAPIDS > Setup Page	179
	Using the Basic Configuration Section	179
	Using the Classification Options Section	180
	Using the Filtering Option Section	181
	Using the Operating System Matches Section	181
	Using the RAPIDS Rogue Score Override	182

	Configuring and Deploying PCI Compliance in OV3600 6.2	183
	Overview of PCI Compliance in OV3600 6.2	184
	Enabling or Disabling PCI Compliance Monitoring	185
Chapter 9	Daily Operations in OV3600	187
	Introduction	187
	Using the OV3600 Users Page	188
	Overview of the Users Page	188
	Using the Users > Connected Page	188
	Using the Users > Detail and Users > Diagnostics Pages	191
	Using the Users > Guest Users Page	193
	Overview of the Users > Guest Users Page	193
	Using the Users > Tags Page	195
	Using the Home Pages	196
	Overview of the Home Pages	196
	Using the Home > Overview Page	196
	Using the Home > License Page	198
	Searching OV3600 with the Home > Search Page	199
	Using the Home > Documentation Page	201
	Using the Home > User Info Page	201
	Using System Pages	202
	Using the System > Status Page	202
	Using the System > Configuration Change Jobs Page	203
	Using the System > Event Logs Page	204
	Using the System > Performance Page	205
	Using Triggers and Alerts	207
	Overview of Triggers and Alerts	207
	Viewing Triggers	208
	Creating New Triggers	209
	Setting Triggers for Devices	211
	Setting Triggers for Radios	213
	Setting Triggers for Discovery	215
	Setting Triggers for Users	216
	Setting Triggers for RADIUS Authentication Issues	218
	Setting Triggers for IDS Events	219
	Setting Triggers for OV3600 Health	220
	Delivering Triggered Alerts	220
	Viewing Alerts	221
	Performing Backups with OV3600	222
	Overview of Backups	222
	Viewing and Downloading Backups	222
	Running Backup on Demand	222
	Restoring from a Backup	223
	OV3600 Failover	223
	Navigation Section of OV3600 Failover	223
	Adding Watched OV3600 Stations	223
	Using the Master Console	225
Chapter 10	Creating, Running, and Emailing Reports	229
	Introduction	229
	Overview of OV3600 6.2 Reports	229
	Supported Report Types in OV3600 6.2	229
	Reports > Definitions Page Overview	230
	Reports > Generated Page Overview	231
	Viewing Reports	232
	Emailing and Exporting Reports	234

	Emailing Reports in General Email Applications	234
	Emailing Reports to Smarthost	234
	Exporting Reports to XML	234
	Creating and Running Custom Reports	235
	Defining Custom Reports	235
	Overview of Custom Reports and Scheduling Options	237
	Using Daily Reports in OV3600 6.2	238
	Capacity Planning Report	239
	Using the Most Recent Capacity Planning Report	239
	Configuration Audit Report	242
	Using the Most Recent Configuration Audit Report	242
	Device Summary Report	243
	Using the Most Recent Device Summary Report	243
	Device Uptime Report	245
	Using the Most Recent Device Uptime Report	245
	IDS Events Report	246
	Using the Most Recent IDS Events Report	246
	Inventory Report	247
	Using the Most Recent Inventory Report	247
	Memory and CPU Utilization Report	249
	Using the Most Recent Memory and CPU Utilization Report	249
	Network Usage Report	251
	Using the Most Recent Network Usage Report	251
	New Rogue Devices Report	252
	Using the Most Recent New Rogue Devices Report	253
	New Users Report	256
	Using the Most Recent New Users Report	256
	PCI Compliance Report	257
	Using the Most Recent PCI Compliance Report	257
	Defining and Generating PCI Compliance Reports	258
	RADIUS Authentication Issues Report	259
	Using the Most Recent RADIUS Authentication Issues Report	259
	User Session Report	260
	Using the Most Recent User Session Report	260
Chapter 11	Using the OV3600 Helpdesk	263
	Introduction	263
	OV3600 Helpdesk Overview	263
	Monitoring Incidents with Helpdesk	264
	Creating a New Incident with Helpdesk	265
	Creating New Snapshots or Incident Relationships	266
	Using the Helpdesk Tab with an Existing Remedy Server	267
Chapter 12	Package Management for OV3600 Version 6.2	271
	Yum for OV3600 6.2	271
	Package Management System Advisories for OV3600 6.2	271
Appendix A	WLSE Configuration	273
	Overview	273
	Helpful Cisco Links	273
	Performing Initial WLSE Configuration	273
	Adding an ACS Server	273
	Enabling Rogue Alerts	274
	Configuring WLSE to Communicate with APs	274
	Discovering Devices	274

	Managing Devices	274
	Inventory Reporting	274
	Defining Access	275
	Grouping	275
	Configuring IOS APs for WDS Participation	275
	WDS Participation	275
	Primary or Secondary WDS (Optional)	275
	Configuring ACS for WDS Authentication	276
Appendix B	Security Integration for OV3600	277
	Bluesocket Integration (Optional)	277
	Requirements	277
	Bluesocket Configuration	277
	ReefEdge Integration (Optional)	277
	Requirements	277
	ReefEdge Configuration	278
	HP ProCurve 700wl Series Secure Access Controllers Integration (Optional)	278
	Requirements	279
	Example Network Configuration	279
	HP ProCurve 700wl Series Configuration	279
Appendix C	Access Point Notes	281
	Resetting Cisco (VxWorks) Access Points	281
	Introduction	281
	Connecting to the AP	281
	Determining the Boot-Block Version	281
	Resetting the AP (for Boot-Block Versions from 1.02 to 11.06)	282
	Resetting the AP (for Boot-Block Versions 11.07 and Higher)	282
	IOS Dual Radio Template	283
	Speed Issues Related to IOS Firmware Upgrades	284
	OV3600 Firmware Upgrade Process	284
Appendix D	Cisco Clean Access Integration (Perfigo)	287
	Requirements	287
	Adding OV3600 as RADIUS Accounting Server	287
	Configuring Data in Accounting Packets	287
Appendix E	HP Insight Install Instructions for OV3600 Servers	289
Appendix F	Configuring Templates for Symbol APs	291
Appendix G	Installing OV3600 6.2 on VMware ESX (3i v. 3.5)	293
	Creating a New Virtual Machine to Run OV3600	293
	Installing OV3600 on the Virtual Machine	293
	OV3600 Post-Installation Issues on VMware	294
Appendix H	Third-Party Copyright Information	295
	Copyright Notices	295
	Packages	295
	Net::IP:	295
	Net-SNMP:	295
	Crypt::DES perl module (used by Net::SNMP):	298
	Perl-Net-IP:	299
	Berkeley DB 1.85:	299
	SWFObject v. 1.5:	300
	mod_auth_tacacs - TACACS+ authentication module:	300
	Index	303

This preface provides an overview of this document, general documentation supporting OV3600 Version 6.2, and contact information for Alcatel-Lucent. This preface contains the following sections:

- Document Organization
- Text Conventions
- 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 the OmniVista 3600 Air Manager, Version 6.2. This includes wide deployment of wireless access points (APs), device administration, wireless controller devices, security, reports, and additional features of OV3600 6.2.

Table 2 Document Organization and Purposes

Chapter	Description
Chapter 1, "Introduction to the OmniVista 3600 Air Manager"	Introduces and presents the OmniVista 3600 Air Manager, Version 6.2, OV3600 components, and general network functions.
Chapter 2, "Installing The OmniVista 3600 Air Manager"	Describes system and network requirements, Linux OS installation, and OV3600 6.2 installation.
Chapter 3, "Configuring the OmniVista 3600 Air Manager"	Describes configuration, startup, and launch of OV3600 6.2 to result in immediate presence and functions on the wireless network.
Chapter 4, "Enabling OV3600 to Manage Your Devices"	Describes general configurations and processes once OV3600 6.2 is installed and present on the network.
Chapter 5, "Configuring and Using Groups in OV3600"	Describes configuration and deployment for group device profiles.
Chapter 6, "Creating and Using Templates"	Describes and illustrates the use of templates in group and global device configuration.
Chapter 7, "Discovering and Managing Devices"	Describes how to discover and manage devices on the network, whether they operate within larger group profiles or do not.
Chapter 8, "Configuring and Using Security in OV3600"	Describes the security features, technologies, configuration, and deployment on OV3600 Version 6.2.
Chapter 9, "Daily Operations in OV3600"	Describes the most common daily operations in OV3600 6.2, and the OV3600 6.2 GUI for OV3600 6.2 deployment.
Chapter 10, "Creating, Running, and Emailing Reports"	Describes report generation options, configuration, and distribution on OV3600 6.2.
Chapter 11, "Using the OV3600 Helpdesk"	Describes how to use the OV3600 6.2 Helpdesk GUI and related functions.
Chapter 12, "Package Management for OV3600 Version 6.2"	Describes the Yum packaging management system, and provides advisories on alternative methods that may cause issues with OV3600 6.2.
Appendix A, "WLSE Configuration"	Describes the configuration of Cisco WLSE in OV3600 Version 6.2.

Table 2 Document Organization and Purposes

Chapter	Description
Appendix B, "Security Integration for OV3600"	Describes additional and optional security configurations in OV3600 Version 6.2.
Appendix C, "Access Point Notes"	Provides points and suggestions for Access Point devices in OV3600 Version 6.2.
Appendix D, "Cisco Clean Access Integration (Perfigo)"	Provides instructions for integrating Cisco Clean Access within OV3600 Version 6.2.
Appendix E, "HP Insight Install Instructions for OV3600 Servers"	Provides instructions for installing HP Insight on OV3600 6.2 Servers.
Appendix F, "Configuring Templates for Symbol APs"	Provides instructions for non-global templates that support Symbol Access Point devices.
Appendix G, "Installing OV3600 6.2 on VMware ESX (3i v. 3.5)"	Provides instructions for an alternative installation option on VMware ESX for OV3600 Version 6.2.
Appendix H, "Third-Party Copyright Information"	Presents multiple copyright statements from multiple equipment vendors that interoperate with OV3600 Version 6.2.
Index	Provides extensive citation of and links to document topics, with emphasis on the OV3600 6.2 GUI and tasks relating to OV3600 6.2 installation and operation.

Text Conventions

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

Table 3 Text Conventions

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
System items	This fixed-width font depicts the following: <ul style="list-style-type: none"> ● 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: <pre># send <text message></pre> 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	https://service.esd.alcatel-lucent.com
Email Contact	
<ul style="list-style-type: none">Alcatel-Lucent Enterprise Service and OmniVista 3600 Support	support@ind.alcatel.com

Thank you for choosing the OmniVista 3600 Air Manager (OV3600). OV3600 is the centerpiece of the OmniVista 3600 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 3600 Air Manager. This chapter contains the following topics:

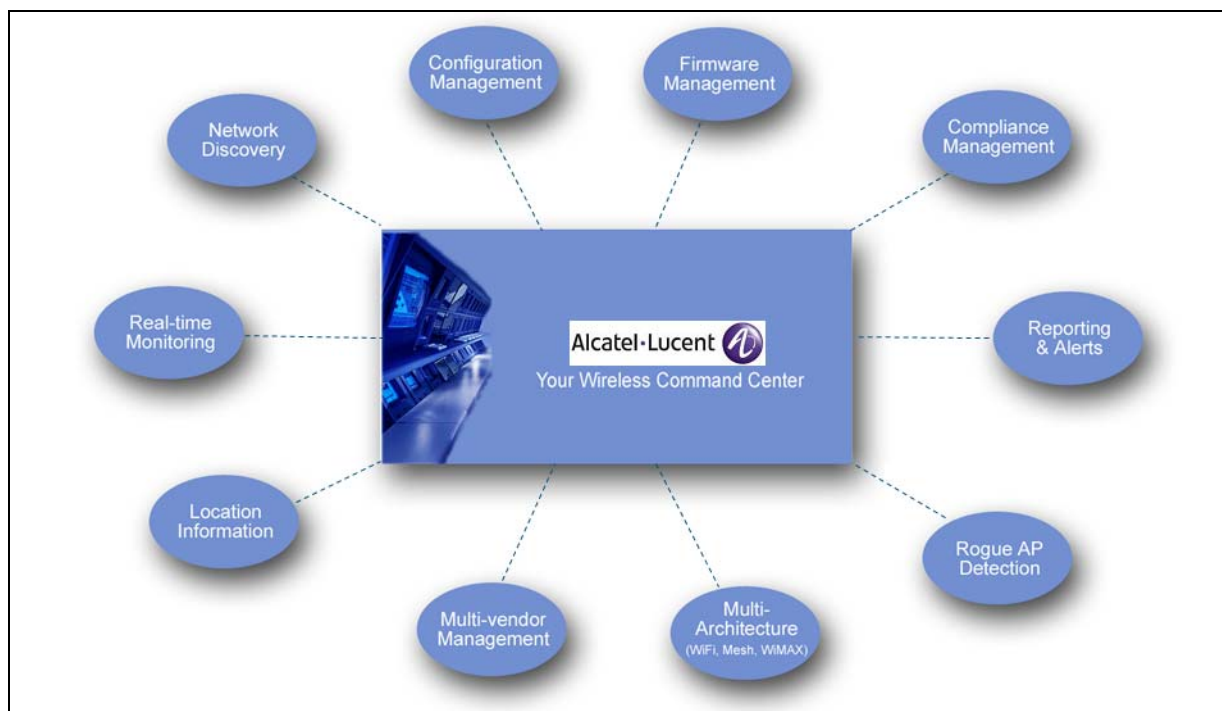
- [OV3600—A Unified Wireless Network Command Center](#)
- [OmniVista Air Manager 3600](#)
- [VisualRF™](#)
- [RAPIDs™](#)
- [Master Console and Failover](#)
- [Integrating OV3600 into the Network and Organizational Hierarchy](#)
- [OV3600 Hardware Requirements and Installation Media](#)

If you have any questions or comments, please contact Alcatel-Lucent Enterprise Support at support@ind.alcatel.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.

Figure 1 OV3600 — Your Wireless Command Center



The OmniVista 3600 Air Manager supports hardware from leading wireless vendors, including Alcatel-Lucent, 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 core components of the OmniVista 3600 Air Manager are as follows:

- *OV3600 Air Manager (OV3600)* wireless network management software
- *VisualRF* location and RF mapping software module
- *RAPIDS* rogue access point detection software module
- *OV3600 Master Console and Failover Servers* for scalability and high-availability

OmniVista Air Manager 3600

The OmniVista Air Manager (OV3600) offers the following functions and benefits:

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

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.
- 3-D campus and building 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
- 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 switch port.

Master Console and Failover

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

- Provides network-wide visibility, even when the WLAN grows to 25,000+ devices.
- Executive Portal allows executives to view high-level usage and performance data
- Aggregated Alerts
- Failover
 - Many-to-one failover
 - One-to-one failover
- The **Master Console** and **Failover** servers can now 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 [“Using Triggers and Alerts” on page 232](#).

Integrating OV3600 into the Network and Organizational Hierarchy

OV3600 generally resides in the NOC and communicates with various components of your WLAN infrastructure. In basic deployments, OV3600 communicates solely with indoor wireless access points and WLAN controllers over the wired network. In more complex deployments OV3600 seamlessly integrates and communicates with authentication servers, accounting servers, TACACS+ servers, routers, switches, network management servers, wireless IDS solutions, 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 becomes 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
Rogue APs	Unauthorized APs not registered in 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 given read-only access to monitoring all devices from the **Master Console**.

OV3600 Hardware Requirements and Installation Media

The OV3600 installation CD includes all software (including the Linux OS) required to complete the installation of the OmniVista 3600 Air Manager. OV3600 supports any hardware that is RedHat 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 **Home > Documentation** page, or contact Alcatel-Lucent Enterprise Support at support@ind.alcatel.com.

Introduction

This chapter contains information and procedures to install and launch the OmniVista 3600 Air Manager, Version 6.2. This chapter contains the following topics:

- Installing Linux CentOS 5 (Phase 1)
- Installing OV3600 Software (Phase 2)
- Configuring and Mapping Port Usage for OV3600 Version 6.2
- OV3600 Navigation Basics
- Getting Started with OV3600

This chapter presumes that hardware requirements are verified for the system(s) on which OV3600 Version 6.2 is to operate, as described in the following section:

- “OV3600 Hardware Requirements and Installation Media” on page 18

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 Version 6.2 on the network management system.



WARNING

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 in manual fashion, 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.

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.

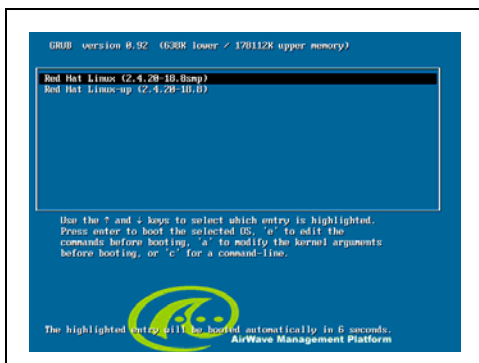
2. Remove the CD from the drive and store in a safe location.

Installing OV3600 Software (Phase 2)

Getting Started

After the reboot, the **GRUB** screen appears. [Figure 2](#) illustrates the OV3600 **GRUB** screen.

Figure 2 GRUB Screen



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](#)” on page 21. 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 Enterprise Support at support@ind.alcatel.com.

Step 2: Installing OV3600 Software

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's 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 Enterprise Support at support@ind.alcatel.com. 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 the 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 modern browser. The OV3600 GUI then prompts for your license key. If you are entering a dedicated **Master Console** or **OV3600 Failover** license, refer to “Using the Master Console” on page 225 for additional information.

Configuring and Mapping Port Usage for OV3600 Version 6.2

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
192	UDP	OSU	Discovery probe	<	Proxim
443	TCP	HTTPS	Web management	<	Laptop or workstation
443	TCP	VTUN	Support connection (optional)	>	Alcatel-Lucent support home office
1701	TCP	HTTPS	AP and rogue discovery	>	WLSE

Table 2 OV3600 Protocol and Port Chart (Continued)

Port	Type	Protocol	Description	Dataflow Direction	Device Type
1813	UDP	RADIUS	Retrieve client authentication info	<	Accounting Server
1813	UDP	RADIUS	Retrieve client authentication info	<	AP or Controllers
2002	TCP	HTTPS	Retrieve client authentication info	>	ACS
2719	UDP	OSU	Discovery probe	<	Proxim
5050	UDP	RTLS	Real Time Location Feed	<	Alcatel-Lucent thin APs
8211	UDP	PAPI	Real Time Feed	< >	Alcatel-Lucent WLAN Switches
		ICMP	Ping Probe	>	APs or controllers

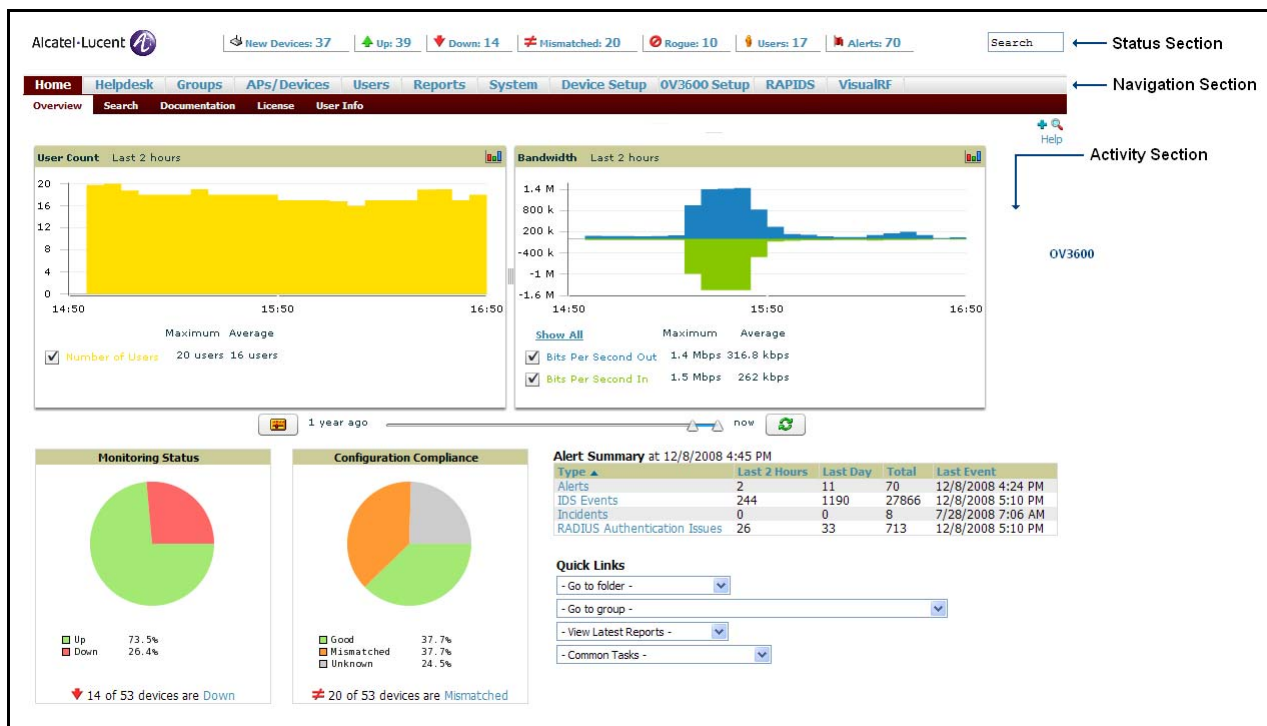
OV3600 Navigation Basics

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 3](#) illustrates these sections.

Figure 3 OV3600 GUI Layout: Home > Overview Example



Status Section

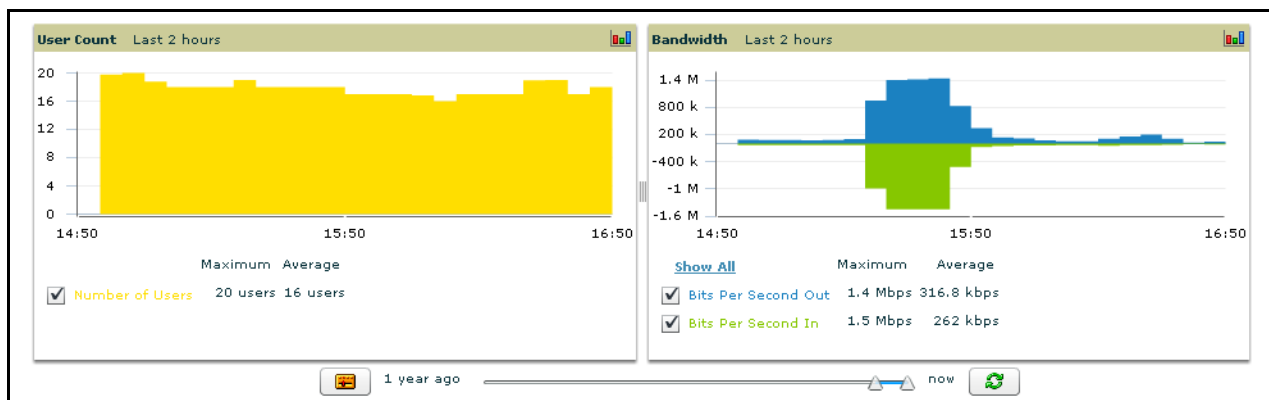
The **Status** Section provides a snapshot view of overall WLAN performance and provides direct links for immediate access to key system components. The table below describes these elements in further detail.

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	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	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 APs. An AP is considered mismatched when the desired configuration in OV3600 does not match the actual device configuration read off of the AP.
Rogue	The number of unknown APs detected on the network by OV3600 with a score of five. A score of five means the rogues were discovered via wireless or wireline fingerprint scanning techniques. When you click this link, OV3600 will direct you to a page that displays a detailed list of all Rogue APs. NOTE: A newly discovered AP is considered a "Rogue" if it is not a supported AP that OV3600 can manage and monitor. If the newly discovered AP is capable of being managed and monitored by OV3600 it will be classified as a "New" device rather than a "Rogue."
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.
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.

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

Figure 4 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.
- Deselect (remove the check for) the boxes to change the data displayed on each graph. The button with green arrows refreshes data on the graph.
- 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 Enterprise Support at support@ind.alcatel.com for more information on activating this feature in the OV3600 database.

Navigation Section

The **Navigation** Section displays tabs to all main GUI pages within the 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	<p>The Home page provides basic OV3600 information including system name, host name, IP address, current time, running time, and software version.</p> <p>The Home page also provides a central point for network status information and monitoring tools, giving graphical display of network activity.</p> <p>The Home > Overview page provides links to many of the most frequent tools in OV3600.</p> <p>For additional information, refer to “Using the Home Pages” on page 196.</p>	<ul style="list-style-type: none"> • Overview • Search • Documentation • License • User Info
Helpdesk	<p>The Helpdesk page provides an interface for support and diagnostic tools.</p> <p>For additional information refer to Chapter 11, “Using the OV3600 Helpdesk” on page 263.</p>	<ul style="list-style-type: none"> • Incidents • Setup
Groups	<p>The Groups page provides information on the logical "groups" of devices that have been established for efficient monitoring and configuration. For additional information, see Chapter 5, “Configuring and Using Groups in OV3600” on page 65.</p> <p>NOTE: Some of the tabs will not appear for all groups. Tabs are visible based on the device type field on the Groups > Basic page.</p> <p>NOTE: When specified, device-level settings override the default Group-level settings.</p>	<ul style="list-style-type: none"> • List • Focused Sub-Menus <ul style="list-style-type: none"> • Monitor • Basic • Templates • Security • SSIDs • AAA Servers • Radio • Cisco WLC Radio • LWAPP APs • WiMAX • Proxim Mesh • Colubris • MAC ACL • Firmware

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

Main Tab	Description	Sub-Menus
APs/Devices	<p>The APs/Devices page provides detailed information about all authorized APs and wireless LAN switches or controllers on the network, including all configuration and current monitoring data.</p> <p>This page interacts with several additional pages in OV3600. One chapter to emphasize the APs/Devices page is Chapter 7, “Discovering and Managing Devices” on page 141.</p> <p>NOTE: When specified, device-level settings override the default Group-level settings.</p>	<ul style="list-style-type: none"> ● List ● New ● Up ● Down ● Mismatched ● Ignored ● Focused Sub-Menus <ul style="list-style-type: none"> Ⓢ Manage Ⓢ Audit Ⓢ Compliance
Users	<p>The Users page provides detailed information about all client devices and users currently associated to the WLAN. For additional information, refer to “Using the OV3600 Users Page” on page 188.</p>	<ul style="list-style-type: none"> ● Connected ● All ● Guest Users ● Tags ● User Detail
Reports	<p>The Reports page lists all the standard and custom reports generated by OV3600. OV3600 Version 6.2 supports 13 reports in the primary GUI module. For additional information, refer to Chapter 10, “Creating, Running, and Emailing Reports” on page 229.</p>	<ul style="list-style-type: none"> ● Generated ● Definition ● Focused Sub-Menus <ul style="list-style-type: none"> Ⓢ Details
System	<p>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 “Using System Pages” on page 202.</p>	<ul style="list-style-type: none"> ● Status ● Event Log ● Triggers ● Alerts ● Configuration Change Jobs ● Firmware Upgrade Jobs ● Performance
Device Setup	<p>The Device Setup page provides information related to the configurations of devices on the WLANs, including AP discovery parameters, firmware management, VLAN definition, and so forth. For additional information, refer to Chapter 4, “Enabling OV3600 to Manage Your Devices” on page 57.</p>	<ul style="list-style-type: none"> ● Discover ● Add ● Communication ● Upload Files
OV3600 Setup	<p>The OV3600 Setup page provides 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 the OmniVista 3600 Air Manager” on page 33.</p> <p>NOTE: The OV3600 Setup page may not be visible, depending on the role and license set in OV3600.</p>	<ul style="list-style-type: none"> ● General ● Network ● Users ● Roles ● Authentication ● WLSE ● ACS ● NMS ● RADIUS Accounting ● PCI Compliance
RAPIDS	<p>The RAPIDS page provides all information relating to rogue access points. Including methods of discovery and lists of discovered and possible rogues. For additional information, refer to “Deploying RAPIDS in OV3600 6.2” on page 173.</p> <p>NOTE: The RAPIDS page may not be visible, depending on the role and license set in OV3600.</p>	<ul style="list-style-type: none"> ● Overview ● Rogue APs ● Setup ● Score Override

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

Main Tab	Description	Sub-Menus
VisualRF	<p>VisualRF pages provide access to floor plans, client location, and RF visualization. For additional information, refer to the <i>VisualRF User Guide</i>.</p> <p>NOTE: VisualRF may not be visible, depending on the role and license set in OV3600.</p>	<ul style="list-style-type: none"> ● Overview ● Floor Plans ● Campus/Building ● Setup ● Import
Master Console	<p>The Master Console page provides a centralized location to manage multiple OV3600s. For additional information, refer to “Using the Master Console” on page 225.</p> <p>NOTE: The Master Console page may not be visible, depending on the role and license set in OV3600.</p>	<ul style="list-style-type: none"> ● Overview ● Managed OV3600s ● Alerts ● Search



The OV3600 Setup tab varies based on your or the user’s role. The Master Console, 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 help document with information describing the OV3600 page that is currently displayed.



[Adobe Reader](#) must be installed to view the settings and default values.PDF help file.

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		Acknowledge and clear an OV3600 alert.
Add		Add the object to both OV3600' database and the onscreen display list.
Add Folder		Add a new folder to hierarchically organize APs.
Alert		Indicates an alert.
Apply		Apply all "saved" configuration changes to devices on the WLAN.

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

Buttons and Icons	Appearance ^a	Description
Attach		Attach a snapshot of an OV3600 screen to a Helpdesk incident.
Audit		Read device configuration, compare to desired, and update status.
Bandwidth		Current bandwidth for group.
Choose		Choose a new Helpdesk incident to be the Current Incident.
Create		Create a new Helpdesk incident.
Customize		Ignore selected settings when calculating the configuration status.
Delete		Delete an object from OV3600' database.
Down		Indicate down devices and radios.
Duplicate		Duplicate or makes a copy of the configuration of an OV3600 object.
Edit		Edit the object properties.
Email		Link to email reports.
Filter		Filter rogue list by score and/or ad hoc status.
Google Earth		View device's location in Google Earth (requires plug-in).
Manage		Manage the object properties.
Monitor		Indicates an access point is in "monitor only" mode.
Ignore		Ignore specific device(s) - devices selected with check boxes.
Import		Update a Group's desired settings to match current settings.
Mismatched		Indicates mismatched access points.
New Devices		Indicates new access points and devices.
Poll Now		Poll device (or controller) immediately, override group polling settings.
Preview		Display a preview of changes applicable to multiple groups.
Print		Print the report.
Reboot		Reboot devices or OV3600.
Relate		Relates an AP, Group or Client to a Helpdesk incident.

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

Buttons and Icons	Appearance ^a	Description
Replace Hardware		Confers configuration and history of one AP to a replacement device.
Revert		Return all configurable data on the screen to its original status.
Rogue		Indicates a rogue access point.
Run		Run a new user-defined report.
Save		Save the information on the page in the OV3600 database.
Save & Apply		Save changes to OV3600' database and apply all changes to devices.
Scan		Scans for devices and rogues using selected networks.
Schedule		Schedule a window for reports, device changes, or maintenance.
Search		Search OV3600 for the specified name, MAC or IP address.
Up		Indicates access points which are in the up status.
Update Firmware		Apply a new firmware image to an AP/device.
User		Indicates a user.
VisualRF		Link to VisualRF - real time visualization.
XML		Link 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.

Initial Login

Use your browser to navigate to the static IP address assigned to internal page of the OV3600. Once your session launches, the **Authentication Dialog Box** appears as shown in [Figure 5](#).

Figure 5 *Authentication Dialog Box*



Perform these steps to complete the initial login.

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



OV3600 pages are protected via SSL.

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



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 42](#) for additional information.

OV3600 Version 6.2 Interface Overview

This document presents many tools for managing and optimizing the wireless network. The two primary graphical user interfaces (GUIs) in Version 6.2 include the OV3600 and VisualRF modules.

Introduction

This chapter provides basic procedures for configuring OV3600 on the network after installation is complete. This chapter contains the following procedures:

Required Configurations

- Specifying General OV3600 Server Settings
- Defining OV3600 Network Settings
- Creating OV3600 User Roles

Optional Configurations

- Configuring TACACS+ Integration (Optional)
- Integrating with WLSE Rogue Scanning (Optional)
- Integrating ACS (Optional)
- Integrating with an Existing Network Management Solution (Optional)
- Integrating OV3600 with a RADIUS Accounting Server (Optional)

WMS Offload in OV3600 Version 6.2

- Deploying WMS Offload in OV3600
 - Overview of WMS Offload in OV3600
 - General Configuration Tasks Supporting WMS Offload in OV3600
 - Additional Information Supporting WMS Offload

**NOTE**

Additional configurations of multiple types remain available after basic configurations are complete. Some or several advanced configurations in later chapters may require completion of the required or optional configurations contained in this chapter.

Specifying General OV3600 Server Settings

The first step in configuring OV3600 is to specify the general settings for the OV3600 server. [Figure 6](#) illustrates the page sections in which these settings are defined and changed. This procedure describes fields in columns, progressing first through the left-side columns, then continue down the right side of this GUI. This page features the following major sections:

- **General**
- **Local Network Device Discovery**
- **Display Options**
- **Configuration Options**
- **External Syslog**
- **Historical Data Retention**
- **Default Firmware Upgrade Options**
- **Additional OV3600 Services**
- **Performance Tuning**

Figure 6 OV3600 Server Settings

General	
System Name:	OV3600
Automatically Monitor/Manage New Devices:	No
Default Group:	Acme Corporation (SSID: LucID)
Device Configuration Audit Interval:	Never
Automatically Repair Misconfigured Devices:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Send Debugging Messages to AirWave Wireless:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Nightly Maintenance Time (00:00 - 23:59):	17:59
AMP User Authorization Lifetime (0-240 min):	5

Local Network Device Discovery	
Devices can also be discovered through SNMP and HTTP scans on the Device Discovery page.	
Proxim/ORINOCO Autonomous APs:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Symbol and Intel Autonomous APs (WNMP):	<input type="radio"/> Yes <input checked="" type="radio"/> No

Display Options	
Use Fully Qualified Domain Names: Cisco IOS only	<input checked="" type="radio"/> Yes <input type="radio"/> No
Show Vendor-Specific Device Settings For:	All devices
Look up Wireless User Hostnames:	<input checked="" type="radio"/> Yes <input type="radio"/> No
DNS Hostname Lifetime:	24 hours

Configuration Options	
Allow Guest User Configuration in Monitor-Only Mode:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow WMS Offload Configuration in Monitor-Only Mode:	<input type="radio"/> Yes <input checked="" type="radio"/> No

External Syslog	
Syslog Server:	10.51.51.51
Syslog Port:	514
Include Event Log Messages:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Event log facility:	local3
Include Audit Log Messages:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Audit log facility:	local1
<input type="button" value="Send Test Email"/>	

Historical Data Retention	
Inactive User Data (2-1500 days):	1500
User Association History (2-550 days):	30
Tag History (2-550 days):	14
Rogue AP Discovery Events (2-550 days): <small>Cannot be smaller than the delete rogues not heard for window (14) configured on the RAPIDS Setup page.</small>	60
Reports (2-550 days):	30
Automatically Acknowledge Alerts (0-550 days, 0 disables):	7
Acknowledged Alerts (2-550 days):	14
Traps from Managed Devices (0-550 days, 0 disables):	14
Archived Device Configurations (1-100):	10
Guest Users (0-550 days, 0 disables):	30
Closed Helpdesk Incidents (0-550 days, 0 disables):	30

Default Firmware Upgrade Options	
Allow Firmware Upgrades in Monitor-Only Mode:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Simultaneous Jobs (1-20):	20
Simultaneous Devices Per Job (1-1000):	20
Failures Before Stopping (0-20, 0 disables):	1

Additional AMP Services	
Enable FTP Server: <small>required to manage Cisco Aironet 4800 APs, also optionally for Aruba, Cisco IOS and Trapeze firmware upgrades.</small>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use Embedded Mail Server:	<input checked="" type="radio"/> Yes <input type="radio"/> No
<input type="button" value="Send Test Email"/>	

Performance Tuning	
Monitoring Processes (1-4):	2
Maximum Number Of Configuration Processes (1-20):	10
Maximum Number Of Audit Processes (1-20):	10
Verbose Logging Of SNMP Configuration:	<input checked="" type="radio"/> Yes <input type="radio"/> No
SNMP Rate Limiting for Monitored Devices:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Perform the following steps to configure the general OV3600 server settings.

1. Browse to the **OV3600 Setup > General** page, locate the **General** area, and enter the information itemized in [Table 6](#):

Table 6 *OV3600 Setup > General Page, General Section Fields*

Setting	Default	Description
System Name	OV3600	Defines your name for the OV3600 server, with a maximum limit of 20 alphanumeric characters.
Console Refresh Rate	60	Launches a drop-down menu that specifies the number of seconds (5, 10, 15, 30, 60, 120 and never) between screen refreshes on OV3600 monitoring screens.
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 on the Groups > List page.
Default Folder*	NA	Sets the folder used when automatically monitoring or managing new devices. The default folder is the top folder of the default group. It is calculated as the lowest folder that is still able to view all of the APs in a group. The Default Folder field is only visible when OV3600 is set to Automatically Monitor or Manage New Devices.
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 greater 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 OV3600 detects a variance between actual device settings and the Group configuration policy in the OV3600 database.
Email 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 bandwidth demand.
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.
DNS Lookup of 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 Cleanup Period	1 hour	Sets the period after which OV3600 refreshes the DNS lookup.

- On the **OV3600 Setup > General** page, locate the **Local Network Device Discovery** area, and indicate whether or not you want to use the specified local broadcast protocols for discovering new and rogue devices. [Table 7](#) describes the settings and default values of this section.



Local broadcast protocols typically work only on the local subnet to which OV3600 is connected. Cisco Discovery Protocol (CDP) works on both local and remote subnets when it is enabled and OV3600 is configured to access (read only) CDP information from the appropriate routers and switches.

Table 7 OV3600 Setup > General, *Auto-Discovery*

Setting	Default	Description
Proxim/ORiNOCO	Disabled	When enabled, OV3600 runs the OSU-NMS Protocol service to discover ORiNOCO Devices on the local subnet. Every 20 seconds OV3600 sends a packet to the broadcast address of the local network. Proxim/ORiNOCO Devices respond to OV3600.
Symbol and Intel Autonomous APs (WNMP)	Disabled	When enabled, OV3600 runs WNMP and the Intel IAPP service to discover Symbol and Intel access points on the local OV3600 subnet.

- 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 groups.



Changes to this section apply across the entire OV3600 implementation. These changes affect all users and all new groups.

[Table 8](#) describes the settings and default values in this section.

Table 8 OV3600 Setup > General, *Display Options*

Setting	Default	Description
Show Device Settings For:	All Devices	Launches a drop-down menu that determines which Group tabs and options are viewable by default in new groups. This field has three options, as follows: <ul style="list-style-type: none"> All Devices—When selected, OV3600 displays all Group tabs and setting options. Only Devices on this OV3600—When selected, OV3600 hides all options and tabs that do not apply to the APs and devices currently on OV3600. Selected device types—When selected, this option allows the user to specify the device types for which OV3600 displays Group settings.
Selected Device Types	None	Selects the device types that are likely to be in a group. When selected, OV3600 only displays configuration information related to the defined device types.

- 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 9](#) describes the settings and default values of this section.

Table 9 OV3600 Setup > General, Configuration Options

Setting	Default	Description
Allow Guest User Configuration in Monitor-Only Mode	No	When Yes is defined, new Cisco WLC and Alcatel-Lucent guest access users can be pushed to the controller while the controller is in monitor-only mode in OV3600. The controller does not reboot as a result of the push.
Allow WMS Offload Configuration in Monitor-Only Mode (for Alcatel-Lucent devices only)	No	When Yes is defined, the WMS offload feature on the Groups > Basic page can be enabled for Alcatel-Lucent WLAN Switches in monitor-only mode. Enabling WMS offload does not cause a controller to reboot.

- On the **OV3600 Setup > General** page, locate the **External Syslog** section and adjust settings as required.
- On the **OV3600 Setup > General** page, locate the **Historical Data** 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.

Table 10 OV3600 Setup > General, Historical Data Retention

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.
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.
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, 0 disables)	14	Defines the number of days OV3600 retains information about SNMP traps from Managed Devices.

- 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

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.
Number of Simultaneous Jobs (1-20)	20	Defines the number of jobs OV3600 runs at the same time. A job can include multiple APs.
Default number of devices to be upgraded simultaneously (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.
Default number of failures before stopping	1	Sets the default number of upgrade failures before OV3600 pauses the upgrade process. User intervention is required to resume the upgrade process.
Serve firmware files from this page	Primary	Sets the IP address from which the devices retrieve the firmware file.

8. On the **OV3600 Setup > General** page, locate the **Display Options** section, and adjust settings as required. [Table 12](#) describes the settings and default values of this section.

Table 12 OV3600 Setup > General, Display Options

Setting	Default	Description
Use Fully Qualified Domain Names	Enabled	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."
Show Device Settings For	All Devices	Selects the device types for which to use fully qualified domain names.

9. On the **OV3600 Setup > General** page, locate the **Additional OV3600 Services** section, and adjust settings as required. [Table 13](#) describes the settings and default values of this section.

Table 13 OV3600 Setup > General, Additional OV3600 Services

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.

10. 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 Enterprise Support at support@ind.alcatel.com if you think you might need to change any of these settings. [Table 14](#) describes the settings and default values of this section.

Table 14 OV3600 Setup > General, Performance Tuning

Setting	Default	Description
Monitoring Processes	Based on the number of cores for your sever	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 Enterprise Support at support@ind.alcatel.com 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. contact Alcatel-Lucent Enterprise Support at support@ind.alcatel.com 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 are auditing configurations for your devices, as an option. The optimal setting for your network depends on the resources available, especially ram. Please contact Alcatel-Lucent Enterprise Support at support@ind.alcatel.com if you think you might need to increase this setting for your network.

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

What Next?

- Continue with the additional required or optional setup configurations contained in this chapter.
- Click the **Setup** button to return to the starting point for additional setup configurations.
- Several additional chapters in this document describe additional configurations or tasks that enable critical functions of OV3600. *Complete the required and desired 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.
- Return to any monitoring screen to commence or to continue network monitoring.

Defining OV3600 Network Settings

The next step in configuring OV3600 is confirming the network settings. These settings are defined by selecting **OV3600 Setup > Network** in the OV3600 GUI. [Figure 7](#) illustrates the contents of this page section.

Figure 7 Setup > Network Page, Activity Section

Perform the following steps to define the OV3600 network settings:

1. Browse to the **OV3600 Setup > Network** page and locate the **Primary Network Interface** area. The information in this section should match those defined during initial network configuration and should not require changes. [Table 15](#) describes the settings and default values.

Table 15 OV3600 Setup > Network, Primary Network Interface

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.

2. On the **OV3600 Setup > Network** page, locate the **Secondary Network Interface** area. The information in this section only needs to be completed if the server running OV3600 is using a second network interface. [Table 16](#) and [Table 17](#) describe these settings in more detail.

Table 16 OV3600 Setup > Network, Secondary Network Interface

Setting	Default	Description
IP Address	None	Sets the IP address of the OV3600 secondary network interface. This address must be a static IP address.
Subnet Mask	None	Sets the subnet mask for the OV3600 secondary network interface.

- On the **OV3600 Setup > Network** page, locate the **Network Time Protocol (NTP)** area. The Network Time Protocol is used to synchronize the time between OV3600 and your network reference server.



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

To disable NTP services, simply 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 17](#) describes the settings and default values in more detail.

Table 17 OV3600 Setup > Network, Secondary Network

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.

- On the **OV3600 Setup > Network** page, locate the **External Syslog** area. Use this section to configure OV3600 to send audit and system events to an external syslog server. [Table 18](#) describes these settings and default values.

Table 18 OV3600 Setup > Network, External Syslog

Setting	Default	Description
Include event log messages	No	Select yes radio button to send event log messages to an external syslog server.
Include audit log messages	No	Select yes radio button to send audit log messages to an external syslog server.

- On the **OV3600 Setup > Network** page, locate the **Static Routes** area. Use this section when OV3600 needs to reach certain networks that are inaccessible through the default gateway. It is likely that you leave this section blank in most circumstances.
 - To add a new static route, click the **Add** button. On the following screen enter the Network (IP address), Subnet Mask, and Gateway information, then click **Add**.
 - To delete an existing static route, check the box next to the static route you want to remove and click **Delete**.
- Click **Save** when all changes have been completed. This action restarts any affected services and may disrupt temporarily your network connection.

What Next?

- Continue with the additional required or optional setup configurations contained in this chapter.
- Click the **Setup** button to return to the starting point for additional setup configurations.
- Several additional chapters in this document describe additional configurations or tasks that enable critical functions of OV3600.
 - 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.
 - The optional procedures in this chapter may be completed or changed at any time.
- Return to any monitoring screen to commence or to continue network monitoring.

Creating OV3600 User Roles

The **User Role** page of the OV3600 GUI 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 that they have access to in OV3600 (although only visible APs appear on the floorplan).

Users can also see any building that contains a visible floorplan, 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. [Figure 8](#) illustrates the OV3600 GUI for such role configurations.

Commencing with OV3600 Version 6.2, User Roles can be created with access to folders within multiple branches of the overall hierarchy. This feature is designed to assist non-administrative users (such as help desk or IT staff) who support a subset of accounts or sites within a single OV3600. Prior to the 6.2 release, OV3600 user roles could only be assigned to a single top folder (such as "West Coast" or "European Stores"). 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-admin users will only be able to see data and users for devices within their assigned subset of folders.

Figure 8 *OV3600 Setup > Roles*

Role Name	Enabled	Type	Access Level	Top Folder	RAPIDS	VisualRF
Administration	Yes	AMP Administrator	-	Top	Read/Write	Enabled
Read-Only Monitoring & Auditing	Yes	AP/Device Manager	Audit (Read Only)	Top	None	Disabled

Role	
Role Name:	Read-Only Monitoring & Auditi
Enabled:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Type:	AP/Device Manager
AP/Device Access Level:	Manage (Read/Write)
Top Folder:	Top
RAPIDS:	None
VisualRF:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Roles define the type, privileges and the viewable groups and APs. [Table 19](#) describes the settings and default values of this section.

Table 19 *OV3600 Setup > Roles, Roles*

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

Table 19 OV3600 Setup > Roles, Roles (Continued)

Setting	Default	Description
Type	None	<p>Defines the type of role. OV3600 supports the following types of roles:</p> <ul style="list-style-type: none"> ● OV3600 Administrator—The OV3600 (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 (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. ● OV3600 Management Client—Defines the OV3600 user. The user information defined in AMC must match the user with the OV3600 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.
Access Level	None	<p>Defines the privileges the role has over the viewable APs. OV3600 supports three privilege levels, as follows:</p> <ul style="list-style-type: none"> ● 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 the devices and Groups. Monitor users can not view the APs/Devices > Audit page which may contain sensitive information, including AP passwords.
Top Folder	None	<p>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.</p> <p>NOTE: OV3600 Version 6.2 enhances folder viewability as defined by roles. Version 6.2 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 <i>subset of accounts or sites</i> within a single OV3600 deployment, such as help desk or IT staff.</p> <p>Prior to Version 6.2, 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.</p>
RAPIDS	None	<p>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:</p> <ul style="list-style-type: none"> ● Read/Write—The user may ignore, delete, override scores and perform OS scans. ● Read Only—The user can view the RAPIDS pages but cannot make any changes to rogue APs or perform OS scans. ● None—Cannot view the RAPIDS tab or any Rogue APs.
VisualRF	None	<p>Defines custom VisualRF settings. Default privileges with regard to VisualRF are as follows:</p> <ul style="list-style-type: none"> ● Administrators have access to VisualRF. ● Read-Only users have access to VisualRF. ● Read/Write AP/Device Managers, and VisualRF permissions are set with the radio button. <p>Whether a Role is defined as Manage or Monitor, a user is able to view floor plans in VisualRF and Quick View.</p> <p>When specifying VisualRF rights, selecting Yes for a Role defined as Manage allows the user to modify VisualRF as well.</p> <p>Selecting No in a Role defined as Manage allows the user only to view floor plans in VisualRF, not to modify them.</p>

User Roles in VisualRF and QuickView

Note the following factors in relation to user roles and VisualRF and QuickView:

- Whether a Role is defined as Manage or Monitor, the user can view floor plans in VisualRF and QuickView.
- Specifying **VisualRF: Yes** in a Role defined as Manage allows the user to modify VisualRF as well.
- Specifying **VisualRF: No** in a Role defined as Manage allows the User only to view floor plans in VisualRF, not modify them.

What Next?

- Continue with the additional required or optional setup configurations contained in this chapter.
- Click the **Setup** button to return to the starting point for additional setup configurations.
- Several additional chapters in this document describe additional configurations or tasks that enable critical functions of OV3600.
 - *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.
 - The optional procedures in this chapter may be completed or changed at any time.
- Return to any monitoring screen to commence or to continue network monitoring.

Creating OV3600 Users

OV3600 installs with only one user, the OV3600 **administrator**, **admin**. The administrator has these specific parameters and authorizations within OV3600:

- The administrator is able to define additional users with varying levels of privilege.
- The administrator can limit the viewable devices as well as the type of access a user has to the devices.

For each **user**, a **Username**, **Password** and a **Role** are defined. The username and password are used when logging in to the OV3600 GUI. It is helpful to use unique and meaningful user names as they are recorded in the log files when changes are made in OV3600.

The **role** defines the user type, access level and the top folder. Roles are defined on the OV3600 **Setup > Roles** page. The **admin** can provide optional additional information about the user including the user's real name, email address, phone number, and so forth. [Figure 9](#) illustrates the contents and layout of this page.

Figure 9 OV3600 Setup > Users, Activity Section

The screenshot displays the 'Users, Activity' section of the OV3600 Setup interface. At the top left, there is an 'Add' button and a 'New User' link. Below this is a table with the following columns: Username, Role, Enabled, Type, Access Level, Top Folder, RAPIDS, Name, Email Address, Phone, and Notes. The table contains three entries: 'admin' (Role: Administration, Enabled: Yes, Type: Administrator, Access Level: -, Top Folder: Top, RAPIDS: Read/Write), 'Bryan' (Role: Administration, Enabled: Yes, Type: Administrator, Access Level: -, Top Folder: Top, RAPIDS: Read/Write, Name: Bryan, Email Address: Bryan@ave.com), and 'Paul' (Role: Administration, Enabled: Yes, Type: Administrator, Access Level: -, Top Folder: Top, RAPIDS: Read/Write, Name: Paul, Email Address: paul@ave.com). Below the table are 'Check All' and 'Uncheck All' links, and a 'Delete' button. At the bottom, there is a 'User' form with fields for Username, Role (a dropdown menu currently set to 'Administration'), Password, Confirm Password, Name, Email Address, Phone, and Notes.

Username	Role	Enabled	Type	Access Level	Top Folder	RAPIDS	Name	Email Address	Phone	Notes
admin	Administration	Yes	Administrator	-	Top	Read/Write				
Bryan	Administration	Yes	Administrator	-	Top	Read/Write	Bryan	Bryan@ave.com		
Paul	Administration	Yes	Administrator	-	Top	Read/Write	Paul	paul@ave.com		

Perform the following steps to create and configure OV3600 users.

1. On the **OV3600 Setup > Users** page, set and change **Usernames**, **Passwords** and **Roles**.

- Roles are defined on the **Setup > Roles** page. The role defines the top viewable folder, type and access level of the user.

OV3600 Version 6.2 enhances folder viewability as defined by roles. Version 6.2 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 6.2, 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.

- The **Name, E-Mail, Phone** and **Notes** fields are completely optional. They are provided to help administrators keep track of their users.



The **Username** field is ignored when a role of type OV3600 Management Client is selected.

2. To delete a user from OV3600, select the user by clicking the checkbox, and click the **Delete** button.

[Table 20](#) describes the settings and default values for the user attributes that can be defined in this procedure.

Table 20 *OV3600 Setup > User*

Setting	Default	Description
Username	None	Sets the username as an alphanumeric string. The Username is used when logging in to OV3600 and in the log files.
Role	None	Specifies the User Role that defines the Top viewable folder, type and access level of the user.
Enabled	Yes	Displays the status of the Role. If a Role is disabled, any users associated with it are not be able to log in to OV3600. Roles are enabled from the Setup > Roles page.
Type	None	Defines the type for the user being configured. There are three types of users in OV3600, as follows: <ul style="list-style-type: none"> ● OV3600 Administrator—The OV3600 Administrator has full access to OV3600 and all of the APs. The administrator can view and edit all settings and all APs in OV3600. Only the OV3600 Administrator can create new Users and access all of the OV3600 Setup pages. ● 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. AP/Device Managers are limited to the NMS sub tab of the OV3600 Setup pages. ● OV3600 Management Client—Defines the AMC user. The user information defined in AMC must match the user with the OV3600 Management Client type.
Access Level	None	Specifies the privileges an AP/Device Manager has over the viewable APs. Any one of three privilege levels may be defined: <ul style="list-style-type: none"> ● Manage (Read/Write)— Manage users have read/write access to the viewable APs and Groups. They can change all OV3600 settings for the APs and Groups they can view. ● Audit (Read Only)— Audit users have read only access to the viewable APs and Groups. Audit users have access to the APs/Devices > Audit page, which may contain sensitive information, including AP passwords. ● Monitor (Read Only)— Similar to the Audit role, monitor users have read only access to the APs and Groups. However monitor users can not view the APs/Devices > Audit page which may contain sensitive information including AP passwords.

Table 20 *OV3600 Setup > User*

Setting	Default	Description
Top Folder	None	Defines the Top viewable folder for the user. The user is able to view all APs and groups contained by the Top folder. You cannot assign a top folder that would give a user access to only part of a group. If the top folder and its subfolders contain one AP from a group, they must contain all APs in that group.
RAPIDS	None	Specifies the RAPIDS privileges for the user's role. Any one of three privilege levels may be defined. <ul style="list-style-type: none"> • Read/Write—The user may Ignore, Delete, override scores and perform OS scans. • Read Only—The user can view the RAPIDS pages but can not make any changes to rogue APs or perform OS scans. • None—Cannot view the RAPIDS tab or any Rogue APs.
Name	None	Allows you to define an optional and alphanumeric text field that takes note of the user's actual name.
E-Mail	None	Allows you to define an optional text field that takes note of the user's email address.
Phone	None	Allows you to define an optional field that takes note of the user's phone number.
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. NOTE: OV3600 installs with one default user " admin ". Because the default user's password is identical to its name, it is strongly recommended that this password be changed. You must create a " client " user with a type of OV3600 Management Client to facilitate communication between an OV3600 and an AMC. Alcatel-Lucent strongly recommends that you immediately change the default OV3600 " admin " password.

What Next?

- Continue with the additional required or optional setup configurations contained in this chapter.
- Click the **Setup** button to return to the starting point for additional setup configurations.
- Several additional chapters in this document describe additional configurations or tasks that enable critical functions of OV3600.
 - *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.
 - The optional procedures in this chapter may be completed or changed at any time.
- Return to any monitoring screen to commence or to continue network monitoring.

Configuring TACACS+ Integration (Optional)

OV3600 can be configured to use an external user database to simplify password management for OV3600 administrators and users. For this capability, OV3600 needs to be configured with the IP/Hostname of the TACACS+ server, port and server secret. [Figure 10](#) illustrates these settings.

Figure 10 OV3600 Setup > TACACS Configuration

TACACS Configuration	
Enable TACACS+ Authentication and Authorization:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Primary TACACS+ Server IP/Hostname:	<input type="text"/>
Primary TACACS+ Server Port:	<input type="text" value="49"/>
Primary TACACS+ Server Secret:	<input type="text"/>
Confirm Primary TACACS+ Server Secret:	<input type="text"/>
Secondary TACACS+ Server IP/Hostname:	<input type="text"/>
Secondary TACACS+ Server Port:	<input type="text" value="49"/>
Secondary TACACS+ Server Secret:	<input type="text"/>
Confirm Secondary TACACS+ Server Secret:	<input type="text"/>

Perform these steps to configure optional TACACS+ integration:

1. 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.
2. Next, you must 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 exactly match name of the role defined on the **Setup > Roles** page.
 - The defined role should use the following format: `role=<name_of_OV3600_role>`. One example is as follows:

```
role=DormMonitoring
```

Like routers and switches, OV3600 does not need to know anything about the usernames.

3. 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 **Setup > TACACS+** page.
4. 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.

What Next?

- Continue with the additional required or optional setup configurations contained in this chapter.
- Click the **Setup** button to return to the starting point for additional setup configurations.
- Several additional chapters in this document describe additional configurations or tasks that enable critical functions of OV3600.
 - *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.
 - The optional procedures in this chapter may be completed or changed at any time.
- Return to any monitoring screen to commence or to continue network monitoring.

Integrating with WLSE Rogue Scanning (Optional)

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.

Refer to “[WLSE Configuration](#)” on page 273 for instructions about configuring the Cisco WLSE to communicate with OV3600.

[Figure 11](#) illustrates and itemizes the OV3600 settings for communication that is enabled between OV3600 and WLSE.

Figure 11 *OV3600 Setup > WLSE*

The screenshot displays the 'WLSE' configuration page in the OV3600 interface. At the top, there is an 'Add' button and a 'New WLSE' link. Below this is a table with the following data:

IP/Hostname	Protocol	Port	Username	Poll for AP Discovery	Poll for Rogue Discovery	Polling Period	Last Contacted	Errors
<input type="checkbox"/> wlse.dev.airwave.com	HTTPS	443	admin	Yes	Yes	10 minutes	5/14/2007 1:09 PM	

Below the table, there is a 'Delete' button and a 'Select All - Unselect All' link. A 'Delete' button is also present to the left of the configuration form. The configuration form is titled 'WLSE' and contains the following fields:

- IP/Hostname: [Text Input]
- Protocol: HTTP (Dropdown)
- Port: 1741 (Text Input)
- Username: [Text Input]
- Password: [Text Input]
- Confirm Password: [Text Input]
- Poll for AP Discovery: Yes No
- Poll for Rogue Discovery: Yes No
- Polling Period: 10 minutes (Dropdown)

At the bottom of the form are 'Add' and 'Cancel' buttons.

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 21](#) describes the settings and default values.

Table 21 OV3600 Setup > WLSE

Setting	Default	Description
IP Address/ Hostname	None	This field designates the IP address or DNS Hostname for the WLSE server, which must already be configured on the Cisco WLSE server.
Protocol	HTTP	This drop-down menu specifies the protocol to be used when polling the WLSE.
Port	1741	This field defines the port OV3600 uses to communicate with the WLSE server.
Username	None	This field 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	This field 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	This option 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	This field displays the last time OV3600 was able to contact the WLSE server.
Polling Period	10 minutes	This setting determines how frequently OV3600 polls WLSE to gather rogue scanning data.
Error	None	To aid in debugging, this field displays helpful error messages if errors occur.

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?

- Continue with the additional required or optional setup configurations contained in this chapter.
- Click the **Setup** button to return to the starting point for additional setup configurations.
- Several additional chapters in this document describe additional configurations or tasks that enable critical functions of OV3600.
 - *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.
 - The optional procedures in this chapter may be completed or changed at any time.
- Return to any monitoring screen to commence or to continue network monitoring.

Integrating ACS (Optional)

The **OV3600 Setup > ACS** page allows OV3600 to poll one or more Cisco ACS servers for wireless username information. When an ACS server is specified using the **OV3600 Setup > ACS** page, OV3600 gathers information about your networks wireless users. Refer to the “[Configuring TACACS+ Integration \(Optional\)](#)” on page 47 section if you want to use your ACS server to manage your OV3600 users.

Figure 12 illustrates the for this optional configuration.

Figure 12 **OV3600 Setup > ACS**

The screenshot displays the 'OV3600 Setup > ACS' configuration page. At the top, there is an 'Add' button and the text 'New ACS Server'. Below this, a message states: 'Enter one or more Cisco ACS servers to be polled for wireless username information.' A table lists the configured ACS servers:

	IP/Hostname	Protocol	Port	Username	Polling Period	Last Contacted	Errors
<input type="checkbox"/>	tacacs.dev.com	HTTPS	2002	admin	10 minutes	Never	

Below the table, there is a 'Delete' button and a 'Check All - Uncheck All' link. A modal form titled 'ACS Server' is open, showing the following fields:

- Hostname/IP Address: [Text Input]
- Protocol: HTTP (Dropdown)
- Port: 2002 (Text Input)
- Username: [Text Input]
- Password: [Text Input]
- Confirm Password: [Text Input]
- Polling Period: 10 minutes (Dropdown)

Perform the following steps to configure the OV3600 polling of ACS Servers.

1. To specify one or more ACS servers for communication with OV3600, browse to the **OV3600 Setup > ACS** configuration page and provide the information requested. [Table 22](#) summarizes the settings of this configuration page.

Table 22 **OV3600 Setup > ACS**

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

2. 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?

- Continue with the additional required or optional setup configurations contained in this chapter.
- Click the **Setup** button to return to the starting point for additional setup configurations.
- Several additional chapters in this document describe additional configurations or tasks that enable critical functions of OV3600.
 - *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.
 - The optional procedures in this chapter may be completed or changed at any time.
- Return to any monitoring screen to commence or to continue network monitoring.

Integrating with an Existing Network Management Solution (Optional)

The **OV3600 Setup > NMS** configuration page allows OV3600 to integrate with other Network Management Solution (NMS) consoles. This optional 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 **Setup > NMS** configuration page, as follows. For additional information, contact Alcatel-Lucent Enterprise Support at support@ind.alcatel.com.

Figure 13 illustrates the contents of this optional NMS configuration.

Figure 13 OV3600 Setup > NMS, Options

To specify the NMS server that is used for OV3600 communications, browse to the **Setup > NMS** configuration page, click **Add**, and provide the information itemized and described in [Table 23](#):

Table 23 OV3600 Setup > NMS

Setting	Default	Description
Host	None	Cites the DNS name or the IP address of the NMS.
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.
Role	None	Restricts NMS servers by role, relating to the Setup > Users page.

What Next?

- Continue with the additional required or optional setup configurations contained in this chapter.
- Click the **Setup** button to return to the starting point for additional setup configurations.
- Several additional chapters in this document describe additional configurations or tasks that enable critical functions of OV3600.
 - *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.
 - The optional procedures in this chapter may be completed or changed at any time.
- Return to any monitoring screen to commence or to continue network monitoring.

Integrating OV3600 with a RADIUS Accounting Server (Optional)



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

OV3600 supports RADIUS server accounting. The **OV3600 Setup > Radius Accounting** configuration page enables this configuration, allowing OV3600 to receive RADIUS accounting records from a wide variety of RADIUS-based authentication servers and APs. OV3600 uses these records to correlate each user's MAC address to an AP with a user name from the authentication server. This capability allows OV3600 to monitor and track each user by name rather than by MAC address.

This is an optional configuration, enabling the advanced functionality just described. This capability is not required for basic OV3600 operation, but can increase the user-friendliness of OV3600 administration in large networks. [Figure 14](#) illustrates the settings of this optional configuration interface.

Supporting RADIUS Server Accounting in OV3600

Perform the following steps and configurations to enable OV3600 to receive accounting records from a separate RADIUS server. [Figure 14](#) illustrates the display of RADIUS accounting clients already configured, and [Figure 15](#) illustrates the **Add RADIUS Accounting Client** page.

Figure 14 *OV3600 Setup > Radius Accounting*

	IP/Network	Nickname
<input type="checkbox"/>	10.0.0.0/8	test
<input type="checkbox"/>	10.11.0.0/16	off_site_network

Check All - Uncheck All

Delete

Figure 15 *OV3600 Setup > RADIUS, Add RADIUS Accounting Client*

RADIUS Accounting Client

IP/Network:
Example Network entry: 10.0.0.0/8

Nickname:

Shared Secret:

Confirm Shared Secret:

Add Cancel

1. To specify the RADIUS authentication server or network, browse to the **OV3600 Setup > RADIUS Accounting** page and click **Add**, illustrated in [Figure 15](#), and provide the information described in [Table 24](#).

Table 24 OV3600 Setup > Radius Accounting

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 [“Security Integration for OV3600” on page 277](#).
- Continue with the additional required or optional setup configurations contained in this chapter.
- Click the **Setup** button to return to the starting point for additional setup configurations.
- Several additional chapters in this document describe additional configurations or tasks that enable critical functions of OV3600.
 - *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.
 - The optional procedures in this chapter may be completed or changed at any time.
- Return to any monitoring screen to commence or to continue network monitoring.

Deploying WMS Offload in OV3600

Overview of WMS Offload in OV3600

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

- Alcatel-Lucent OS Version 2.5.4 or later
- OV3600 Version 6.0 or later

The *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 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. Support for WMS Offload continues with upcoming versions of OV3600 after version 6.2, which are pending availability at the time of document publication.

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 Alcatel-Lucent WLAN Switches for optimal OV3600 monitoring.
 - Disable debugging.
 - Ensure OV3600 server is a trap receiver host.
 - Ensure proper traps are enabled.
2. Configure OV3600 to optimally monitor the Alcatel-Lucent infrastructure.
 - Enable WMS offload.
 - Configure SNMP communication.
 - Create a proper policy for monitoring Alcatel-Lucent infrastructure.
 - Discover the infrastructure.
3. Configure device classification.
 - Set up rogue classification.
 - Set up rogue classification override.
 - Establish user classification override devices.
4. Deploy 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. Utilize RTLS for increasing location accuracy (optional).
 - Enable RTLS service on the OV3600 server.
 - Enable RTLS on Alcatel-Lucent Infrastructure.

Additional Information Supporting WMS Offload

For additional information, to include detailed concepts, configuration procedures, restrictions, Alcatel-Lucent infrastructure, and OV3600 version differences in support of WMS Offload, refer to the following resources:

- *Aruba/Alcatel-Lucent's Best Practices Guide*—primary WMS Offload support information

Introduction

Once OV3600 is configured and operational on the network, the next task is to define the basic settings that allow OV3600 to communicate with and manage your devices. This chapter contains the following procedures for doing so, both of which are required:

- [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 6.2](#)

This chapter presumes that OV3600 installation and initial configuration are complete, as described in the prior chapters of this document.

Configuring Communication Settings for Discovered Devices

To configure OV3600 to communicate with your devices, define the default shared secrets and SNMP polling information. [Figure 16](#) illustrates the page for this configuration.

Figure 16 *Device Setup > Communication*

Default Credentials	SNMP Settings
The credentials below are used to communicate with devices that are discovered by AMP (regardless of the credentials used for discovery). Changing these credentials does not affect APs that are already being managed or are already in the <i>New Devices</i> list.	SNMP Timeout (3-60 seconds): <input type="text" value="3"/>
3Com Edit	SNMP Retries (1-20): <input type="text" value="3"/>
3Com 8750 Edit	Telnet/SSH Settings
Alcatel-Lucent Edit	Telnet/SSH Timeout (3-120 seconds): <input type="text" value="120"/>
Apple AirPort Graphite Base Station Edit	HTTP Discovery Settings
Aruba Edit	HTTP Timeout (3-120 seconds): <input type="text" value="3"/>
Avaya Edit	ICMP Settings
BelAir Edit	Attempt to ping down devices: <input checked="" type="radio"/> Yes <input type="radio"/> No
Cisco Aironet 4800 Edit	Colubris Administration Options
Cisco IOS Edit	<input checked="" type="radio"/> Do not modify security/HTTPS settings
Cisco VxWorks Edit	<input type="radio"/> Replace existing user with specified user
Cisco WLC Edit	Cisco Aironet VxWorks User Creation Options
Colubris Edit	<input checked="" type="radio"/> Do not modify security/SNMP settings
Compaq WL400 Edit	<input type="radio"/> Create and use a specified user
Custom Device Edit	Symbol 4131/Intel 2011B, Cisco Aironet IOS and Nomadix AG2000w SNMP Initialization
Enterasys Edit	Upon authorization into read-write manage mode, AMP can enable read-write SNMP on a device using telnet commands for Cisco IOS and Nomadix devices and using the web interface for Symbol 4131/Intel 2011B devices.
Enterasys RoamAbout AP2000 Edit	<input type="radio"/> Do not modify SNMP settings
Enterasys RoamAbout AP3000/AP4102 Edit	<input checked="" type="radio"/> Enable read-write SNMP
Enterasys RoamAbout R2 Edit	<input type="button" value="Save"/> <input type="button" value="Revert"/>
Foundry Edit	
Funkwerk Artem W-1000 Edit	
HP ProCurve 420 Edit	
HP ProCurve 520WL Edit	
HP ProCurve 530 Edit	
HP Wireless Service Module Edit	

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. It is required to enter the credentials for each device model on your network.

The default credentials are assigned to all newly discovered APs. To change the credentials of APs already managed and monitored by OV3600, use the **Edit** button for the device.



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 25](#) describes the settings and default values.

Table 25 Device Setup > Communication, SNMP Settings

Setting	Default	Description
Default Polling Interval	5 minutes	Specifies the interval at which OV3600 polls each device for all newly created groups (this default setting may be overridden on the Group management page). A frequent (short) polling interval provides more up-to-date monitoring information, but also increase SNMP traffic on your network, especially on larger3. WLANs. This increases the load placed on the OV3600 server. Alcatel-Lucent recommends an initial five-minute polling interval for most networks.
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 <i>Down</i> .

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 26](#) itemizes the setting and default value.

Table 26 Device Setup > Communication, Telnet/SSH Settings

Setting	Default	Description
Telnet/SSH Timeout (3-120 seconds)	10	Defines the timeout period 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 27](#) itemizes these settings and default values.

Table 27 Device Setup > Communication, HTTP Discovery Settings

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

- On the **Device Setup > Communication** page, locate the **ICMP Settings** section. Complete the settings or revise the default values as required. [Table 28](#) itemizes the setting and default value of this section.

Table 28 Device Setup > Communication, ICMP Settings

Setting	Default	Description
Attempt to ping down devices	Yes	<p>Enables a function that applies when an AP is unreachable over SNMP.</p> <ul style="list-style-type: none"> 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. <p>NOTE: If ICMP is disabled on the network, select No to avoid the performance penalty caused by numerous ping requests.</p>

- On the **Device Setup > Communication** page, locate the **Concurrent Process Limits** section. Complete the settings or revise the default values as required. [Table 29](#) itemizes the fields of this section.

Table 29 Device Setup > Communication, Concurrent Process Limits

Setting	Default	Description
Maximum number of audit processes (1-50)	3	Defines the maximum number of configuration audit processes that are run at one time. Alcatel-Lucent recommends setting this to one fewer than the number of CPU cores in the box. Adding additional process speeds up the configuration audit of multiple APs. Setting the maximum too high results in diminished OV3600 performance.
Maximum number of configuration processes (1-50)	5	Defines the maximum number of configuration processes that are run at one time. The configuration processes are responsible for pushing configurations to devices. Alcatel-Lucent recommends setting this to one more than the number of CPU cores in the box. Setting the maximum too high results in diminished OV3600 performance.

- 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 three options listed. [Table 30](#) itemizes these settings and default values.

Table 30 Device Setup > Communication, Colubris Administration Options

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.
Create and use a specified user	N/A	Enables OV3600 to replace the existing user with a new user account (specified below) on each AP, with all permissions enabled.
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.

- 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 31](#) describes the settings and default values of this section.

Table 31 *Device Setup > Communication, Cisco Aironet VxWorks User Creation Options*

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.

- 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 32](#) describes the settings and default values.

Table 32 *Device Setup > Communications*

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 manufacturer, you can upload this firmware to OV3600 for distribution to devices via the **Device Setup > Upload Files** page.

[Figure 17](#) 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 in OV3600 6.2 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 17 Device Setup > Upload Files

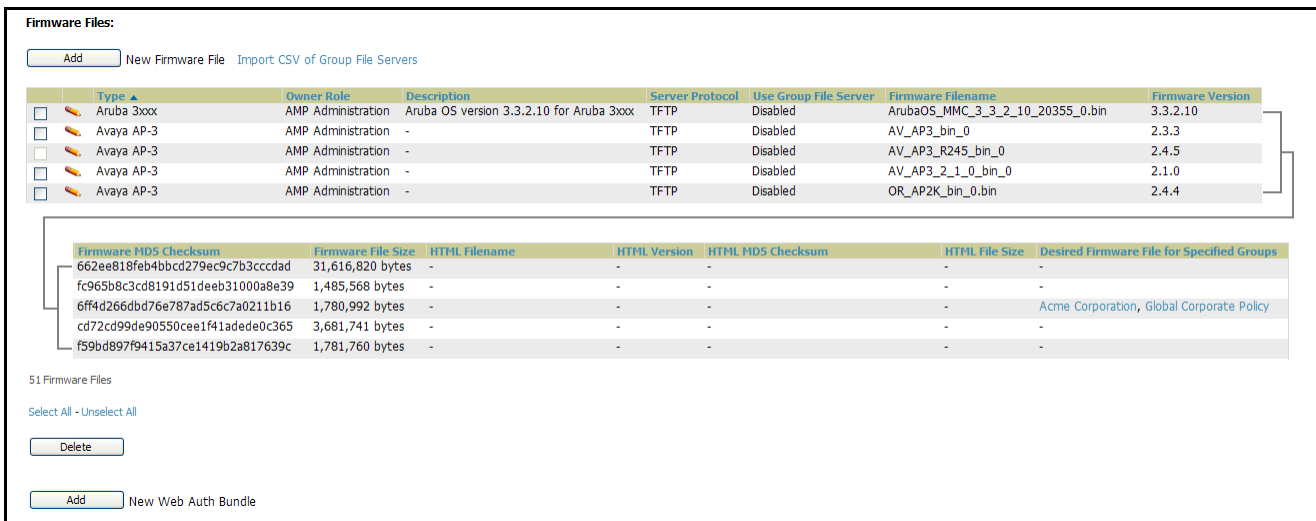


Table 33 below itemizes the contents, settings, and default values for the **Upload Files** page.

Table 33 Device Setup > Upload Files

Setting	Default	Description
Type	None	Displays a drop-down list of the primary AP makes and models that OV3600 supports with automated firmware distribution.
Owner Role	None	Displays the user role that uploaded the firmware file. This is the role that has access to the file when an upgrade is attempted.
Description	None	Displays a user-configurable text description of the firmware file.
Server Protocol	None	Displays the file transfer protocol by which the firmware file was obtained from the server.
Use Group File Server	None	Displays the name of the file server supporting the group.
Firmware Filename	None	Displays the name of the file that was uploaded to OV3600 and to be transferred to an AP when the file is used in an upgrade.
Firmware Version	None	Displays the firmware version number. This is a user-configurable field.
Firmware MD5 Checksum	None	Displays the MD5 checksum of the file after it was uploaded to OV3600. The MD5 checksum is used to verify that the file was uploaded to OV3600 without issue. The checksum should match the checksum of the file before it was uploaded.
Firmware File Size	None	Displays the size of the firmware file in bytes.
HTML Filename	None	Supporting HTML, displays the name of the file that was uploaded to OV3600 and to be transferred to an AP when the file is used in an upgrade.
HTML Version	None	Supporting HTML, displays the version of HTML used for file transfer.
HTML MD5 Checksum	None	Supporting HTML, displays the MD5 checksum of the file after it was uploaded to OV3600. The MD5 checksum is used to verify that the file was uploaded to OV3600 without issue. The checksum should match the checksum of the file before it was uploaded.
HTML File Size	None	Supporting HTML, displays the size of the file in bytes.

Table 33 Device Setup > Upload Files

Setting	Default	Description
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 6.2

Before you can upload a file to OV3600, you must download the appropriate firmware files from the manufacturer's website to a location on your network. Once this is complete, perform the following steps to load the device firmware file onto OV3600.

1. Browse to the **Device Setup > Upload Files** page.
2. Click the **Supported Firmware Versions and Features** link to view a list of supported firmware versions.



Unsupported and untested firmware may cause device mismatches and other problems. Please contact Alcatel-Lucent Enterprise Support at support@ind.alcatel.com before installing non-certified firmware.

3. From the **Upload Files** page, click the **Add** button. The **Add Firmware File** dialog box appears. [Figure 18](#) illustrates this dialog box.

Figure 18 Device Setup > Upload Files, Add Firmware Dialog Box

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 34](#) itemizes the settings of this page.

Table 34 Supported Firmware Versions and Features

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.
Firmware Version	None	Provides a user-configurable field to specify the firmware version number.
HTML Version*	None	Provides a user-configurable field to identify the HTML firmware version for Symbol and Intel APs.

Table 34 Supported Firmware Versions and Features (Continued)

Setting	Default	Description
Description	None	Provides a user-configurable text description of the firmware file.
Use Built-in or External TFTP 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 Filename. You can also choose to assign the external TFTP server on a per-group basis. If you check that box, you must enter the IP address on the Groups > Firmware page.
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.
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.
HTML File*	None	Click the Browse button to locate the appropriate Intel or Symbol HTML firmware file on your network.



Fields only appear for Intel and Symbol APs. 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.

- 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**. Select the file from the pick list window in the **Delete Firmware File** area and click **Delete**.



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.

Introduction

This chapter describes and applies the concept of Groups within the Alcatel-Lucent OV3600 system. This chapter provides the following topics and procedures for configuring many types of group-level settings that govern devices on your wireless network. Several of these topics or procedures have additional sub-topics or sub procedures. Procedures here are required unless specifically cited as optional.



For group settings that use templates, refer to the dedicated chapter, [Chapter 6, “Creating and Using Templates”](#) on page 127.

- [OV3600 Group Overview](#)
- [Viewing All Defined Device Groups](#)
- [Configuring Basic Group Settings](#)
- [Configuring Group Security Settings](#)
- [Configuring Group SSIDs and VLANS \(Optional\)](#)
- [Configuring Group Radio Settings](#)
- [Configuring Cisco WLC Radio Settings](#)
- [Configuring LWAPP AP Settings](#)
- [Configuring Group PTMP/WiMAX Settings](#)
- [Configuring Mesh Radio Settings](#)
- [Configuring Colubris Advanced Settings \(Optional\)](#)
- [Configuring Group MAC Access Control Lists \(Optional\)](#)
- [Specifying Minimum Firmware Versions for APs in a Group \(Optional\)](#)
- [Creating New Groups](#)
- [Deleting a Group](#)
- [Changing Multiple Group Configurations](#)
- [Modifying Multiple Devices](#)
- [Using Global Groups for Group Configuration](#)

OV3600 Group Overview

Enterprise-class APs and controllers 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 prone to human error. 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 manufacturers or hardware models—the core requirement and benefit of this approach is that all devices within a group share certain basic configuration settings.

Group Configuration Overview

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 and applied to every device in **Managed** 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. AP level settings are configured on the **APs/Devices > Manage** configuration 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 allows the user 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 124 as well as the section on the “Using the Master Console” on page 225.

Viewing All Defined Device Groups

To see a list of all Groups that have been defined within OV3600, browse to the **Groups > List** configuration page, illustrated in Figure 19. Table 35 describes the contents and functions of this page.

Figure 19 *Groups > List*

Name	Is Global Group	Global Group	SSID	Total Devices	Down	Mismatched	Ignored	Users	BW (kbps)	Up/Down
Access Points	No	-	-	10	1	5	0	15	66	5 mir
Aruba	No	-	-	1	0	1	0	0	0	5 mir
globalgrouponMC	Yes	-	-	0	0	0	0	0	0	5 mir
IOS-global	No	-	-	2	1	1	0	0	0	5 mir
Lancom/Hirschmann	No	-	-	2	1	2	0	0	92	5 mir
non-HQ group	No	-	-	16	7	13	0	2	0	30 m
proxim	No	-	51_ssid, 52_ssid	3	2	2	0	0	13	5 mir
subscribedgroup	No	globalgrouponMC	-	0	0	0	0	0	0	30 m
switch2	No	-	-	1	0	0	0	0	0	5 mir
Symbol	No	-	-	3	3	0	0	0	0	5 mir
test	Yes	-	-	0	0	0	0	0	0	5 mir

Table 35 *Groups > List*

Column	Description
Add new group button	Links to a form to add a new group by name.
Manage	The pencil represents a hyperlink to Group > Basic configuration page to begin editing Group configuration settings.

Table 35 Groups > List (Continued)

Column	Description
Default	Indicates the default group where devices are automatically assigned unless otherwise specified. If Automatically Monitor/Manage New Devices is enabled on OV3600 configuration page, all newly discovered devices immediately transition into the default group. The default group cannot be deleted.
Name	Sets a user-defined name that uniquely identifies the group by location, manufacturer, department or any other identifier (such as "Accounting APs," "Floor 1 APs," "Cisco APs," "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	Identifies the global group to which the group is subscribed, if any.
Unapplied Changes	Column is visible if configuration changes have been saved in the database, but the devices have not received the configuration changes.
SSID	Column represents the Service Set Identifier (SSID) assigned to all devices within the group.
Total Devices	Column represents the total number of access points contained in the group.
Down	Column represents the number of access points within the group, which are not reachable via SNMP.
Mismatched	Column represents the number of access points within the group that are in a mismatched state.
Users	Column represents the number of mobile users associated with all access points within the group.
BW (kbps)	Column represents a running average of the sum of bytes in and bytes out for the managed radio page.
Up/Down Polling Interval	Column represents the time between Up/Down SNMP polling periods for each device in the group. By default, all SNMP polling periods match the Up/Down period. Detailed SNMP polling period information is available on the Groups > Basic configuration page.
Duplicate	Column represents a hyperlink, and the link creates a new group with the name Copy of <Group Name> with the same group configuration.



When you first configure OV3600, there is only one pre-defined default group labeled Access Points.

Configuring Basic Group Settings

The **Groups > Basic** configuration page allows you to specify basic information about a Group, including the Group name. The first step in configuring your own Group on OV3600 is to edit the default group. Figure 19 illustrates the sections that configure group settings.

Figure 20 **Groups > Basic**

The screenshot shows the 'Groups > Basic' configuration page for the 'Access Points' group. The page is organized into several sections:

- Basic:** Name (Access Points), Mibed SNMP Poll Threshold (1), Regulatory Domain (United States), Timezone (AMP system time), Allow On-to-Off NAT (No).
- SNMP Polling Periods:** Up/Down Status Polling Period (15 seconds), Override Polling Period for Other Services (No), User Data Polling Period (15 seconds), Thin AP Discovery Polling Period (60 seconds), Device-to-Device Link Polling Period (15 seconds), Device Bandwidth Polling Period (30 seconds), 802.11 Counters Polling Period (60 seconds), Rogue AP and Device Location Data Polling Period (60 seconds), CDP Neighbor Data Polling Period (60 seconds).
- Notes:** A text area for notes.
- Group Display Options:** Show device settings for (All devices).
- Automatic Static IP Assignment:** Assign static IP addresses to devices (No).
- Spanning Tree Protocol:** Spanning Tree Protocol (Enabled), Bridge Priority (32768), Bridge Maximum Age (6-40) (20), Bridge Hello Time (1-10) (2), Bridge Forward Delay (4-30) (15).
- RIPv:** NTP Server #1, NTP Server #2, NTP Server #3, UTC Time Zone, Daylight Saving Time (Enabled).
- Cisco IOS/VoWorks:** Cisco IOS SNMP Version (2), Cisco IOS CLI Communication (Telnet), Cisco IOS Config File Communications (HTTP), Track usernames on Cisco Aronet VoWorks APs (No).
- Cisco Airespace:** Syslog Server, NTP Polling Interval (80/00), Cisco Airespace Controller SNMP Version (2), SNMP Trap Receiver #1 Name, IP, #2 Name, IP, #3 Name, IP.
- Proxim/Airvana:** Proxim SNMP Version (1), Enable DNS client (No), HTTP Server Port (80), Country Code (United States).
- HP ProCurve:** HP ProCurve 420 SNMP Version (2), ProCurve M WASH CLI Communications (Telnet).
- Symbol/Intel:** Symbol Controller SNMP Version (2), Symbol/Intel Client Inactivity Timeout (1-500) (10), Web Config Interface (Enabled).
- Aruba:** Aruba Controller SNMP Version (2).
- Routers and Switches:** Read ARP Table (Disabled), Read CDP Table for Device Discovery (Disabled), Read Bridge Forwarding Table (Disabled).
- Universal Devices, Routers and Switches:** SNMP Version (1).

Buttons at the bottom: Save, Save and Apply, Revert.

Perform the following steps to configure basic Group settings.

1. Browse to the **Groups > List** page.
2. Click the **Access Points** link in the **Name** column. This directs you to the **Groups > Monitoring** configuration page.
3. Select the **Groups > Basic** configuration page in the Navigation Section.
4. Edit the information on this configuration page for your default Group. Table 36 describes the settings and default values of this page.

Table 36 Groups > Basic

Setting	Default	Description
Name	Access Points	User-defined name that uniquely identifies the group by location, manufacturer, department or any other identifier (such as “Accounting APs,” “Floor 1 APs,” “Cisco APs,” “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 an AP 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.
Itemizing	OV3600 System Time	Allows group configuration changes to be scheduled relative to the time zone in which the access points are located.
Allow One-to-One NAT for Groups	No	Allows OV3600 to talk to the devices on a different address than the one configured in 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.

- To configure the polling intervals for your devices in the group, locate the **SNMP Polling Periods** section on the **Groups > Basic** configuration page. The **Group SNMP Polling Period** information overrides the default. [Table 37](#) describes the settings in this field.

Table 37 Group SNMP Polling Period

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.
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.
Rogue AP and Device Location Data Polling Period	5 minutes	Sets time between SNMP polls for Rogue AP and Device Location Data polling.

6. To record additional information and comments about the group, locate the **Notes** section on the **Groups > Basic** configuration page. [Table 38](#) describes the settings and default values.

Table 38 Groups > Basic, Notes

Setting	Default	Description
Notes	Blank	Functions as a free-form text field.

7. To configure which options and tabs are visible for the group, locate the **Group Display Options** section of the **Groups > Basic** configuration page. [Table 39](#) describes the settings and default values.

Table 39 Groups > Basic, Group Display Options

Setting	Default	Description
Show device settings for:	All Devices	Drop-down menu determines which Group tabs and options are to be viewable by default in new groups. Settings include the following: <ul style="list-style-type: none"> • 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 APs and devices currently in 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.

8. 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. [Table 40](#) describes the settings and default values.

Table 40 Group > Basic, Automatic Static IPO Assignment

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

9. To configure Spanning Tree Protocol on WLSE devices and Proxim APs locate the Spanning Tree Protocol section on the **Groups > Basic** configuration page. [Table 41](#) describes the settings and default values.

Table 41 Groups > Basic, Spanning Tree Protocol Configuration

Setting	Default	Description
Spanning Tree Protocol	Enabled	Enables 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.
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.

10. To configure NTP settings locate the **NTP** section on the **Groups > Basic** configuration page. [Table 42](#) describes the settings and default values.

Table 42 Groups > Basic, NTP

Setting	Default	Description
NTP Server #1,2,3	None	The IP address of the NTP server that is to be configured on the AP.
UTC Time zone	0	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	Disabled	Enable the advanced daylight saving time settings in the Proxim and HP ProCurve 420 sections of the Groups > Basic configuration page.

11. To configure Cisco IOS/VxWorks specific settings locate the **Cisco IOS/VxWorks** section on the **Groups > Basic** configuration page. [Table 43](#) describes the settings and default values.

Table 43 Groups > Basic, Cisco IOS/VxWorks

Setting	Default	Description
Cisco IOS SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the AP.
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 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 RADIUS accounting packets to OV3600. See the OV3600 Setup > RADIUS Accounting configuration page to ensure OV3600 is accepting RADIUS accounting packets from the APs.

12. To configure settings specific to Cisco WLC, locate the **Cisco WLC** section of the **Groups > Basic** configuration page. [Table 44](#) describes the settings and default values.

Table 44 Group > Basic, Cisco WLC

Setting	Default	Description
Cisco WLC SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate to WLC controllers.
SNMP Trap Receiver 1,2,3	None	Specifies the IP addresses of the SNMP Trap Receivers.
Syslog Server	None	Sets the IP address or Hostname of the syslog server.
NTP Polling Interval (3600-604800 seconds)	86400	Sets the amount of time between NTP polls.
Configure SNMP Trap Controls (link)	None	Links to the SNMP Trap Controls configuration page. Traps that can be configured include Miscellaneous, Client Related, Cisco AP, Auto RF Profile, Auto RF Update, AAA, IP Security and 802.11 Security .

13. To configure Proxim/Avaya specific settings locate the **Proxim/Avaya** section on the **Groups > Basic** configuration page. [Table 45](#) describes the settings and default values.

Table 45 Group > Basic, Proxim/Avaya

Setting	Default	Description
Proxim SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the AP.
Enable DNS Client (Proxim Only)	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.
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.
DST Offset*	+1	Configures the amount of time, in hours, that will be jumped when entering/leaving daylight saving time. NOTE: DST Offset is only visible if Daylight Saving Time is enabled in the NTP section of the Groups > Basic configuration page.

14. To configure HP ProCurve 420 specific settings, locate the **HP ProCurve 420** section on the **Groups > Basic** configuration page. [Table 46](#) describes the settings and default values.

Table 46 Group > Basic, HP ProCurve 420

Setting	Default	Description
Hp ProCurve 420 SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the AP.
DST Start Month*	1	Specifies the month that begins daylight saving time. 1 is January and 12 is December.
DST Start Day*	1	Specifies the day of the month that begins daylight saving time.
DST End Month*	12	Specifies the month that ends daylight saving time. 1 is January and 12 is December.
DST End Day*	31	Specifies the day of the month that ends daylight saving time.
ProCurve XLWeSM 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.



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.

15. To configure Symbol/Intel specific settings locate the **Symbol/Intel** section on the **Groups > Basic** configuration page. [Table 47](#) describes the settings and default values of this section.

Table 47 Group Basic, Symbol/Intel

Setting	Default	Description
Symbol Controller 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.
Web Config Page	Enable	Enables or disables the <code>http/https</code> configuration page for the Symbol 4131 and Intel 2011.

16. To configure Aruba/Alcatel Lucent-specific settings locate the **Aruba/Alcatel-Lucent** section on the **Groups > Basic** configuration page. [Table 48](#) describes the settings and default values of this section.

Table 48 Groups > Basic, Aruba/Alcatel Lucent

Setting	Default	Description
Alcatel-Lucent WLAN Switch SNMP Version	2c	Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the AP.
Offload Aruba/Alcatel Lucent WMS database	No	Configures commands previously documented in the <i>Aruba/Alcatel-Lucent Best Practices Guide</i> . See the current <i>Best Practices</i> guide for more information about this feature. When enabled, this feature allows OV3600 to display historical information for Alcatel-Lucent WLAN Switches. Changing the setting to Yes pushes commands via SSH to all Alcatel-Lucent 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 .

17. Click **Save** when the configurations of the **Groups > Basic** configuration page are complete.

Configuring Group Security Settings

The **Groups > Security** configuration page allows you to specify critical security policies for APs in the Group. These policies include the following security-related parameters:

- **VLANs** field: Configuring VLAN and SSID parameters in the **VLANs** field
- **General** field: Configuring general network parameters, such as closed network creation or blocking inter-client communication
- **Cisco WLC Options** field: Setting authentication options for Cisco WLC devices
- **TACACS+ Authentication** field: Defining multiple TACACS+ settings, such as authentication, authorization, and accounting servers
- **EAP Options** field: *New in Version 6.2*, sets multiple options for the Extensible Authentication Protocol (EAP)
- **RADIUS** fields: Defining multiple RADIUS server functions, to include **RADIUS Authentication**, **RADIUS Accounting**, and **RADIUS Management Authentication**
- **MAC Address Authentication**

Perform these steps to configure security policy for APs in a group.

1. Browse to the **Groups > Security** configuration page to enable wireless security coupled or decoupled with VLANs. [Figure 21](#) illustrates this configuration page and multiple security configurations.

Figure 21 *Groups > Security*

The screenshot displays the **Groups > Security** configuration page, organized into several sections:

- VLANs:** Includes options for VLAN Tagging and Multiple SSIDs (Enabled/Disabled), Management VLAN ID (0-4094, Untagged), Permit RADIUS-Assigned Dynamic VLANs (Yes/No), and VLAN ID Format (HP ProCurve 420 only, ASCII/Hex).
- General:** Includes options for Create Closed Network (Yes/No) and Block All Inter-Client Communication (Yes/No).
- Cisco Airespace Options:** Includes Authentication Priority #1 and #2 (RADIUS/Local) and LWAPP AP Groups VLAN Enabled (Yes/No).
- TACACS+ Authentication:** Includes three TACACS+ Authentication Servers (Select).
- TACACS+ Authorization:** Includes three TACACS+ Authorization Servers (Select).
- TACACS+ Accounting:** Includes three TACACS+ Accounting Servers (Select).
- EAP Options:** Includes WEP Key Rotation Interval (300), Session Key Refresh Rate (0), Session Timeout (0), Cisco TKIP (Yes/No), and Cisco MIC (MMH/Disabled).
- RADIUS Authentication Servers:** Includes four RADIUS Authentication Servers (IP addresses and Select) and Authentication Profile Name (Defined Server #1).
- RADIUS Accounting Servers:** Includes four RADIUS Accounting Servers (Select) and Accounting Profile Name (Accounting).
- RADIUS Management Authentication Servers:** Includes four RADIUS Management Authentication Servers (Select).
- MAC Address Authentication:** Includes MAC Address Authentication (Yes/No), MAC Address Format (Single Dash), Authorization Lifetime (1800), and Primary RADIUS Server Reattempt Period (0).

Buttons at the bottom include **Save**, **Save and Apply**, and **Revert**.

2. Locate the **General** area on the **Groups > Security** configuration page and configure these settings. [Table 49](#) describes the settings and default values.

Table 49 Groups > Security, General Area

Setting	Default	Description
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.

3. Locate the **Cisco WLC Options** area on the **Groups > Security** configuration page. [Table 50](#) describes the settings and default values.

Table 50 Groups > Security, Cisco WLC Options

Setting	Default	Description
Authentication Priority	RADIUS	Sets the first source of authentication for WLSE devices.
Cisco LWAPP AP Group VLAN	Disabled	Enables or disables VLAN overrides for the group. This setting requires that multiple SSIDs are defined.

4. To configure local net users on Cisco WLC controllers click the **Configure local net users** link in the **Cisco WLC Options** area on the **Groups > Security** configuration page, and define the **Local Net User** settings. [Figure 22](#) illustrates this page. [Table 51](#) describes the settings and default values.

Figure 22 Groups > Security Configure Local Net Users

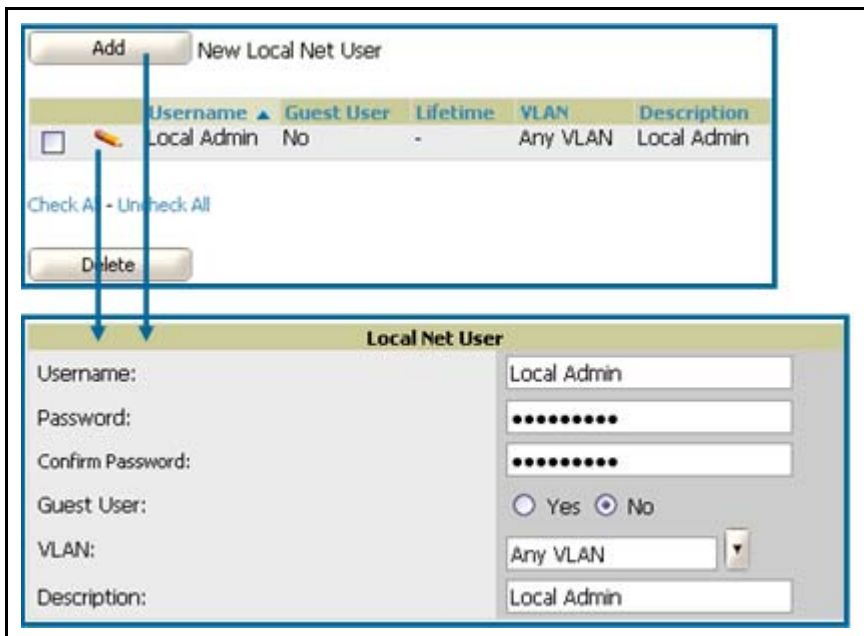


Table 51 *Groups > Security Configure Local Net Users*

Setting	Default	Description
Username	None	The username for the Local Net User.
Password	None	The password for the Local Net User.
Guest User	No	Enables or disables guest user mode for the Local Net User.
VLAN	Any VLAN	Drop-down menu that restricts the Local Net User to the specified VLAN.
Description	None	Text description of the Local Net User account.

5. Locate the **EAP Options** area on the **Groups > Security** configuration page. [Table 52](#) describes the settings and default values.

Table 52 *Group > Security, EAP Options*

Setting	Default	Description
WEP Key Rotation Interval (seconds)	120	Sets the time (in seconds) at which the AP rotates between WEP keys.
Session Key Refresh Rate (0-1440 min) (HP ProCurve 420 only)	0	Sets the time, in minutes, between session key refreshes.
Session Timeout (0-65535 sec.) (HP ProCurve 420 only)	0	Allows you to specify the time, in seconds, before users are forced to re-authenticate.
Cisco Temporal Key Integrity Protocol (TKIP)	Disabled	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 Message Integrity Check (MIC)	Disabled	If enabled, MIC adds several bytes per packet to make it more difficult to tamper with the packets.

6. Locate the **RADIUS Accounting Servers** area on the **Groups > Security** configuration page. These RADIUS servers dictate where the AP sends RADIUS accounting packets. Once the RADIUS Accounting servers are configured on the **Group > AAA Servers** configuration page, they appear in the drop-down menus on the **Groups > Security** page.

Refer to “[Configuring Group AAA Servers](#)” on [page 86](#) as required.

[Table 53](#) describes these **Groups > Security** settings and default values.

Please note the following operational characteristics of this feature, when it is configured:

- This feature enables OV3600 to authenticate users from a RADIUS or TACACS+ database, instead of requiring additional Group configuration for authentication purposes.
- The RADIUS server passes the client IP address, the URL that it accesses, and any additional information the RADIUS Server requires to control access.
- In this configuration, the Server checks OV3600 to verify whether or not a user is present, and checks either RADIUS or TACACS+. The user must define which authentication to use.
- The interface used for RADIUS auditing is the IP address assigned to the OV3600 Ethernet Interface 0.

Configuring the AP to send RADIUS accounting packets directly to OV3600 allows OV3600 to pull usernames from the packets. The usernames are then correlated with MAC addresses and displayed in OV3600. To configure OV3600 to accept the RADIUS accounting packets from APs, refer to the **OV3600 Setup > RADIUS Accounting** configuration page, and to the following procedure:

- “Integrating OV3600 with a RADIUS Accounting Server (Optional)” on page 53

Table 53 Group > AAA Servers

Setting	Default	Description
RADIUS Accounting Server1-4	None	Pull-down menu to select RADIUS Accounting servers previously entered on the Group > AAA configuration page. These RADIUS servers dictate where the AP sends RADIUS Accounting packets
Accounting Profile Name	Accounting	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	1	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.

7. Locate **RADIUS Authentication Servers** area on the **Groups > Security** configuration page. These RADIUS servers dictate how wireless clients authenticate onto the network. For RADIUS-based authentication, every AP must be configured to authenticate associated users to a specific RADIUS server. RADIUS servers need to be configured on the **Group > AAA Servers** configuration page to appear in the drop-down menus. [Table 54](#) describes the settings and default values.



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

Table 54 Groups > Security, RADIUS Authentication Servers

Setting	Default	Description
RADIUS Authentication Server 1-4	None	Pull-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	OV3600-Defined Server #1	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	1	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. Locate **RADIUS Management Servers** area on the **Groups > Security** configuration page. These RADIUS servers dictate who can log in to the **APs/Devices**. RADIUS servers need to be configured on the **Group > AAA Servers** configuration page to appear in the drop-down menus. [Table 55](#) describes the settings and default values.

Table 55 Groups > Security, RADIUS Management Servers Setting and Default Value

Setting	Default	Description
RADIUS Management Server 1-4	None	Pull-down menu to select RADIUS Management servers previously entered on the Group > RADIUS configuration page. These RADIUS servers dictate who can login and manage the APs/Devices.

9. Locate the **MAC Address Authentication** area on the **Groups > Security** configuration page and adjust these settings as required. [Table 56](#) describes the settings and default values.

Table 56 Groups > Security, MAC Address Authentication

Setting	Default	Description
MAC Authentication	Disabled	If enabled, only MAC addresses known to the RADIUS server are permitted to associate to APs in the Group.
MAC Address Format (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)	Dash Delimited	Allows selection of the format for MAC addresses used in RADIUS authentication and accounting requests: <ul style="list-style-type: none"> ⑩ Dash Delimited: xx-xx-xx-xx-xx-xx (default) ⑩ Colon Delimited: xx:xx:xx:xx:xx:xx ⑩ Single-Dash: xxxxxx-xxxxxx ⑩ No Delimiter: xxxxxxxxxxxx
Authorization Lifetime (900 - 432000 seconds)	1800	Sets the amount of time a user can be connected before reauthorization is required.
Primary RADIUS Server Reattempt Period (minutes)	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

10. Locate the **TACACS+ Authentication, Authorization and Accounting** areas on the **Groups > Security** configuration page (this area is for WLSE devices only). These settings configure TACACS+ servers on the controller, and they control users logging in to the controller. TACACS+ servers need to be configured on the **Group > AAA Servers** configuration page to appear in the drop-down menus. [Table 57](#) describes the settings and default values.

Table 57 Groups > AAA Servers, TACACS+ Authentication, Authorization and Accounting

Setting	Default	Description
RADIUS Authentication, Authorization and Accounting Servers 1-3	None	Pull-down menu to select TACACS+ Authentication servers previously entered on the Group > AAA configuration page.

11. If you are using VLAN tagging, select **Enable VLAN Tagging** at the top of the configuration page. Refer to the **Groups > SSIDS** configuration page to configure individual SSIDs and VLANs. [Figure 23](#) illustrates this option, and [Table 58](#) describes the settings and default values of this configuration page.

Figure 23 Groups > Security, Enable VLAN Tagging Option

Group: **Outdoor**

VLANs

VLAN Tagging and Multiple SSIDs: Enabled Disabled

Create and edit VLANs and SSIDs on this group's [SSIDs](#) page.

Management VLAN ID (0-4094, Untagged):
Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL; ProCurve420, Enterasys AP3000 only

Permit RADIUS-Assigned Dynamic VLANs:
HP ProCurve 420 only

VLAN ID Format: HP ProCurve 420 only

Ethernet Untagged VLAN ID (1-4094): RoamAbout AP3000 only

EAP Options

WEP Key Rotation Interval (0-10000000 sec):

Session Key Refresh Rate (0-1440 min): HP ProCurve 420 only

Session Timeout (0-65535 sec): HP ProCurve 420 only

Cisco TKIP: Yes No

Cisco MIC: MMH Disabled

General

Create Closed Network: Yes No

Block All Inter-Client Communication: Yes No

RADIUS Authentication Servers

RADIUS Authentication Server #1:

RADIUS Authentication Server #2:

RADIUS Authentication Server #3:

RADIUS Authentication Server #4:

Authentication Profile Name: Proxim Only

Authentication Profile Index: Proxim Only

Cisco WLC Options

Authentication Priority #1:

Authentication Priority #2:

LWAPP AP Groups VLAN Enabled: Yes No

RADIUS Accounting Servers

RADIUS Accounting Server #1:

RADIUS Accounting Server #2:

RADIUS Accounting Server #3:

RADIUS Accounting Server #4:

Accounting Profile Name: Proxim Only

Accounting Profile Index: Proxim Only

TACACS+ Authentication

Cisco WLC only

TACACS+ Authentication Server #1:

TACACS+ Authentication Server #2:

TACACS+ Authentication Server #3:

MAC Address Authentication

MAC Address Authentication: Yes No

MAC Address Format: Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL v2.1.0 and higher only

Authorization Lifetime (900-43200 sec):

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

TACACS+ Authorization

Cisco WLC only

TACACS+ Authorization Server #1:

TACACS+ Authorization Server #2:

TACACS+ Authorization Server #3:

TACACS+ Accounting

Cisco WLC only

TACACS+ Accounting Server #1:

TACACS+ Accounting Server #2:

TACACS+ Accounting Server #3:

Table 58 Groups > Security, Enable VLAN Tagging

Setting	Default	Description
VLAN Tagging and Multiple SSIDs	Yes	Enables or disables tagging for VLANs and multiple SSIDs. When enabled, several additional settings must be configured.
Management VLAN ID (0-4094)	Untagged	Sets the management VLAN on the Device
Permit RADIUS-assigned Dynamic VLANs (HP ProCurve 420)	No	Allows or denies RADIUS-assigned Dynamic VLANs on HP ProCurve 420s.
VLAN ID Format (HP ProCurve420)	ASCII	Sets the VLAN ID format to ASCII or Hex for HP ProCurve 420s.
Ethernet Untagged VLAN ID (RoamAbout AP3000)	1	Defines the untagged VLAN ID for the RoamAbout AP3000.

Additional sections in the **Groups > Security** page entail **General**, **Cisco WLC**, **TACACS+ Authentication**, **TACACS+ Authorization**, **TACACS+ Accounting**, **EAP Options**, **RADIUS Authentication Servers**, **RADIUS Accounting Servers**, and **MAC Address Authentication**. For additional information for these sections and their respective settings, refer to additional procedures in this document.

Configuring Group SSIDs and VLANs (Optional)

The **Groups > SSIDs** configuration page allows you to create and edit VLANs associated with the group of access points. Perform these steps to create or edit VLANs and to set SSIDs.



OV3600 Version 6.2 introduces enhancements in SSID information display, and this influences the content of several pages or reports. In addition to reporting users by radio, OV3600 now reports users based on SSID. Graphs on the AP and controller monitoring pages now have check boxes to display bandwidth in and out based on SSID. For data prior to the 6.2 upgrade, user counts are reported under an **Unknown** SSID. 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.



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

1. Browse to the **Groups > SSIDs** configuration page to create and edit the group's VLANs. [Figure 24](#) illustrates this page.

Figure 24 *Groups > SSIDS*

Group: Outdoor										
<input type="button" value="Add"/> New SSID/VLAN										
	SSID ▲	VLAN ID	Name	Encryption Mode	First Radio		Second Radio		Native VLAN	Profile
<input type="checkbox"/>	corp	51	-	No Encryption	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	-
<input type="checkbox"/>	distribution	1	-	No Encryption	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	-
<input type="checkbox"/>	stores	11	-	No Encryption	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	-

Select All - Unselect All

The initial **Groups > SSIDs** configuration page provides the ability to add, modify, or delete VLANs. [Table 59](#) describes the settings and default values when making these configurations.

Table 59 *Groups > SSIDs*

Setting	Description
SSID	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	Defines the name of the VLAN.
Encryption Mode	Sets 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 59 Groups > SSIDs (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.
Profile	The profile name, applying only to Cisco WLC.

2. Click **Add** to create a new SSID or VLAN. Alternatively, to edit an existing SSID or VLAN, check the box next to the SSID/VLAN to edit, and click the pencil icon. The **SSID/VLAN** configuration page appears with the following major sections:

- **SSID/VLAN**
- **Encryption**
- **EAP Options**
- **Cisco WLC Options**
- **RADIUS Authentication Servers**
- **RADIUS Accounting Servers**

Figure 25 illustrates the first three of six sections on this page.

Figure 25 Groups > SSIDs, SSID/VLAN Configuration Page, SSID/VLAN, Encryption, and EAP Options

The screenshot displays the configuration interface for an SSID/VLAN. It is divided into three main sections:

- SSID/VLAN Section:** Contains fields for 'Enable VLAN Tagging' (radio buttons for Yes/No, with 'Yes' selected), 'VLAN ID (1-4094):' (text input), 'SSID:' (text input), 'Profile: Cisco WLC only' (text input), 'Name:' (text input), 'Service Priority: Cisco VxWorks only' (dropdown menu set to 'default'), 'Maximum Allowed Associations (0-2007):' (text input set to '255'), 'Broadcast SSID: Cisco WLC, Colubris, Proxim, and Symbol 4131 only' (radio buttons for Yes/No, with 'No' selected), 'Partial Closed System: Proxim only' (radio buttons for Yes/No, with 'No' selected), 'Unique Beacon: Proxim only' (radio buttons for Yes/No, with 'No' selected), and 'Block All Inter-Client Communication: Colubris only' (radio buttons for Yes/No, with 'Yes' selected).
- Encryption Section:** Contains 'Encryption Mode:' (dropdown menu set to 'No Encryption').
- EAP Options Section:** Contains 'WEP Key Rotation Interval (0-10000000 sec):' (text input set to '120'), 'Cisco TKIP:' (radio buttons for Yes/No, with 'No' selected), and 'Cisco MIC:' (radio buttons for MMH/Disabled, with 'Disabled' selected).

3. Locate the **SSID/VLAN** section on the **Groups > SSIDS** configuration page. This section encompasses the basic VLAN configuration. [Table 60](#) describes the settings and default values.

Table 60 *Groups > SSIDs, SSID/VLAN Section*

Setting	Default	Description
Enable VLAN Tagging (WLSE, Colubris and Symbol only)	Yes	Enables or disables VLAN tagging on the AP.
VLAN ID	None	Indicates the number of the VLAN designated as the Native VLAN , typically for management purposes
SSID	None	Service Set Identifier (SSID) 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.
Profile (WLC only)	None	Allows the same SSID to be defined with up to four different security settings (Cisco WLC only).
Name	None	Sets a user-definable name associated with SSID/VLAN combination.
Service Priority (VxWorks only)	None	Identifies the delivery priority which packets receive on the VLAN/SSID (VxWorks only).
Maximum Allowed Associations	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 (Airspace, Colubris and 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)	Disabled	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)	Disabled	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.

4. Locate the **Encryption** area on the **Groups > SSIDs** configuration page, and complete the setting configurations. [Table 61](#) describes the settings and default values.

Table 61 Groups > SSIDs, Encryption Section

Setting	Default	Description
Encryption Mode	No Encryption	<p>Pull-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 settings that must be defined. Complete the associated settings for any encryption type chosen:</p> <ul style="list-style-type: none"> • 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
WPA2 WPA Compatibility Mode	Enabled	Enables compatibility mode. In compatibility mode, WPA clients are able to associate to the AP.
WPA2 Allow TKIP	Enabled	Allows TKIP encryption. Typically WPA2 only allows AES encryption.
WPA Preshared Key (Cisco IOS, HP ProCurve 420, Colubris, Symbol)	None	<p>Allows specification of a pre-shared key material for securing the wireless connection. This only appears when WPA/PSK is selected on the Encryption Mode pull-down menu.</p> <p>NOTE: This is not recommended for high-security enterprise connectivity.</p>

5. Locate the **EAP Options** area on the **Groups > SSIDS** configuration page, and complete the configuration. [Table 62](#) describes the settings and default values.

Table 62 Groups > SSIDs, EAP Options Section

Setting	Default	Description
WEP Key Rotation Interval (seconds)	120	Time (in seconds) between WEP key rotation on the AP.
Cisco Temporal Key Integrity Protocol (TKIP)	Disabled	<p>If enabled, TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.</p> <p>NOTE: TKIP can only be enabled when EAP-based security is used.</p>
Cisco MIC (Message Integrity Check)	Disabled	If enabled, MIC adds several bytes per packet to make it more difficult to tamper with the packets.

6. Locate the **Cisco WLC Options** area on the **Groups > SSIDS** configuration page, and define the settings. [Figure 26](#) illustrates this section, and [Table 63](#) describes the settings and default values.

Figure 26 Groups > SSIDs, Cisco WLC Options

Table 63 Groups > SSIDs, Cisco WLC Options

Setting	Default	Description
Radio Policy	All	Defines the 802.11 standard for this SSID group.
Admin Status	Enable	Enables or disables administrative status for the SSID being defined.
Session Timeout	0	Configures the session timeout option on the WLC controllers in the group.
Client Exclusion	No	Enables or disables the Client Exclusion option on the WLC controllers in the group.
DHCP Server	None	Defines the DHCP server for the WLSE controllers in the group.
Require DHCP	No	Enables or disables the Require DHCP command line setting. Sets the DHCP Address Assignment to Required.
Aironet IE Support	Yes	Enables or disables Aironet IE support.
Quality of Service	Silver (Best Effort)	Defines the QOS for the network or VLAN.
WMM Policy	Disabled	Enables or disables the WMM policy.
MFP Signature Generation	Enabled	Enables or disables MFP signature generation.
H-REAP Local Switching	Disabled	Enables or disables H-REAP local switching.
Web Policy	Disabled	Drop-down menu that specifies the web authentication policy. <ul style="list-style-type: none"> ● Disabled—No web authentication. ● Authentication—Sets the feature to prompt the user for a login and password when the users connects to the network ● Passthrough—Sets the user to be able to access the network without entering an email or password.
Email Input	Enabled	Prompts the user for their email address before allowing them to access the network. NOTE: This field is only visible if the Web Policy setting is set to Passthrough.

Table 63 Groups > SSIDs, Cisco WLC Options (Continued)

Setting	Default	Description
Mobility Anchor	N/A	Selects the mobility Anchors for this VLAN/SSID.

7. Locate the **RADIUS Authentication Servers** area on the **Groups > SSIDs** configuration page, and define the settings. [Table 64](#) describes the settings and default values.

Table 64 Groups > SSIDs, RADIUS Authentication Servers

Setting	Default	Description
RADIUS Authentication Server 1-3	None	Pull-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	None	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	None	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 65](#) describes the settings and default values.

Table 65 Groups > SSIDs, Radius Accounting Servers

Setting	Default	Description
RADIUS Accounting Server 1-3	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	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	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.

Configuring Group AAA Servers

RADIUS and TACACS+ servers get defined on the **Group > AAA Servers** configuration page. Once defined, they are selectable in the drop-down menus on the **Groups > Security** configuration page. TACACS+ servers are configurable only for Cisco WLC devices. [Figure 27](#) illustrates this configuration page for AAA Servers.

Figure 27 Adding a RADIUS or TACACS+ Server

Group: **Outdoor**

New RADIUS Server

	Hostname/IP Address ▲	Authentication	Management Authentication	Authentication Port	Accounting	Accounting Port	Timeout	Max Retries
<input type="checkbox"/>	10.2.25.180	Yes	No	1812	No	-	3	0
<input type="checkbox"/>	10.2.25.181	Yes	No	1812	No	-	4	0
<input type="checkbox"/>	10.2.25.183	Yes	No	1812	No	-	2	0
<input type="checkbox"/>	10.51.2.182	Yes	No	1812	No	-	2	0

4 RADIUS Servers

Select All - Unselect All

New TACACS+ Server Cisco WLC only

Groups > AAA Servers > Add RADIUS Server

Group: **Outdoor**

RADIUS Server

Hostname/IP Address:
Not all devices support hostnames.

Secret:

Confirm Secret:

Authentication:
 Yes No

Management Authentication:
(Cisco Only)
 Yes No

Accounting:
 Yes No

Timeout (0-86400):

Max Retries (0-20):

Groups > AAA Servers > Add TACACS+ Server

Group: **Outdoor**

TACACS+ Server

IP Address:

Secret:

Confirm Secret:

Retransmit Timeout (2-30 seconds):
2

Authentication Port:
49

Authorization Port:
49

Accounting Port:
49

1. For TACACS+, click the **Add** button associated with the New TACACS+ Server field. This setting is supported only for Cisco WLC devices. Define the settings in the **TACACS+ Server** dialog box that appears. [Table 66](#) describes the settings and default values.

Table 66 Adding a TACACS+ Server

Setting	Default	Description
IP	None	Defines the IP address for the TACACS+ server.
Secret & Confirm Secret	None	Sets the shared secret that is used to establish communication between OV3600 and the TACACS+ server. NOTE: The shared secret entered in OV3600 must match the shared secret on the server.
Authentication Port	49	Sets the port used for communication between the AP and the TACACS+ authentication server.
Accounting Port	49	Sets the port used for communication between the AP and the TACACS+ accounting server.
Authorization Port	49	Sets the port used for communication between the AP and the TACACS+ accounting server.
Retransmit Timeout (2-30 Seconds)	2	Sets the time (in seconds) that the access point waits for a response from the TACAS+ server.

2. Click the **Add** button to add a new RADIUS server. [Table 67](#) describes the settings and default values.

Table 67 Adding a RADIUS Server

Setting	Default	Description
IP/Hostname	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 & 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 Port	1812	Sets the port used for communication between the AP and the RADIUS authentication server. NOTE: The default 1812 should not be changed unless using older versions of RADIUS 1645.
Accounting Port	1813	Sets the port used for communication between the AP and the RADIUS accounting 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.

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



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

To make additional RADIUS configurations for device groups, use the **Groups > Security** page, and refer to “[Configuring Group Security Settings](#)” on page 74.

Configuring Group Radio Settings

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



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. Browse to the **Groups > Radio** configuration page and locate the Radio Settings area. [Figure 28](#) illustrates this page, and [Table 68](#) describes the settings and default values.

Figure 28 *Groups > Radio (Split View)*

The screenshot displays the configuration interface for the 'Outdoor' group. It is split into two main sections: 'Radio Settings' and device-specific configurations.

Radio Settings (Left Pane):

- Allow Automatic Channel Selection (2.4 GHz): Yes No
- Allow Automatic Channel Selection (5 GHz): Yes No
- Allow Automatic Channel Selection (4.9 GHz Public Safety): Yes No
- 802.11b Data Rates (Mb/sec): 1.0: Required, 2.0: Required, 5.5: Optional, 11.0: Optional
- 802.11a Data Rates (Mb/sec): 6.0: Required, 9.0: Required, 12.0: Required, 18.0: Optional, 24.0: Optional, 36.0: Optional, 48.0: Optional, 54.0: Optional
- 802.11g Data Rates (Mb/sec): 1.0: Required, 2.0: Required, 5.5: Required, 6.0: Required, 9.0: Optional, 11.0: Optional, 12.0: Optional, 18.0: Optional, 24.0: Optional, 36.0: Optional, 48.0: Optional, 54.0: Optional
- Frag Threshold Enabled: Yes No
- RTS/CTS Threshold Enabled: Yes No
- RTS/CTS Maximum Retries (1-255): 32
- Maximum Data Retries (1-255): 32
- Beacon Period (19-5000 Kusec): 102
- DTIM Period (1-255): 3
- Ethernet Encapsulation: 802.1H RFC1
- Radio Preamble: Long Short

Device-Specific Settings (Right Pane):

- HP ProCurve 420:** Slot Time: Auto; Multicast Data Rate: 5.5 Mbps; Rogue Scanning: Yes No; Rogue Scanning Interval: 720; Rogue Scanning Duration: 350; Rogue Scan Type: Dedicated Periodic
- HP ProCurve 420, Enterasys AP3000 and Enterasys AP4102:** Operational Mode: 802.11b + 802.11g; Max Station Data Rate: 54 Mbps
- Enterasys AP3000/AP4102:** 802.11a Multicast Data Rate: 6 Mbps; 802.11b/g Multicast Data Rate: 5.5 Mbps; Rogue Scanning: Yes No; Rogue Scanning Interval: 720; Rogue Scanning Duration: 350
- Cisco VxWorks:** Use Aironet Extensions: Yes No; Lost Ethernet Action: Repeater Mode; Lost Ethernet Timeout: 2; Upgrade Radio Firmware: Yes No
- Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL:** Load Balancing: Yes No; Interference Robustness: Yes No; Distance Between APs: Large; 802.11g Operational Mode: 802.11b + 802.11g; 802.11abg Operational Mode: 802.11b + 802.11g; 802.11b Transmit Rate: Auto Fallback; 802.11g Transmit Rate: Auto Fallback; 802.11a Transmit Rate: Auto Fallback; Rogue Scanning: Yes No; Rogue Scanning Interval: 15
- Proxim 4900M:** 4.9GHz Public Safety Channel Bandwidth: 20; 802.11a/4.9GHz Public Safety Operational Mode: 802.11a
- Colubris:** Rogue Scanning: Yes No; Rogue Scanning Interval: 600; Automatic Channel Interval: 12 Hours; First Radio: Operational Mode: 802.11b only; Multicast Data Rate: 1 Mbps; Second Radio: CN330 Only; Operational Mode: 802.11b only; Multicast Data Rate: 1 Mbps
- Symbol:** Rogue Scanning: Yes No; Rogue Scanning Interval: 240
- Enterasys R2:** Operational Mode: 802.11b + 802.11g

Buttons at the bottom right: Save, Save and Apply, Revert

Table 68 Groups > Radio

Setting	Default	Description
Allow Auto Channel Select (2.4, 5 GHz and 4.9GHz Public Safety)	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: <ul style="list-style-type: none"> ● 1.0 ● 2.0 Optional: <ul style="list-style-type: none"> ● 5.5 ● 11.0 	Displays pull-down menus for various data rates for transmitting data. The three values in each of the pull-down menus are as follows: <ul style="list-style-type: none"> ● 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 APs.) ● Optional—The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of basic on Cisco APs.) ● Not Used—The AP does not transmit data at the specified data rate. (Corresponds to a setting of no on Cisco APs.)
802.11a Data Rates (Mb/sec)	Required: <ul style="list-style-type: none"> ● 6.0 ● 9.0 ● 12.0 Optional: <ul style="list-style-type: none"> ● 18.0 ● 24.0 ● 36.0 ● 48.0 ● 54.0 	Displays pull-down menus for various data rates for transmitting data. The three values in each of the pull-down menus are as follows: <ul style="list-style-type: none"> ● Required—The AP transmits only unicast packets at the specified data rate; multicast packets is sent at a higher data rate set to optional. (Corresponds to a setting of yes on Cisco APs.) ● Optional—The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of basic on Cisco APs.) ● Not Used—The AP does not transmit data at the specified data rate. (Corresponds to a setting of no on Cisco APs.)
802.11g Data Rates (Mb/sec)	Required: <ul style="list-style-type: none"> ● 1.0 ● 2.0 ● 5.5 ● 6.0 ● 9.0 Optional: <ul style="list-style-type: none"> ● 11.0 ● 12.0 ● 18.0 ● 24.0 ● 36.0 ● 48.0 ● 54.0 	Provides pull-down menus for various data rates for transmitting data. The three values in each of the pull-down menus are as follows: <ul style="list-style-type: none"> ● Required—The AP transmits only unicast packets at the specified data rate; multicast packets will be sent at a higher data rate set to optional. (Corresponds to a setting of Yes on Cisco APs.) ● Optional—The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of Basic on Cisco APs.) ● Not Used—The AP does not transmit data at the specified data rate. (Corresponds to a setting of No on Cisco APs.)
Fragmentation Threshold Enabled	Disabled	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.
Fragmentation 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	Disabled	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.

Table 68 Groups > Radio (Continued)

Setting	Default	Description
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 Retires	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.
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.

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

To configure these settings, locate the **Proprietary Settings** area on the **Groups > Radio** page.



Proprietary settings are only applied to APs in the group from the specific manufacturer and are not configured on APs from manufacturers that do not support the functionality.

- To configure HP ProCurve 420 only settings, locate the **HP ProCurve 420** section of the **Proprietary Settings** area. [Table 69](#) describes the settings and default values.

Table 69 HP ProCurve 420 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 will be unable to associate to the AP.

- 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 indicated. [Table 70](#) describes the settings and default values of this page.

Table 70 HP ProCurve 240, Enterasys AP 3000 and AP 4102 of the Proprietary Settings

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.

- 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 71](#) describes the settings and default values of this page.

Table 71 Enterasys AP3000 and Enterasys AP4102, Proprietary Settings

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.

Table 71 Enterasys AP3000 and Enterasys AP4102, Proprietary Settings

Setting	Default	Description
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.

- WLC Radio settings are configured on the **Groups > WLC Radio** configuration page. Refer to [“Configuring Cisco WLC Radio Settings” on page 95](#) for details.
- To configure settings that apply to the LWAPP APs in the group, including WLAN override, controller assignment settings and HREAP options navigate to the **Groups > LWAPP APs** configuration page. Refer to [“Configuring LWAPP AP Settings” on page 110](#) for details. [Table 72](#) describes the settings and default values of this page.

Table 72 Groups > LWAPP APs

Setting	Default	Description
Use Aironet Extensions	Yes	When enabled, this option allows Cisco APs to provide functionality not supported by 802.11 IEEE standards, including the following: <ul style="list-style-type: none"> 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.
Lost Ethernet Action (Cisco VxWorks Only)	Repeater Mode	Pull-down menu that specifies the action to take when the Lost Ethernet Timeout threshold is exceeded: <ul style="list-style-type: none"> 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.
Short Slot-Time	Enabled	If enabled, the Cisco devices use the short slot time which may slightly increase throughput. This setting can cause compatibility problems with certain radios. Upgrade radio firmware when AP firmware is upgraded
(Require Use of Radio Firmware x.xx) (Cisco Only)	Yes	If enabled, this setting mandates that the radio firmware be upgraded to a firmware version compatible with the current version of AP firmware.

8. 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 the **Proprietary Settings** area, and define the required fields. [Table 73](#) describes the settings and default values.

Table 73 Groups > LWAPP APs, Proprietary Settings

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.
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	Disabled	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.

9. To configure **Proxim Mesh** settings, click the **Configure settings on the Proxim Mesh** page link.
10. To configure settings specific to the **Proxim 4900M** settings, locate the appropriate section of the **Proprietary Settings** area, and define the required fields. [Table 74](#) describes the settings and default values of this configuration page.

Table 74 Proxim 4900, Proprietary Settings

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, locate the **Colubris** section of the **Proprietary Settings** area, and define the required fields. [Table 75](#) describes the settings and default values of this configuration page.

Table 75 Colubris-only Proprietary Settings

Setting	Default	Description
Rogue Scanning	Disabled	If enabled, Colubris access points in the group (with the appropriate firmware) passively scan for rogue access points at the specified interval. This rogue scan will not break a user's association to the network. NOTE: This feature can affect the data performance of the access point.
Rogue Scan Interval	600 seconds	If rogue scanning is enabled, this setting controls the frequency with which scans are conducted (in seconds). 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 amount of time in between automatic channel selections on Colubris APs.
First or Second Radio: Operational Mode	802.11b only	Specifies the Operational Modes for the first or second radio.
First or Second Radio: Multicast Data Rate	1 Mbps	Selects the Multicast Data Rate for the first or second radio.

12. To configure **Symbol**-only settings locate the **Symbol** section of the **Proprietary Settings** area, and define the required fields. [Table 76](#) describes the settings and default values of this configuration page.

Table 76 Symbol-only of the Proprietary Settings

Setting	Default	Description
Rogue Scanning (Symbol Access Points with 3.9.2 firmware or above)	Disabled	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-only settings, locate the **Enterasys R2** section of the **Proprietary Settings** area and define the required fields. [Table 77](#) describes the required settings and default values.

Table 77 Enterasys R2 Section of the Proprietary Settings

Setting	Default	Description
Operational Mode	802.11b + 802.11g	Specify the Operational Mode of the R2, either 802.11b only, 802.11g only, 802.11a only, or 802.11b + 802.11g.

14. Click **Save** when proprietary-specific configurations as described above are complete.

Configuring Cisco WLC Radio Settings

To configure *WLC Radio* settings, navigate to the **Groups > WLC Radio Settings** configuration page. This page configures the radio settings on WLC controllers. All APs take their radio settings from their controllers even if the thin APs are in another group in OV3600.

The figures, tables, and steps in this procedure progress down each column of the WLC Radio Settings page. The settings in the left-side column are presented, explained, and configured first, then the settings in the right-side column are presented, explained, and configured next, starting at the top in both cases.

Configuring Global Controller Settings

Figure 29 and Table 78 illustrate and explain **Global Controller Settings**.

1. Configure the **Global Controller Settings** as described below for each field.

Figure 29 *Groups > Cisco WLC Radio, Global Controller Settings*

The screenshot shows the 'Global Controller Settings' configuration page. The settings are as follows:

Setting	Value
Keep All Self-Signed Certificates:	<input checked="" type="radio"/> Yes <input type="radio"/> No
LWAPP Transport Mode:	Layer 3
Aggressive Load Balancing:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
RF Network Name: <small>Up to 19 characters.</small>	RF Network
Authentication Response Timeout (5-60 secs):	11
User Idle Timeout (seconds):	301
ARP Timeout (seconds):	301
802.3x Flow Control Mode:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Peer to Peer Blocking Mode:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Over the Air Provisioning of AP:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
AP Fallback:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Apple Talk Bridging:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Fast SSID change:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Ethernet Multicast Support:	Multicast
Multicast Group Address:	0.0.0.0
Protection Type:	AP Authentication
AP Neighbor Authentication Trigger Threshold:	2
Default Mobility Domain Name:	Mobility Domain
Short Preamble:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Configure Group Mobility settings on the [LWAPP Mobility Groups page](#).

Table 78 Groups > WLC Radio Settings, Global Controller Settings

Setting	Default	Description
Keep All Self-Signed Certificates	Yes	Retains self-signed certificates.
LWAPP Transport Mode	Layer 3	Specifies the layer that the controller will use to communicate with the APs. In Layer 2 mode the controller uses a proprietary protocol to communicate with the APs. In layer 3 mode the controller uses IP addresses to communicate to the APs.
Aggressive Load Balancing	Disabled	Enable or Disable Aggressive Load Balancing.
RF Network Name	Default RF Network	The RF Network Name determines which Radio Resource Management packets will be accepted by the AP. For the receiving AP to accept a RRM packet the RF Network Name must be the same as the transmitting AP.
Authentication Response Timeout (5-60 secs)	10	The amount of time, in seconds, before an authentication response times out.
User Idle Timeout (seconds)	300	The amount of time, in seconds, a user must idle before the controller will disassociate them.
ARP Timeout (seconds)	300	The lifetime, in seconds, of ARP information.
802.3x Flow Control Mode	Disabled	Enable or disable 802.3x Flow Control.
Peer to Peer Blocking Mode	Disabled	Enable or disable Peer to Peer Blocking mode. When disabled the WLC switch routes traffic between local clients. When disabled the controller sends data through a higher level router even if both clients are connected to it.
Over the Air Provisioning of AP	Disabled	Enables or disables provisioning APs over the air.
AP Fallback	Disabled	Determines the behavior of the AP when communication with the controller is lost.
Apple Talk Bridging	Disabled	Enables or disables Apple talk bridging.
Fast SSID change	Disabled	Enable or disable Fast SSID changing. Users will not get new IPs from the DHCP server when they change SSIDs if enabled.
Wireless Packet Sniffer Server	None	Specifies the address of a Wireless Packet Sniffer Server for use with the controller.
Ethernet Multicast Support	Disabled	Enables or disables support for Ethernet multicasting.
Protection Type	None	Defines the wireless Protection Type.
AP Neighbor Authentication Trigger Threshold *	1	Defines the trigger threshold for AP Neighbor authentication when Protection type AP Authentication is selected. NOTE: This field is only visible if Protection Type "AP Authentication" is selected.

Table 78 Groups > WLC Radio Settings, Global Controller Settings (Continued)

Setting	Default	Description
Default Mobility Domain Name	Default Mobility Domain	Sets a user-defined name for the Mobility Group.
Short Preamble	Enabled	A short preamble may improve throughput performance, but a long preamble is more likely to be compatible with older devices.

- To configure **Group Mobility** settings, click the link to the **LWAPP Mobility Groups** page and complete or adjust the default values as required. [Figure 30](#) illustrates this page and [Table 79](#) describes the settings and default values.

Figure 30 Groups > Cisco WLC Radio > LWAPP Mobility Groups

Group: **Outdoor**

Mobility Group Elements | [Return to Cisco WLC Radio page.](#)

Automatically create mobility group elements for "Mobility Domain":

New Cisco AP Mobility Group Element

	Mobility Group Name ▲	Member MAC address	Member IP address
<input type="checkbox"/>	Mobility Domain	00:08:85:00:08:85	10.1.1.23
<input type="checkbox"/>	Mobility Domain	00:19:AA:00:19:AA	10.1.3.19
<input type="checkbox"/>	Mobility Domain	00:08:85:00:08:85	10.1.1.31
<input type="checkbox"/>	Mobility Domain	00:08:85:00:08:85	10.1.1.14

4 Cisco AP Mobility Group Elements

Select All - Unselect All

Add New Cisco AP Mobility Group Element Page

Group: **Outdoor**

Cisco AP Mobility Group Element

Mobility Group Name:

Member IP address:

Member MAC address:

Table 79 Groups > WLC Radio Settings

Setting	Default	Description
Mobility Group Name	Default Mobility Domain	The name of the Mobility Group containing the controller. A controller should only be in one Mobility Group.
Member MAC address	None	The MAC address of the member controller. This field will be autopopulated when a Member IP address is selected.
Member IP address	None	Drop-down menu specifying the IP address of the member device.

- To configure **Bridge Settings**, locate the **Bridge Settings** section of the **Groups > WLC Radio** configuration page, and complete or adjust the default values as required. [Figure 31](#) illustrates this section, and [Table 80](#) describes the settings and default values.

Figure 31 *Groups > WLC Radio, Bridge Settings*

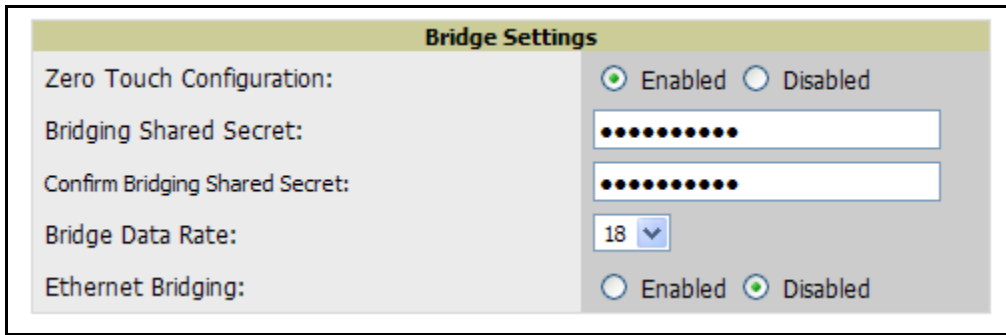


Table 80 *Groups > WLC Radio, Bridge Settings*

Setting	Default	Description
Zero Touch Configuration	Enabled	Enables or disables the Cisco Zero Touch Configuration on the controller. Zero Touch Configuration configures numerous settings, including whether the device should be PAP, backhaul page, and channel and security options between the controller and AP.
Bridge Shared Secret	None	Sets the shared secret used by Bridges in the group.
Bridge Data Rate	18	Sets the data rate used by bridges in the group.
Ethernet Bridging	Disabled	Enables or disables Ethernet bridging.

- To configure **Web Login** settings, locate the **Web Login Settings** section of the **Groups > WLC Radio** configuration page and complete the settings or default values. [Figure 32](#) illustrates this section, and [Table 81](#) describes the settings and default values.

Figure 32 *Groups > WLC Radio, Web Login Settings*

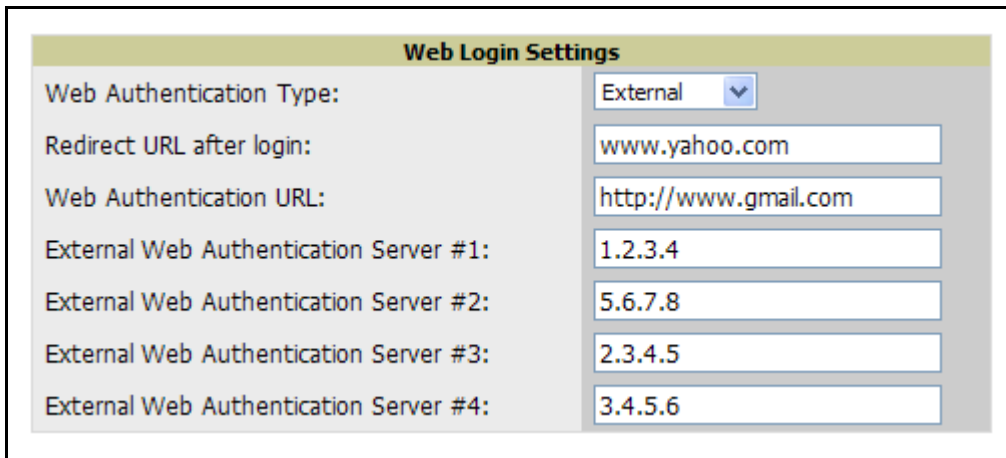


Table 81 Groups > WLC Radio, Web Login Settings

Setting	Default	Description
Web Authentication Type	Internal	Drop-down menu that defines the Web Authentication type. This menu has the following options: <ul style="list-style-type: none"> ● Internal—Web login information is authenticated locally on the controller. ● External—Web login information is authenticated against an external authentication server.
Display Manufacturer Logo	Yes	Enables or disables displaying the manufacturer’s logo on the web authentication configuration page.
Redirect URL after login	None	Sets URL users to be redirected after they have logged in.
Web Login Page Title	None	Sets the title displayed for the web login configuration page.
Web Login Page Message	None	Sets the message displayed to users on the web login configuration page.
Web Authentication URL	None	Sets the web authentication URL users visit when logging in.
External Web Authentication Server 1-4	None	Sets the IP address or Hostname of the external web authentication servers.

- To configure **802.11a Global RF Settings**, locate the **Global RF Settings** section of the **Groups > WLC Radio** configuration page. [Figure 33](#) illustrates this section, and [Table 82](#) describes the settings and default values.

Figure 33 Groups > WLC Radio, 802.11a Global RF Settings

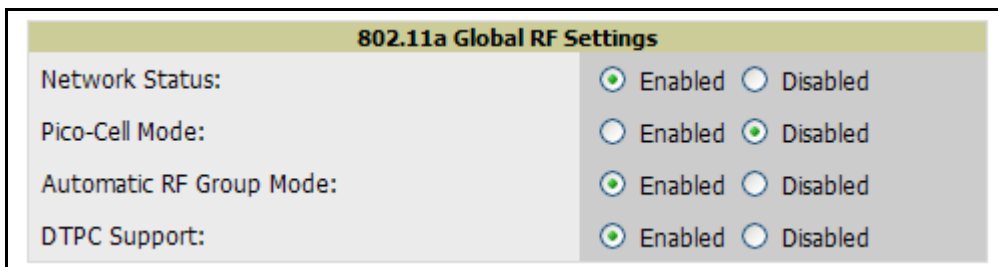


Table 82 Groups > WLC Radio, 802.11a Global RF Settings

Setting	Default	Description
Network Status	Enabled	Enables or disables the A, B or G networks.
Pico-Cell Mode	Disabled	When Pico-Cell Mode is enabled, the APs are set to a low transmit power and have high minimum connection speeds.
Automatic RF Group Mode	Enabled	Enables Automatic RF management for the AP Group.
DTPC Support	Enabled	Dynamic Transmit Power Control; sets access points to add channel transmit power information to beacons.

- To configure **802.11a RF Channel Assignment Settings**, locate the **RF Channel Assignment** section of the **Groups > Cisco WLC Radio** configuration page. [Figure 34](#) illustrates this section, and [Table 83](#) describes the settings and default values.

Figure 34 *Groups > WLC Radio, RF Channel Assignment Settings*

802.11a RF Channel Assignment	
Channel Assignment Method:	<input checked="" type="radio"/> Automatic <input type="radio"/> Static
Avoid Foreign AP Interference:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Avoid Cisco AP Load:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Avoid non-a Noise:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Table 83 *Groups > WLC Radio, RF Channel Assignment Settings*

Setting	Default	Description
Automatic Channel Assignment Method	Static	Automatic enables automatic channel assignment. When static is selected the AP will use the same channel until it is rebooted.
Avoid Foreign AP Interference	No	When enabled, the controller factors in foreign interference when determining the optimal channel.
Avoid Cisco AP Load	No	When enabled, the controller considers the amount of traffic observed on APs to determine optimal channel assignments.
Avoid non-802.11 Noise	No	When enabled, the controller attempts to avoid noise from non-radio devices. Other devices including air conditioner motors, microwaves and refrigerators can interfere with channels.

- To configure **Automatic Transmit Power** settings, locate the **Automatic Transmit Power** section of the **Groups > Cisco WLC Radio** configuration page and adjust the settings as required. [Figure 35](#) illustrates this section, and [Table 84](#) describes the settings and default values.

Figure 35 *Groups > WLC Radio, Automatic Transmit Power*

802.11a Automatic Transmit Power	
Power Level Assignment Method:	<input checked="" type="radio"/> Automatic <input type="radio"/> Fixed

Table 84 *Groups > WLC Radio, Automatic Transmit Power*

Setting	Default	Description
Automatic Transmit Power	Disabled	Allows the controller to determine the transmit power. Automatic transmit power must be enabled if you want to let the controller decide the power for all the APs or to have the controller set one uniform power for all of the APs.
Power Level Assignment Method	Fixed	Sets the power level assignment method to Fixed or Automatic . When it is Fixed , the same power value will be set for all APs. The power is decided individually for each AP if Automatic is selected.
Fixed Power Level	5	Sets the power level for the thin APs. Enter a number from 1 to 5, with 1 being the most powerful and 5 the least powerful.

8. To configure **802.11a Profile Thresholds**, locate this section in the **Groups > Cisco WLC Radio** configuration page, and adjust the settings as required. [Figure 36](#) illustrates this section, and [Table 85](#) describes the settings and default values.

Figure 36 Groups > WLC Radio, 802.11a Profile Thresholds

802.11a Profile Thresholds	
Interference (0-100%):	<input type="text" value="10"/>
Clients (1-75):	<input type="text" value="12"/>
Noise (-127 to 0 dBm):	<input type="text" value="-70"/>
Coverage (3-50 dBm):	<input type="text" value="16"/>
Utilization (0-100%):	<input type="text" value="80"/>
Coverage Exception Level (0-100%):	<input type="text" value="25"/>
Data Rate (1-1000 Kbps):	<input type="text" value="1000"/>
Client Minimum Exception Level (1-75):	<input type="text" value="3"/>

Table 85 Groups > Cisco WLC Radio, 802.11a Profile Thresholds

Setting	Default	Description
Interference (0-100%)	10%	Sets the Unknown Interference threshold. Enter a percentage value between 0 and 100%.
Clients (1-75)	12	Sets the Client threshold. Enter a numeric value between 1-75.
Noise (-127 to 0 dBm)	-70 dBm	Sets the noise threshold. Enter a numeric value between -127 and 0 dBm.
Coverage (3-50 dBm)	802.11a: 16 dBm 802.11bg: 12dBm	Sets the coverage threshold. Enter a numeric value between 3-50 dBm.
Utilization (0-100%)	80	Sets the utilization threshold. Enter a percentage value between 0% and 100%.
Coverage Exception Level (0-100%)	25	Sets the coverage exception threshold. enter a percentage value between 0% and 100%.
Data Rate (1-1000 Kbps)	1000	Sets the data rate threshold. Enter a numeric value between 1 and 1000.
Client Minimum Exception Level	3	Sets the client minimum exception level threshold. Enter a numeric value between 1-75.

9. To configure **802.11a Noise/Interference/Rogue Monitoring Channels**, locate the **Noise/Interference/Rogue Monitoring Channels** section of the **Groups > Cisco WLC Radio** configuration page and adjust the settings as required. [Figure 37](#) illustrates this section, and [Table 86](#) describes the settings and default values.

Figure 37 802.11a Noise/Interference/Rogue Monitoring Channels

802.11a Noise/Interference/Rogue Monitoring Channels	
Monitoring Channels:	<input type="text" value="Country Channels"/>

Table 86 Groups > Cisco WLC Radio, Noise/Interference/Rogue Monitoring Channels

Setting	Default	Description
Monitoring Channels	Country Channels	Specifies the channels that the AP should monitor for noise, interference and rogue devices.

10. To configure the **802.11a Monitor Intervals**, locate the **Monitor Intervals** section of the **Groups > WLC Radio** configuration page and adjust the settings as required. [Figure 38](#) illustrates this section, and [Table 87](#) describes the settings and default values.

Figure 38 Groups > WLC Radio, 802.11a Monitor Intervals

Table 87 Groups > WLC Radio, Monitor Intervals

Setting	Default	Description
Signal Measurement (60-3600 sec)	300	Specifies how often the controller should monitor the AP Signal measurements. Enter a value between 60 - 3600 seconds.
Noise Measurement (60-3600 sec)	300	Specifies how often the controller should monitor the AP Noise measurements. Enter a value between 60 - 3600 seconds.
Load Measurement (60-3600 sec)	300	Specifies how often the controller should monitor the AP Load measurements. Enter a value between 60 - 3600 seconds.
Coverage Measurement (60-3600 sec)	300	Specifies how often the controller should monitor the AP Coverage measurements. Enter a value between 60 - 3600 seconds.

11. To configure the **802.11a Voice Settings**, locate the **Voice Settings** section of the **Groups > Cisco WLC Radio** configuration page. [Figure 39](#) illustrates this section, and [Table 88](#) describes the settings and default values.

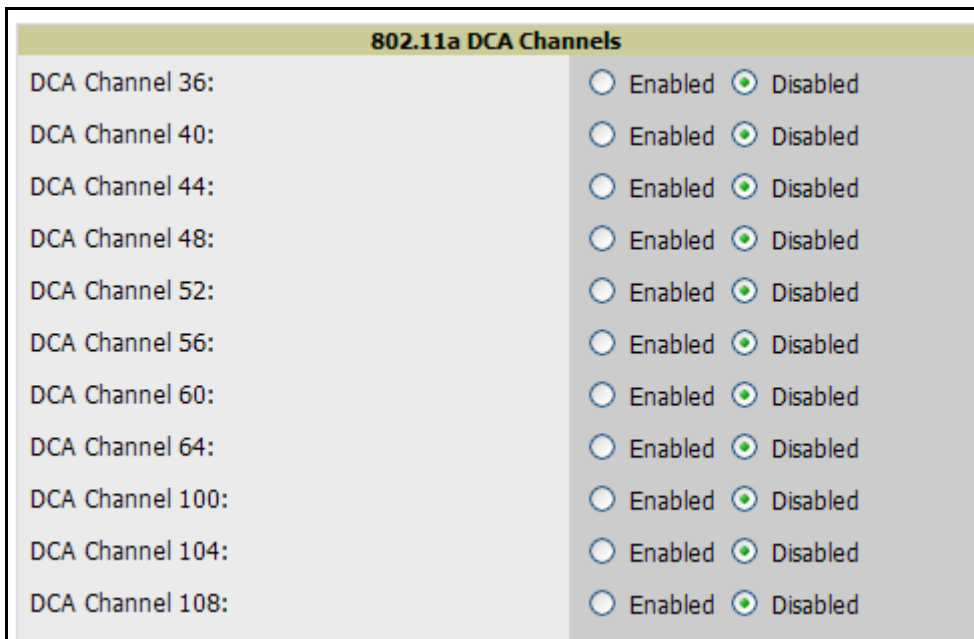
Figure 39 Groups > Cisco WLC Radio, 802.11a Voice Settings

Table 88 Groups > Cisco WLC Radio, Voice

Setting	Default	Description
Voice Admission Control (ACM)	Enabled	Denies network access under congested conditions.
Load-based AC	Disabled	Establishes admission control policy based on load.
Max RF Bandwidth (40-85%)	N/A	Defines the threshold for maximum RF bandwidth in the admission control policy.
Reserved Roaming Bandwidth	6%	Sets reserved bandwidth for roaming voice clients. Range is from 0% to 25%. This control not contained in 6.2 GUI, for snapshot.
Expedited Bandwidth	Disabled	Sets AP to reject new calls on this radio band after this value is reached. Range is from 40% to 85%.
Metrics Collection	Disabled	Sets OV3600 to collect traffic stream metrics between the AP and client.

12. To configure **802.11a DCA Channels**, navigate to this section of the **Groups > Cisco WLC** configuration page, and select the channels to enable or disable for DCA functionality. Dynamic Channel Allocation (DCA) is a method by which OV3600 selects the optimal operational frequencies, adjusting for the best operational channels to use in response to environmental demand. This is a method by which to provide continuous coverage in a dense wireless environment. All DCA channels are disabled by default. [Figure 40](#) illustrates this interface. Channels range from 36 to 196, in increments of every other four, as shown.

Figure 40 Groups > Cisco WLC, 802.11a DCA Channels, Partial View



13. To configure **802.11a EDCA settings**, navigate to this section of the **Groups > Cisco WLC** configuration page, and select the settings desired for EDCA functionality. Enhanced Dynamic Channel Allocation (EDCA) is a method by which high-priority traffic is given preference over lower priority traffic, increasing the chances for high-priority traffic to be sent. [Figure 41](#) illustrates this section, and [Table 89](#) describes the settings and default values.

Figure 41 *Groups > Cisco WLC, 802.11a EDCA Settings*

802.11a EDCA

EDCA Profile:

Enable Low Latency MAC: Enabled Disabled

Table 89 *Groups > Cisco WLC Radio, Voice*

Setting	Default	Description
EDCA Profile	WMM	Selects the EDCA profile to use for this group. Drop-down menu options include WMM (default), Spectralink Voice Priority, Voice Optimized, or Voice and Video Optimized.
Enable Low Latency MAC	Disabled	Enables low latency MAC for the EDCA profile.

14. To configure the **802.11a Video Parameters**, locate the **802.11a Video Parameters** section of the **Groups > Cisco WLC Radio** configuration page.

Figure 42 *Groups > Cisco WLC Radio, 802.11a Video Parameters*

802.11a Video Parameters

Video Admission Control (ACM): Enabled Disabled

Table 90 *Groups > Cisco WLC Radio, Video Parameters*

Setting	Default	Description
Voice Admission Control (ACM)	Disabled	Denies network access to video data under congested conditions.

15. To configure the power constraint and channel announcement parameters for 802.11a and 802.11h, locate the **802.11a 802.11h Parameters** section of the **Groups > Cisco WLC Radio** configuration page, and define these settings. [Figure 43](#) illustrates this section, and [Table 91](#) describes the settings and default values.

Figure 43 *Groups > Cisco WLC Radio, 802.11a 802.11h Parameters*

802.11a 802.11h Parameters

Power Constraint: Yes No

Local Power Constraint (0-30 dB):

Channel Announcement: Yes No

Channel Quiet Mode: Yes No

Table 91 *Groups > Cisco WLC Radio, 802.11a 802.11h Parameters*

Setting	Default	Description
Power Constraint	No	Enables or disables the 802.11a and 802.11h power constraint option on the controller.
Channel Announcement	No	Enables or disables the 802.11h channel announcement on the controller.

16. To configure the DCA channel width for 802.11a, locate the **802.11a DCA Channel Width** section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 44 *Groups > Cisco WLC Radio, 802.11a DCA Channel Width*

802.11a DCA Channel Width

DCA Channel Width: 20 MHz ▼

Table 92 *Groups > Cisco WLC Radio, DCA Channel Width Setting*

Setting	Default	Description
DCA Channel Width	20 MHz	Defines the width for the DCA channel in MHz.

17. To configure the **802.11an Settings**, locate this section in the **Groups > Cisco WLC Radio** configuration page and adjust these values as required.

Figure 45 *Groups > Cisco WLC Radio, 802.11an Settings (Partial View)*

802.11an Settings

11n Mode: Enabled Disabled

MCS Index 0 (7 Mbps): Enabled Disabled

MCS Index 1 (14 Mbps): Enabled Disabled

MCS Index 2 (21 Mbps): Enabled Disabled

MCS Index 3 (29 Mbps): Enabled Disabled

MCS Index 4 (43 Mbps): Enabled Disabled

MCS Index 5 (58 Mbps): Enabled Disabled

MCS Index 6 (65 Mbps): Enabled Disabled

MCS Index 7 (72 Mbps): Enabled Disabled

MCS Index 8 (14 Mbps): Enabled Disabled

MCS Index 9 (29 Mbps): Enabled Disabled

MCS Index 10 (43 Mbps): Enabled Disabled

MCS Index 11 (58 Mbps): Enabled Disabled

MCS Index 12 (87 Mbps): Enabled Disabled

MCS Index 13 (116 Mbps): Enabled Disabled

Table 93 Groups > Cisco WLC Radio, 802.11an Settings

Setting	Default	Description
11n Mode	Enabled	Enables or disables the 802.11n option on the controller.
MCS Index (0-15)	Enabled	Enables or disables the MCS index on the controller.

18. To configure **Client Exclusion** parameters, locate the **Client Exclusion Settings** section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 46 Groups > Cisco WLC Radio, Client Exclusion Settings

Client Exclusion Settings

Excessive 802.11 Association Failures:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Excessive Web Authentication Failures:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Excessive 802.1X Authentication Failures:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Excessive 802.11 Authentication Failures:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
IP Theft or IP Reuse:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Table 94 Groups > Cisco WLC Radio, Client Exclusion Settings

Setting	Default	Description
Excessive 802.11 Association Failures	Disabled	Excludes client with excessive 802.11 association failures.
Excessive Web Authentication Failures	Disabled	Excludes client with excessive web authentication failures.
Excessive 802.1x Authentication Failures	Disabled	Excludes client with excessive 802.1x authentication failures.
Excessive 802.11 Authentication Failures	Disabled	Excludes client with excessive 802.11 authentication failures.
IP Theft or IP Reuse	Disabled	Excludes client based on IP reuse or theft.

19. To configure **802.11bg Global RF Settings**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings. The **Network Status** field defines the 802.11 standard to be enabled, and the remaining fields define modes supported an DTPC support.

Figure 47 Groups > Cisco WLC Radio, 802.11bg Global RF Settings

802.11bg Global RF Settings

Network Status:	802.11b/g Enabled <input type="button" value="v"/>
Pico-Cell Mode:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Automatic RF Group Mode:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DTPC Support:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

20. To configure **802.11bg RF Channel Assignments**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 48 *Groups > Cisco WLC Radio, 802.11bg RF Channel Assignments*

802.11bg RF Channel Assignment	
Channel Assignment Method:	<input checked="" type="radio"/> Automatic <input type="radio"/> Static
Avoid Foreign AP Interference:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Avoid Cisco AP Load:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Avoid non-bg Noise:	<input checked="" type="radio"/> Yes <input type="radio"/> No

21. To configure **802.11bg RF Automatic Transmit Power**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 49 *Groups > Cisco WLC Radio, 802.11bg Automatic Transmit Power*

802.11bg Automatic Transmit Power	
Power Level Assignment Method:	<input checked="" type="radio"/> Automatic <input type="radio"/> Fixed

22. To configure **802.11bg RF Profile Thresholds**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 50 *Groups > Cisco WLC Radio, 802.11bg Automatic Transmit Power*

802.11bg Profile Thresholds	
Interference (0-100%):	<input type="text" value="10"/>
Clients (1-75):	<input type="text" value="12"/>
Noise (-127 to 0 dBm):	<input type="text" value="-70"/>
Coverage (3-50 dBm):	<input type="text" value="12"/>
Utilization (0-100%):	<input type="text" value="80"/>
Coverage Exception Level (0-100%):	<input type="text" value="25"/>
Data Rate (1-1000 Kbps):	<input type="text" value="1000"/>
Client Minimum Exception Level (1-75):	<input type="text" value="3"/>

23. To configure **802.11bg Noise/Interference/Rogue Monitoring Channels**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 51 *Groups > Cisco WLC Radio, 802.11bg Noise/Interference/Rogue Monitoring Channels*

802.11bg Noise/Interference/Rogue Monitoring Channels	
Monitoring Channels:	<input type="text" value="Country Channels"/>

24. To configure **802.11bg Monitor Intervals**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 52 *Groups > Cisco WLC Radio, 802.11bg Monitor Intervals*

802.11bg Monitor Intervals	
Signal Measurement (60-3600 sec):	<input type="text" value="300"/>
Noise Measurement (60-3600 sec):	<input type="text" value="300"/>
Load Measurement (60-3600 sec):	<input type="text" value="300"/>
Coverage Measurement (60-3600 sec):	<input type="text" value="300"/>

25. To configure **802.11bg Voice Settings**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 53 *Groups > Cisco WLC Radio, 802.11bg Voice Settings*

802.11bg Voice Settings	
Voice Admission Control (ACM):	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Expedited Bandwidth:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Metrics Collection:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

26. To configure **802.11bg DCA Channels**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 54 *Groups > Cisco WLC Radio, 802.11bg DCA Channels*

802.11bg DCA Channels	
DCA Channel 1:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DCA Channel 2:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DCA Channel 3:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DCA Channel 4:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DCA Channel 5:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DCA Channel 6:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DCA Channel 7:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DCA Channel 8:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DCA Channel 9:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DCA Channel 10:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DCA Channel 11:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

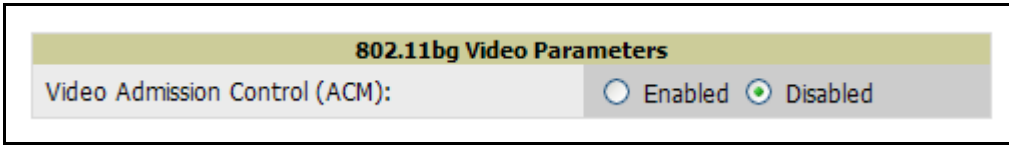
27. To configure **802.11bg EDCA**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 55 *Groups > Cisco WLC Radio, 802.11bg EDCA*

802.11bg EDCA	
EDCA Profile:	<input type="text" value="WMM"/>
Enable Low Latency MAC:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

28. To configure **802.11bg Video Parameters**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 56 *Groups > Cisco WLC Radio, 802.11bg Video Parameters*



29. To configure **802.11bgn Settings**, locate this section of the **Groups > Cisco WLC Radio** configuration page, and define these settings.

Figure 57 *Groups > Cisco WLC Radio, 802.11bgn Setting*

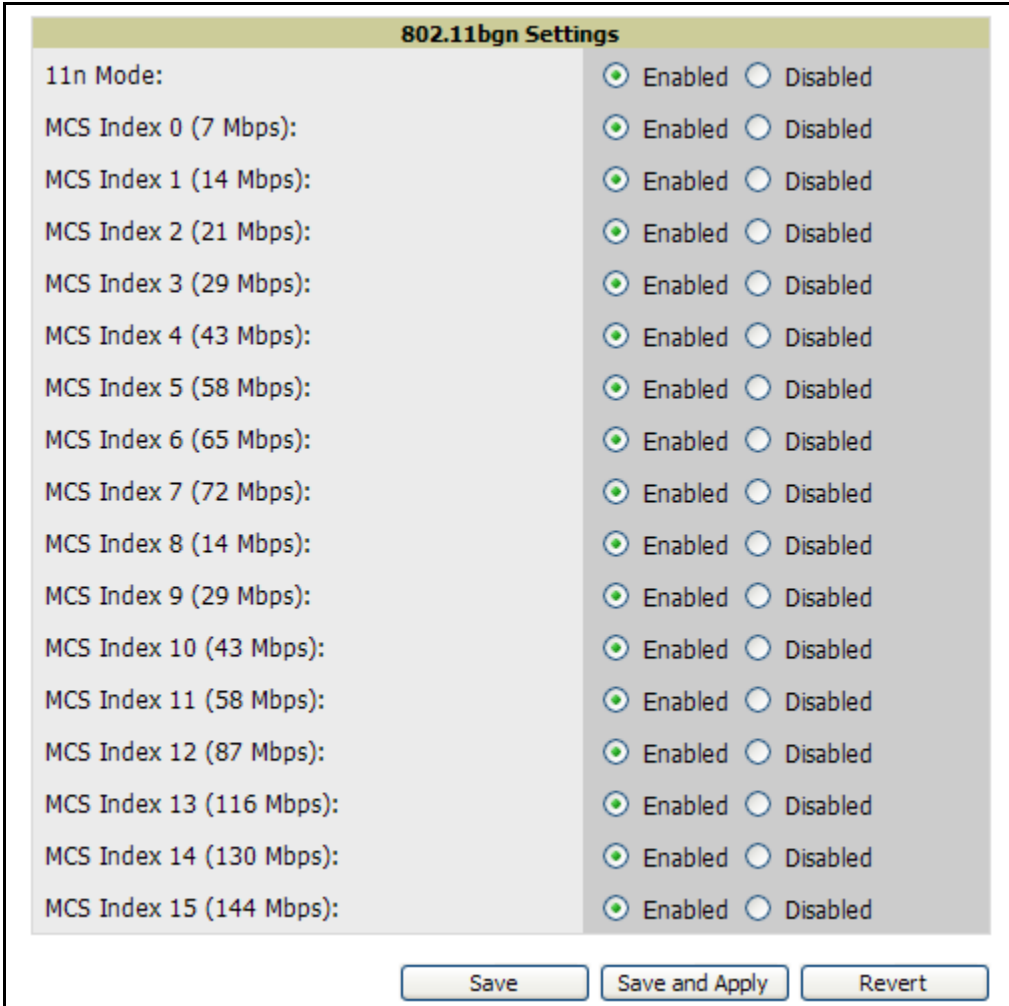


Table 95 *Groups > Cisco WLC Radio, 802.11bgn Setting*

Setting	Default	Description
11n Mode	Enabled	Enables or disables the 802.11n option on the controller.
MCS Index (0-15)	Enabled	Enables or disables the MCS index on the controller.

30. Click **Save** or **Save and Apply** when configurations are complete.

Configuring LWAPP AP Settings

1. Navigate to the **Groups > LWAPP AP Settings** configuration page to configure LWAPP AP specific settings.

The settings on this configuration page apply to all thin APs in the group even if the controller is in another group. [Figure 58](#) illustrates this configuration page and [Table 96](#) describes the settings and default values.

Figure 58 *Groups > LWAPP AP Settings*

Table 96 *Groups > LWAPP AP Settings*

Setting	Default	Description
Override per-AP controller choices	No	Allows you to define the primary, secondary and tertiary controller for all of the APs in the group.
Primary/Secondary/Tertiary Controller	None	Drop-down menu allows you to specify the primary, secondary and tertiary controller for all of the APs in the group. The drop-down menu lists all of the controllers in OV3600.
VLAN Support	Disabled	Configures VLAN support for HREAP APs. If enabled, a field to override the per-AP native VLAN ID is given, as is a link to add new H-REAP VLAN mapping. If you don't override the native VLAN ID ("no" radio button is selected) you can configure the setting on each AP's manage configuration page instead.
Native VLAN ID	1	Defines the native VLAN for HREAP devices.
Apply Group WLAN Override	No	Enables or disables Group WLAN Override. Click the Add new WLAN Override link to add a WLAN override.
LWAPP AP Group	None	For Cisco WLC devices, allows override of the SSID based on the AP Group VLAN configured on the Groups > Security configuration page. If No is selected, this value can be configured on the AP > Manage configuration page.
Distribute Self-Signed Certificates	Disabled	Enables distribution by groups of controllers, mobility groups or primary/secondary/tertiary controllers.

2. Click **Save** when configurations are complete.

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 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. [Figure 59](#) illustrates this configuration page and [Table 97](#) describes the settings and default values.

Figure 59 *Groups > PTMP/WiMAX*

Table 97 *Groups > PTMP/WiMAX*

Setting	Default	Description
3.5GHz WiMAX Channel Bandwidth (Proxim MP.16)	3.5GHz	Sets the frequency used by the WiMAX devices in the group.
BSID (Proxim MP.16)	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.
802.11a Radio Channel (Proxim MP.11)	56	Selects the channel used for 802.11a radios by the devices in this group.
802.11g Radio Channel (Proxim MP.11)	10	Selects the channel used for 802.11g radios by the devices in this group.
Channel Bandwidth (Proxim MP.11)	20	Defines the channel bandwidth used by the devices in this group.
Network Name (Proxim MP.11)	None	Sets the Network name, with a range of length supported from two to 32 alphanumeric characters.
Network Secret and Confirm Network Secret (Proxim MP.11)	None	Sets a shared password to authenticate clients to the network.

1. 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 60](#) illustrates this page and [Table 98](#) describes the settings and default values.

Figure 60 Groups > PTMP/WiMAX Configuring Packet Identification Rules

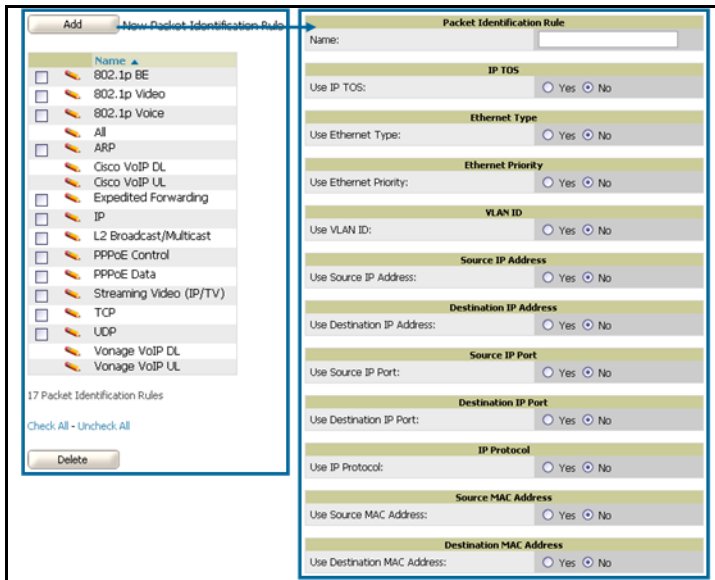


Table 98 Groups > PTMP/WiMAX Configuring Packet Identification Rules

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.
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.

Table 98 Groups > PTMP/WiMAX Configuring Packet Identification Rules (Continued)

Setting	Default	Description
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.

- 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 61](#) illustrates this page and [Table 99](#) describes settings and default values.

Figure 61 Groups > PTMP/WiMAX Configuring Service Flow Classes

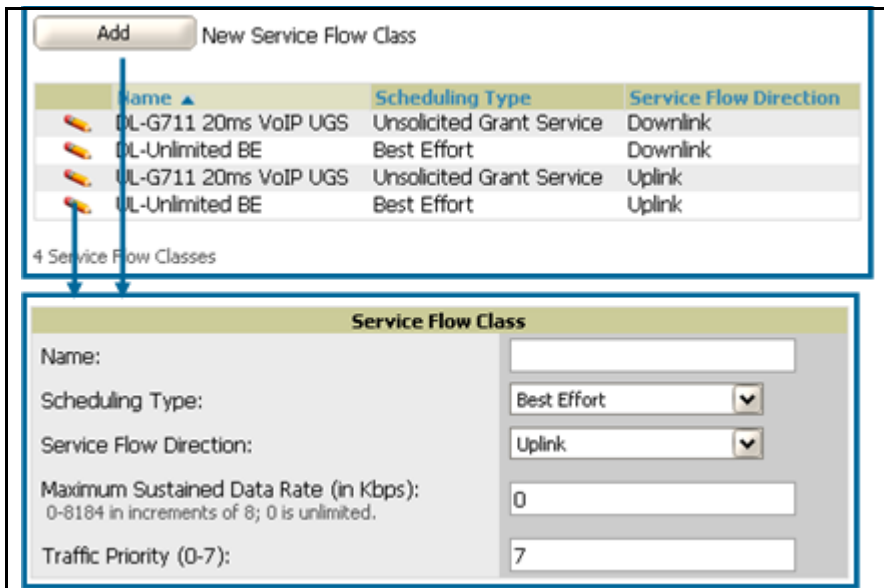


Table 99 Groups > PTMP/WiMAX Configuring Service Flow Classes

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: <ul style="list-style-type: none"> • 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.

- 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 62](#) illustrates this page and [Table 100](#) describes the settings and default values.

Figure 62 Groups > PTMP/WiMAX Configuring Subscriber Station Classes

Table 100 Groups > PTMP/WiMAX Configuring Subscriber Station Classes

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.

4. Click **Save** when configurations are complete.

Configuring Mesh Radio Settings

1. Navigate to the **Groups > Proxim Mesh Radio Settings** configuration page to configure Mesh-specific radio settings.
2. Define the settings as required for your network. [Figure 63](#) illustrates this page. [Table 100](#) and [Table 102](#) describe the settings and default values.

Figure 63 Groups > Mesh Radio Settings

General		Security	
Mesh Radio:	4.9/5 Ghz	SSID:	Wireless Mesh
Maximum Mesh Links:	6	Enable AES:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Neighbor RSSI Smoothing:	16	Mesh Cost Matrix	
Roaming Threshold:	80	Hop Factor:	2
Deauth Client When Uplink is Down:	<input checked="" type="radio"/> Yes <input type="radio"/> No	Maximum Hops to Portal:	4
		RSSI Factor:	5
		RSSI Cut-Off:	10
		Medium Occupancy Factor:	5
		Current Medium Occupancy Weight:	7

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

Table 101 Groups > Mesh Radio Settings, General

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 will roam. 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.

Table 101 Groups > Mesh Radio Settings, General

Setting	Default	Description
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 102 Groups > Mesh Radio Settings, Security

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 page sections contain settings for hop factor and maximum hops to portal, RSSI factor and cut-off, medium occupancy factor and current medium occupancy weight. Define these settings as required for your network. [Table 103](#) describes these settings and default values.

Table 103 Groups > Mesh Radio Settings, Mesh Count Matrix

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.

Configuring Colubris Advanced Settings (Optional)

The **Groups > Colubris** configuration page provides a mechanism to fetch a *master* AP's configuration and apply that configuration to all access points that match the *master* model in the group. The **Groups > Colubris Advanced** configuration page requires that Colubris APs be present in the group. If Colubris APs are not discovered yet or are placed in the group, refer to “[Discovering and Managing Devices](#)” on page 141 in this document.

OV3600 retrieves five categories of configuration items from the master AP, as follows:

1. Configuration items that are read-only (for example., serial number)
2. Configuration items that are AP specific (for example, primary IP address)
3. Configuration items that are configurable on the **APs Devices > Manage** configuration page or on the group management configuration pages
4. Configuration items that should always be applied to all the APs in the Group
5. Configuration items that should be applied to all the APs in the group only in certain situations.

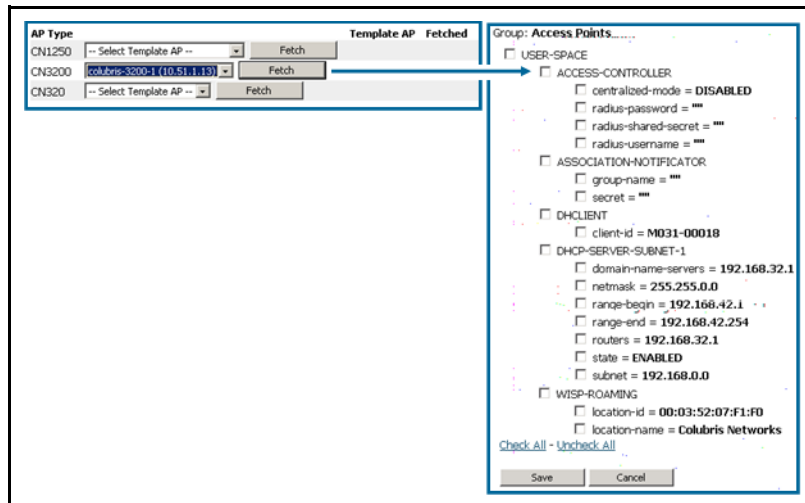
This configuration page displays the configuration items in category 5. Select the items that should be applied to all APs in this group.



OV3600 pushes settings that are not displayed on the screen to ensure the AP functions properly with the selected changes.

1. Browse to the **Groups > List** configuration page and select the group you wish to manage and then navigate to the **Groups > Colubris** configuration page.
2. Select the Master AP in the drop-down menu whose configuration you wish to apply to all applicable APs in the group. The **Fetch** button instructs OV3600 to fetch immediately the configuration of the *master* AP. [Figure 64](#) illustrates this configuration page.

Figure 64 *Fetching a Colubris Template*



For additional and more general information about group templates, refer to “[Creating and Using Templates](#)” on page 127.

3. Click the **Save** button to save the configuration items in category 4 and any items from category 5 you selected. OV3600 automatically redirects you back to the **Groups > Colubris** configuration page. [Figure 65](#) illustrates this configuration page.

Figure 65 Groups > Colubris

Group: **Access Points**
Note: There are unapplied changes for this group. You must click 'Save and Apply' to make them take effect.

AP Type	Template AP	Fetched
CN1250	-- Select Template AP --	
CN3200	colubris-3200-1	9/22/2004 4:01 PM
CN320	-- Select Template AP --	

4. Click the **Save and Apply** button to see the list of configuration items you selected from category 4. [Figure 66](#) illustrates this page.

Figure 66 Confirming Colubris Changes

Confirm changes:

Colubris Advanced Configuration for CN3200

Colubris Advanced Configuration for CN3200: Deleted

Colubris Advanced Configuration for CN3200

Date fetched from AP:	(none)	9/17/2004 9:00 AM
Template AP:	(none)	colubris-3200-1
USER-SPACE PPTP-CLIENT-SETTINGS auto-discovery-route:	(none)	ENABLED
USER-SPACE PPTP-CLIENT-SETTINGS lcp-echo-request:	(none)	DISABLED
USER-SPACE PPTP-CLIENT-SETTINGS nat:	(none)	ENABLED
USER-SPACE PPTP-CLIENT-SETTINGS rip:	(none)	ENABLED
USER-SPACE PPTP-CLIENT-SETTINGS rip-mode:	(none)	passive
USER-SPACE RADIUS-SRV-GATEWAY radius-nas-id:	(none)	(empty string)
USER-SPACE RADIUS-SRV-GATEWAY radius-secret-primary:	(none)	(empty string)
USER-SPACE RADIUS-SRV-GATEWAY radius-secret-secondary:	(none)	(empty string)

2:00 A.M. (02:00 AM)

Select other groups to change:

Group

Group 2

[Check All](#) - [Uncheck All](#)

5. Click the **Confirm Edit** button to apply the configuration immediately to all applicable access points in the group. Alternately, click the **Schedule** button to schedule changes for a later time.

Configuring Group MAC Access Control Lists (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.



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 manufacturers 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 67](#) illustrates this configuration page.

Figure 67 Groups > MAC ACL

A screenshot of a web configuration page for "Groups > MAC ACL". The page title is "Group: Access Points". There is a "Use MAC ACL:" label followed by a dropdown menu currently set to "Yes". Below this, there is a list of supported manufacturers: "Intel; Symbol; Cisco VxWorks; Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL only." A note states: "Set a list of whitespace-separated MAC addresses that are allowed to associate to an access point. This list will not be set on Cisco VxWorks APs." Below the note is a text input field containing three MAC addresses: "2b:0a:59:00:19:02", "1a:1a:1a:1a:1a:1a", and "2b:2b:2b:2b:2b:2b".

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

Specifying Minimum Firmware Versions for APs in a Group (Optional)

OV3600 allows you to define 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. [Figure 68](#) illustrates this configuration page.

Figure 68 *Groups > Firmware*

Desired Version	
Choose the desired firmware version to be applied to the devices in this group. Upload firmware files on the Device Setup Firmware Files page.	
Apple AirPort Graphite Base Station:	NONE
Avaya AP-3:	NONE
Avaya AP-4/5/6:	NONE
Avaya AP-7:	NONE
Avaya AP-8:	NONE
Cisco Airespace 2000:	NONE
Cisco Airespace 4000:	NONE
Cisco Airespace 4400:	NONE
Cisco Aironet 1100 IOS:	NONE
Cisco Aironet 1130 IOS:	NONE
Proxim AP-4000MR:	NONE
Proxim AP-4000MR-LR:	NONE
Proxim AP-4900M:	NONE
Proxim AP-4900MR-LR:	NONE
Proxim AP-600:	NONE
Proxim AP-700:	NONE
Proxim MP.16 3500-BS:	NONE
Proxim MP.16 3500-SS:	NONE
Proxim Tsunami MP.11a:	NONE
Symbol 4121:	NONE
Symbol 4131:	NONE
Systimax AirSpeed AP542:	NONE

1. Browse to the **Groups > Firmware** configuration page.
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 placed 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 19](#) for the **Groups > List** configuration page.
8. From the list of Groups, check the **Default** radio button next to the Group to make the default.

Creating New Groups

OV3600 enables you to create a new Group either by (1) duplicating an existing Group's settings or by (2) defining an entirely new Group.



If the new Group shares common settings with an existing Group, duplicating that existing Group is typically more efficient. When defining an entirely new Group, all configuration settings are set to OV3600 default values.

Perform the following steps to create a new Group by duplicating an existing Group.

1. Browse to the **Groups > List** configuration page.
2. Select the existing Group to be duplicated and click the **Duplicate** link.
3. OV3600 automatically creates a new Group with the name **Copy of [Group Name]** and directs you to the **Groups > Basic** configuration page for you to review and modify any settings.

Perform the following steps to create an entirely new Group.

1. Browse to the **Groups > Create** configuration page.
2. Enter a name for the new Group in the Name field and click **Create Group**.
3. OV3600 automatically creates a new Group with the specified name and directs you to the **Groups > Basic** configuration page. All configurations settings are set to the default values.

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 for the Group you wish to edit.
3. OV3600 automatically directs you to the **Groups > Basic** configuration page.
4. 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.
5. 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

Confirm changes:

Group "Access Points"

Allow One-to-One NAT: No Yes

Schedule

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

Current time: December 20, 2007 2:45 pm PST

Start Date/Time:

6. OV3600 displays a **Configuration Change** screen confirming the changes that will be applied to the Group's settings.
7. 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**.

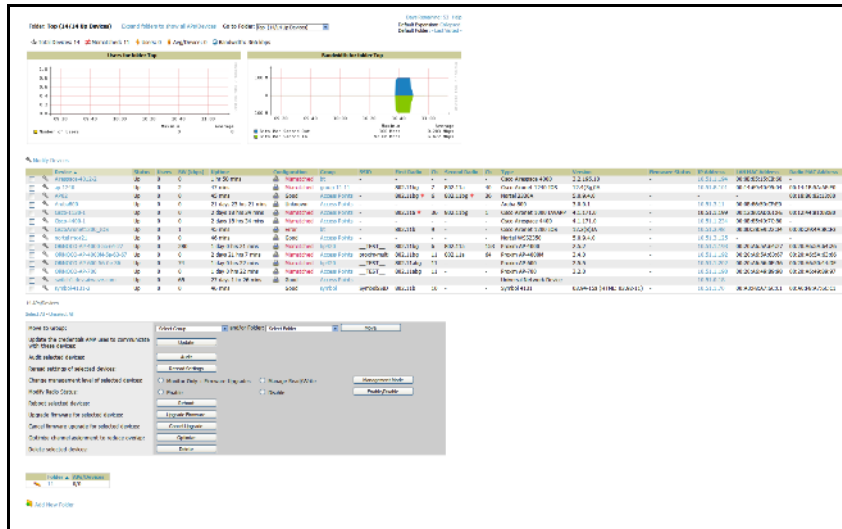
8. Apply changes to multiple groups by selecting the appropriate group or groups and clicking **Preview**.

Modifying Multiple Devices

OV3600 provides a very powerful utility that modifies all APs or a subset of access points unrelated to OV3600's normal 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 the **APs/Devices > List, APs/Devices > Up, APs/Devices > Down, APs/Devices > Mismatched or Groups > Monitor** configuration pages. Click the **Modify Devices** link above the list of APs. [Figure 70](#) illustrates this page.

Figure 70 Modifying Multiple Devices



2. Select the devices you wish to modify and click on the corresponding button.
3. 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.
4. 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 104](#) describes these action and controls.

Table 104 Modify Devices Configuration

Action	Description
Delete	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.
Move to 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.
Optimize channel assignment to reduce overlap	OV3600 uses the APs neighbor table to determine the optimal channel for the selected APs.
Update the credentials OV3600 uses to communicate with these devices.	Update... changes the credentials OV3600 uses to communicate with the device. Update... does <i>not</i> change the credentials on the AP.
Import settings	Imports settings from the selected device

Table 104 *Modify Devices Configuration*

Action	Description
Ignore selected devices	Ignores selected APs, preventing OV3600 from generating any alerts or including the AP in an up/down count. The device's history is preserved but it will not be polled. Ignored devices can be seen and taken out of ignore status by navigating to the New Devices configuration page and clicking the View Ignored Devices link at the bottom.
Modify Radio Status	Enables or disables the radios on the selected device. Does <i>not</i> apply Cisco IOS APs.
Change management level of selected devices	Places the selected APs into management or monitored mode. APs start to be reconfigured when they are put into Management.
Audit selected devices	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.
Cancel firmware update for selected devices	Cancels any firmware upgrades that are scheduled or in progress for the selected APs.
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.
Audit selected devices	Fetches the current configuration from the device and compares it to OV3600s desired configuration. The audit action will cause the Configuration Status to get updated.

Using Global Groups for Group Configuration

To apply group configurations using 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*

Local Groups											
1-1 of 1 Groups Page 1 of 1											
	Name ▲	SSID	Total Devices	Down	Mismatched	Ignored	Users	BW (kbps)	Up/Down Status	Polling Period	Duplicate
<input type="checkbox"/>	Access Points	-	0	0	0	0	0	0	5 minutes		

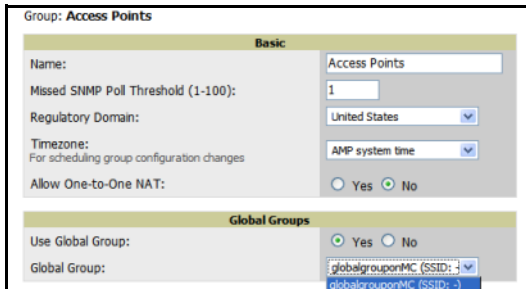
- To set a group as a global group, navigate to the **Groups > Basic** configuration page for an existing or a newly created group. Select **Yes** for the **Is Global Group** field under the global group section. When the change is saved and applied, the group will have a check box next to fields on the **Basic, Security, SSIDs, AAA Servers, Radio, WLC Radio, LWAPP APs, PTMP/WiMAX, Proxim Mesh** and **MAC ACL** tabs. [Figure 72](#) illustrates this configuration page.

Figure 72 *Groups > Basic for a Global Group*



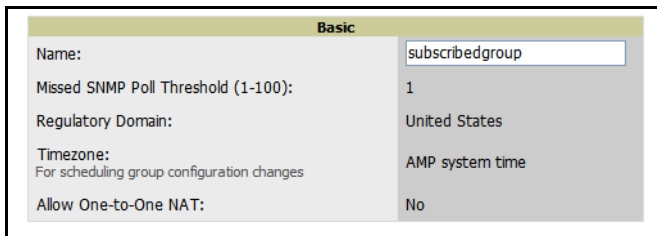
- When a global group configuration is pushed to subscriber groups, all settings are static except for settings with the checkbox selected; for fields with checkboxes selected, the value or setting can be changed on the corresponding tab for each managed group. In the case of the **Groups > SSIDs** configuration 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 127](#) 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*



- 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 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 [“Using the Master Console” on page 225](#).

Introduction

This chapter describes and illustrates the use of templates in group and global device configuration. This chapter contains the following topics.

General Template Use

- Overview of Group Templates
- Adding Templates
- Configuring General Template Files and Variables
 - Configuring General Templates
 - Using Template Syntax
 - Using Directives to Eliminate Reporting of Configuration Mismatches
 - 📄 `<ignore_and_do_not_push>substring</ignore_and_do_not_push>`
 - 📄 `<push_and_exclude>command</push_and_exclude>`
 - Using Conditional Variables in Templates
 - Using Substitution Variables in Templates
 - Using AP-Specific Variables

Templates for Cisco IOS Devices

- Configuring Cisco IOS Templates
 - 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

Global Templates

- Configuring a Global Template

Overview of Group Templates

Templates are powerful configuration constructs that allow OV3600 to manage virtually all settings on an AP device. 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 Access Point (AP) equipment manufacturers:

- Alcatel-Lucent
- Cisco IOS
- HP ProCurve
- Hirschmann
- Lancom
- Nomdix
- Symbol
- Trapeze

The OV3600 template understands many variables including the following:

- %channel%
- %ofdmpower%
- %ip_address%
- %hostname%

The variables are populated with the corresponding values on the **APs/Devices > Manage** configuration page of the specific AP that is getting configured. Refer to [“Configuring Cisco IOS Templates” on page 137](#) for template and variable details, and to additional procedures for information about creating global templates for subscriber groups.



Changes made on the OV3600 standard Group configuration pages (Basic, Radio, Security, VLANs, and so forth) are not applied to any APs that manage template-based devices.

[Figure 75](#) illustrates the **Groups > Templates** configuration page, and [Table 105](#) describes the settings for these configurations.

Figure 75 Groups > Templates

Group: **Acme Corporation**

Note: No template is available for Cisco Aironet 1200 IOS devices with firmware version 12.3(8)JA2.
Note: No template is available for Cisco Aironet 1200 IOS devices with firmware version 12.3(8)JEC.
Note: No template is available for Cisco Aironet 1240 IOS devices with firmware version 12.4(10b)JDA.
Note: No template is available for Aruba 5000 devices with firmware version 3.3.2.10.
Note: No template is available for Aruba 5000 devices with firmware version 3.3.2.4.
Note: No template is available for Aruba 2400 devices with firmware version 3.3.2.10.
Note: No template is available for Symbol W55100 devices with firmware version 3.2.0.0-040R.
Note: No template is available for Aruba 3600 devices with firmware version 3.3.2.7.
Note: No template is available for Cisco Aironet 1250 IOS devices with firmware version 12.4(10b)JA3.
Note: No template is available for Aruba 3400 devices with firmware version 3.3.2.7.
Note: No template is available for Aruba 3200 devices with firmware version 3.3.2.8-rn-3.0.
Note: No template is available for Symbol RFS7000 devices with firmware version 1.1.1.0-003R.
Note: No template is available for Cisco Aironet 871W devices with firmware version 12.4(11)T.

New Template

Templates allow you to manage the configuration of 3Com, Alcatel-Lucent, Aruba, Cisco Aironet IOS, Enterasys, HP, Hirschmann, LANCOM, Nomadix, Nortel, Symbol and Trapeze devices in this group using a configuration file. Variables in the templates are used to configure device-specific properties (like name, IP address and channel) as well as group level properties (ssid, radius server, etc).

	Name ▲	Device Type	Status	Fetch Date	Version Restriction
<input type="checkbox"/>	Aruba 200	Aruba 200	Template saved	1/19/2008 11:43 PM	3.2.0.3
<input type="checkbox"/>	Aruba 200 - 3.3.1.1	Aruba 200	Template saved	2/28/2008 6:24 AM	None
<input type="checkbox"/>	Aruba 3600 - 3.2.0.3	Aruba 3600	Template saved	1/18/2008 11:06 AM	3.2.0.3
<input type="checkbox"/>	Aruba 800	Aruba 800	Template saved	2/27/2008 10:58 PM	None
<input type="checkbox"/>	Aruba 800 - 3.1.1.7	Aruba 800	Template saved	1/20/2008 2:09 AM	3.1.1.7
<input type="checkbox"/>	Aruba 800 - 3.3.1.3	Aruba 800	Template saved	7/16/2008 2:55 PM	None
<input type="checkbox"/>	Cisco Aironet 1200 IOS - 12.3(7)JA2	Cisco Aironet 1200 IOS	Template saved	2/27/2008 9:52 PM	12.3(7)JA2
<input type="checkbox"/>	Cisco Aironet 1200 IOS - 12.3(8)JA	Cisco Aironet 1200 IOS	Template saved	2/27/2008 9:49 PM	12.3(8)JA
<input type="checkbox"/>	Cisco Aironet 350 IOS - 12.3(4)JA	Cisco Aironet 350 IOS	Template saved	5/23/2007 1:54 AM	None
<input type="checkbox"/>	Hirschmann BAT-54 - 7.00.0070	Hirschmann BAT54-Rail	Template saved	8/10/2007 10:27 AM	7.00.0070
<input type="checkbox"/>	HP ProCurve ZLWeSM - WT.01.03	HP ProCurve ZLWeSM	Template saved	1/25/2008 1:51 PM	None
<input type="checkbox"/>	LANCOM 3550 - 7.10.0022	LANCOM 3550	Template saved	8/10/2007 10:27 AM	None
<input type="checkbox"/>	Office WPA/WPA2	Aruba 800	Template saved	2/27/2008 10:55 PM	3.3.1.3
<input type="checkbox"/>	Symbol WS2000 - 2.3.1.0-012R	Symbol WS2000	Template saved	1/9/2009 9:51 AM	None

14 Templates

[Select All - Unselect All](#)

Table 105 Groups > Templates

Setting	Description
Note	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 Cisco IOS (Any Model) is selected, the template applies to all IOS APs that do not have a version specific template defined. If there are two templates that might apply to a device, the template with the most restrictions takes precedence.
Status	Displays the status of the template.
Fetch Date	Sets the date that the template was originally fetched from a device.
Version Restriction	Designates that the template only applies to APs running the version of firmware specified. If the restriction is None , then the template applies to all the devices of the specified type in the group. If there are two templates that might apply to a device the template with the most restrictions takes precedence. If there is a template that matches a devices firmware it will be used instead of a template that does not have a version restriction.

Adding Templates

1. To create a new template and add it to the OV3600 template inventory, click **Groups > Templates**, and click **Add**.
2. Complete the configurations illustrated in [Figure 76](#), and the settings described in [Table 106](#).

Figure 76 *Groups > Templates, Add Template*

Cisco Aironet 1200 IOS

Name:

Device Type: Cisco Aironet 1200 IOS

Reboot devices after configuration changes: Yes No

Restrict to this version: Yes No

Template firmware version:

Template Select

Fetch template from device: -- Select Device --

Fetch

Template

The following variables may be used in the template. The value of each variable is configured on the APs/Devices Manage page for each device in the group. Each variable must be surrounded by percent signs: `%hostname%`. The `%if...%` statements must be terminated by `%endif%` and cannot be nested.

`<ignore_and_do_not_push></ignore_and_do_not_push>`, `[]`, `<push_and_exclude></push_and_exclude>` and `()` tags can be used to achieve a good configuration. Please refer to the User Guide for more information.

Available Variables:

antenna_receive	hostname
antenna_transmit	if interface=Dot11Radio0
ap_include_1	if interface=Dot11Radio1
ap_include_10	if ip=dhcp
ap_include_2	if ip=static
ap_include_3	if radio_type=a
ap_include_4	if radio_type=an
ap_include_5	if radio_type=b
ap_include_6	if radio_type=bgn
ap_include_7	if radio_type=g
ap_include_8	if wds_role=backup
ap_include_9	if wds_role=client
cck_power	if wds_role=master
certificate	ip_address
channel	location
channel_width	netmask
chassis_id	ofdm_power
contact	power
domain	
enabled	
gateway	

Credentials

Change credentials the AMP uses to contact devices after successful config push.

Community String:

Confirm Community String:

Telnet/SSH Username:

Telnet/SSH Password:

Confirm Telnet/SSH Password:

"enable" Password:

Confirm "enable" Password:

SNMPv3 Username:

Auth Password:

Confirm Auth Password:

Privacy Password:

Confirm Privacy Password:

SNMPv3 Auth Protocol: MD5

Add Cancel

Table 106 Groups > Templates, Add Template

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 <i>User Guide</i> .
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 .

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](#)
 - `<ignore_and_do_not_push>substring</ignore_and_do_not_push>`
 - `<push_and_exclude>command</push_and_exclude>`
- [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 model AP from the drop-down list, and click **Fetch**.
5. OV3600 automatically attempts to replace some values from the configuration of that AP with *variables* to enable AP-specific options to be set on an AP-by-AP basis. Refer to [“Using Template Syntax” on page 134](#)

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 Enterprise Support at support@ind.alcatel.com.

6. Specify the device types for the template. The templates only apply to devices of the specified type.
 - Specify if 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 possible. Copying the configuration from startup configuration file to running configuration file merges the two configurations and can cause undesired configuration lines to remain active on the AP.

7. Restrict the template to apply only to the specified version of firmware. If the template should only apply to a specific version of firmware, select Yes and enter the firmware version in the **Template Firmware Version** text field.
8. Click the **Save and Apply** button to instruct OV3600 to re-verify the configuration of each AP in the Group.



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
...
```

9. 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's 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>`

Instead of using the full tags you may use the bracketed shorthand, `[substring]`. 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 107](#):

```
%if variable=value%
...
%endif%
```

Table 107 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 108](#) 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's 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). Below is a list of the default values that causes lines to be suppressed in this way when reporting configuration mismatches.

Table 108 *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%	-

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.

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 281](#) 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 XXXXXXXXXXXX
%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 AP's configuration file and the AP must have the SCP server enabled. These three settings correspond to the following lines in the AP's configuration file.

- username Cisco privilege 15 password 7 0802455D0A16
- aaa authorization exec default local
- ip scp server enable

The username line is a guideline and will vary based on the username being set, in this case Cisco, and the password and encoding type, in this case 0802455D0A16 and 7 respectively.

These values can be set on a group wide level using Templates and TFTP. Once these lines are set, SCP can be enabled on the **Groups > Basic** configuration page without problems.

Supporting Multiple Radio Types via a Single IOS Template

Some lines in an IOS configuration file should only apply to 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%
```

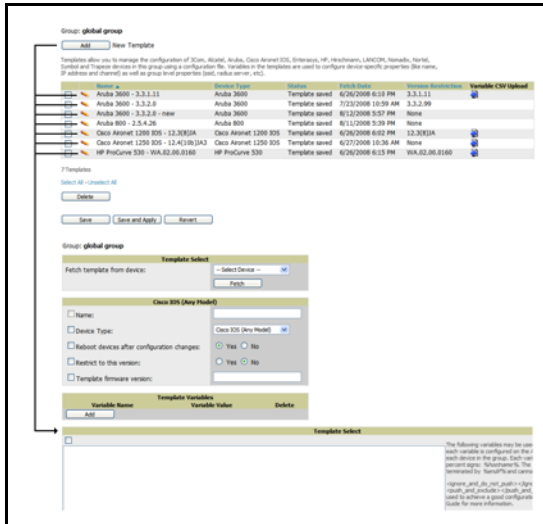
Configuring a Global Template

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:

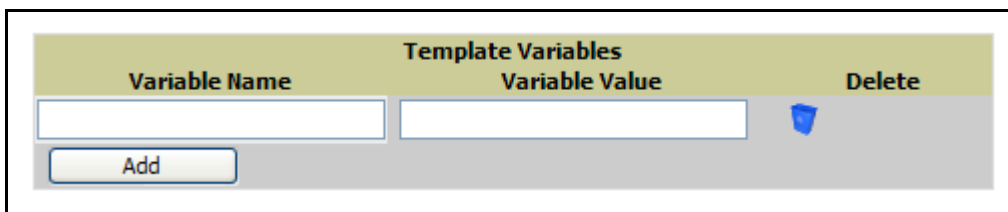
1. Navigate to the **Group > Templates** configuration page for the global group that owns it.
2. Click the **Add** button to add a new template, or click the **pencil** icon next to an existing template to edit that template.
3. Examine the configurations illustrated in [Figure 77](#).

Figure 77 *Group > Templates, Add*



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 78](#).

Figure 78 *Template Variables*



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 79](#) illustrates this page.

Figure 79 *Groups > Templates Edit, Topmost Portion*

Aruba 3600	
Name:	Aruba 3600 - 3.3.1.11
Device Type:	Aruba 3600
Restrict to this version:	Yes
Template firmware version:	3.3.1.11

Group Template Variables	
location:	<input type="text" value="Building1.floor1"/>

9. You are not be able to edit the template itself from the subscriber group's **Groups > Templates** tab. 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.
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.

Introduction

The previous chapter, “Configuring and Using Groups in OV3600” on page 65, describes the configuration and implementation of *groups*. The *group* concept is critical to supporting many thousands of individual devices that can be classified, configured, enabled, monitored and supported as *groups*. This concept is critical to an efficient network management system.

Individual devices must become operational within the wireless network and within such groups. Individual devices must also be configured to maximize their vendor-specific attributes and benefits where these apply. This chapter describes the processes and tools for device-specific configurations and activity, once groups are enabled on the wireless network.

This chapter contains the following device-specific topics, with the goal of enabling individual devices for the groups described in the previous chapter where possible:

- Discovery of Devices Overview
 - Enabling AP Automatic Discovery
 - Defining Networks for SNMP/HTTP Scanning
 - Defining Credentials for Scanning
 - Defining a Scan
 - Executing a Scan
- Manually Adding Individual Devices
 - Adding Access Points, Routers and Switches with a CSV File
- Adding Universal Devices
- Assigning Newly Discovered Devices to Groups
 - Overview
 - Adding a Newly Discovered Device to a Group
 - Verifying That Devices Are Successfully Added to a Group
- Troubleshooting a Newly Discovered Device with Down Status
- Replacing a Broken Device
- Verifying the Device Configuration Status
 - Moving a Device from Monitor Only to Manage Read/Write Mode
- Configuring Individual Device Settings
 - Overview of Individual Device Configuration
 - Configuring AP Settings
- Configuring AP Communication Settings
 - Using the OV3600 APs/Devices Pages

Discovery of Devices Overview

Once you have configured OV3600 on the network and defined at least one Group for Access Points (APs), the next step is to discover all existing APs connected to your network, and to assign them to a configuration Group. OV3600 uses four methods to discover APs, as follows:

- SNMP/HTTP scanning
- Cisco Discovery Protocol (CDP)
- Layer 2 methods (ORiNOCO and Intel/Symbol)
- Manual device entry

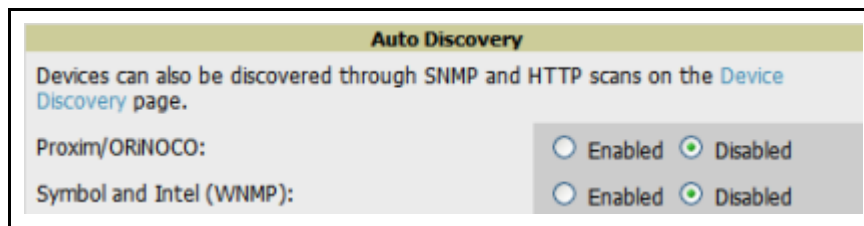
The primary method for OV3600 to discover APs on your network is to scan specified network segments using SNMP and/or HTTP. This chapter covers each of these four methods.

Enabling AP Automatic Discovery

Perform the following steps to use automatic discovery of individual devices.

1. To enable automatic CDP (Cisco and Colubris), Proxim/ORiNOCO and Intel/Symbol (WNMP) scanning, browse to the OV3600 page and locate the **Auto Discovery** section. This page is illustrated in [Figure 80](#) below:

Figure 80 , Auto Discovery



2. Check the corresponding box for the appropriate Auto Discovery methods relating to your deployed access points.
 - The ORiNOCO and Intel/Symbol methods send packets to the broadcast address and listen every 30 seconds.
 - The Cisco CDP uses the polling interval configured for each individual switch or router on the page.
 - For CDP discovery, OV3600 requires read-only access to a router or switch for all subnets that contain APs. As each router or switch is added to the OV3600 database, OV3600 pings that device and initiates an SNMP connection with the specified community string. This verifies that the proper IP address and community string have been provided. Refer to [Table 109](#) for description of the **Auto Discovery** page.

Table 109 , Auto Discovery

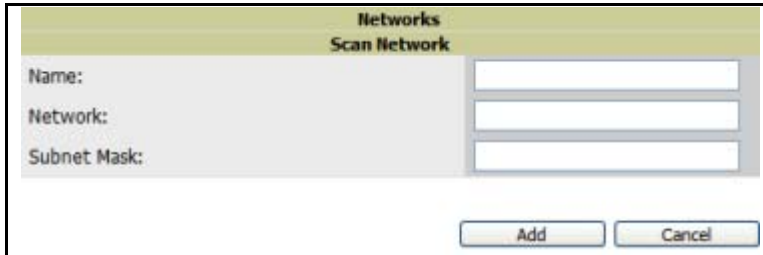
Setting	Default	Description
Proxim/ ORiNOCO	Disabled	When enabled, OV3600 runs the OSU-NMS Protocol service to discover Proxim/ORiNOCO APs on the local subnet.
Intel/Symbol (WNMP)	Disabled	When enabled, OV3600 runs WNMP and the Intel IAPP service to discover Symbol and Intel access points on the local OV3600 subnet.

Defining Networks for SNMP/HTTP Scanning

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

1. Browse to the **Device Setup > Discover** page and locate the **New Network** area. [Figure 81](#) illustrates this page.

Figure 81 *Device Setup > Discover, New Network page*



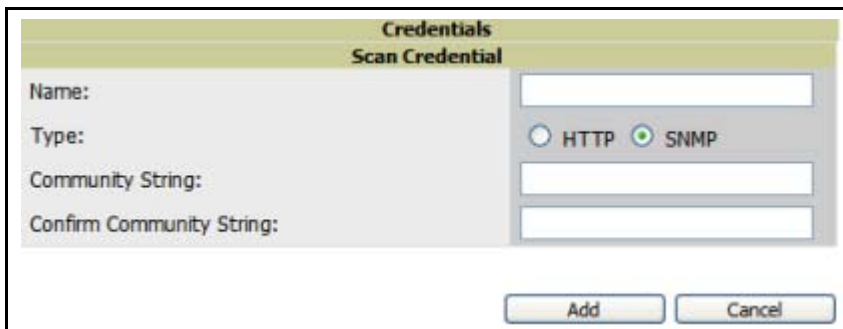
2. Provide a name for the network to be scanned in the **Label** field (for example, **Accounting Network**).
3. In the **Network** field, define the network range (or the first address on the network) to be scanned. One example would be 10.52.0.0, as an illustration.
4. Specify the **Subnet Mask** for the network to be scanned (for example, 255.255.252.0). The largest subnet accepted by OV3600 is 255.255.0.0.
5. Click **Add**.
6. Repeat these steps as required to add as many networks as you would like to the OV3600 database.

Defining Credentials for Scanning

The next step to enable scanning is to define the credentials that are used to scan the network. OV3600 only uses credentials defined for scans during discovery. New access points inherit credentials from the System Credentials configured on the OV3600 **Device Setup > Communications** page. Perform these steps:

1. Locate the **New Credentials** area on the **Device Setup > Discover** page. [Figure 82](#) illustrates this page.

Figure 82 *Device Setup > Discover, New Credentials*



2. Specify the type of scan to be completed (**SNMP** or **HTTP**). In most cases, SNMP scans should be used for discovery.
3. Provide a name for the credential in the **Label** field (for example, **Default**).



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

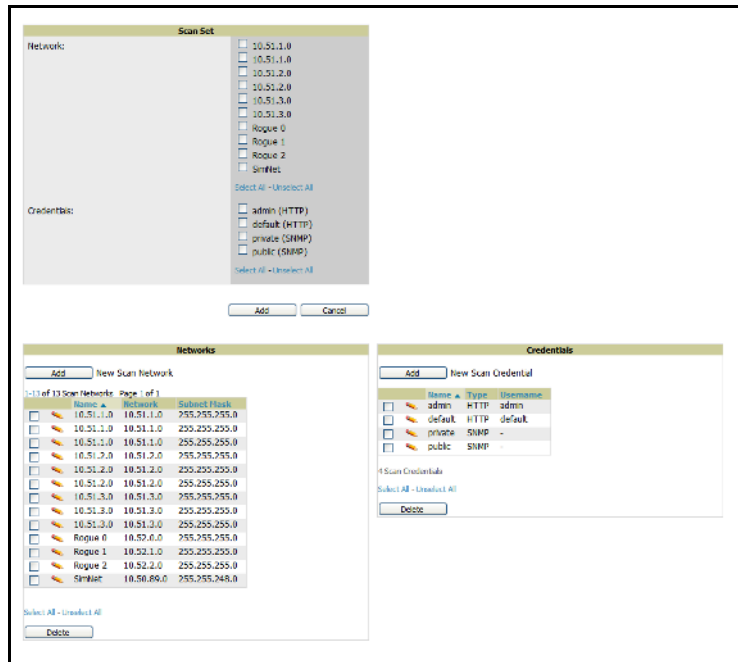
4. Define and confirm the community string to be used. In this section, the community string used can be either **read-only** or **read/write**, as OV3600 only uses it for discovering APs. To bring APs under management, OV3600 uses the credentials supplied in the **Device Setup > SNMP** page.
5. Click **Add**.
6. Repeat these steps to add as many credentials as you would like to the OV3600 database.

Defining a Scan

Once at least one network and one credential have been specified, using the previous procedures in this chapter, you can define a network scan. Perform these steps.

1. Locate the **Define Scan** area of the **Device Setup > Discover** page. [Figure 83](#) illustrates this page.

Figure 83 Device Setup > Discover, New Scan Set



2. Select the **Network(s)** to be scanned and the **Credentials** 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.
3. Click the **Add** button to define the selected scans. The newly defined scans appear in a list at the top of the **Device Setup > Discover** page.
4. To edit an existing scan, click the **pencil** icon next to the scan on the **Device Setup > Discover** page.



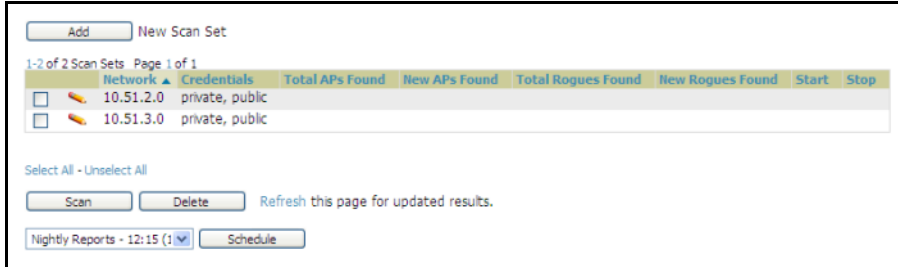
Scheduling an HTTP scan to run daily on your network can help you to discover rogues. Some consumer access points, most D-Link, Linksys, NetGear models, do not support SNMP and are found only on the wired side with an HTTP scan. These devices are discovered only if they have a valid IP address. Proper credentials are not required to discover these access points. Wireless scans and the OV3600 discover these rogues without any special changes.

Executing a Scan

Once a scan has been defined on **Setup > Discover** page, OV3600 can now execute the scan. Perform these steps.

1. Browse to the **Device Setup > Discover** page and locate the **Discovery Execution** area at the top of the page. [Figure 84](#) illustrates this page.

Figure 84 *Device Setup > Discover, Discovery Execution*



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 commences.
4. Click **Show Schedule Options** and enter the desired date and time to schedule a future scan.
5. After several minutes have passed, click the **Refresh** button to refresh the screen and view the results of the scan. [Table 110](#) describes the scan results and related information.

Table 110 *Device Setup > Discover, Discovery Execution*

Column	Description
Supported Devices (Total)	The total number of APs detected during the scan that OV3600 has the ability to configure and monitor. Total includes both APs that are currently being managed by OV3600 as well as newly discovered APs that are not yet under management.
Supported Devices (New)	The number of newly discovered APs that are not yet under OV3600 management but can be managed by OV3600.
Rogue APs (Total)	The total number of APs detected during the scan that OV3600 could not configure and monitor. Total includes both APs that have been discovered on prior scans as well as newly discovered APs from the most recent scan.
Rogue APs (New)	The number of rogue APs discovered on the most recent scan.
Start	Date/time the scan was most recently started.
End	Date/time the scan most recently completed.

6. Navigate to the **APs/Devices > New** page to see a full list of the newly discovered devices.

Manually Adding Individual Devices

Although OV3600 has very robust discovery capabilities, there are deployment situations that dictate manually adding devices to OV3600. Routers and switches need to be added manually to OV3600 by importing a CSV file. More information is provided below. Access points can be added manually with a CSV file, or on the **Device Setup > Add** page, both of which are described.

The first step to adding an AP manually is to select the manufacturer and model. Perform these steps.

1. Browse to the **Device Setup > Add** page and select the manufacturer and model of the device to add.

Figure 85 illustrates this page.

Figure 85 *Device Setup > Add*

2. Select the appropriate group and folder for the AP.
3. Select either the **Monitor only** or **Management read/write** radio button.
4. Click **Add** to finish creating the devices in the network.



If **Manage read/write** is selected, 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 versus Group Policy.

Table 111 further describes the contents of this page.

Table 111 *Device Setup > Add*

Setting	Default	AP Type	Description
Name	None	All	This is a user-configurable name for the AP (maximum of 20 characters).
IP Address (Required)	None	All	This is the IP address of the AP's 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	All	This is the port OV3600 uses to communicate with the AP via SNMP.
Community String Confirm	Taken from the Device Setup > Communication page	All Except Cisco VxWorks	This is a community string used to communicate with the AP. NOTE: The Community String should have RW (Read-Write) capability.

Table 111 Device Setup > Add (Continued)

Setting	Default	AP Type	Description
Username & Password	Taken from the Device Setup > Communication page	Cisco VxWorks	This 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 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 APs typically have SNMP disabled and a blank username and password combination for HTTP and Telnet. Cisco supports multiple community strings per AP.
Telnet Username & Password	Taken from the Device Setup > Communication page	Cisco IOS, Acton, HP 420, RoamAbout AP-3000	This is the 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	Cisco IOS	This is the password that allows OV3600 to enter enable mode on the AP.
HTTP Username & Password	Taken from the Device Setup > Communication page	Colubris Intel 2011b Symbol 4131	This is the 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	Enterasys R2	This is the 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.
Telnet Port	23	Cisco IOS Acton HP 420 RoamAbout AP-3000	This is the port OV3600 uses to communicate with the AP via the Telnet protocol.
HTTPS Port	443	Colubris	This is the port OV3600 uses to communicate with the AP via the HTTPS protocol.
Privacy Password	Taken from the Device Setup > Communication page	Enterasys R2	This is the SNMPv3 privacy password.
Group	Default Group	All	This is a drop-down menu used to assign the AP to a Group .
Folder	Top	All	This is drop-down menu used to assign the AP to a Folder .

Adding Access Points, Routers and Switches with a CSV File

Adding routers and switches into your OV3600 as managed devices allows OV3600 to complete the following functions:

- Leverage CDP to more efficiently discover new access points.
- Read the ARP table to correlate MAC Addresses of client devices and rogues to IP addresses on your network.
- Read the bridge forwarding tables to discover Rogue access points.

OV3600 needs **read-only** access to a router or switch for all subnets that contain devices. As each router or switch is added to the OV3600 database, OV3600 pings that device and initiates an SNMP connection with the specified community string. This verifies that the proper IP address and community string have been provided.



This is an optional step to enable OV3600 to track client devices by IP address, auto-discover Cisco APs and/or enable RAPIDS MAC scanning. It is not required for basic OV3600 operation. If you are using a VPN client to get username info, you must enable ARP scanning. Colubris access points using the VPN on the AP automatically provides this information to OV3600.

You can use a comma-separated values file to import lists of devices (access points, routers and switches) into OV3600. The 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**

Table 112 illustrates these requirements in a hypothetical configuration.

Table 112 Sample Configuration of Adding Access Points, Routers and Switches with a CSV File

Item	Example
IP Address	10.34.64.163
SNMP Community String	private
Name	switch1.example.com
Type	Router/Switch
Auth Password	nonradiance
SNMPv3 Auth Protocol	md5
Privacy Password	privacy
SNMPv3 Username	sv3user
Telnet Username	telnetuser
Telnet Password	telnetpwd
Enable Password	enable
SNMP Port	161

1. To import a CSV file, navigate to the OV3600 **Device Setup > Add** page and click the link to **Import Devices via CSV**. [Figure 86](#) illustrates the page.

Figure 86 *Device Setup > Add (import from CSV)*

Upload a list of devices

Location

Group: Access Points (SSID: -) ▾

Folder: Top ▾

2. Select a group and folder into which to import the list of devices, or leave the default menu selections of **Access Points group** and **Top folder**. Click the browser button and navigate for the list, and then click **Upload** to add the list of devices into OV3600.

Adding Universal Devices

OV3600 is able to get basic monitoring information from any device that supports SNMP including switches, routers and unsupported access points. This allows monitoring of 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, UDS also enables basic monitoring of many of the less commonly used APs.

Perform these steps to add universal devices to OV3600. The first step to manually adding an AP is to select the manufacturer and model.

1. Browse to the OV3600 **Device Setup > Add** page and select the manufacturer and model.
2. Select **Universal Network Device** from the drop-down menu and 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 unmonitored or to be 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 Newly Discovered Devices to Groups

Overview

Once you have discovered devices on your network, you must assign these devices to a Group. To configure a new group, refer to “Configuring and Using Groups in OV3600” on page 65.

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.

Adding a Newly Discovered Device to a Group

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, device manufacturer and model, MAC Address, IP Address, and the date/time of discovery. [Figure 87](#) illustrates this page.

Figure 87 *APs/Devices > New*

<input type="checkbox"/>	Cisco-4400-1	Cisco Airespace 4400	10.51.1.234	00:0B:85:40:7C:80	2/8/2007 7:11 PM
<input type="checkbox"/>	symbol-4121-1	Symbol 4121	10.51.1.100	00:A0:F8:97:A9:AA	2/8/2007 7:11 PM

22 APs/Devices

[View Ignored Devices](#)

[Check All - Uncheck All](#)

Group:

Folder:

Monitor Only

Manage Read/Write

2. Select the device(s) to be added to a Group.
3. 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.
4. Select either the **Monitor only** or the **Manage read/write** radio button and click the **Add** button.



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.

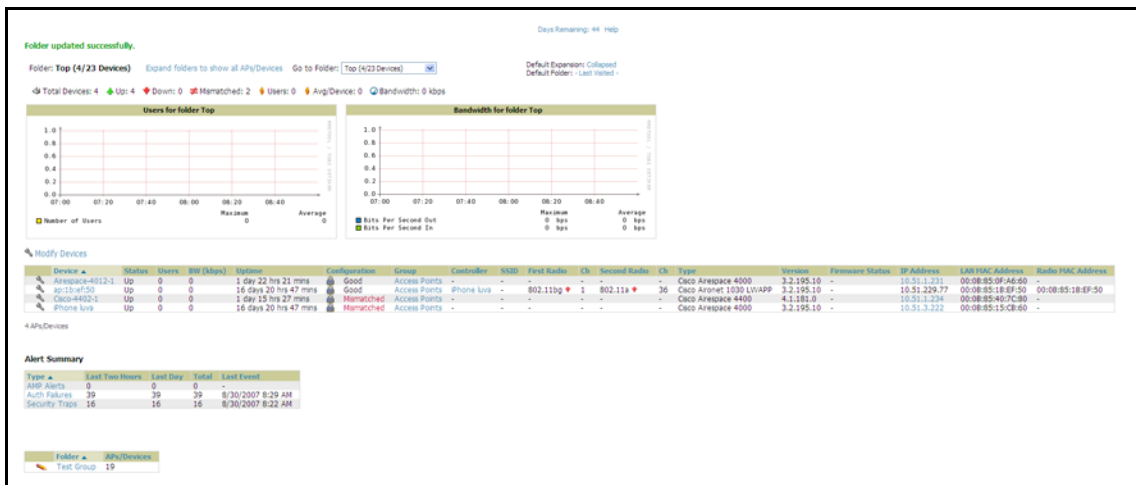
- If you do not wish to manage or monitor a discovered device, you may select the device(s) from the list and click either **Ignore Selected Devices** or **Delete Selected Devices**. If you choose to **Ignore** the devices, they will not be displayed in the **APs/Devices > New** list if they are discovered 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.

Verifying That Devices Are Successfully Added to a Group

When you add a newly discovered device to a Group in either **Monitor** or **Manage** mode, you should verify that the process completed successfully. Perform the following steps:

- 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 Group. [Figure 88](#) illustrates this page.

Figure 88 *APs/Devices > List*



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



Immediately after you have added the device to a Group, notice the device Status change to **Down** while OV3600 verifies the configuration of the device and compares it to Group settings. The device status changes to **Up** when verification is complete.

- Navigate to the **Alert Summary** section of the **APs/Devices > List** page. This section displays OV3600 **Alerts**, **Auth Failures**, and **Security Traps**. The same section also appears on the **Groups > Monitoring** page, and is linked from a controller's monitoring interface.
- Clicking on the **Auth Failures** link takes you to a summary page of authentication failures. Authentication failures can be configured for WLC devices on the **Group > Basic** page, and for IOS devices by adding this line to the template:

```
snmp-server host <OV3600_ip_address> version 2c <community> aaa_server authenticate-fail deauthenticate snmp syslog
```

[Figure 89](#) illustrates the page for authentication failures.

Figure 89 Authentication Failures Summary

Return to List | Authentication Failures for Folder Top Help

Summary

Event Type ▲	Last Two Hours	Last 24 Hours	Total
Client blocked (Failed 802.1x authentication)	3	3	3
Client blocked (Failed association)	5	5	5
Client blocked (Failed authentication)	12	12	12
Client blocked (Failed web authentication)	11	11	11
Client blocked (P smart)	8	8	8
5 Authentication Failure Types	39	39	39

1/20 of 39 Authentication Failures Page 1 of 2 > > |

Event Type	AP	Controller	Radio Type	Username	Client MAC Address	RADIUS Server Address	Creation Time ▲
<input type="checkbox"/> Client blocked (Failed web authentication)	ap1b0ef50	Phone Lvs	802.11bg	-	83:88:82:3C:2A:CE	-	8/30/2007 8:27 AM
<input type="checkbox"/> Client blocked (Failed web authentication)	ap1b0ef50	Phone Lvs	802.11bg	-	02:78:91:1F:93:3D	-	8/30/2007 8:27 AM
<input type="checkbox"/> Client blocked (Failed authentication)	ap1b0ef50	Phone Lvs	802.11bg	-	4E:81:27:A6:9E:18	-	8/30/2007 8:27 AM
<input type="checkbox"/> Client blocked (P smart)	ap1b0ef50	Phone Lvs	802.11a	-	C6:99:37:79:55:C0	-	8/30/2007 8:27 AM
<input type="checkbox"/> Client blocked (Failed web authentication)	ap1b0ef50	Phone Lvs	802.11bg	-	94:85:2E:75:5F:54	-	8/30/2007 8:27 AM
<input type="checkbox"/> Client blocked (Failed association)	ap1b0ef50	Phone Lvs	802.11a	-	84:96:A8:35:A0:EB	-	8/30/2007 8:27 AM
<input type="checkbox"/> Client blocked (Failed 802.1x authentication)	ap1b0ef50	Phone Lvs	802.11bg	-	39:92:79:74:02:F3	-	8/30/2007 8:27 AM
<input type="checkbox"/> Client blocked (P smart)	ap1b0ef50	Phone Lvs	802.11a	-	7C:9F:25:74:05:A2	-	8/30/2007 8:27 AM
<input type="checkbox"/> Client blocked (Failed 802.1x authentication)	ap1b0ef50	Phone Lvs	802.11a	-	C6:99:37:79:55:C0	-	8/30/2007 8:27 AM
<input type="checkbox"/> Client blocked (Failed authentication)	ap1b0ef50	Phone Lvs	802.11a	-	4E:81:27:A6:9E:18	-	8/30/2007 8:27 AM
<input type="checkbox"/> Client blocked (P smart)	ap1b0ef50	Phone Lvs	802.11bg	-	84:96:A8:35:A0:EB	-	8/30/2007 8:28 AM
<input type="checkbox"/> Client blocked (Failed association)	ap1b0ef50	Phone Lvs	802.11a	-	C6:99:37:79:55:C0	-	8/30/2007 8:28 AM
<input type="checkbox"/> Client blocked (Failed web authentication)	ap1b0ef50	Phone Lvs	802.11a	-	E9:2F:00:00:A7:A6	-	8/30/2007 8:28 AM
<input type="checkbox"/> Client blocked (P smart)	ap1b0ef50	Phone Lvs	802.11a	-	4E:81:27:A6:9E:18	-	8/30/2007 8:28 AM
<input type="checkbox"/> Client blocked (Failed web authentication)	ap1b0ef50	Phone Lvs	802.11a	-	89:3F:00:80:3F:A6	-	8/30/2007 8:28 AM
<input type="checkbox"/> Client blocked (Failed association)	ap1b0ef50	Phone Lvs	802.11a	-	4E:81:27:A6:9E:18	-	8/30/2007 8:28 AM
<input type="checkbox"/> Client blocked (Failed web authentication)	ap1b0ef50	Phone Lvs	802.11a	-	8C:76:5C:CA:49:57	-	8/30/2007 8:28 AM
<input type="checkbox"/> Client blocked (Failed authentication)	ap1b0ef50	Phone Lvs	802.11bg	-	63:79:41:AF:79:3D	-	8/30/2007 8:28 AM
<input type="checkbox"/> Client blocked (P smart)	ap1b0ef50	Phone Lvs	802.11a	-	03:76:41:AF:79:3D	-	8/30/2007 8:28 AM
<input type="checkbox"/> Client blocked (Failed authentication)	ap1b0ef50	Phone Lvs	802.11a	-	03:78:91:1F:93:3D	-	8/30/2007 8:28 AM

Select All - Unselect All

- The **Summary** section of the page details the number of events that have occurred in the last two hours, the last 24 hours, and total.
 - The **List** section of the page details each recorded event. The AP and Controller names are links that will take you directly to the AP or Controller.
5. Clicking on the **Security Traps** link of the **Alert Summary** section takes you to the **Cisco WLC Security Attacks** summary page. This page displays information from the Intrusion Detection System from the WCS. IDS traps do not need to be enabled independently in OV3600. **Figure 90** illustrates this page.

Figure 90 Cisco WLC Security Attacks

Return to List | Cisco AireSpace Security Attacks for Folder Top

Summary

Attack Signature ▲	Last Two Hours	Last 24 Hours	Total
Assoc flood	1	1	1
Bcast deauth	3	3	3
Broadcast Probe flood	1	1	1
Death flood	1	1	1
NetStumbler 3.2.0	1	1	1
NetStumbler 3.2.3	1	1	1
NetStumbler generic	1	1	1
NULL probe resp 1	1	1	1
Reassoc flood	1	1	1
Res mgmt D	2	2	2
Res mgmt E & F	2	2	2
Some Custom Sig	1	1	1
12 Signature Attack Types	16	16	16

1-16 of 16 AireSpace IDSs Page 1 of 1

Description	Time ▲	Precedence	Channel	Attacker	Controller	AP	Radio
<input type="checkbox"/> NetStumbler generic DESCRIPTION	8/30/2007 8:21 AM	21304	16371	AA:00:00:00:00:0E	Phone Lvs	ap1b0ef50	802.11a
<input type="checkbox"/> Res mgmt E & F DESCRIPTION	8/30/2007 8:21 AM	29548	16371	AA:00:00:00:00:1E	Phone Lvs	ap1b0ef50	802.11bg
<input type="checkbox"/> Broadcast Probe flood DESCRIPTION	8/30/2007 8:21 AM	3324	59115	AA:00:00:00:00:1E	Phone Lvs	ap1b0ef50	802.11a
<input type="checkbox"/> Broadcast Probe flood DESCRIPTION	8/30/2007 8:21 AM	46806	10318	AA:00:00:00:00:10	Phone Lvs	ap1b0ef50	802.11a
<input type="checkbox"/> NetStumbler generic DESCRIPTION	8/30/2007 8:21 AM	21384	29274	AA:00:00:00:00:13	Phone Lvs	ap1b0ef50	UNB
<input type="checkbox"/> Res mgmt E & F DESCRIPTION	8/30/2007 8:21 AM	41393	8350	AA:00:00:00:00:2A	Phone Lvs	ap1b0ef50	802.11a
<input type="checkbox"/> Res mgmt E & F DESCRIPTION	8/30/2007 8:22 AM	23806	8906	36:62:79:74:65:73	Phone Lvs	ap1b0ef50	UNB
<input type="checkbox"/> NetStumbler 3.3.0 DESCRIPTION	8/30/2007 8:22 AM	40675	16371	AA:00:00:00:00:1F	Phone Lvs	ap1b0ef50	UNB
<input type="checkbox"/> NetStumbler 3.3.0 DESCRIPTION	8/30/2007 8:22 AM	320	42972	AA:00:00:00:00:10	Phone Lvs	ap1b0ef50	002.11a
<input type="checkbox"/> Res mgmt E & F DESCRIPTION	8/30/2007 8:22 AM	40814	29274	AA:00:00:00:00:26	Phone Lvs	ap1b0ef50	UNB
<input type="checkbox"/> Death flood DESCRIPTION	8/30/2007 8:22 AM	30508	1443	AA:00:00:00:00:15	Phone Lvs	ap1b0ef50	UNB
<input type="checkbox"/> Res mgmt E & F DESCRIPTION	8/30/2007 8:22 AM	320	8906	AA:00:00:00:00:2B	Phone Lvs	ap1b0ef50	802.11a
<input type="checkbox"/> NetStumbler 3.2.3 DESCRIPTION	8/30/2007 8:22 AM	40814	8906	AA:00:00:00:00:27	Phone Lvs	ap1b0ef50	802.11a
<input type="checkbox"/> Deassoc flood DESCRIPTION	8/30/2007 8:22 AM	3324	10318	AA:00:00:00:00:12	Phone Lvs	ap1b0ef50	802.11bg
<input type="checkbox"/> NULL probe resp 2 DESCRIPTION	8/30/2007 8:22 AM	29548	22443	AA:00:00:00:00:11	Phone Lvs	ap1b0ef50	802.11bg
<input type="checkbox"/> NetStumbler 3.2.3 DESCRIPTION	8/30/2007 8:22 AM	61039	22443	AA:00:00:00:00:23	Phone Lvs	ap1b0ef50	802.11a

Select All - Unselect All

- The **Summary** section of the page details the number of events that have occurred in the last two hours, the last 24 hours, and total. OV3600 displays signature attack types
- The **List** section of the page details each recorded event. The **AP** and **Controller** names are links that will take you directly to the AP or Controller.

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.

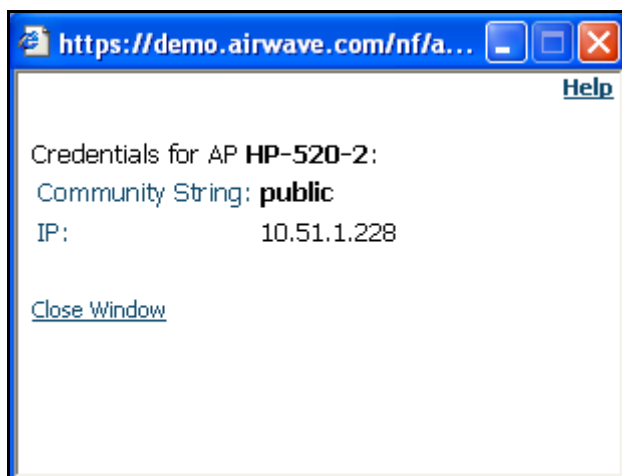
1. Click the **Name** of the device in the list of devices on the **APs/Devices > List** page. This automatically directs you to the **APs/Device > Monitor** page for that device.
2. Locate the **Status** section. If the Status is **Down**, there is an onscreen error message indicating the cause of the problem. Some of the common system messages are as follows in [Table 113](#):

Table 113 Common System Messages for Down Status

Message	Meaning
SNMP Get Failed	The 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	The 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. 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 the OV3600 for security reasons by setting a flag in the database. 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 Enterprise Support at support@ind.alcatel.com. [Figure 91](#) illustrates this page.

Figure 91 View AP Credentials





The **View AP Credentials** message may appear slightly different depending on the manufacture and model.

5. If the credentials are incorrect, return to the **Device Communications** area on the **APs/Devices > Manage** page. [Figure 92](#) illustrates this page.

Figure 92 APs/Devices > Manage, Device Communication

Device Communication

[View Device Credentials](#)

If this device is down because its IP address or management ports have changed, update the fields below with the correct information.

IP Address:

SNMP Port:

If this device is down because the credentials on the device have changed, update the fields below with the correct information.

This device is currently using SNMP version 1

Community String:

Confirm Community String:

Auth Password:

Confirm Auth Password:

Privacy Password:

Confirm Privacy Password:



The **Device Communication** area may appear slightly different depending on the particular manufacture 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**.

Replacing a Broken Device

When a device goes down due to hardware failure, OV3600 provides a simple process to replace the device.

1. The first step is to replace the broken hardware.
2. Once the new device is on the network, run a discovery scan in OV3600.
3. When the new AP is discovered, add it to the same group as the broken device. Navigate to the broken devices **APs/Devices > Manage** page and click **Replace hardware**.
4. You will then be asked to specify the new device that is replacing the broken hardware. Select the new hardware in the drop-down menu and click **Replace**. The two device records will be merged and the new device will inherit the broken devices history.
5. If the new device has the same IP address as the broken device, you will need to add it manually to OV3600 via the **Device Setup > Add** page before it appears in the **Replace Hardware** drop-down menu.

Verifying the Device Configuration Status

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

1. Browse to the **APs/Devices > List** page. See [Figure 88](#).
2. Locate the device in the list and check the **Configuration** column.
3. If the device is in **Monitor** mode, the **lock** symbol appears next to the **Configuration** column, indicating that the device is locked and will not be configured by OV3600.
4. Verify the **Configuration** status of the device.
5. 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.
6. 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.
7. 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 on the left side of the page.

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 93](#) illustrates this page.

Figure 93 *APs/Devices > Audit*

General	
Name:	Test 2
Status:	Up (OK)
Configuration:	Mismatched (More Details)
Last Contacted:	2/8/2007 7:36 PM
Type:	Proxim AP-700
Firmware:	3.2.1
Group:	Access Points
Folder:	Top
Management Mode:	<input checked="" type="radio"/> Monitor Only <input type="radio"/> Manage Read/Write

8. 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.
 - To change Group settings, return to the **Groups > List** section, select the Group to be edited from the list, and go through the Group configuration pages to change the Group configuration policies. When complete, return to the **APs/Devices > Audit** page for the AP and click the **Audit** button to refresh the screen. If the new AP Configuration status is not **Good**, review any remaining discrepancies between the AP's current configuration and the Group policy to ensure that the changes are appropriate.
 - You can also click **Import** to update many of the group's settings based on the device's current configuration. This will take you first to a confirmation page where you will need to enter shared secrets manually, with security credentials that cannot be read from the device.
 - To ensure you have the current device configuration, click **Audit**. This causes OV3600 to reread the device configuration and to compare it against the group's desired configuration.

- To ignore specific mismatches, click the **Customize** button. OV3600 is able to ignore specific settings on specific APs when calculating mismatches. Once you have clicked **Customize**, select the settings you would like to ignore and click **Save**.
- To reassign the AP to another Group, go to the **APs/Devices > Manage** page for that AP and reassign it to a different Group using the drop-down menu. Click **Apply** to add the AP to the new Group. Remember to ensure that the AP remains in **Monitor** mode if you do not want configuration changes to be applied automatically to the AP. The **Manage This AP** field on the **APs/Devices > Manage** page should be in the **No** position. Return to the **APs/Devices > Audit** page to review any configuration changes before shifting the AP to **Manage** mode.

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. Perform the following steps.

1. Browse to the **APs/Devices > List** page and click the **wrench** icon next to the name of the AP to be shifted to **Manage Read/Write** mode. This directs you to the **APs/Devices > Manage** page.
2. Locate the **General** area. [Figure 94](#) illustrates this page.

Figure 94 *APs/Devices > Manage, General*

General	
Name:	Test 2
Status:	Up (OK)
Configuration:	Mismatched (More Details)
Last Contacted:	2/8/2007 7:36 PM
Type:	Proxim AP-700
Firmware:	3.2.1
Group:	Access Points
Folder:	Top
Management Mode:	<input checked="" type="radio"/> Monitor Only <input type="radio"/> Manage Read/Write

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 **Apply**. OV3600 presents a confirmation screen reminding you of all configuration changes that will be applied to the device in **Manage** mode.
5. 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.
6. 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.
7. To move multiple devices into managed mode at once, use the **Modify these devices** link. Refer to [“Modifying Multiple Devices”](#) on page 123 for more information.

Configuring Individual Device Settings

This section contains the following topics describing individual device configuration within the network and within groups:

- “Overview of Individual Device Configuration” on page 157
- “Configuring AP Settings” on page 157

Overview of Individual Device Configuration

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 interference.



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 **AP > Audit** page and identified by name. By default, this is the date and time it was created; devices are also archived by date. Click the **pencil** icon next to the configuration name to change the name, add notes, or view the archived configuration.

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 **AP > Audit** page. This applies to startup or to running configuration files.

Comparing two configurations highlights specific lines that are mismatched, and provides links to the OV3600 pages where the mismatched settings can be configured.

Configuring AP Settings

1. Browse to the **APs/Devices > List** page and click the **Name** of the device. This directs you to the **APs/Devices > Monitor** page.
2. Click the **APs/Devices > Manage** tab and locate the **Settings** area. [Figure 95](#) illustrates this page.

Figure 95 *APs/Devices > Manage*

The screenshot shows the configuration page for an AP. It is divided into two main sections: **General** and **Settings**. The **General** section contains fields for Name (11.1.2), Status (Up (OK)), Configuration (Good), Last Contacted (2/19/2009 9:57 AM), Type (Aruba AP 61), Firmware (3.3.2.10), Controller (ethersphere-lms4), Group (Acme Corporation), and Folder (Top > HQ). Below this is a **Notes** section with a text area. The **Settings** section contains fields for Name (11.1.2), Latitude, Longitude, Altitude (m), Group (Acme Corporation (SSID: employee, infrastructure)), and Folder (HQ). Below the settings is a **Neighboring APs** table:

AP	Channel	Signal
11.1.3	40	38
11.1.4	149	36
11.1.6	149	27
APB121_100-k121	48	19
11.1.5	40	18

At the bottom of the page are several buttons: Save and Apply, Revert, Delete, Ignore, Import Settings, and Replace Hardware.

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.

3. Locate the **General** section—this section provides general information about the AP's current status. [Table 114](#) describes the fields, information, and settings.

Table 114 *APs/Devices > Manage*

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 via 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.

4. 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 manufacturers 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 manufacturer and model.

[Table 115](#) describes field settings, default values, and additional information for this page.

Table 115 APs/Devices > Manage, Settings

Setting	Default	Device Type	Description
Name	None	All	User-configurable name for the device (max. 20 characters)
Domain	None	IOS	Field is populated upon initial device discover or rereading settings. If option on OV3600 Setup > Network page is chosen will display fully-qualified domain names for IOS APs. Used in conjunction with Domain variable in IOS templates.
Location	Read from the device	All	The SNMP location set on the device.
Contact	Read from the device	All	The SNMP contact 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.
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.
Mesh Role:	Mesh AP	Mesh Devices	Drop-down menu specifies the mesh role for the AP. <ul style="list-style-type: none"> • 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 placed for example 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.
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 can operate in bridge or router mode.
Ethernet Interface Configuration	100 Mbps Full Duplex	PTMP/WiMAX	Bandwidth rates for uploading and downloading.
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.

Table 115 APs/Devices > Manage, Settings

Setting	Default	Device Type	Description
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ⑩ 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. ⑩ Primary Only—The AP transmits and receives on the primary antenna only. Secondary Only: The AP transmits and receives on the secondary antenna only. ⑩ 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.
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.

Table 115 APs/Devices > Manage, Settings

Setting	Default	Device Type	Description
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. NOTE: 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 via DHCP. If disabled, the AP will use a static IP address. NOTE: 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's 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). NOTE: 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. NOTE: 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. NOTE: 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.

6. [Table 116](#) describes field settings, default values, and additional information for this page.

Table 116 APs/Devices > Manage, IOS Template Options

Setting	Default	Device Type	Description
WDS Role	Client	Cisco IOS	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.

- For Cisco WLC Controllers, 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 96](#) illustrates this interface, and [Table 117](#) describes the settings and default values.

Figure 96 APs/Devices > Manage, Interfaces

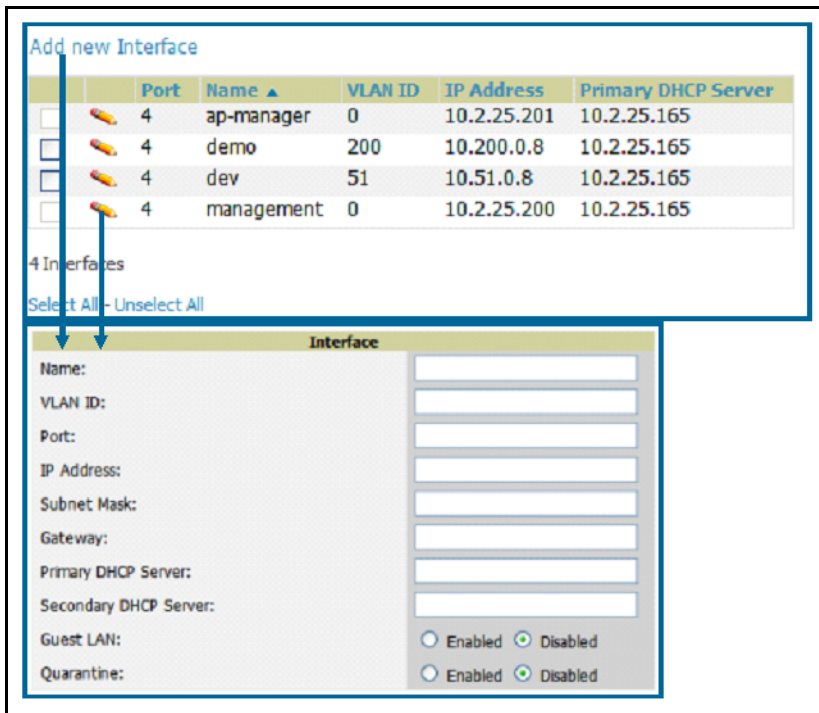


Table 117 MP APs/Devices > Manage

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.

Table 117 MP APs/Devices > Manage (Continued)

Field	Default	Description
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 AP Communication Settings

Perform the following steps to configure AP communication settings for individual device support.

1. Locate the **Device Communication** area on the **APs/Devices > Manage** page.
2. Specify the credentials to be used to manage the AP. [Figure 97](#) illustrates this page.

Figure 97 APs/Devices > Manage, Device Communication



The **Device Communication** area may appear slightly different depending on the particular manufacture 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 the database by the root user. Contact Alcatel-Lucent Enterprise Support at support@ind.alcatel.com for detailed instructions on disabling the link.
5. Click **Apply**. OV3600 presents a confirmation screen 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.



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.

6. Click **Upgrade Firmware** to upgrade the device's firmware.



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 accordingly plan their upgrades using OV3600.

Figure 98 illustrates this page and Table 118 describes the settings and default values.

Figure 98 APs/Devices > Manage Firmware Upgrades

Table 118 APs/Devices > Manage Firmware Upgrades

Setting	Default	Description
Desired Version	None	Drop-down menu 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.

Using the OV3600 APs/Devices Pages

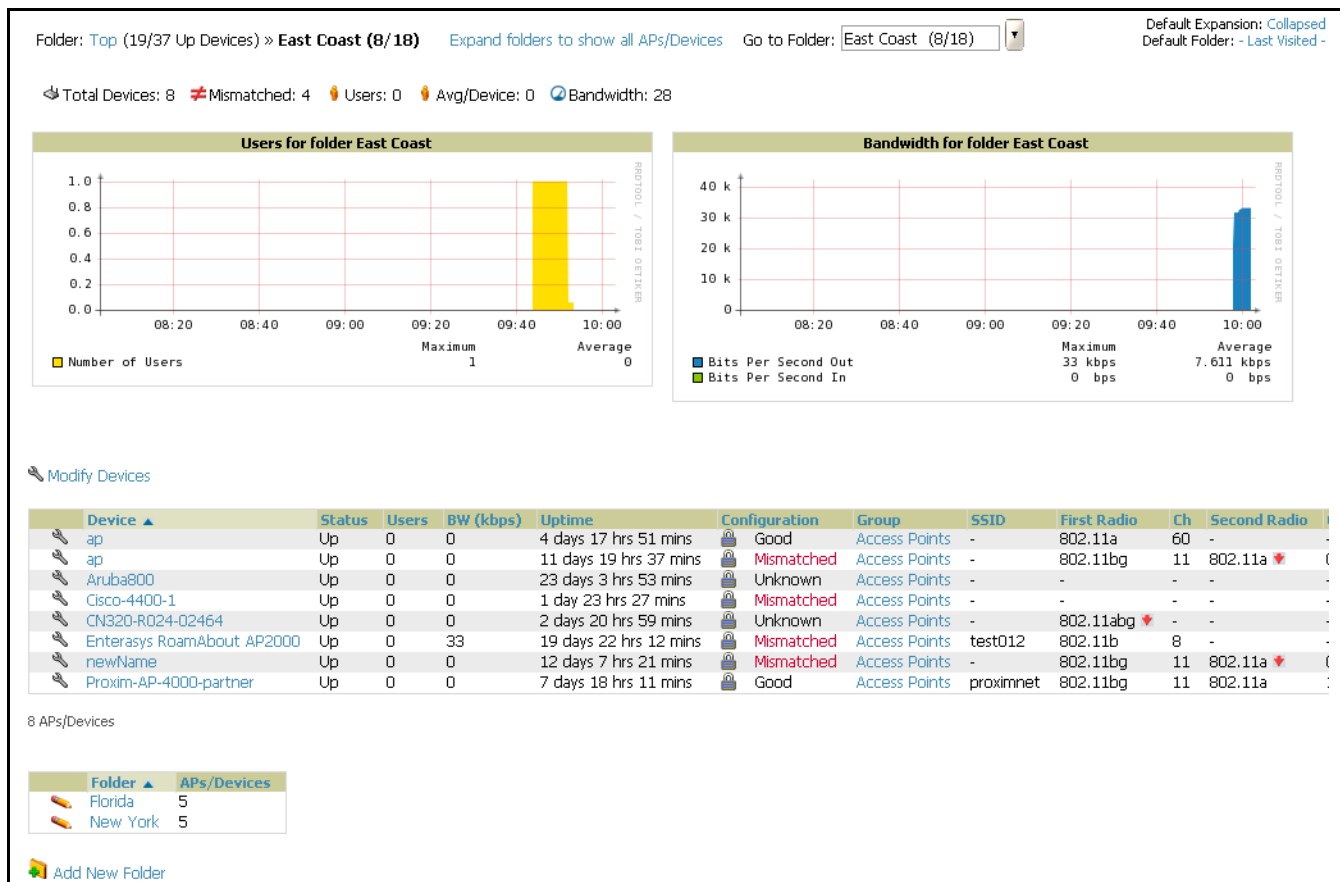
This section describes optional components of the **APs/Devices** page, with explanation to controls, settings, and default values. This section has the following inter-related procedures:

- [Using Device Folders \(Optional\)](#)
- [Monitoring APs with the Monitoring and Controller Pages](#)

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 that is 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 viewable to OV3600 users. [Figure 99](#) and [Figure 100](#) illustrate this component.

Figure 99 *APs/Devices > Up, Example*



In the figure above, observe the **APs/Devices > Up** page for the East Coast folder. There are currently eight **up** devices in the East Coast folder and five **up** devices in each of the subfolders. Folders are created in a standard hierarchical tree structure.

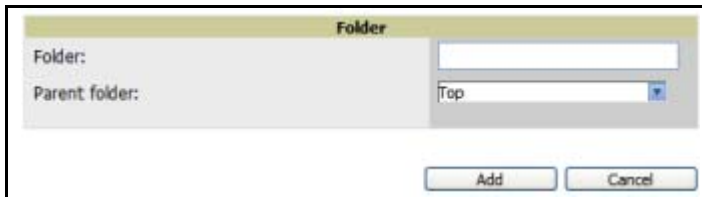
Folder views are persistent in OV3600. If you select the **East Coast** folder and then click the **Down** link at the top of the page, you are taken to all of the down devices in the folder.

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 100](#) illustrates the page that appears.

Figure 100 Folder Creation



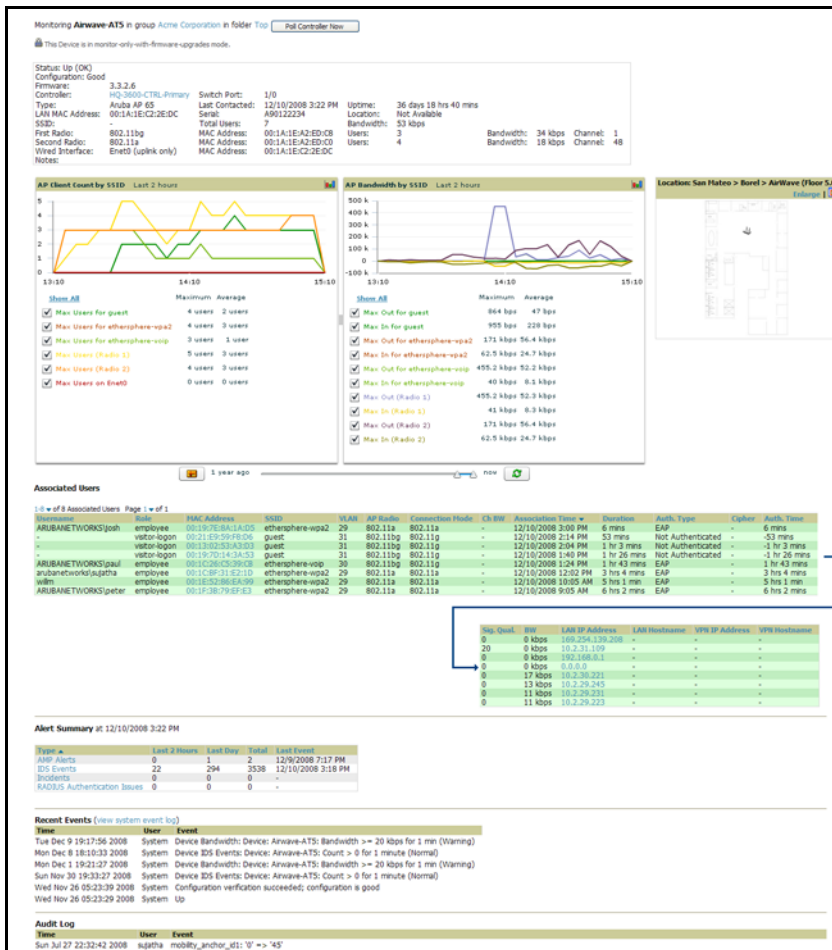
2. Enter the name of the new folder.
3. Select the **Parent** folder.
4. Click **Add**.

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.

Monitoring APs with the Monitoring and Controller Pages

The **APs/Devices > Monitoring** page can be reached by navigating to the **APs/Devices > List** page and clicking any device name. The **APs/Devices > Monitor** page provides a QuickView™ of important data regarding the AP. **Figure 101** illustrates this page.

Figure 101 APs/Devices > List > Monitor



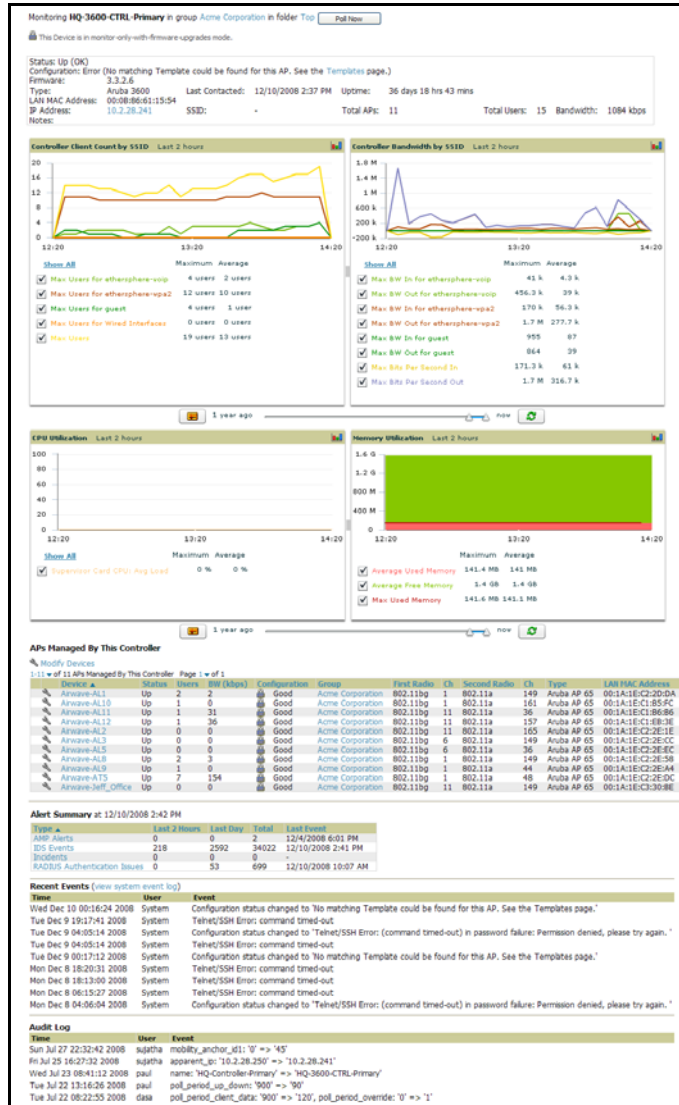
Some data on this page is displayed based on the device type.

The AP Monitoring page has seven distinct sections, as follows:

- Text Status
- Graph Statistics
- QuickView (hidden by default)
- Associated Users
- Alerts
- Recent Events
- Audit Log

Figure 102 illustrates the **Controller** page that appears by clicking the name of a controller in the **Controller** field.

Figure 102 APs/Devices > Monitoring, Controller Page Launched by Clicking Controller Name



Perform the following steps to use this page:

1. Locate the **General** area on the **APs/Devices > Monitor** page. Table 119 describes the fields and information displayed.

Table 119 APs/Devices > Monitor, General

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	The Status field displays OV3600's ability 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 via 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 via SNMP and is unable to ping the AP. This usually means OV3600 is blocked from connecting to the AP or the AP needs to be rebooted or reset.
Configuration	Good means all the settings on the AP agree with the settings OV3600 wants them to have. Mismatched means there is a configuration mismatch between what is on the AP and what OV3600 wants to push to the AP. The Mismatched link directs you to this specific APs/Devices > Audit page where each mismatch is highlighted.
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 102 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's 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.

Table 119 APs/Devices > Monitor, General

Field	Description
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.
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.

2. Locate the **Statistics** link on the **APs/Devices > Monitor** page. This link launches the dot11counters graphs which include the following information:
 - Max and Average users on the Radio
 - Bits per Second In and Out
 - Frame Check Sequence Error Rate - increments when an FCS error is detected in an MPDU.
 - Frame Duplicate Rate - increments when a frame is received that the Sequence Control field indicates is a duplicate.
 - WEP Undecryptable Rate
 - TX Frame Rate
 - Multicast TX/RX Frame Rate
 - TX/RX Fragment Rate
 - Retry Rate
 - Multiple Retry Rate
 - Failed Rate
 - ACK Failure Rate
 - RTS Success/Failure Rate

3. Locate the **Graphical Data** area on the **APs/Devices > Monitor** page. This area displays flash-based graphs of users and bandwidth reported by the device, as well as graphs for CPU and memory utilization for controllers. [Table 120](#) describes graph information displayed in this page.

Table 120 APs/Devices > Monitor, Graphical Data

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.

4. Locate the **Associated Users** area on the **APs/Devices > Monitor** page. The **Associate Users** area provides details about the users associated to devices. This information also appears on the **Users > All** page. [Table 121](#) describes the fields and information displayed.

Table 121 APs/Devices > Monitor, Associated Users

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.
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 will be considered not authenticated.
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.

Table 121 APs/Devices > Monitor, Associated Users

Field	Description
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.

5. Locate the **Pending Alerts** area on the **APs/Devices > Monitor** page. The **Pending Alerts** area displays all unacknowledged alerts for the AP.
6. For Alcatel-Lucent devices, **Remote Access Monitoring** is displayed on the **AP > Monitor** page. OV3600 displays wired interfaces as well as the user count for wired ports in tunnel mode. These users also appear in the **User Session** report.
7. Locate the **Mesh Links** area on the **APs/Devices > Monitor** page. The **Mesh Links** section displays detailed information about all of the mesh links on the device.
8. Locate the **View in Google Earth** area on the **APs/Devices > Monitor** page. This section is only present for APs with latitude and longitude data configured on the **APs/Devices > Manage** page.
If you have at least version 4.0 of Google Earth installed, clicking this button opens Google Earth and displays the location of the AP. Google Earth also displays mesh and bridge links.
9. The **QuickView** tool allows users at lower levels of administrative permissions (such as helpdesk staff) a window into OV3600's **VisualRF** tool. By clicking the location map on the **APs/Devices > Monitor** page you can see the heatmap for a device.
10. **QuickView** runs faster than **VisualRF** because it has fewer features. It is geared toward resolving issues with single clients or single access points.

[Table 122](#) further describes the fields of this **QuickView** page.

Table 122 QuickView

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 the day and time when the link was initiated.
Duration	Displays the length of time the two APs have been linked.
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.

11. Locate the **Recent Events** area on the **APs/Devices > Monitor** page. The **Recent Events** area lists the most recent events specific to the AP. This information also appears on the **System > Events Log** page. [Table 123](#) describes the fields in this page display.

Table 123 APs/Devices > Monitor, Recent Events

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.

12. Locate the **Recent Events** area on the **APs/Devices > Monitor** page. The **Audit Log** area lists the most recent changes made to the AP. [Table 124](#) describes the components of this display.

Table 124 APs/Devices > Monitor, Recent Events

Field	Description
Time	Displays the day and time the event was recorded.
User	Displays the user that triggered the event. Configuration changes will be logged as the OV3600 user that submitted them. Automated OV3600 events are logged as the System user.
Event	Displays a text description of the change made to the device. Please contact Alcatel-Lucent Enterprise Support at support@ind.alcatel.com for detailed explanation of any events logged.

Introduction

OV3600 6.2 supports wide security standards and functions within the wireless network, and the additional wired networks to which they connect. This chapter describes the security systems supported, security configurations, and the OV3600 GUI by which security is deployed and monitored. This chapter presumes that group-level and device-level configurations are deployed and operational on the network, as described in earlier chapters of this document.

This chapter contains the following sections:

- [Deploying RAPIDS in OV3600 6.2](#)
 - [RAPIDS Overview](#)
- [Monitoring Rogue AP Devices with RAPIDS > Rogue APs Pages](#)
- [Using the RAPIDS > Setup Page](#)
 - [Using the Basic Configuration Section](#)
 - [Using the Classification Options Section](#)
 - [Using the Filtering Option Section](#)
 - [Using the Operating System Matches Section](#)
- [Using the RAPIDS Rogue Score Override](#)
- [Configuring and Deploying PCI Compliance in OV3600 6.2](#)
 - [Overview of PCI Compliance in OV3600 6.2](#)
 - [Enabling or Disabling PCI Compliance Monitoring](#)

For information and illustration of PCI Compliance and requirements on OV3600 Version 6.2, refer to “Configuring and Deploying PCI Compliance in OV3600 6.2” on page 183.

Deploying RAPIDS in OV3600 6.2

RAPIDS Overview

RAPIDS is an acronym that stands for the Rogue Access Point Detection System, a widely deployed security scheme within wireless and wired networks.

OV3600 provides the most comprehensive Rogue Access Point Detection System in the industry. OV3600 enables organizations to leverage their existing wired and wireless infrastructure without requiring separate rogue scanning devices.

RAPIDS discovers unauthorized devices in your WLAN network through a variety of methods:

- Over the Air
 - Using Enterprise APs (Alcatel-Lucent, Avaya, Cisco WLC, Colubris, Intel, Proxim, and Symbol)
 - Using OV3600 - Optional
- On the Wire
 - Using HTTP and SNMP Scanning
 - Interrogating Routers and Switches

Furthermore, RAPIDS integrates with external IDS systems, as follows:

- Cisco's WLSE (1100 and 1200 IOS)—OV3600 fetches rogue information from the HTTP interface and gets new AP information from SOAP API.
- AirMagnet Enterprise—AirMagnet Enterprise fetches a list of managed APs from OV3600.
- AirDefense—AirDefense uses the OV3600 XML API to keep its list of managed devices up to date.
- WildPackets OmniPeek—OmniPeek fetches a list of managed APs from OV3600.

The **RAPIDS > Overview** page provides a centralized view to all RAPIDS related services currently enabled on OV3600 plus pertinent statistics. [Figure 103](#) illustrates this page, and [Table 125](#) describes the fields and information displayed.

Figure 103 RAPIDS > Overview

RAPIDS™
ROGUE AP DETECTION MODULE

RAPIDS discovers unauthorized devices on your network in three ways: (1) wireline detection using HTTP and SNMP scans and interrogation of routers and switches to identify unknown APs and (2) wireless scanning via your existing authorized access points and (3) RF scans conducted by client devices with the AirWave Management Client utility.

If a device is **definitely** an unknown access point, it has a score of 5 or higher. If an unknown device cannot be positively identified as a wireless access point, RAPIDS assigns it a score (1-4) indicating the likelihood that it is a rogue AP.

Summary
IDS Events for devices in folder [Top](#) and subfolders | [Return to Home Overview](#)

Attack	Last 2 Hours	Last 24 Hours	Total
Deauth-Broadcast	0	0	262
Netstumbler Generic	30	100	1025
Null-Probe-Response	0	8	294
3 Attack Types	30	108	1581

Rogue Data
1037 rogue APs have been identified with a score of 5 or higher (definitely rogue).
0 devices have been identified with a score of 4 (very likely to be rogue).
9 devices have been identified with a score of 3 or lower.

System Information
6 groups have wireless scanning enabled.
0 wireline scans are scheduled. [Configure wireline scanning.](#)
0 WLSEs are being monitored.

[Download AirWave Management Client™.](#)
[View User Guide for the AirWave Management Client.](#)

Table 125 RAPIDS > Overview

Variable	Description
IDS Events	Displays a list of IDS events for the specified 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	<p>Displays and provides links to additional information for AP devices that have RAPIDS scores of various categories.</p> <ul style="list-style-type: none"> ● # Rogue APs—Displays the number of Access Points with RAPIDS scores. ● # of Devices identified with a score of 1—Describes any device on the network. ● # Devices identified with a score of 2—OUI belongs to a manufacturer that produces wireless (802.11) equipment. ● # Devices identified with a score of 3—The devices have been discovered on the wired network by querying the Bridge Forwarding Tables on routers and switches. A Score of 3 means the OUI matches a block contains APs from vendors in the Enterprise and SOHO market. ● # Devices identified with a score of 4—The devices have been discovered on the wired network by querying the Bridge Forwarding Tables on routers and switches. A Score of 4 means the OUI matches a block that belongs to a manufacturer which produces SOHO access points. ● # Devices identified with a score of 5—A score of five, for example, means the AP was discovered over the air or matches an OV3600 HTTP or SNMP Rogue fingerprint. OV3600 has a very high level of certainty that these devices are rogue. ● # Devices identified with a score of 6—Any device with a score of 6 or more is definitely an unknown access point. ● # Devices identified with a score of 7—A score of 7 indicates that these devices have been found on both the wired and the wireless networks.

Table 125 **RAPIDS > Overview** (Continued)

Variable	Description
System Information	<p># Groups Displays the number of Groups with wireless scanning enabled. This number is reflective of the full-time passive scanning supported by Proxim, Avaya, Colubris, and Symbol APs running 3.9.2. Groups > Radio, RAPIDS Scanning radio button</p> <p># Wireline Scans Displays the number of scheduled wireline scans. Use the Device Setup > Discovery page to configure and schedule HTTP scans.</p> <p># WLSE Displays WLSEs monitored by OV3600. WLSE provides RF statistics including Rogue scanning information for 1100 and 1200 IOS access points. Setup > WLSE</p>
Download	Download the Client application.
View User Guide	Displays the <i>Alcatel-Lucent OV3600 User Guide</i> .

Monitoring Rogue AP Devices with RAPIDS > Rogue APs Pages

The **RAPIDS > Rogue APs** page displays all rogue APs and all possible rogues. The device list is filtered by the minimum score selected in the drop-down menu. [Figure 104](#) and [Figure 105](#) illustrate this page in either basic or detailed view.

Classifying Rogue AP Devices in RAPIDS

OV3600 Version 6.2 introduces a new **Classification** column on the **Rogue APs** pages, and this is supported in the **Basic** and **Detail** view. This information is also supported in the **Rogue Devices** report. The **Classification** column allows rogue APs to be categorized and sorted by category.

RAPIDS can be configured so that the act of classifying rogues automatically acknowledges them. Refer to “Using the RAPIDS > Setup Page” on page 179 for this setting and other options related to this feature.

The classification is shared with Alcatel-Lucent OS devices that participate in WMS Offload configuration only in OV3600 Version 6.2, and is not pushed to devices. See “Deploying WMS Offload in OV3600” on page 54.

Using the RAPIDS > Rogue APs Pages

Perform the following steps using the following OV3600 pages to monitor rogue AP devices.

Figure 104 **RAPIDS > Rogue APs, Basic View (Split)**

Minimum Score: 7 - Rogue devices found on the wired network and on the wireless network

Modify Devices

1-9 of 9 Rogue Devices Page 1 of 1

Name	Classification	Ack	Score	Model	Operating System	IP Address	SSID	Network Type	Ch	WEP	RSST	Signal
Trapeze Ne-41:0D:80	Unclassified	No	7	-	unknown	10.51.1.37	Trapeze static wep	AP	1	Yes	-79	-20
Trapeze Ne-40:ED:80	Unclassified	No	7	-	unknown	10.51.1.14	Trapeze static wep	AP	11	Yes	-78	-20
Trapeze Ne-23:CE:00	Unclassified	No	7	-	unknown	10.51.1.4	Trapeze WPA2 EAP	AP	11	Yes	-83	-20
CABLETRON-50:4C:C4	Unclassified	No	7	-	-	-	Wireless Network	AP	8	No	-56	-8
3Com Access Point	Unclassified	No	7	3COM AP7250	unknown	10.51.1.21	3com	AP	1	No	-64	-21
Nortel-82:13:00	Unclassified	No	7	-	unknown	10.51.1.67	Trapeze MXR-2 wpa psk	AP	11	Yes	-58	-20
Enterasys-65:76:96	Unclassified	No	7	-	-	-	radius	AP	9	Yes	-76	-26
Nortel-83:C0:40	Unclassified	No	7	-	unknown	10.51.1.36	Trapeze 8021x WEP	AP	48	Yes	-82	-24
Aruba Netw-C1:AF:17	Unclassified	No	7	-	unknown	10.51.3.240	-	AP	153	-	0	-52

LAN MAC Address	LAN Vendor	Radio MAC Address	Radio Vendor	Last Discovering AP	Switch/Router	Port	Last Seen
00:0B:0E:41:0D:80	Trapeze Networks	00:0B:0E:41:0D:8A	Trapeze Networks	HQZ-1130-West	NOC-SWITCH-24-2-RK1-RW5	-	12/10/2008 5:02 PM
00:0B:0E:40:ED:80	Trapeze Networks	00:0B:0E:40:ED:8A	Trapeze Networks	HQZ-1130-Boardroom	NOC-SWITCH-24-2-RK1-RW5	-	12/10/2008 5:02 PM
00:0B:0E:23:CE:00	Trapeze Networks	00:0B:0E:23:CE:06	Trapeze Networks	HQZ-1130-Boardroom	NOC-SWITCH-24-2-RK1-RW5	-	12/10/2008 5:02 PM
00:E0:63:50:4C:C4	CABLETRON - YAGO SYSTEMS, INC.	00:E0:63:50:4C:C4	CABLETRON - YAGO SYSTEMS, INC.	HQZ-1130-South	NOC-SWITCH-48-1-RK1-RW3	Fa0/47	12/10/2008 5:02 PM
00:00:54:A7:A2:80	3Com Ltd	00:00:54:A7:A2:80	3Com Ltd	HQZ-1130-Boardroom	NOC-SWITCH-24-2-RK1-RW5	49	12/10/2008 5:02 PM
00:18:80:82:13:00	Nortel	00:18:80:82:13:08	Nortel	HQZ-1130-South	NOC-SWITCH-24-2-RK1-RW5	-	12/10/2008 5:02 PM
00:01:F4:65:76:96	Enterasys Networks	00:01:F4:65:76:94	Enterasys Networks	HQZ-1130-West	-	49	12/10/2008 5:02 PM
00:18:80:83:C0:40	Nortel	00:18:80:83:C0:41	Nortel	HQZ-1130-Boardroom	NOC-SWITCH-24-2-RK1-RW5	-	12/10/2008 11:16 AM
00:0B:86:C1:AF:17	Aruba Networks	00:0B:86:C1:AF:17	Aruba Networks	AP-3	NOC-SWITCH-24-2-RK1-RW5	-	12/9/2008 2:24 AM

View Ignored Rogues

Click a device name to launch the **Rogue Detail** page, which provides additional Rogue device information as well as a historical view of all RAPIDS components that have discovered the device.

- 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 AP that they can also see. For additional information in this case, refer to “[Creating OV3600 User Roles](#)” on page 42.
- Discovery events from APs that are not visible to the user are not clickable links, but they still appear on the detail pages.

Figure 105 *RAPIDS > Rogue APs, Detail View*

RSSI	Signal	Channel	SSID	WEP	Network Type	Classification	Switch/Router	Port	IP Address	Time	Discovery Method	Discovery Agent
-	-	-	-	-	AP	Unclassified	NOC-SWITCH-24-2-RK1-RW5	-	10.51.3.240	12/9/2008 2:24 AM	Switch/Router ARP Table Data	-
-77	-	153	-	-	AP	Unclassified	-	-	-	12/8/2008 11:29 PM	Wireless AP scan	AP-1
0	-	153	-	-	AP	Unclassified	-	-	-	12/8/2008 11:29 PM	Wireless AP scan	AP-3
-71	-	0	-	-	AP	Unclassified	-	-	-	12/1/2008 7:09 PM	Wireless AP scan	AP-5
0	-	0	-	-	AP	Unclassified	-	-	-	12/1/2008 7:09 PM	Wireless AP scan	AP-2

- 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. By using these fields and the multiple discovery agents, you can triangulate where the Rogue device is located in physical space and virtually located on the network. If you find the Rogue belongs to a neighboring business, you can migrate it into an **ignored** state. Otherwise, it is highly desirable to extract the device from your building and delete the Rogue device from the system.
- You can also use the global filtering options on the **RAPIDS > Setup** page to filter rogue devices according to signal strength, ad-hoc status, and SSID.
- You can use this page to acknowledge rogue devices that should be reconfigured to be legitimate clients.
- The suggested workflow for RAPIDS is as follows:
 - First, tackle devices ranked as **7**, meaning they are connected to your wired network.
 - Select all with an IP and OS fingerprint and navigate to the device detail page for remaining devices. Click **Modify Devices**, then select all devices that have an IP address. Then click **Identify OS**. OV3600 then performs a port scan on the device and attempts to determine the operating system. OV3600 can be configured to ignore certain operating systems that are known not to run on rogue devices. Refer to the “[Using the RAPIDS > Setup Page](#)” on page 179 section for additional information. You should investigate devices running an embedded Linux OS. 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 mark the device as **ignored** to eliminate future alerts.

Table 126 describes variables in the **RAPIDS > Rogue APs (Detail)** page.



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.

Table 126 RAPIDS > Rogue APs (Detail)

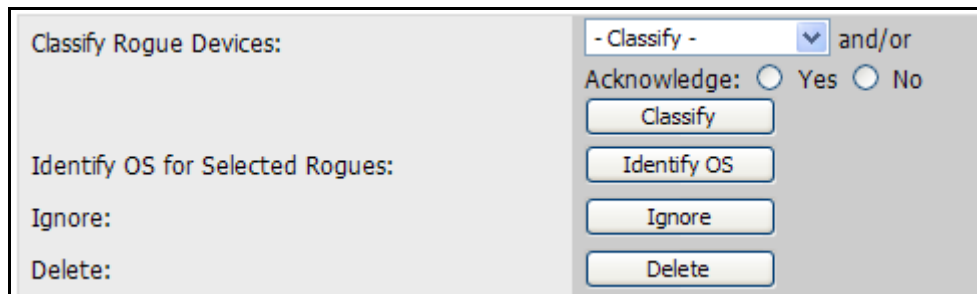
Variable	Description
Name	User configurable name given to the rogue device.
Classification	<p>Introduced in OV3600 Version 6.2, the rogue classifications are as follows:</p> <ul style="list-style-type: none"> ● Rogue ● Neighbor ● Unmanaged ● Suspected Rogue ● Suspected Neighbor ● Unclassified <p>The default setting is configurable on the RAPIDS > Setup page. Refer to “Using the RAPIDS > Setup Page” on page 179 for additional information.</p>
Ack	Displays acknowledge Yes , acknowledge No , or all devices.
Score	An index of the likelihood of a device being a rogue AP. The higher the score the more likely the device is an access point plugged into your network.
Model	The model of the AP. Displayed if the AP is discovered using an http scan.
Operating System	Displays the best OV3600 estimation of the OS type of the rogue device based on a port scan performed by OV3600. OS detection helps weed out the false positives. It is rare for a rogue device to run Windows XP or Mac OS X.
IP Address	The IP address of the device. OV3600 is able to get IP addresses by polling ARP data from routers and switches.
SSID	The SSID of the rogue device. Displayed if the device is discovered via a wireless scan.
Network Type	The type of network used by the rogue AP, either AP, Ad-Hoc or unknown. Displayed when the device is discovered by a wireless scan or the OV3600 Management Client.
Channel	The channel used by the rogue device. Displayed only when the device is discovered by a wireless scan or the OV3600 Management Client.
WEP	The encryption status of the AP. If yes then the AP is secured with WEP encryption.
RSSI	Displays Received Signal Strength Indication (RSSI) designation, a measure of the power present in a received radio signal.
Signal	Displays signal strength.
LAN MAC Address	Displays the LAN MAC address of the device obtained from the bridge forwarding table of a router or switch.
Radio MAC Address	Displays the radio MAC address of the rogue. Displayed if the AP is discovered via Wireless AP scans or the OV3600 management client.
Radio Vendor	Displays the owner of the OUI block of the Radio's MAC address. Displayed if the device is discovered via Wireless AP scans or the OV3600 management client.
Last Discovering AP	Displays discovering APs. Rogues can be discovered via a wireless AP scan, switch/router bridge forwarding table data, the OV3600 Management client or wireline HTTP scan.
Switch/Router	Displays the switch or router associated with the rogue discovery.
Port	When known, displays the router or switch port on which the rogue was discovered.
Last Seen	Displays the date and time that the rogue device was last seen.

Modifying Rogue Devices with the RAPIDS > Rogue APs > Modify Devices Page

OV3600 Version 6.2 introduces the ability to modify rogue devices from the **RAPIDS > Rogue APs** page. Perform these steps.

1. Once rogues have been identified as needing configuration change, select the device to modify from the list on the **RAPIDS > Rogue APs**, page, then click the **Modify Devices** button. The **Classify Rogue Devices** dialog box displays, as shown in [Figure 106](#).

Figure 106 *Classify Rogue Devices*



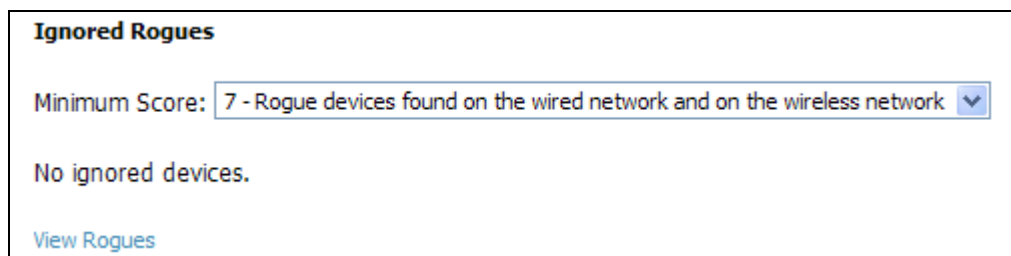
2. Provide a classification from the **Classify Rogue Devices** field. Options include the following:
 - **Suspected Rogue**
 - **Neighbor**
 - **Unclassified**
 - **Contained**
 - **Rogue**
 - **Suspected Neighbor**
 - **Valid**
3. Define whether the device should acknowledge its new classification.
4. Click the **Identify OS for Suspected Rogues** option to obtain operating system information, if available.
5. Click the **Ignore** button if the rogue device is to be ignored.
6. Click the **Delete** button if the rogue devices is to be removed from OV3600 processing.

Viewing Ignored Rogue Devices

OV3600 Version 6.2 introduces the ability to view ignored rogue devices from the **RAPIDS > Rogue APs** page. Ignored devices 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. The only way to display ignored rogue devices in OV3600 is to perform the following steps

1. From the **RAPIDS > Rogue APs** page, click **View Ignored Rogues**. The **Ignored Rogues** page appears, as illustrated in [Figure 107](#).

Figure 107 *Viewing Ignored Rogue Devices*



2. You can define the RAPIDS score by which rogue devices should appear. Once a classification that has rogue devices is chosen from the drop-down menu, a detailed table displays all known information.

Using the RAPIDS > Setup Page

The **RAPIDS > Setup** page allows for RAPIDS configuration on your wireless network. Perform the following steps to make use of this page, illustrated in [Figure 108](#).

Using the Basic Configuration Section

On the **RAPIDS > Setup** page, locate the **Basic Configuration** section. This section allows you to set RAPIDS performance settings. Refer to [Figure 108](#) for setting information and default values.

Figure 108 *RAPIDS > Setup*

The screenshot shows the configuration interface for RAPIDS. It is divided into three main sections:

- Basic Configuration:** Contains input fields for 'Discovery Event Cache Flush Period (10-600 sec):' (120), 'ARP IP Match Timeout (1-168 hours):' (24), 'Default RAPIDS Filter Level:' (7), 'Rogue MAC address correlation (0-8 bits):' (4), and 'Delete rogues not heard for (0-60 days, zero disables):' (14). A legend explains the filter levels from 1 to 7.
- Classification Options:** Includes 'Default Rogue Classification:' (Unclassified), 'Acknowledge Rogues by Default:' (No), and 'Classifying Rogues Automatically Acknowledges them:' (Yes).
- Filtering Options:** Includes 'Filter ad-hoc rogues:' (No), 'Filter rogues by signal strength:' (Yes), 'Minimum Signal Strength (Less than or equal to 0):' (-80), and 'SSID Filter Type:' (No Filter).
- Operating System Matches:** A table for selecting OS types to ignore.

Operating System	Ignore
<input type="checkbox"/> Mac OS	Yes
<input type="checkbox"/> Microsoft Windows	Yes
<input type="checkbox"/> Solaris	Yes

Table 127 *RAPIDS > Setup, Basic Configuration*

Field	Default	Description
Discovery Event Cache Flush Period	300	Sets the length of time OV3600 will cache discovery event information before dumping it to the database.
ARP IP Match Time (1-168 hours)	24	Defines the size of the time window in which RAPIDS will correlate MAC addresses and IPs.
Default RAPIDS filter level	7	Defines the minimum rogue score to display on the RAPIDS > Rogue APs page. Rogues below the minimum score will not be reflected in the Rogues count in the OV3600 header.
Rogue MAC address correlation	4	Display the correlation in which OV3600 assumes that MAC addresses of rogues can be correlated to the same number of bits, and that both belong to the same rogue.
Delete rogues not heard for (0 - 60 days)	14	Displays and defines rogues not heard on the network for more than a certain number of days. These are deleted automatically from OV3600. This setting cannot be larger than the Rogue Discovery Event expiration, which is configured on the OV3600 Setup page.

Using the Classification Options Section

On the **RAPIDS > Setup** page, locate the **Classification Options** section, introduced in OV3600 Version 6.2.

This section enables you to categorize and sort rogue AP devices in one of several categories. The classification defined in this section establishes the default classification for rogue devices on the **RAPIDS > Rogue APs** page. Furthermore, the rogue device classifications enabled in OV3600 Version 6.2 are supported for the Rogue devices report.

In OV3600 Version 6.2, changing the rogue classification within the OV3600 GUI pushes a rogue reclassification message to all controllers that are managed by the OV3600 server, and that are also in Groups with the **Offloading the WMS database** setting set to **Yes**.



This rogue classification is pushed only to Alcatel-Lucent WLAN Switches.

To reset the classification of a rogue device on OV3600, change the classification on the OV3600 GUI to **unclassified**.

Table 128 *RAPIDS > Rogue APs Page*

Field	Default	Description
Default Rogue Classification	Unclassified	Defines the default classification for rogue devices when discovered. This classification can be changed for any individual rogue device type in the RAPIDS > Rogue APs page. The classification default is assigned on this page, and the options are as follows: <ul style="list-style-type: none">• Rogue• Neighbor• Unmanaged• Suspected Rogue• Suspected Neighbor• Unclassified
Acknowledge Rogues by Default	No	This setting determines whether rogue AP devices are acknowledged by OV3600 upon discovery, as the default. As desired, individual device-level settings can be changed using the RAPIDS > Rogue APs page.
Classifying Rogues Automatically Acknowledges Them	Yes	Defines whether acknowledgement happens automatically whenever a rogue device receives classification.

Using the Filtering Option Section

On the **RAPIDS > Setup** page, locate the **Filtering Options** section. This section allows you to set global filtering preferences that can help to hone your list of rogues according to signal strength, ad-hoc status and SSID. Existing rogues that are filtered based on one or more of these settings will not be displayed in the rogue list or included in the rogue count in the OV3600 header. Newly discovered rogues that meet the criteria for filtering will not be added to OV3600 at all.

Table 129 *RAPIDS > Setup, Filtering Options Section*

Field	Default	Description
Filter ad-hoc rogues	No	Filter rogues according to ad-hoc status.
Filter rogues by signal strength	No	Filters rogues according to signal strength in dBm. Selecting yes will display a field for minimum signal strength. Rogues will not be recorded until they exceed the minimum signal strength. It is important to pay attention to the use of a negative value as minimum signal strength. For example, if -85 is entered as the minimum signal strength, a rogue with a value of -86 will be filtered, while a rogue with a score of -84 will be displayed.
Minimum Signal Strength	-80	Defines the signal strength that a rogue device must have to qualify for processing in OV3600.
Filter rogues with SSIDs in this list	No Filter	Filters rogues according to select SSIDs.

Using the Operating System Matches Section

On the **RAPIDS > Setup** page, locate the **Operating System Matches** section. This section allows you to specify the Operating Systems that are considered safe. If **Ignore** is set to **yes**, any rogue device that returns the specified operating system is automatically ignored.

1. To enter additional operating systems to ignore, click the **Add new OS Match** link.
2. Enter a substring to match. When **Yes** is selected, any rogue device with an OS that matches the substring is ignored. If **in** is entered into the **Operating System** field, any OS name containing **in** will be ignored including wINdows, lINux and macINTosh. The substring match is not case sensitive.
3. Alcatel-Lucent recommends using the most specific string possible. Ideally, cut and paste the **Operating System** field from the details page of any rogue devices that you wish to ignore.
4. Click **Add** to add the new OS Match.

Figure 109 *Adding an OS to Ignore in the RAPIDS > Setup, Operating System*

The screenshot shows a dialog box titled "Operating System Match". It has two main input areas: "Operating System:" with a text field, and "Ignore:" with radio buttons for "Yes" and "No". The "No" radio button is selected. At the bottom of the dialog are two buttons: "Add" and "Cancel".

Using the RAPIDS Rogue Score Override

The **RAPIDS > Score Override** page allows the user to override the score assigned to a MAC address prefix by Alcatel-Lucent. If you have devices that receives a higher score than it should, you can adjust the score.

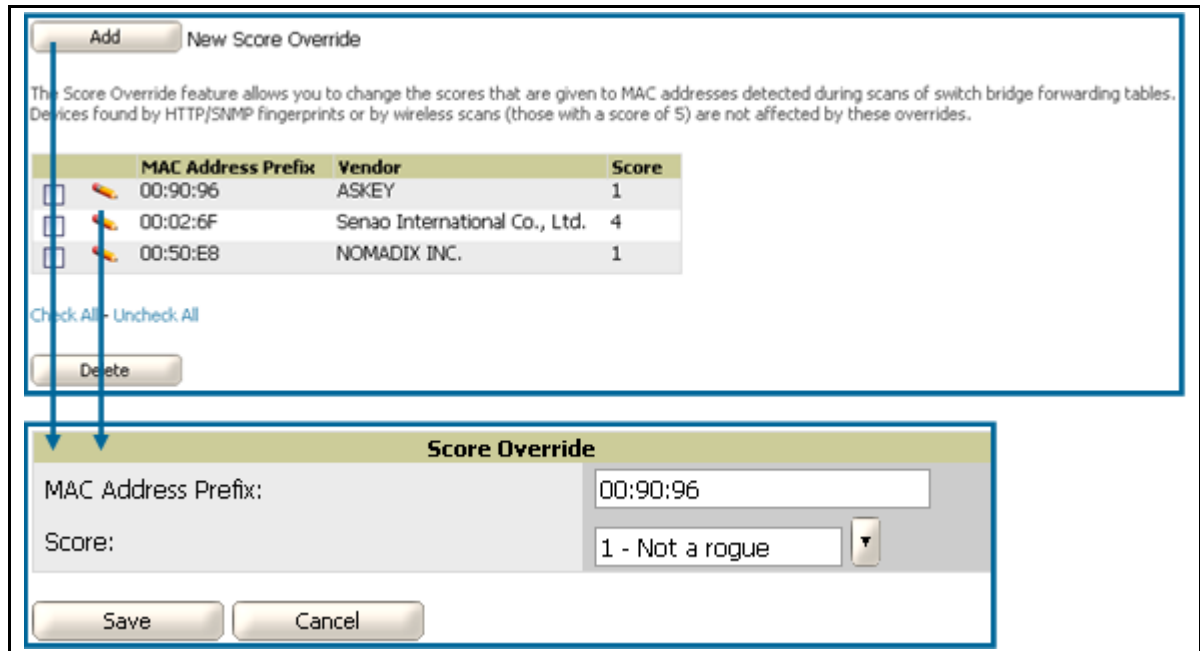
Once a new score is assigned, all devices with the specified MAC address prefix receive the new score.



Note that rescoring a MAC Address Prefix poses a security risk. The block has received its score for a reason. Any rogues that fall within this block receive the new score.

Figure 110 illustrates this page.

Figure 110 *RAPIDS > Rogue APs (Detail), Score Override*



Clicking the **Edit** or **Add** button opens the **Score Override** creation page. 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.

Configuring and Deploying PCI Compliance in OV3600 6.2

OV3600 Version 6.2 introduces support for PCI requirements, allowing you to monitor PCI compliance on the network. There are four primary pages in OV3600 Version 6.2 in which you establish, monitor, and access PCI Compliance:

- 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 Compliance Monitoring](#)” on page 185.
- The **Reports > Definitions** page allows you to create custom-configured and custom-scheduled PCI Compliance reports. See “[Reports > Definitions Page Overview](#)” on page 230.
- 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. “[Reports > Generated Page Overview](#)” on page 231.
- 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 Compliance Monitoring](#)” on page 185.

The Payment Card Industry (PCI) Data Security Standard (DSS) establishes multiple levels in which payment cardholder data is protected in a wireless network. OV3600 6.2 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

This section describes PCI compliance and functions as enabled by OV3600 6.2, with the following topics:

- [Overview of PCI Compliance in OV3600 6.2](#)
- [Enabling or Disabling PCI Compliance Monitoring](#)

Refer also to the following topic in a later chapter:

- “[PCI Compliance Report](#)” on page 257

Overview of PCI Compliance in OV3600 6.2

OV3600 6.2 supports the following PCI requirements, enabling you to display real-time PCI compliance data by several criteria. OV3600 features a report that tracks PCI compliance.

OV3600 grades the network as **pass** or **fail** for each requirement that is enabled.



When any PCI requirement is enabled on OV3600 6.2, then OV3600 grades the network as pass or fail for the respective PCI requirement. Whenever a PCI requirement is not enabled in OV3600 6.2, then OV3600 6.2 does not monitor the network's status in relation to that requirement, and cannot designate Pass or Fail network status.

Table 130 *PCI Requirements and Support in OV3600 6.2*

PCI Requirement	Description
1.1	<p>Monitoring configuration standards for network firewall devices</p> <p>When Enabled: PCI Requirement 1.1 establishes firewall and router configuration standards. A device fails Requirement 1.1 if it is in read-write management mode and there are mismatches between the desired configuration and the configuration on the device, for example.</p> <p>When Disabled: When this PCI requirement is disabled in OV3600 6.2, firewall router and device configurations are not checked for PCI compliance in firewall configuration, and Pass or Fail status is not reported nor monitored.</p>
1.2.3	<p>Monitoring firewall installation between any wireless networks and the cardholder data environment</p> <p>When Enabled: A device passes requirement 1.2.3 if it can function as a stateful firewall.</p> <p>When Disabled: When this PCI requirement is disabled in OV3600 6.2, firewall router and device installation are not checked for PCI compliance.</p>
2.1	<p>Monitoring the presence of vendor-supplied default security settings</p> <p>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 manufacturer default passwords, for example.</p> <p>When Disabled: When this PCI requirement is disabled in OV3600 6.2, device passwords and other manufacturer default settings are not checked for PCI compliance.</p>
2.1.1	<p>Changing vendor-supplied defaults for wireless environments</p> <p>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 6.2 establishes and tracks. The list includes common manufacturer default passwords. The user can input new values to achieve compliance.</p> <p>When Disabled: When this PCI requirement is disabled in OV3600 6.2, then network devices are not checked for forbidden information and PCI Compliance is not established.</p>

Table 130 PCI Requirements and Support in OV3600 6.2

PCI Requirement	Description
4.1.1	<p>Using strong encryption in wireless networks</p> <p>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.</p> <p>When Disabled: When this PCI monitoring function is disabled in OV3600 6.2, then OV3600 6.2 cannot establish a pass or fail status with regard to PCI encryption requirements on the network.</p>
11.1	<p>Identifying unauthorized wireless devices</p> <p>When Enabled: A report will indicate a failure if there are unacknowledged rogue APs present in RAPIDS or there are no wireless rogues discovered in the past three months.</p> <p>When Disabled: When this PCI requirement is disabled in OV3600 6.2, the data and device configurations are not monitored nor reported in real-time or generated data.</p>
11.4	<p>Using intrusion-detection or intrusion-prevention systems to monitor all traffic</p> <p>Enabled: OV3600 reports pass or fail status when monitoring devices capable of reporting IDS events. Recent IDS events are be summarized in the PCI Compliance report or the IDS Report.</p> <p>Disabled: When this function is disabled in OV3600 6.2, 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.</p>

Refer to the following topics in this document for additional information:

- [“Enabling or Disabling PCI Compliance Monitoring” on page 185](#)
- [“Overview of OV3600 6.2 Reports” on page 229](#)

Enabling or Disabling PCI Compliance Monitoring

Perform these steps to verify status and to enable or disable OV3600 6.2 support for PCI 1.2 requirements. enabling one or all PCI Compliance standards on OV3600 6.2 enables real-time information and generated reports that advise on Pass or Fail status. The PCI compliance monitoring supported in OV3600 6.2 is reported in Table 130

1. To determine what PCI Compliance standards are enabled or disabled on OV3600 6.2, navigate to the **OV3600 Setup > PCI Compliance** page.
2. To enable, disable, or edit any category of PCI Compliance monitoring in OV3600 6.2, 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 to enforce PCI requirements in OV3600 6.2. [Figure 111](#) illustrates one example.

Figure 111 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 Compliance on the network, use generated or daily reports. See [“Creating, Running, and Emailing Reports”](#) on page 229. In addition, you can view the real-time PCI Compliance 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 for that specific device. [Figure 112](#) illustrates one example.

Figure 112 Example of **APs/Devices > Compliance**

00:0b:86:00:0b:86 in group Acme Corporation in folder Top > HQ
 This Device is in monitor-only-with-firmware-upgrades mode.

PCI Compliance

PCI Requirement ▲	Description	Status	Detail
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.	Unable to Determine	Device is currently down or was never contacted.
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.	N/A	
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.	Fail	SSID 'employee' for Group 'Acme Corporation' is configured with Encryption Mode 'No Encryption'.
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	Device has intrusion detection/prevention systems.

Introduction

This chapter describes some of the most important and commonly-used pages in OV3600 6.2, and additional tools not described in earlier chapters. This chapter contains the following sections.

Users Pages

- Using the OV3600 Users Page
 - Overview of the Users Page
 - Using the Users > Connected Page
 - Using the Users > Detail and Users > Diagnostics Pages
 - Using the Users > Tags Page
 - Using the Users > Guest Users Page

Home Pages

- Using the Home Pages
 - Using the Home > Overview Page
 - Searching OV3600 with the Home > Search Page
 - Using the Home > Documentation Page
 - Using the Home > User Info Page

System Pages

- Using System Pages
 - Using the System > Status Page
 - Using the System > Configuration Change Jobs Page
 - Using the System > Event Logs Page
 - Using the System > Performance Page

Triggers and Alerts

- Using Triggers and Alerts
 - Overview of Triggers and Alerts
 - Viewing Triggers\
 - Creating New Triggers
 - Viewing Alerts

Backups

- Performing Backups with OV3600
 - Overview of Backups
 - Viewing and Downloading Backups
 - Running Backup on Demand
 - Restoring from a Backup
 - OV3600 Failover
 - Adding Watched OV3600 Stations

Master Console

- Using the Master Console

Using the OV3600 Users Page

Overview of the Users Page

The **Users** page allows administrators to view user data. The data on the **Users** page comes from a number of locations, including data tables on the access points, information from RADIUS accounting servers, and OV3600-generated data.

The **Users** section of OV3600 6.2 contains the following pages:

- **Users > Connected**—Displays all users currently connected in OV3600 6.2, to include enhanced information introduced in OV3600 6.2. See “[Using the Users > Connected Page](#)” on page 188.
- **Users > All**—Displays all users of which OV3600 6.2 is aware, with related information. Non-active users are listed in gray text. “[Using the Users > Detail and Users > Diagnostics Pages](#)” on page 191.
- **Users > Guest Users**—Displays all guest users in OV3600 6.2. See “[Using the Users > Guest Users Page](#)” on page 193.
- **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. “[Using the Users > Tags Page](#)” on page 195.

Using the Users > Connected Page

The **Users > Connected** page displays all users currently connected in OV3600 6.2, and is illustrated in [Figure 113](#) and described in [Table 131](#). 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 Version 6.2 enhances the **Users > Connection** page to include SSID information for users. This enhancement applies to additional graph-based pages in OV3600 6.2. Furthermore, the **Users > Connected** page can display wired users.



Data that was gathered prior to an upgrade to Version 6.2 will be reported under an unknown SSID.

Figure 113 Users > Connected

Folder: Top (0/171 Users) > HQ (170/171) Expand folders to show all Users Go to folder: HQ (170/171)

Total Devices: 55 Mismatched: 1 Users: 170 Avg/Device: 3.09 Bandwidth: 5881 kbps

Users for folder HQ Last 2 hours

160
120
80
40
0

10:15 11:15 12:15

Show All Maximum Average

Max Users: 171 users 152 users

Bandwidth for folder HQ Last 2 hours

14 M
8 M
4 M
0 M
-4 M
-8 M
-12 M
-16 M

10:15 11:15 12:15

Show All Maximum Average

Avg Bits Per Second In: 14.9 Mbps 3.7 Mbps

Avg Bits Per Second Out: 15.2 Mbps 4.1 Mbps

1 year ago now

10 records per page of 173 Users Page 1 of 18 >>

Username	Role	MAC Address	AP/Device	Group	SSID	VLAN	AP Radio	Connection Mode	Ch BW	Association Time
zoca	employee	00:1C:B3:00:1C:B3	AL21	Acme Corporation	ethere-wpa2	65	802.11an	802.11n (5GHz)	HT40	1/23/2009 12:43 PM
NETWORKS\jobs	employee	00:1D:D9:00:1D:D9	AL21	Acme Corporation	ethere-wpa2	65	802.11an	802.11a	-	1/23/2009 12:43 PM
NETWORKS\stell	employee	00:1C:B3:00:1C:B3	AL40	Acme Corporation	ethere-wpa2	65	802.11an	802.11n (5GHz)	HT40	1/23/2009 12:43 PM
cobs	employee	00:1D:D9:00:1D:D9	AL19	Acme Corporation	ethere-voip	66	802.11bgn	802.11g	-	1/23/2009 12:43 PM
md	employee	00:1C:B3:00:1C:B3	AL7	Acme Corporation	ethere-voip	66	802.11bgn	802.11g	-	1/23/2009 12:43 PM
417	visitor	00:1D:D9:00:1D:D9	AL31	Acme Corporation	guest	63	802.11bgn	802.11b	-	1/23/2009 12:43 PM
NETWORKS\ple	employee	00:1C:B3:00:1C:B3	AL16	Acme Corporation	ethere-wpa2	65	802.11an	802.11a	-	1/23/2009 12:43 PM
mel@networks.com	employee	00:1D:D9:00:1D:D9	Fish40	Acme Corporation	ethere-voip	66	802.11bgn	802.11g	-	1/23/2009 12:37 PM
gy	employee	00:1C:B3:00:1C:B3	Fish40	Acme Corporation	ethere-wpa2	65	802.11an	802.11a	-	1/23/2009 12:31 PM
Pe-ext51	vocera	00:1D:D9:00:1D:D9	AL5	Acme Corporation	ethere-voc	66	802.11bgn	802.11g	-	1/23/2009 12:31 PM

Duration	Auth. Type	Cipher	Auth. Time	Sig. Qual.	BW	LAN IP Address	LAN Hostname	Guest User	VPN IP Address	VPN Hostname
0 mins	Authenticated by AP	-	0 mins	10	-	10.6.10.68	-	No	-	-
0 mins	Authenticated by AP	-	0 mins	37	-	10.6.6.20	-	No	-	-
0 mins	Authenticated by AP	-	0 mins	25	1 kbps	10.6.10.68	-	No	-	-
0 mins	Authenticated by AP	-	0 mins	43	-	10.6.6.20	-	No	-	-
0 mins	Authenticated by AP	-	0 mins	-	-	10.6.10.68	-	No	-	-
0 mins	Authenticated by AP (PAP)	-	0 mins	-	-	10.6.6.20	-	No	-	-
0 mins	Authenticated by AP	-	0 mins	29	7 kbps	10.6.10.68	sonid.networks.com	No	-	-
6 mins	EAP	-	6 mins	53	-	10.6.6.20	-	No	-	-
12 mins	EAP	-	12 mins	46	45 kbps	10.6.10.68	-	No	-	-
12 mins	Not Authenticated	-	-0 mins	29	0 kbps	10.6.6.20	-	No	-	-

Alert Summary at 1/23/2009 12:26 PM

Type	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	6	15	1/23/2009 9:57 AM
Incidents	0	0	8	1/12/2009 12:00 PM
RADIUS Authentication Issues	11	1808	22255	1/23/2009 12:07 PM

Folder Lab Users 1

Add New Folder

Table 131 Users > Connected

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.
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 131 Users > Connected (Continued)

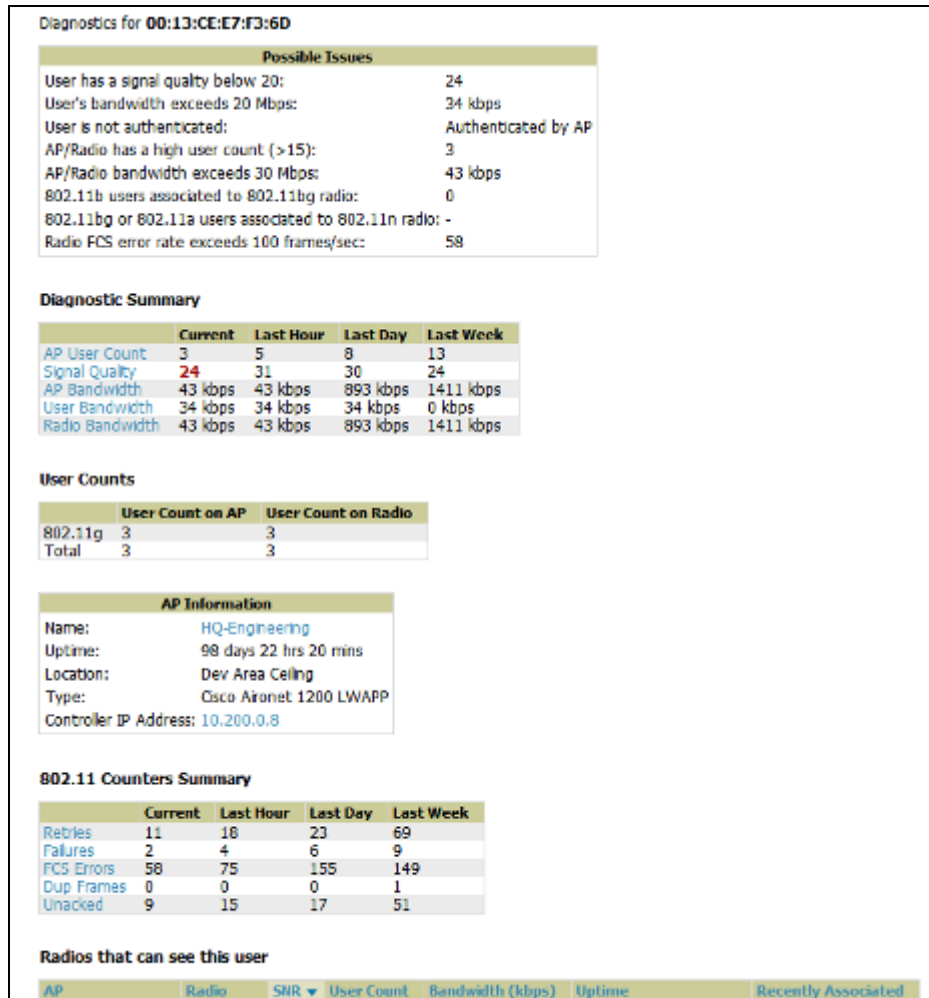
Field	Description
Ch BW	Displays the channel bandwidth that currently supports the user.
User Radio Mode	Displays the Radio mode used by the user to associate to the AP. It will display 802.11a/b/g/bg. 802.11bg is reported when the AP does not provide OV3600 with enough information to determine the exact 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. <ul style="list-style-type: none"> • 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: WEP with 802.11x, WPA PSK (TKIP), WPA with 802.11x, WPA2 PSK (AES), or 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.

Using the Users > Detail and Users > Diagnostics Pages

The **QuickView** tool allows users at lower levels of administrative permissions (such as helpdesk staff) a window into OV3600's **VisualRF** tool. By clicking on the location map on the **User > Detail** page, you can see the location history for a user.

OV3600 enables you to display the **Diagnostics** page for each user. The **Diagnostics** page summarizes data for each user that can help to troubleshoot connectivity problems for the user on your network. [Figure 114](#) illustrates this page.

Figure 114 Users > Diagnostics



Perform these steps to use the **Diagnostics** page:

1. Navigate to the **Diagnostics** section of the **Users > Diagnostics** page. This page displays common issues for wireless users in the left column, and the actual data for the user on your network is displayed on the right.

Values on this page are highlighted in red if they increase or drop by more than ten percent. [Table 132](#) describes the fields of this page section.

Table 132 Users > Diagnostics, Diagnostics

Field	Description
User has a signal quality below 20	A measure of the quality of signal the user enjoyed.
User's bandwidth exceeds 20 Mbps	As reported by the device's bandwidth counters.
User is not authenticated	User authentication protocols are defined in the device's group.
AP/Radio has a user count of over 15	As reported by the device.
AP/Radio bandwidth exceeds 30 Mbps	As reported by the device's bandwidth counters.
802.11b users associated to 802.11 bg radio	As reported in the device's radio data.
802.11 bg or 802.11a radio users associated to n radio	As reported in the device's radio data.
Radio FCS error rate exceeds 100 frames/sec	This value is incremented when a Frame Check Sequence error is detected; it refers to additional checksum characters added when sending data to determine whether any data was lost in transit.

- Navigate to the **Diagnostic Summary** section of the **Users > Diagnostics** page. These sections summarize the user diagnostics data that has been collected currently and in the last hour, last day, and last week. Values are displayed in red when the data exceeds or misses the threshold defined in the **Possible Issues** box. Such instances would include when signal quality is below 20, or when more than 15 users are associated to an AP or radio.

 - Clicking the **blue** link for any row in the table displays the information in graphical form.
 - Users per radio are displayed in the **User Counts** field. This field shows current data per radio and AP for the device to which the user is associated. Data is broken down by type (such as 802.11a).
 - Basic information about the AP to which the users is associated is displayed in the **AP Information** box. This includes name, uptime, location, type and controller IP address (for thin APs).
 - The **802.11 Counters Summary** displays issues for the AP to which the user is associated. The summary of incidents is displayed according to incidents that are current and one hour, one day, and one week old. These counter summaries can offer insight into interference and coverage for the access point. The error counts will be driven up on networks with a lot of activity, but identifying an unexpected spike in the counters can help to troubleshoot new problems.
 - The **Radios That Can See This User** box shows radios on other access points that have reported the user, as well as basic information about those devices, such as uptime and user count. If the user has recently been associated to one of these radios, the **Recently Associated** column shows **Yes**. Clicking the **blue** link for any device in the table takes you to that AP's monitoring page.

Using the Users > Guest Users Page

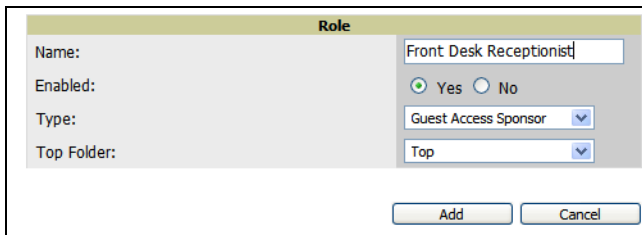
Overview of the Users > Guest Users Page

OV3600 supports guest user provisioning for Alcatel-Lucent and Cisco WLC devices. This allows frontline staff, such as receptionists or help desk technicians, to grant wireless access to visitors or other temporary personnel.

The first step in creating a guest access user is to define a role for the OV3600 users who will be responsible for this task, if those users are to have a role other than Admin. Perform the following steps in the pages described to configure these settings.

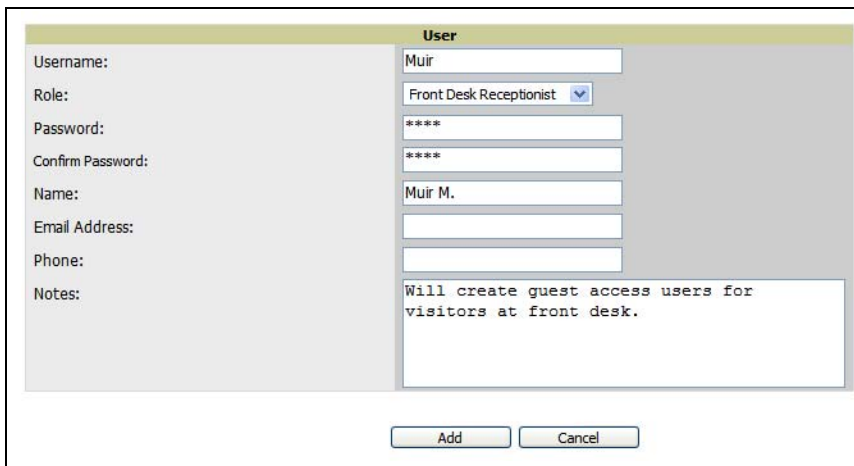
1. Navigate to the **Setup > Roles** page and create a new role of type **Guest Access Sponsor**. [Figure 115](#) illustrates this page.

Figure 115 Setup > Roles



2. Next, navigate to the **Setup > Users** page and create a new user with the role that was just created for **Guest Access Sponsors**. [Figure 116](#) illustrates this page.

Figure 116 Setup > Users



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, new guest users can be added or existing guest users can be edited. There is also a list of all guest users that shows data including the expiration date, the SSID (for Cisco WLC) and other information. [Figure 117](#) illustrates this page and [Table 133](#) describes the fields and information displayed.

Figure 117 Users > Guest Users

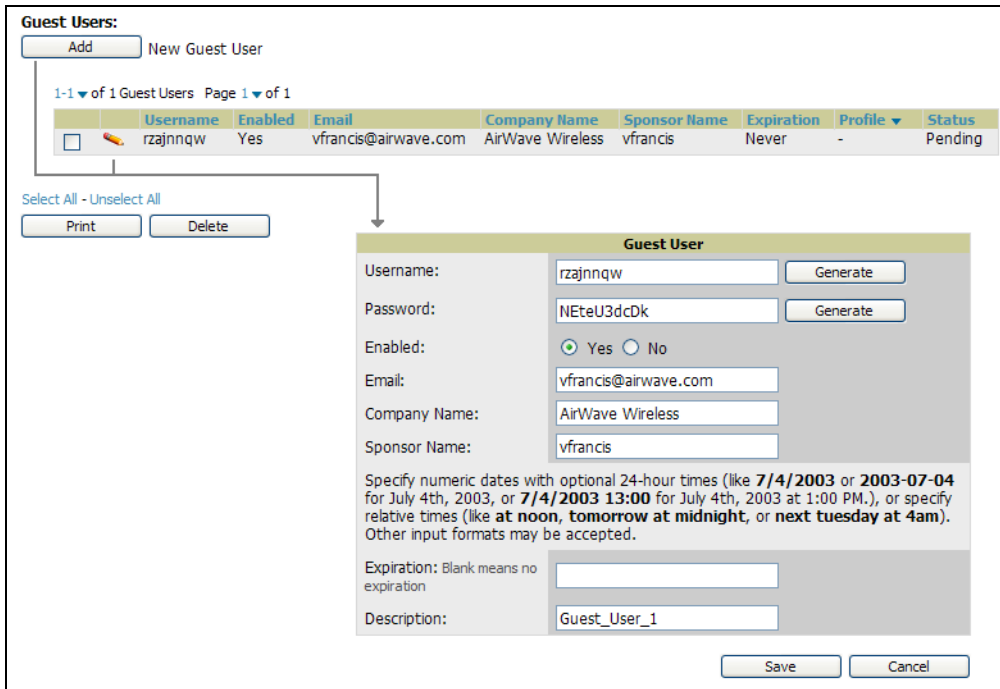


Table 133 Users > Guest Users

Field	Description
Repair Guest User Errors button	OV3600 attempts to push the guest user again in an attempt to repair any errors in the Status column.
Add New Guest Users button	Add a new guest user to a controller via OV3600.
Username	Randomly generated on the guest user detail page.
Enabled	Status of guest user as active (enabled) or expired (disabled); configured on the guest user edit page.
Email	Optional, configured on the guest user edit page.
Company Name	Optional, configured on the guest user edit page.
Sponsor Name	Optional, configured on the guest user edit page.
Expiration	The date the guest user's access will expire; configured on the guest user add page.
Profile/SSID	Applies to Cisco WLC only; the SSID the guest user can access.
Status	Reported by the controller; attempt to repair error messages with the repair 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 will appear on the same list as other wireless users, but will be identified as guest users in the **SSID** column. The **User Detail** page for a guest user also contain a box with the same guest information that appears for each user on the **Users > Guest Users** list.

Using the Users > Tags Page

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 is monitored by OV3600. OV3600 displays the information it receives from the controller in a table on this page. [Figure 118](#) illustrates this page, and [Table 134](#) describes fields and information displayed.

Figure 118 *Users > Tags*

Name	MAC Address	Vendor	Battery Level	Chirp Interval	Last Seen	Closest AP
CD-Burner	00:14:7E:00:14:7E	PanGo Networks, Inc.	Normal	2 mins	1/23/2009 1:19 PM	HQ-Engineering
-	00:14:7E:00:14:7E	InnerWireless	Normal	4 mins	1/23/2009 6:44 AM	-
Water-Cooler	00:14:7E:00:14:7E	Aeroscout Ltd.	-	12 secs	1/22/2009 5:35 AM	-
-	00:14:7E:00:14:7E	InnerWireless	Normal	1 min	1/20/2009 4:13 PM	-
-	00:14:7E:00:14:7E	Aeroscout Ltd.	-	45 secs	1/20/2009 4:02 PM	-

Table 134 *Users > Tags*

Field	Description
Name	Displays the user-editable name associated with the tag.
MAC Address	Displays the MAC address of the AP that reported the tag.
Vendor	Displays the vendor of the tag (Aeroscout, PanGo and Newbury)—display all or filter by type.
Battery Level	Displays battery information—filterable in drop-down menu at the top of the column; is not displayed for Aeroscout tags.
Chirp Interval	Filterable in drop-down menu at the top of the column.
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's 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 [“Using Triggers and Alerts” on page 207](#).

Using the Home Pages

Overview of the Home Pages

There are five pages accessed 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 “Using the Home > Overview Page” on page 196.
- The **Home > Search** page provides a simple way to find users and managed devices. OV3600 Version 6.2 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 199.
- The **Home > Documentation** page provides easy access to all relevant OV3600 documentation. Refer to “Using the Home > Documentation Page” on page 201.
- 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. Refer to “Using the Home > User Info Page” on page 201.

Using the Home > Overview Page

Navigate to **Home > Overview** page with the standard OV3600 6.2 menus. Figure 119 illustrates this page, and Table 135 describes the contents.

Figure 119 Home > Overview

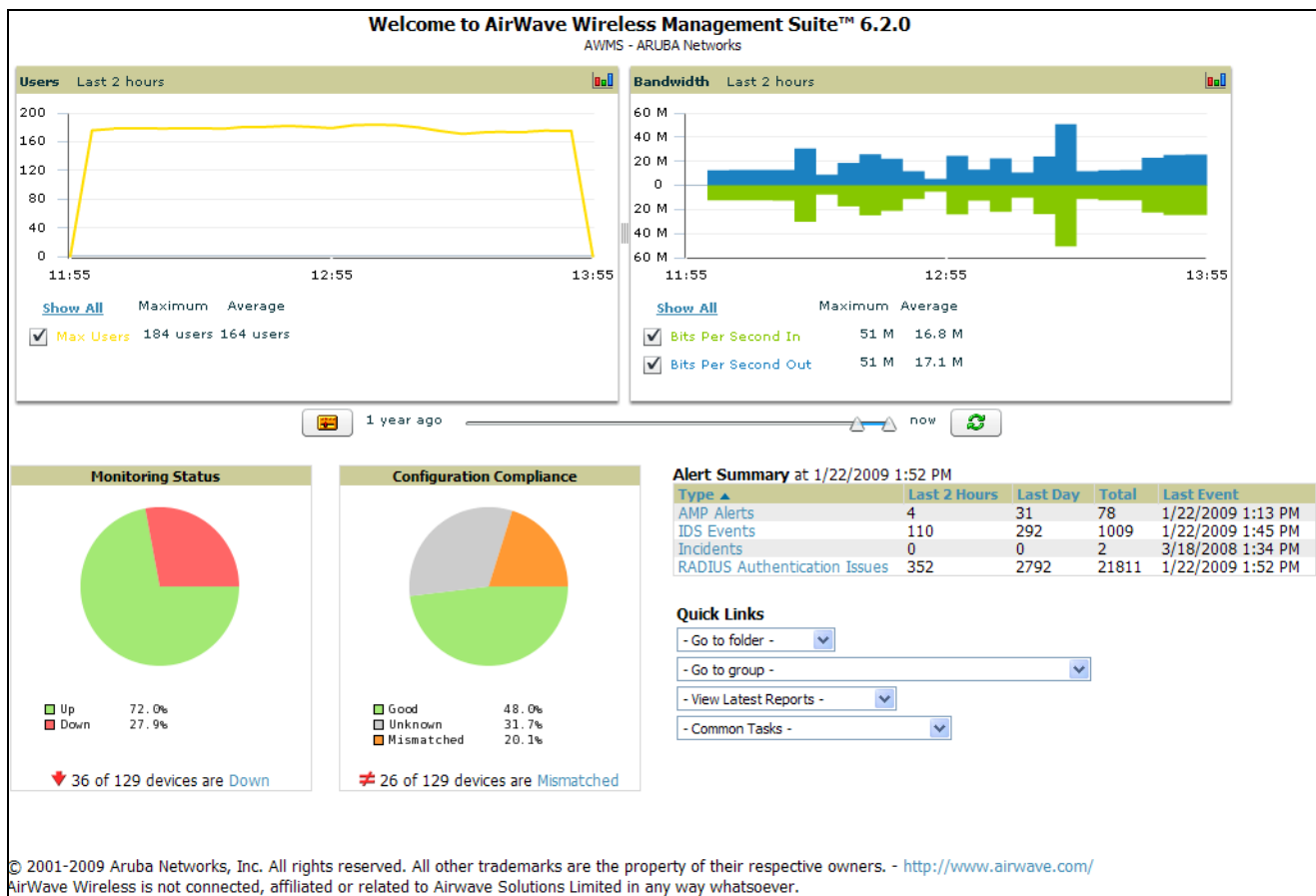


Table 135 *Home > Overview Sections and Descriptions*

Section	Description
Users	<p>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.</p> <p>Click Show All to display a complete list of users.</p> <p>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.</p>
Bandwidth	<p>The Bandwidth section displays bandwidth data, and this display can be adjusted.</p> <p>To remove bandwidth in or out from the graphical display, clear the check box for In or Out.</p> <p>To display details for specific devices, click Show All and select the devices to be included in the graphical bandwidth summary chart.</p>
Monitoring Status	<p>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.</p> <p>To review devices that are down, click Down, and the APs/Devices > Down page displays.</p>
Configuration Compliance	<p>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.</p>
Alert Summary	<p>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).</p> <p>Click any alert type, and the Alert Summary page appears for that alert type, enabling further analysis and investigation.</p>
Quick Links	<p>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 6.2, as follows:</p> <ul style="list-style-type: none"> ● Go to folder—This menu lists all folders defined in OV3600 6.2 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 165. ● Go to group—This menu lists all groups defined in OV3600 6.2, 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 Groups in OV3600” on page 65. ● View latest reports—OV3600 6.2 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. This list duplicates the one-click reports listed at the bottom of the Reports > Generated page. See “Creating, Running, and Emailing Reports” on page 229. ● Common tasks—This menu provides an inventory of and quick links to the most heavily used task-oriented pages in OV3600 6.2, to include the following: <ul style="list-style-type: none"> ■ Configure Alert Thesholds—This link takes you to the System > Triggers page. See “Using Triggers and Alerts” on page 207. ■ Configure Default Credentials—This link takes you to the Device Setup > Communication page. See “Configuring Communication Settings for Discovered Devices” on page 57. ■ Discover New Devices on Your Network—This link takes you to the Device Setup > Discover page. See “Discovering and Managing Devices” on page 141. ■ Supported Devices and Features—This link launches and displays a PDF file that summarizes all supported devices and features in chart format for OV3600 6.2. Adobe Reader is required. ■ Upload Device Firmware—This link launches and displays the Device Setup > Upload Files page. ■ View Event Log—

Using the Home > License Page

Navigate to the Home > License page using the standard OV3600 menu. [Figure 120](#) illustrates this page, and [Table 136](#) describes the contents.

Figure 120 Home > License

System Overview

Days Remaining: 96

System Name:	OV3600	Time:	1/22/2009 1:39 PM
Organization:	Alcatel-Lucent	Uptime:	2 days 1 hr 2 mins
Hostname:	host.Alcatel-Lucent.com	Version:	6.2.0
IP Address:	10.10.15.10	OS:	CentOS release 5

Refer to your license agreement for complete information about the terms of this license.

Enter New License:

```

--- Begin License Key ---
Product: Evaluation
Organization: Networks
Expires: 1240931212
Expires_on: Tue Apr 28 15:06:52 2009 UTC
RAPIDS: Yes
VisualRF: Yes
Helpdesk: Yes
Generated: Mon Apr 28 15:06:52 2008 UTC by LzKmgKn24YOM4bxryRpLA
--- Signature ---
iD8DBQFI FegMvN8PdJTKS2ERA13mAj4rWTfw2VAf12GUpD1OuNYhOBU6pACeM/ew
jCdUQz9wwZE52JxctZgEHUs=
=704T
    
```

Table 136 Home > License

Field	Description
System Name	Displays a user-definable name for OV3600 (maximum 20 characters).
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.
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.
Latest Reports	Provides quick links to the most recently created report of the specified type.
Quick Links	Links to some common OV3600 tasks.

Table 136 Home > License (Continued)

Field	Description
Search	Provides search for managed devices and wireless users. When searching for a MAC address, colons are needed (for example, 00:40:96).
Monitoring Status	Pie chart depicts the number of Up and Down APs.
Configuration Status	Pie chart depicts the number of mismatched APs.
Alert Summary	Provides a summary of OV3600 Alerts, IDS Events, Incidents, RADIUS Authentication Issues.

Searching OV3600 with the Home > Search Page

The **Home > Search** page provides a simple way to find users and managed devices. 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. OV3600 6.2 adds support for rogue devices and tags in search capability.



OV3600 Version 6.2 enhances search functions so that when you search with an IP address, object unique identifier (OUI), LAN IP address, radio MAC address, or name, you receive matching rogue devices and tags.

Figure 121 illustrates this page. In this example, a short text string was used in search, so as to maximize the number of returns for illustrative purposes.

Figure 121 Home > Search

Search for managed devices and wireless users. A single substring match is used. To search by MAC address, include colons (e.g. 00:40:96).

00: Search

APs/Devices

Modify Devices

1:20 of 12 APs/Devices Page 1 of 3 >

Name	Status	Users	RSSI (Mean)	Uptime	Configuration	Group	Folder	Controller	SSID	First Scan	Ch	Second Scan	Ch	Type
2250-911413	Up	0	0	22 hrs 30 mins	Matched	Acme Corporation	Top	HQ2-4400-CTRL-HQ02	802.11bg	11	802.11a	36	802.11a	Cisco Aironet 1250 L1
Arwave-AL1	Up	1	0	22 hrs 8 mins	Good	Acme Corporation	Top	HQ2-3600-CTRL-Primary	802.11bg	11	802.11a	161	802.11a	Aruba AP 65
Arwave-AL10	Up	0	0	37 days 17 hrs 51 mins	Good	Acme Corporation	Acme Corporation	HQ2-3600-CTRL-Primary	802.11bg	11	802.11a	149	802.11a	Aruba AP 65
Arwave-AL11	Up	2	164	34 days 21 hrs 54 mins	Good	Acme Corporation	Acme Corporation	HQ2-3600-CTRL-Primary	802.11bg	11	802.11a	157	802.11a	Aruba AP 65
Arwave-AL12	Up	1	1	37 days 17 hrs 50 mins	Good	Acme Corporation	Acme Corporation	HQ2-3600-CTRL-Primary	802.11bg	11	802.11a	48	802.11a	Aruba AP 65
Arwave-AL2	Up	1	5	22 hrs 8 mins	Good	Acme Corporation	Top	HQ2-3600-CTRL-Primary	802.11bg	11	802.11a	36	802.11a	Aruba AP 65
Arwave-AL3	Up	0	0	22 hrs 8 mins	Good	Acme Corporation	Top	HQ2-3600-CTRL-Primary	802.11bg	6	802.11a	44	802.11a	Aruba AP 65
Arwave-AL5	Up	2	0	22 hrs 8 mins	Good	Acme Corporation	Top	HQ2-3600-CTRL-Primary	802.11bg	11	802.11a	36	802.11a	Aruba AP 65
Arwave-AL8	Up	1	0	22 hrs 8 mins	Good	Acme Corporation	Top	HQ2-3600-CTRL-Primary	802.11bg	11	802.11a	48	802.11a	Aruba AP 65
Arwave-AL9	Up	0	0	22 hrs 8 mins	Good	Acme Corporation	Top	HQ2-3600-CTRL-Primary	802.11bg	11	802.11a	149	802.11a	Aruba AP 65
Arwave-AL15	Up	5	10	22 hrs 8 mins	Good	Acme Corporation	Top	HQ2-3600-CTRL-Primary	802.11bg	11	802.11a	40	802.11a	Aruba AP 65
Arwave-ctrl_office	Up	0	0	22 hrs 8 mins	Good	Acme Corporation	Top	HQ2-3600-CTRL-Primary	802.11bg	11	802.11a	40	802.11a	Aruba AP 65
AP0016-49921442	Up	0	0	22 hrs 30 mins	Matched	Acme Corporation	Top	HQ2-4400-CTRL-HQ02	802.11bg	11	802.11a	48	802.11a	Cisco Aironet 1250 L1
AP-1	Up	1	14	57 days 0 hrs 56 mins	Good	County School District	County School District	menu controller	802.11abg	40	802.11abg	6	Menu AP 208	
AP-2	Up	0	0	12 mins	Good	County School District	County School District	menu controller	802.11bg	6	802.11a	46	Menu AP 150	
AP-3	Up	0	0	57 days 4 hrs 23 mins	Good	County School District	County School District	menu controller	802.11abg	6	-	-	Menu AP 201	
AP-4	Up	0	0	57 days 4 hrs 23 mins	Good	County School District	County School District	menu controller	802.11b	6	-	-	Menu AP 100	
AP-5	Up	0	0	57 days 0 hrs 51 mins	Good	County School District	County School District	menu controller	802.11abg	36	802.11abg	6	Menu AP 320	
so.arwave.com	Down	-	-	-	Matched	Acme Corporation	Top	-	802.11b	-	802.11a	-	-	Cisco Aironet 1200 L1
cisco1500-1	Down	-	-	-	Unknown	Acme Corporation	Top	HQ2-4400-CTRL-HQ02	-	-	-	-	-	Cisco Aironet 1500 L1

Users

Modify Devices

1:20 of 4137 Users Page 1 of 207 >

Username	Role	MAC Address	AP/Device	SSID	VLAN	AP Radio	Connection Mode	Ch BW	Association Time	Duration	LAM IP Address	LAM Hostname	Guest User	VPN IP Address
-	-	00:00:00:00:00:00	-	-	-	-	-	-	4/25/2005 10:29 AM	-	-	-	-	-
-	-	00:00:00:00:00:01	-	-	-	802.11b	802.11g	-	9/25/2006 6:58 PM	-	-	-	-	-
-	-	00:00:00:00:00:10	HQ2-1130-Boardroom	arwave-dev	51	802.11bg	802.11g	-	4/7/2008 4:37 PM	-	0.0.0.0	-	-	-
-	-	00:00:94:04:09:50	-	-	-	-	-	-	11/19/2004 9:29 AM	-	-	-	-	-
-	-	00:00:94:04:09:50	-	-	-	-	-	-	4/14/2005 5:15 PM	-	0.0.0.0	-	-	-
-	-	00:01:24:80:5A:21	-	-	-	-	-	-	8/21/2005 4:47 PM	-	-	-	-	-
-	-	00:01:36:0F:94:07	arwave-guest	200	802.11bg	802.11b	-	-	9/12/2006 8:03 PM	-	10.51.1.44	00:1a:1e:c0:50:74.dev.arwave.com	-	-
-	-	00:01:4A:4A:22:AE	-	-	-	-	-	-	1/7/2008 10:22 PM	-	-	-	-	-
-	-	00:01:4A:50:08:36	arwave-guest	200	802.11bg	802.11b	-	-	1/4/2005 7:09 AM	-	0.0.0.0	-	-	-
-	-	00:01:4A:50:08:36	arwave-guest	200	802.11bg	802.11b	-	-	10/3/2006 7:37 PM	-	0.0.0.0	-	-	-
-	-	00:01:4A:50:08:36	arwave-guest	200	802.11bg	802.11b	-	-	9/11/2006 9:05 PM	-	0.0.0.0	-	-	-
-	-	00:01:4A:50:08:36	arwave-guest	200	802.11bg	802.11b	-	-	8/2/2005 5:40 PM	-	0.0.0.0	-	-	-
-	-	00:01:4A:50:08:36	arwave-guest	200	802.11bg	802.11b	-	-	5/30/2006 5:34 PM	-	0.0.0.0	-	-	-
-	-	00:01:4A:50:08:36	arwave-guest	200	802.11bg	802.11b	-	-	3/4/2006 9:46 PM	-	0.0.0.0	-	-	-
-	-	00:01:4A:50:08:36	arwave-guest	200	802.11bg	802.11b	-	-	8/16/2007 7:27 PM	-	0.0.0.0	-	-	-
-	-	00:01:4A:50:08:36	arwave-guest	200	802.11bg	802.11b	-	-	11/4/2005 7:09 AM	-	0.0.0.0	-	-	-
apn	-	00:01:FA:EE:BA:87	aruba-ap	1	802.11bg	802.11bg	-	-	2/8/2006 3:54 PM	-	0.0.0.0	-	-	-
logon	-	00:02:2D:04:96:47	-	-	-	-	-	-	11/14/2007 9:57 AM	-	0.0.0.0	-	-	-
-	-	00:02:2D:04:96:47	-	-	-	-	-	-	7/29/2005 1:44 PM	-	10.51.1.45	phone-2.dev.arwave.com	-	-
-	-	00:02:2D:00:18:37	-	-	-	-	-	-	5/12/2005 3:16 PM	-	10.51.1.29	00:0b:06:c1:a1:f7.dev.arwave.com	-	-

Rogues

Modify Devices

1:20 of 582 Rogue Devices Page 1 of 20 >

Name	Classification	Ask	Score	Hostid	Operating System	IP Address	SSID	Network Type	Ch	WEP	RSSI	Signal	LAM MAC Address	LAM Vendor
Cisco-00c2c82	Unclassified	No	6	-	-	-	-	AP	2	No	-10	-20	-	-
Symbol Tsc-00:30:21	Unclassified	No	6	-	-	-	-	AP	6	No	-35	-20	-	-
NOMADIX Bt-23:02:80	Unclassified	No	6	-	-	-	-	AP	7	No	-44	-49	-	-
Aruba Netw-61:83:140	Unclassified	No	6	-	-	-	-	AP	6	No	-24	-21	-	-
Sensio Intc-43:79:81	Unclassified	No	6	-	-	-	-	AP	11	No	-41	-20	-	-
Watson Net-74:51:7F	Unclassified	No	6	-	-	-	-	AP	10	No	-61	-37	-	-
Foundry-8A:85:8A9	Unclassified	No	6	-	-	-	-	AP	6	No	-41	-24	-	-
Aruba Netw-61:AD:C1	Unclassified	No	6	-	-	-	-	AP	1	Yes	-13	-20	-	-
Hewlett-PhA-02:1:0	Unclassified	No	6	-	-	-	-	AP	153	No	-23	-27	-	-
Symbol Tsc-00:75:80	Unclassified	No	6	-	-	-	-	AP	0	No	-32	-20	-	-
Aruba Netw-81:AD:02	Unclassified	No	6	-	-	-	-	AP	149	No	-18	-21	-	-
Cisco Syst-F5:74:40	Unclassified	No	6	-	-	-	-	AP	3	No	-31	-20	-	-
ACCTON-69:5E:58	Unclassified	No	6	-	-	-	-	AP	0	No	-30	-21	-	-
Aruba Netw-6F:80:40	Unclassified	No	6	-	-	-	-	AP	1	No	-24	-20	-	-
Watson Net-35:13:56	Unclassified	No	6	-	-	-	-	AP	1	No	-22	-20	-	-
Cisco Link-65:CC:63	Unclassified	No	6	-	-	-	-	AP	11	No	-22	-27	-	-
Cisco Syst-A7:31:58	Unclassified	No	6	-	-	-	-	AP	0	No	-40	-36	-	-
Sensio Intc-43:7C:81	Unclassified	No	6	-	-	-	-	AP	11	No	-29	-10	-	-
Cisco SAUF-ED	Unclassified	No	6	-	-	-	-	AP	3	No	-19	-22	-	-
Aruba Netw-9A:05:20	Unclassified	No	6	-	-	-	-	AP	1	No	-29	-20	-	-

Tags

1:2 of 3 Tags Page 1 of 1

Name	MAC Address	Vendor	Battery Level	Chap Interval	Last Seen	Client AP
CD-Burner	00:14:7E:00:4C:0C	Panasonic Networks, Inc.	Normal	4 secs	12/11/2008 2:54 PM	HQ2-1130-Boardroom
11n-Laptop	00:0C:CC:7A:56:9A	Aerocoust Ltd.	Normal	50 secs	12/11/2008 2:53 PM	HQ2-1130-Boardroom
	00:14:7E:00:4C:09	InnerWireless	Normal	4 secs	12/11/2008 2:53 PM	HQ2-1130-Boardroom
RF-Cape	00:0C:CC:58:71:96	Aerocoust Ltd.	Normal	45 secs	12/11/2008 2:53 PM	HQ2-1130-Boardroom
Water-Cooler	00:0C:CC:7A:28:8A	Aerocoust Ltd.	Normal	50 secs	12/11/2008 2:52 PM	HQ2-1130-Boardroom
Copio-Spec-Anal	00:14:7E:00:4C:04	Panasonic Networks, Inc.	Normal	1 sec	12/11/2008 8:38 AM	-
	00:14:7E:00:4C:02	InnerWireless	Normal	2 secs	12/8/2008 5:18 PM	-

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 sorting 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**

Using 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. If you have any questions that are not answered by the documentation please contact Alcatel-Lucent Enterprise Support at support@ind.alcatel.com.

Documentation that supports Alcatel-Lucent OV3600 would include the following titles:

- *OmniVista 3600 Air Manager (OV3600) User Guide*, Version 6.2, part number 0510589-01
- *OV3600 Device Compatibility Matrix*, part number 0510590-01
- *OV3600 Firmware Matrix*, part number 0510591-01
- *OmniVista 3600 Air Manager Quick Start Guide*, part number 0510592-01
- *Alcatel-Lucent Best Practices Guide*
- *OmniVista 3600 VisualRF User Guide*

Using the Home > User Info Page

The **Home > User Info** page displays information about the user logged in to OV3600 including the role, authentication type (local user or TACACS+) and access level. It also provides the user with the ability to change securely change their password without going through an OV3600 administrator. Users can also set preferences for the display of alerts in the OV3600 header, the minimum alert severity to display, and the default number of records to appear in a list and the refresh rate for the console. [Figure 122](#) illustrates this page.

Figure 122 Home > User

admin is logged in as a local user with role *AMP Administration* and Read/Write access to RAPIDS.

User Information	
Name:	<input type="text"/>
Email:	<input type="text"/>
Phone:	<input type="text"/>
Notes:	<input type="text"/>

User Preferences	
Display Severe Alerts:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Display Alerts >= Severity:	Major <input type="button" value="v"/>
Default Number of Records per List:	30 records per page <input type="button" value="v"/>
Console Refresh Rate:	Never <input type="button" value="v"/>

Change Password	
New Password:	<input type="text"/>
Confirm New Password:	<input type="text"/>

Using System Pages

The **System > Event Logs** page is a very useful debugging tool. The **System** pages provide a centralized location for system wide OV3600 data and settings. The **System > Status** page displays the status of all of OV3600 services.

Schedule configuration change jobs are summarized on the **System > Configuration Change Jobs** page.

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 Enterprise Support at support@ind.alcatel.com. The **Reboot** button provides a graceful way to restart your OV3600 remotely when it is needed. [Figure 123](#) illustrates this page.

Figure 123 System > Status



The screenshot shows the 'System > Status' page. At the top, there is a 'Refresh' link and a diagnostic report file path: 'Diagnostic report file for sending to customer support: diagnostics.tar.gz'. Below this is a table with three columns: 'Service', 'Status', and 'Logs'. The table lists 34 services. Most are 'OK', but 'FTP Server', 'Master Console', and 'Cisco ACS' are 'Disabled'. At the bottom of the table is a 'Reboot System' button.

Service	Status	Logs
Database	OK	/var/log/pgsql
Web Server	OK	/var/log/httpd/ssl_error_log
RADIUS Accounting Server	OK	/var/log/radius/radius.log
NTP Client	OK	
Postfix Mail Server	OK	/var/log/maillog
Airbus Message Server	OK	/var/log/airbus.log
Alert Monitor	OK	/var/log/alertd
Device Monitor	OK	/var/log/ap_watcher
Device Monitor (Poll Now)	OK	/var/log/ap_watcher_pol_now
Client Monitor	OK	/var/log/async_logger
Firmware Server	OK	/var/log/firmware_enforcer
Configuration Server	OK	/var/log/config_pusher
Configuration Monitor	OK	/var/log/config_verifier
WEP Key Setter	OK	/var/log/wep_key_setter
SNMP Fetcher	OK	/var/log/snmp_fetcher
SNMP V2 Fetcher	OK	/var/log/snmp_v2_fetcher
SNMP Trap Handler	OK	/var/log/snmp_trap_handler
SNMP Enabler	OK	/var/log/snmp_enabler
HTTP/SNMP Scanner	OK	/var/log/ap_scanner
Device List Cacher	OK	/var/log/ap_list_cacher
Graphing Agent	OK	
802.11 Counter Collector	OK	/var/log/dot11_counter_collector
Device Discovery Event Logger	OK	/var/log/discovery_event
Performance Monitor	OK	/var/log/perf_collector
FTP Server	Disabled	/var/log/vsftpd.log
Master Console	Disabled	/var/log/mc_stat_collector
Cisco WLSE Poller	OK	/var/log/wlse
Switch Poller	OK	/var/log/rapids
CDP Detector	OK	/var/log/cisco_discover
Proxim/ORINOCO Detector	OK	/var/log/lucent_discover
Symbol/Intel W/NMP Detector (Primary)	OK	/var/log/intel_discover_eth0
Symbol/Intel W/NMP Detector (Secondary)	Disabled	/var/log/intel_discover_eth1
Cisco ACS	Disabled	/var/log/acs
VisualRF Engine	OK	/var/log/visualrf.log
VisualRF Poller	OK	/var/log/visualrf_poller
Fallover Monitor	Disabled	/var/log/amp_watcher
Whitelist Collector	Disabled	/var/log/whitelist_collector

- 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**.
- 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 Technical Support Engineers may request these logs for help in troubleshooting problems and will provide detailed instructions on how to retrieve them. [Table 137](#) describes the log information.

Table 137 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 > 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 124](#).

Figure 124 System > Configuration Change Jobs

The screenshot shows a web interface for editing a configuration change job. At the top, there is a table with columns: Subject, Description, Scheduled Time, User, Folder, and Group. The job details are as follows:

Subject	Description	Scheduled Time	User	Folder	Group
AP02	Change Radio Status on AP "AP02" 802.11bg and AP "AP02" 802.11a	September 9th 2007 at 12:00 am	admin	Top > .controller.thin.ap > trapeze	Access F

Below the table, the job is titled "To run at: September 9th 2007 at 12:00 am". It lists two APs:

- AP "AP02" 802.11bg: Radio: (none) [dropdown arrow] Enabled
- AP "AP02" 802.11a: Radio: (none) [dropdown arrow] Enabled

Buttons for "Apply Changes Now", "Delete", and "Cancel" are visible. Below this is a "Schedule" section with instructions: "Specify numeric dates with optional 24-hour times (like 7/4/2003 or 2003-07-04 for July 4th, 2003, or 7/4/2003 13:00 for July 4th, 2003 at 1:00 PM.), or specify relative times (like at noon, tomorrow at midnight, or next tuesday at 4am). Other input formats may be accepted." The "Start Date/Time" field is set to "September 9th 2007 at 12:00" and has a "Schedule" button below it.

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 > 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 125](#) illustrates this page, and [Table 138](#) describes the page components.

Figure 125 System > Event Logs

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 15:19:37 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 138 System > Event Logs

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.
Type	Displays the Type of event recorded, which is one of four types, as follows: <ul style="list-style-type: none"> ● 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 > 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 126](#) illustrates this page and [Table 139](#) describes fields and information displayed.

Figure 126 System > Performance (Partial Screen Shown)

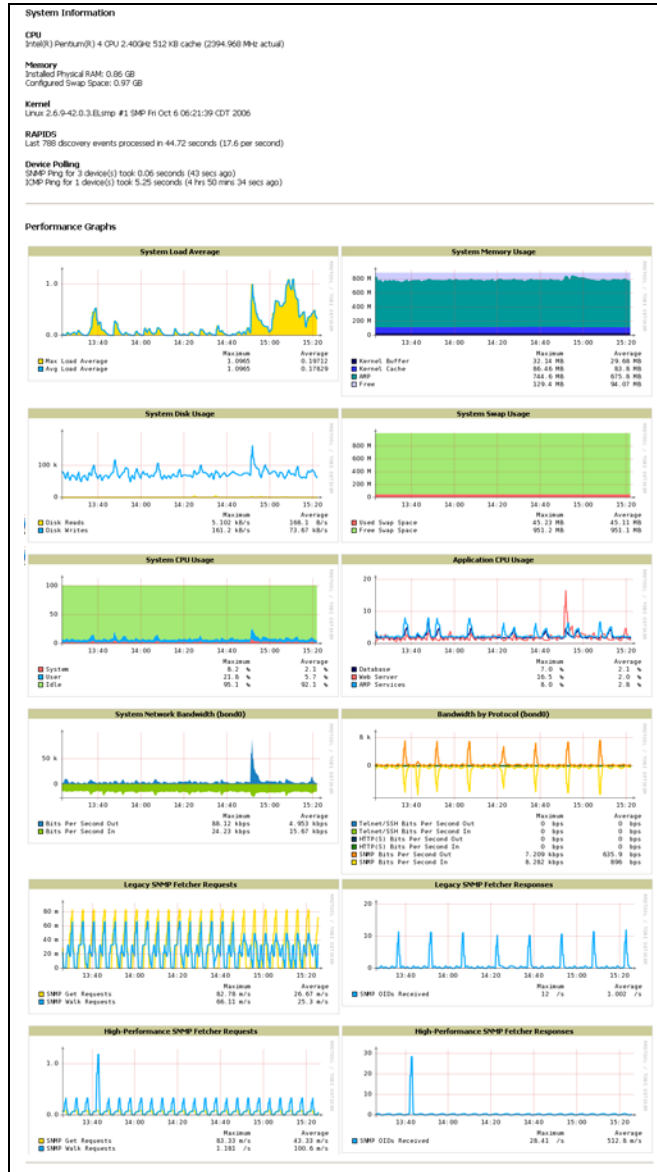


Table 139 System > Performance

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.

Table 139 System > Performance (Continued)

Field	Description
Device Polling	Displays some AP/Device polling statistics.
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 an unusable OV3600. To lower the load average try increasing a few polling periods. Increasing the polling period for APs, routers/switches, WLSE, ACS, etc 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 milli 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 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.

Table 139 System > Performance (Continued)

Field	Description
Database Table Scans	The number of Database table scans performed by the database.
Database Row Activity	The number of insertions, deletions and updates performed to the database.
Database Transaction Activity	The number of commits and rollbacks performed by the database.
Disk 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 Enterprise Support at support@ind.alcatel.com.

Using Triggers and Alerts

This section covers triggers and alerts in OV3600 6.2 with the following topics:

- [Overview of Triggers and Alerts](#)
- [Viewing Triggers](#)
- [Creating New Triggers](#)
- [Delivering Triggered Alerts](#)
- [Viewing Alerts](#)

Overview of Triggers and Alerts

OV3600 is designed to monitor key aspects of wireless LAN performance and to generate alerts when parameters are outside normal bounds. This enables problems to be addressed before users are impacted. OV3600 uses configurable triggers to provide alerts about events on the network. OV3600 deploys two types of alerts:

- normal alerts that are triggered when a particular event occurs
- synthetic alerts that are triggered when a condition persists for longer than a specified period

These synthetic alerts, enabled by the near real-time monitoring capabilities of OV3600, help network administrators differentiate between minor, one-time events and sustained performance issues.

Viewing Triggers

To view defined system triggers, go to the **System > Triggers** page. Figure 127 illustrates this page.

Figure 127 System > Triggers (Split View)

Triggers:

New Trigger

<input type="checkbox"/>	Type	Trigger	Additional Notification Options
<input type="checkbox"/>	User Bandwidth	Bandwidth kbps (combined) >= 5000 kbps for 1 hour	NMS
<input type="checkbox"/>	New Rogue Device Detected	Score = 7	NMS
<input type="checkbox"/>	Device IDS Events	Count > 0 for 1 minute	NMS
<input type="checkbox"/>	New User	New User Association	NMS
<input type="checkbox"/>	Device Down	All device types	NMS
<input type="checkbox"/>	Radio Down	-	NMS
<input type="checkbox"/>	Device RADIUS Authentication Issues	Count >= 1 for 15 secs	NMS
<input type="checkbox"/>	Connected Users	9D:04:C2:9D:04:C2 5C:00:99:5C:00:99	Email
<input type="checkbox"/>	Inactive Tag	for >= 1 hr 0 mins	-
<input type="checkbox"/>	802.11 Frame Counters	WEP Undecryptable Rate >= 10 frames/sec for 1 hour	-

10 Triggers

Select All - Unselect All

NMS Trap Destinations	Severity	Folder	Group	Include Subfolders	Logged Alert Visibility	Suppress Until Acknowledged
-	Normal	Top	-	Yes	By Role	Yes
10.51.1.7	Normal	Top	-	Yes	By Role	Yes
10.51.1.7	Normal	Top	Outdoor	Yes	By Role	Yes
-	Normal	Top	-	Yes	By Role	Yes
-	Normal	Top	-	Yes	By Role	Yes
-	Normal	Top	-	Yes	By Role	Yes
10.51.1.7	Minor	Top	-	Yes	By Role	Yes
10.51.1.7	Major	Top	-	Yes	By Role	Yes
10.51.1.7	Critical	Top	-	Yes	By Role	Yes
-	Critical	Top	-	Yes	By Role	No

No Triggers for other roles found.

Creating New Triggers

Perform the following steps to create and configure one or more new triggers. This procedure defines settings that are required for any type of trigger. Ensuing procedures define **Conditions** that are specific to each 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 128](#).

Figure 128 *System > Trigger Detail*

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 settings. [Table 140](#) describes the options for trigger restrictions.

Table 140 *System > Trigger Condition Detail*

Notification Option	Description
Folder	The trigger will only apply 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 will only apply to the intersection of the two. It will only apply to APs in the group and in the folder.
Include Subfolders	Including subfolders will apply the trigger to all devices in the top folder and all of the devices in folders under the top folder.
Group	The trigger will only apply to APs/Devices in the specified group. NOTE: If the trigger is restricted by folder and group, it will only apply to the intersection of the two. It will only apply to APs in the group and in the folder.

- b. Specify the **Alert Notifications** for the trigger to be defined. [Table 141](#) describes the options for this page.

Table 141 System > Trigger Condition Detail Alert Notifications for Defined Alert

Notification Option	Description
Notification Type	Itemizes the action OV3600 should take when an alert is triggered. When the log checkbox is checked OV3600 will log the alert in OV3600' log files. When the NMS checkbox is checked OV3600 will send an SNMP trap to the NMS servers defined for the role.
Sender Address	The From field of alert emails will list this email address.
Recipient Email Addresses	The user, users or distribution lists that will receive any email alerts.
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. NOTE: You may select more than one Notification Option for each alert by pressing the CTRL button and clicking the options with the mouse.

- c. Configure the **Alert Notifications** settings. In addition to appearing on the **System > Triggers** page, triggers can be configured to be distributed to email or to a network management system (NMS), or to both.
 - If you select **email**, then you are prompted to set the sender's email address and recipient email addresses.
 - If you select **NMS**, then 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 be distributed 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.
3. In the **Trigger** field, choose the desired trigger **Type** and the desired **Severity**, according to your business needs. [Figure 129](#) illustrates the trigger types supported in OV3600 Version 6.2, and [Table 142](#) describes severity levels available for triggers.

Figure 129 System > Triggers, Add Trigger Type Drop-down Menu

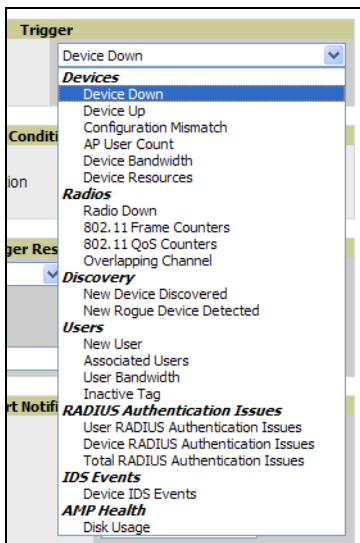


Table 142 Severity Level Options for New Triggers

Severity Level	Description
Normal	Triggers marked Normal generate standard alerts that have no additional emphasis in the OV3600 GUI. Full functionality is supported for Normal alerts.
Warning	Triggers marked Warning generate Severe Alerts . When Severe Alerts exist they appear at the right of the status bar as a bold, red component. Severe Alerts are visible for users based on the settings on the Home > User Info page. Other functionality mirrors that of regular alerts.
Minor	Triggers marked as minor indicate lower-priority events.
Major	Triggers marked as major indicate events that should be considered larger in scope or urgency.
Critical	Triggers marked Critical generate Severe Alerts . When Severe Alerts exist they appear at the right of the status bar as a bold, red component. Severe Alerts are visible for users based on the settings on the Home > User Info page. Other functionality mirrors that of regular alerts.

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 the following procedures:

- “Setting Triggers for Devices” on page 211
- “Setting Triggers for Radios” on page 213
- “Setting Triggers for Discovery” on page 215
- “Setting Triggers for Users” on page 216
- “Setting Triggers for RADIUS Authentication Issues” on page 218
- “Setting Triggers for IDS Events” on page 219
- “Setting Triggers for OV3600 Health” on page 220

Setting Triggers for Devices

After completing steps 1-3 in “Creating New Triggers” on page 209, perform the following steps to complete the configuration of device-related triggers.

- If you have not already done so, choose a device type from the **Devices** listed in the **Type** drop-down menu. See [Figure 129](#). [Table 143](#) itemizes and describes device trigger options and condition settings.

Table 143 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.

Table 143 *Devices Trigger Types*

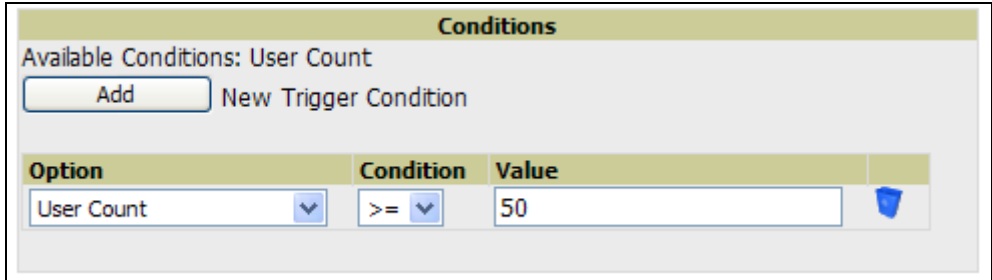
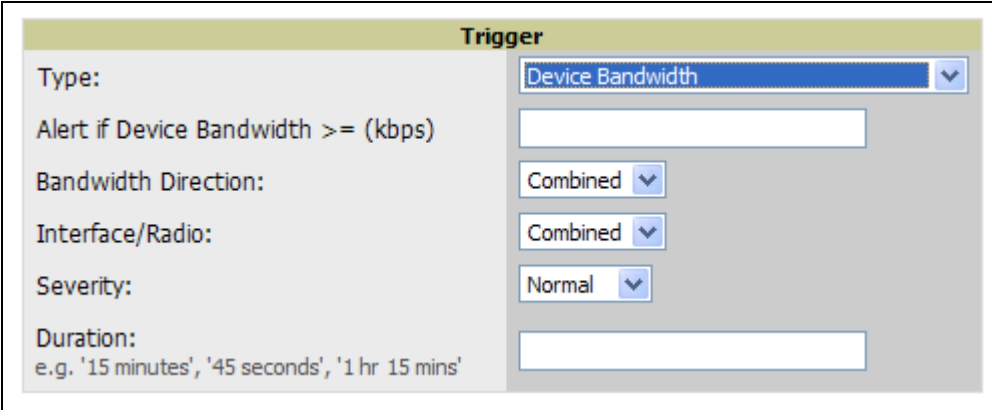


Devices Trigger Options	Description
<p>Configuration Mismatch</p>	<p>This trigger type activates when the actual configuration on the AP does not match the defined Group configuration policy.</p> <p>To set the conditions for this trigger type, click Add in the Conditions section. Complete the conditions 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.</p>
<p>AP User Count</p>	<p>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.</p> <p>Figure 130 <i>Sample of Trigger Condition for AP Device User Count</i></p> 
<p>Device Bandwidth</p>	<p>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.</p> <p>Figure 131 <i>Trigger Type Section for Device Bandwidth Type</i></p>  <ul style="list-style-type: none"> ● 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 209. ● Duration—The Duration level is likely defined already from an earlier step in this procedure. See “Creating New Triggers” on page 209.

Table 143 *Devices Trigger Types*

Devices Trigger Options	Description
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 143](#).
 -  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 209 to create a new trigger.

Setting Triggers for Radios

After completing steps 1-3 in “[Creating New Triggers](#)” on page 209, 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. See [Figure 129](#). [Table 144](#) itemizes and describes the Radios-related trigger types, and condition settings for each.

Table 144 *Radios Trigger Types and Condition Settings*

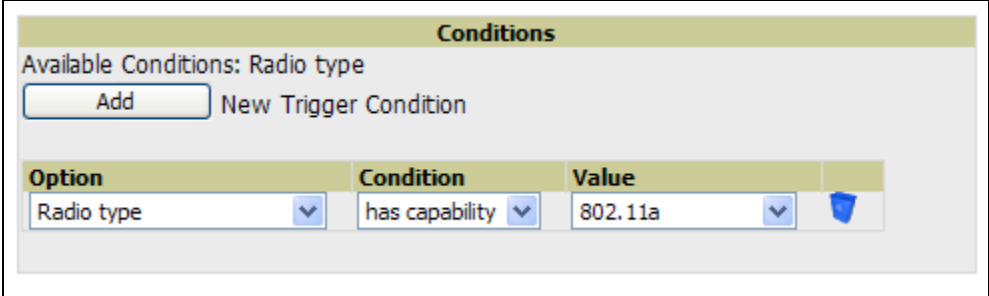





Radio Trigger Options	Description																				
Radio Down	<p>This trigger indicates when a device’s radio is down on the network. Once you choose this trigger type, click Add New Trigger Condition to create at least one condition. The Radio Down trigger requires that a radio capability be set as a condition. The Value drop-down menu supports several condition options. The following example illustrates a Radio trigger that has 802.11a capability:</p> <p>Figure 132 <i>Sample of Trigger Condition for Radio Type</i></p>  <table border="1" data-bbox="462 1449 1445 1743"> <thead> <tr> <th colspan="4">Conditions</th> </tr> </thead> <tbody> <tr> <td colspan="4">Available Conditions: Radio type</td> </tr> <tr> <td colspan="4"><input type="button" value="Add"/> New Trigger Condition</td> </tr> <tr> <th>Option</th> <th>Condition</th> <th>Value</th> <th></th> </tr> <tr> <td>Radio type</td> <td>has capability</td> <td>802.11a</td> <td></td> </tr> </tbody> </table>	Conditions				Available Conditions: Radio type				<input type="button" value="Add"/> New Trigger Condition				Option	Condition	Value		Radio type	has capability	802.11a	
Conditions																					
Available Conditions: Radio type																					
<input type="button" value="Add"/> New Trigger Condition																					
Option	Condition	Value																			
Radio type	has capability	802.11a																			

Table 144 Radios Trigger Types and Condition Settings (Continued)

Radio Trigger Options	Description
<p>802.11 Frame Counters</p>	<p>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.</p> <p>Click Add New Trigger Condition to access these settings. Define at least one condition for this trigger type.</p> <p>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.</p>
<p>802.11 QoS Counters</p>	<p>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.</p> <p>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.</p>
<p>Overlapping Channel</p>	<p>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.</p> <p>Selecting this trigger type displays a new option which you can enable as desired: Alert if neighbor within channels.</p> <p>Figure 133 Trigger Type Section for Overlapping Channel Type</p> <div data-bbox="701 947 1203 1058" data-label="Image"> </div> <p>NOTE: There is no Conditions configuration for Radios: Overlapping Channel triggers.</p>

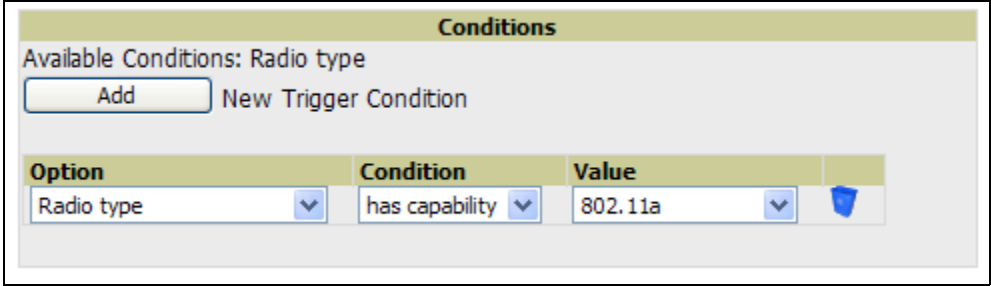
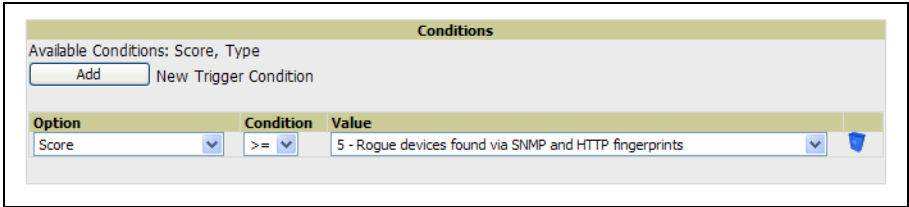
- b. Delete conditions as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.
- d. You can edit or delete any trigger as desired from the **System > 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 143](#).
 -  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 209](#) to create a new trigger.

Setting Triggers for Discovery

After completing steps 1-3 in “Creating New Triggers” on page 209, 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 129. Table 145 itemizes and describes the Discovery-related trigger types, and condition settings for each discovery trigger type.

Table 145 *Discovery Trigger Types and Condition Settings*

Discovery Trigger Options	Description
<p>New Devices Discovered*</p>	<p>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.</p> <p>The following example illustrates the Add Condition section for a New Devices Discovered trigger.</p> <p>Figure 134 <i>Sample of Condition for New Device Discovered Trigger Type</i></p> 
<p>New Rogue Device Detected</p>	<p>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 “Deploying RAPIDS in OV3600 6.2” on page 173 for more information on score definitions and discovery methods.</p> <p>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.</p> <ul style="list-style-type: none"> • 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. <p>Figure 135 <i>Sample of Trigger Condition for A Rogue Detected Trigger</i></p> 

- 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 143](#).
 - ☞ 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 209 to create a new trigger.

Setting Triggers for Users

After completing steps 1-3 in “[Creating New Triggers](#)” on page 209, 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 129](#). [Table 146](#) itemizes and describes the User-related trigger types, and condition settings for each discovery trigger type.

Table 146 *User Trigger Types and Condition Settings*

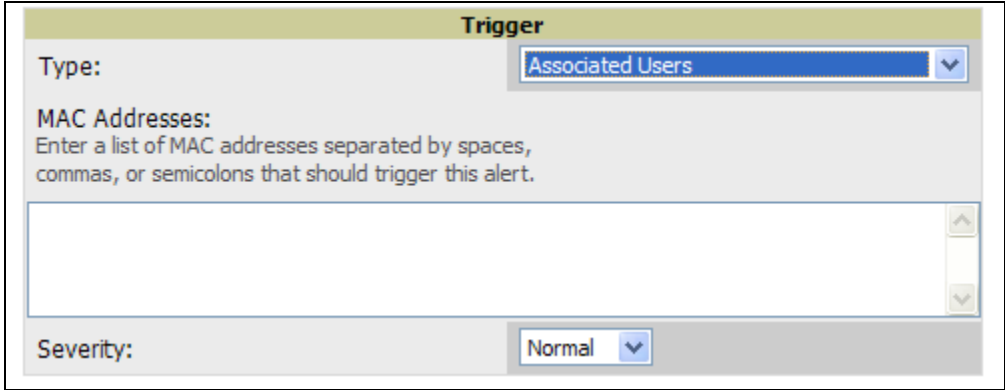
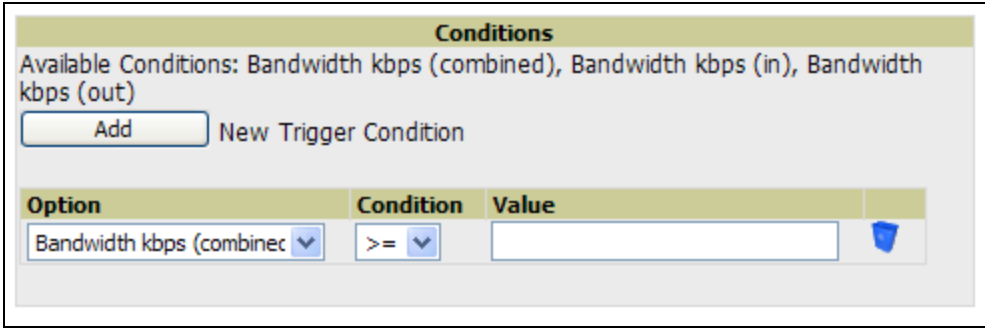
User Trigger Option	Description
New User	This trigger type indicates when a new user has associated to a device within a defined set of groups or folders. Note that the New User trigger type does not require the configuration of any condition settings, so the Condition section disappears.
Associated Users	<p>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.</p> <p>Figure 136 <i>Example of Associated User Configuration Section</i></p> 

Table 146 User Trigger Types and Condition Settings (Continued)

User Trigger Option	Description
<p>User Bandwidth</p>	<p>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).</p> <p>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.</p> <p>The Option drop-down menu provides these options:</p> <ul style="list-style-type: none"> • Bandwidth kbps (Combined) • Bandwidth kbps (in) • Bandwidth kbps (out) <p>The Condition drop-down menu provides these options:</p> <ul style="list-style-type: none"> • = – 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... <p>The Value field requires that you input a numerical figure for kilobits per second (kbps).</p> <p>Figure 137 Sample of User Bandwidth Trigger Condition</p> 
<p>Inactive Tag</p>	<p>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.</p>

- 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 143](#).
 - ☞ 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 209 to create a new trigger.

Setting Triggers for RADIUS Authentication Issues



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

After completing steps 1-3 in “[Creating New Triggers](#)” on page 209, 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 129](#). [Table 147](#) itemizes and describes the condition settings for each **RADIUS Authentication** trigger type.

Figure 138 RADIUS Authentication Trigger Condition Settings

Table 147 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.

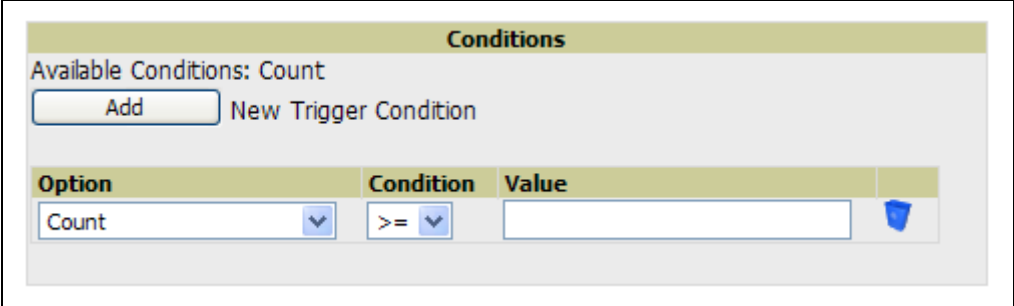
- b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.
- d. You can edit or delete any trigger as desired 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 143](#).
 - 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 209 to create a new trigger.

Setting Triggers for IDS Events

After completing steps 1-3 in “Creating New Triggers” on page 209, perform the following steps to complete the configuration of 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 129. Table 148 describes condition settings for this trigger type.

Table 148 Device IDS Events Authentication Trigger Types and Condition Settings

IDS Trigger Options	Description
Device IDS Events	<p>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.</p> <p>Figure 139 IDS Events Trigger Condition Settings</p> 

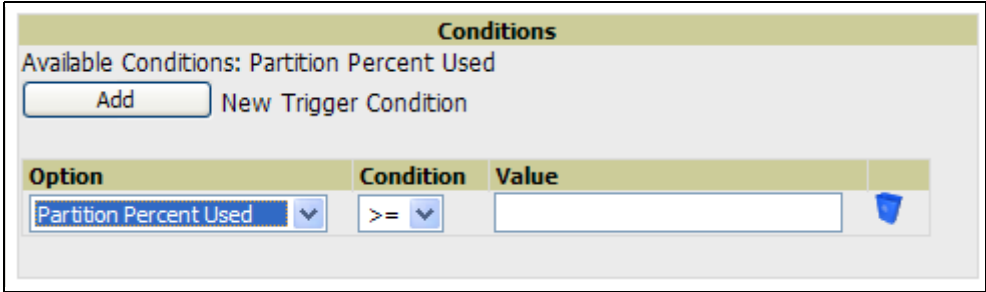
- b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.
- d. You can edit or delete any trigger as desired 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 143.
 - 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 209 to create a new trigger.

Setting Triggers for OV3600 Health

After completing steps 1-3 in “Creating New Triggers” on page 209, 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 129](#) for trigger types. [Table 149](#) describes the condition settings for this trigger type.

Table 149 *Disk Usage Trigger and Condition Settings*

OV3600 Health Trigger	Description
Disk Usage	<p>This trigger type is based on the disk usage of the OV3600 system. This type of trigger indicates that disk usage for the OV3600 server has met or surpassed a defined threshold.</p> <p>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.</p> <p>Figure 140 <i>Condition Settings for Disk Usage Trigger</i></p> 

- 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 143](#).
 - 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 209 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. Check the mail log to ensure mail was sent

```
tail -f /var/log/maillog
```


Viewing Alerts

When OV3600 generates a system alert, the **Alerts** counter in the **Status Bar** at the top of each page increments. To view the active alerts, click the **Alerts** or the **Severe Alerts** counter or navigate to the **System > Alerts** page. [Figure 141](#) illustrates this page.

Figure 141 System > Alerts

<input type="checkbox"/>	Trigger Type	Trigger Summary	Triggering Agent	Time ▼	Severity
<input type="checkbox"/>	User Bandwidth	>= 100 kbps for 30 seconds	00:18:DE:09:B9:09	2/12/2007 12:54 PM	Warning
<input type="checkbox"/>	Device Up		hp-530-1	2/12/2007 12:32 PM	Normal
<input type="checkbox"/>	Device Down		hp-530-1	2/12/2007 12:27 PM	Critical
<input type="checkbox"/>	New Rogue AP Detected	>= 5 for rogue score	Unknown Lo-72:8F:26	2/12/2007 11:51 AM	Minor
<input type="checkbox"/>	Device Up		roamabout-4102-3	2/12/2007 10:24 AM	Normal
<input type="checkbox"/>	Device Down		roamabout-4102-3	2/12/2007 10:19 AM	Critical
<input type="checkbox"/>	User Bandwidth	>= 100 kbps for 30 seconds	00:90:4B:F1:F0:D9	2/12/2007 9:09 AM	Warning
<input type="checkbox"/>	New Rogue AP Detected	>= 5 for rogue score	Locally Ad-03:00:43	2/12/2007 3:00 AM	Minor
<input type="checkbox"/>	New Rogue AP Detected	>= 5 for rogue score	Unknown Gr-02:02:01	2/11/2007 12:58 PM	Minor
<input type="checkbox"/>	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 150](#).

Table 150 System > Alerts

Field	Description
Trigger Type	Selects 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 on the AP name will bring you to 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.

Once you have viewed an alert, you may take one of the following courses of action:

- Leave it in active alert status if it is unresolved. The alert will remain on the New Alerts list until you Acknowledge or Delete it. If an alert already exists the trigger for that AP or User will not fire again until it has been acknowledged or deleted. If AP 7 exceeds a max bandwidth trigger that trigger will not fire again 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 page. Click the **New Alerts** link to return to the list of new alerts only).
- Delete the alert by selecting the alert from the list and clicking the Delete button at the bottom of the page.

Performing Backups with OV3600

Overview of Backups

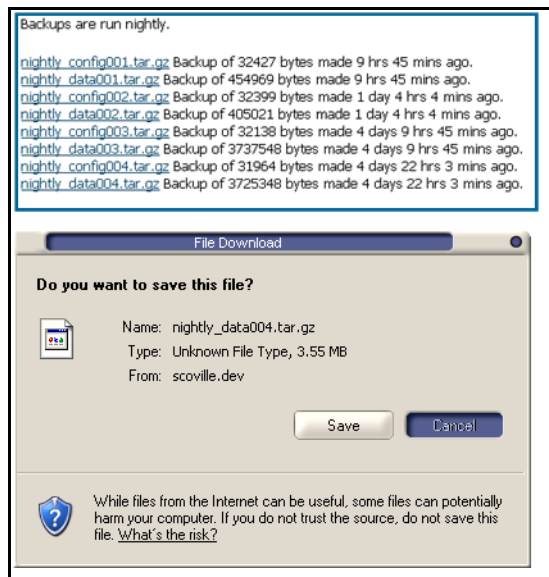
OV3600 creates nightly archives of all relational data, statistical data, and log files. This occurs by default at 4:15 AM, but is configurable on the OV3600 page.

Although OV3600 only keeps the last four sets of archives, the archives can be manually or automatically downloaded off-site for more extensive backup strategies. OV3600 creates two backup files each night, a configuration backup and a data backup. The data backup contains all of the device and group information as well as all of the historical data. The configuration backup contains the OV3600 system files including IP address, NTP information, mail relay hosts and other OV3600 settings.

Viewing and Downloading Backups

To view current backups, go to the **System > Backups** page. [Figure 142](#) illustrates this page.

Figure 142 System > Backups



To download a backup, click the filename URL and the **File Download** popup appears as shown. Alcatel-Lucent recommends regularly saving both backup files to another machine or media. This process can easily be automated with a nightly script.

Running Backup on Demand

To create an immediate backup, use the following procedure:

1. Log into the OV3600 system as root.
2. Change to the **scripts** directory by typing '**scripts**'.
3. Run the backup script by typing **/bin/sh ov3600_backup**.

This creates a backup of the system located in `/alternative/databackup.tar.gz` and `/alternative/configbackup.tar.gz`.

For an OV3600 with 1000 APs it will take about 40 seconds to copy a backup. For an OV3600 with 2500 APs it will take about two minutes.

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. `/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 will allow you to transfer the `nightly00[1-4].tar.gz` file from your local PC to the new OV3600 using the secure copy protocol (SCP).
3. Log onto the new server as root
4. Change to the **scripts** directory by typing **scripts**.
5. Run the restore script by typing **`.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 they are 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 151](#) describes the contents of this page.

Table 151 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.	<ul style="list-style-type: none">● Overview● Watched● OV3600s● 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).	<ul style="list-style-type: none">● 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.	<ul style="list-style-type: none">● General● Network● Users● TACACS+

Adding Watched OV3600 Stations

Navigate to the **Home > Watched OV3600s** page to begin backing up and monitoring OV3600 stations. Once an OV3600 installation has been added to the Watched OV3600s 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 [“Performing Backups with OV3600” on page 222](#). [Figure 143](#) illustrates the **Home > Watched** page.

Figure 143 Home > Watched

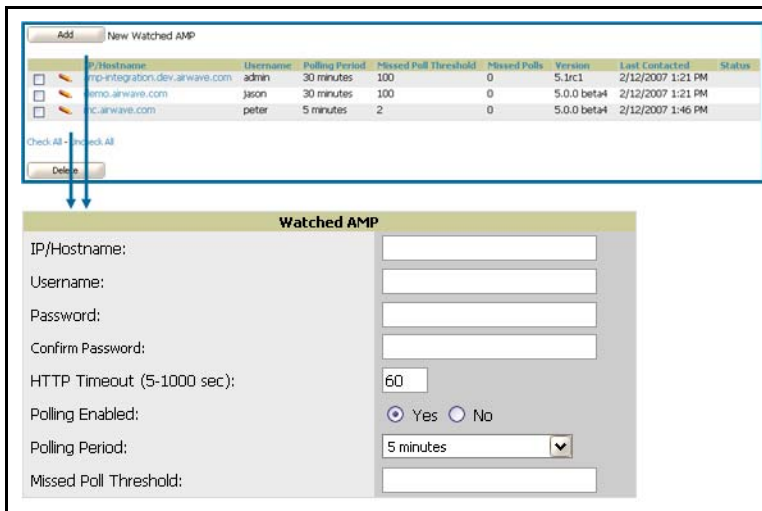


Table 152 Home > Watched

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. If a Watched OV3600 is going down for scheduled maintenance it is recommended to set the polling enabled flag to No.
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 OV3600s APs.

Using 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.
- Commencing with Version 6.2, the **Master Console** supports the following new enhancements:
 - The **Master Console** now offers a display of devices that are in a **down** or **error** state, anywhere on the network. This new 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 “[Specifying General OV3600 Server Settings](#)” on page 33.
 - The **Master Console** and **Failover** servers can now 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 “[Using Triggers and Alerts](#)” on page 207.

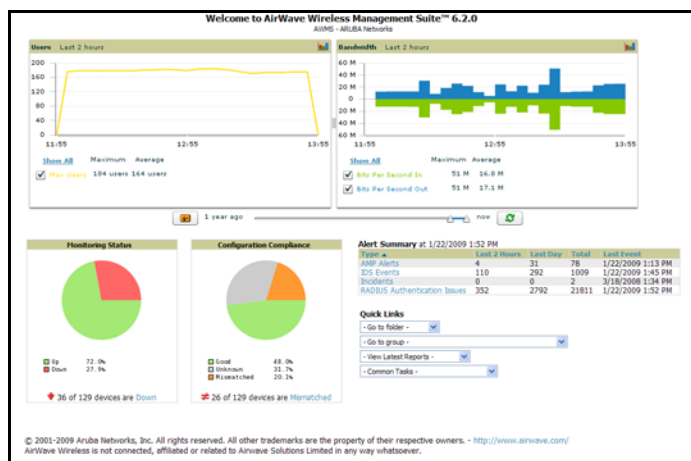
There are two forms of **Master Console**, the standalone server and the OV3600 add-on. *The license key determines if the Master Console is enabled and the mode it should run.*

- While running in *add-on* mode, the OV3600 functions like a normal OV3600, but has an extra MC tab that is used to access the master console.
- When in *standalone* mode, the server only polls other OV3600 installations and does not directly monitor any APs.

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 because no OV3600 or **Master Console** login is required to view the public portal. It can be enabled by navigating to the page 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*. The public portal was once enabled in the **Master Console** license key, but beginning in 6.2 it became an option in the web page. Upon upgrading to 6.2, it is disabled by default, regardless of the type of license.

Figure 144 illustrates the **Master Console** page.

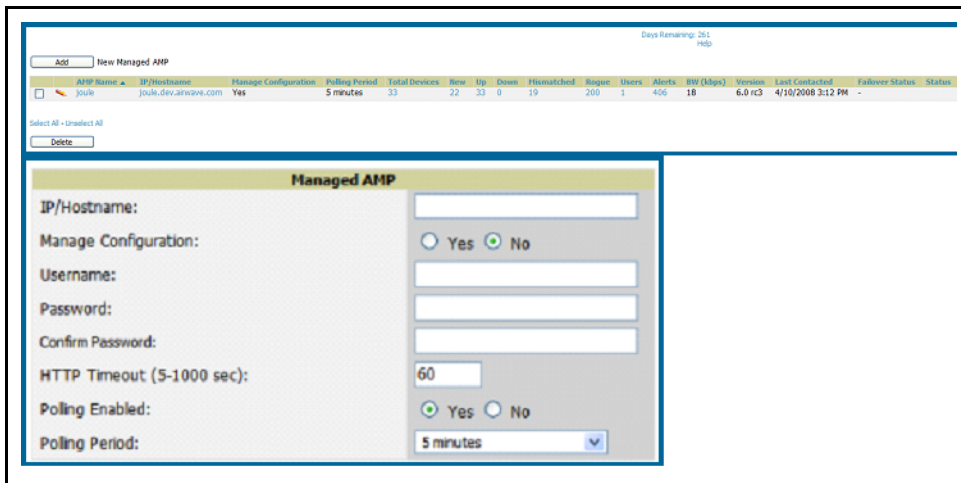
Figure 144 **Home > Overview of Master Console**



Much like the normal **Home > Overview** page, the **Master Console Home > Overview** page provides summary statistics for the entire network at a glance.

To add a managed OV3600, navigate to the **Home > Managed OV3600s** page and click on the **Add** button. [Figure 145](#) illustrates this page.

Figure 145 Master Console > Manage OV3600s



Clicking the **IP/Hostname** link redirects your browser to the specified OV3600. [Table 153](#) describes the fields.

Table 153 Master Console > Manage OV3600s, IP/Hostname

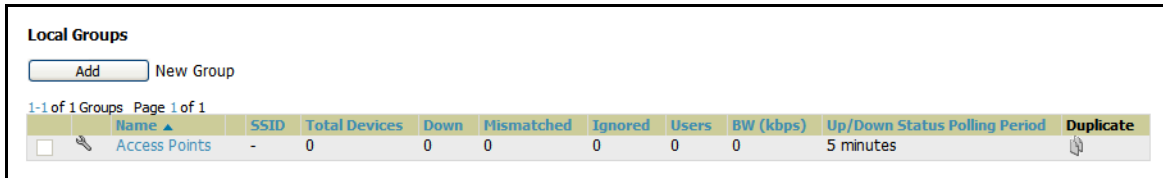
Field	Description
IP/Hostname	The IP or Hostname of the managed OV3600.
Manage Group Configuration	If yes is selected, group configurations can be pushed from the Master Console to the OV3600. This option is disabled (No) by default.
Username	The username used by the Master Console to login to the managed OV3600s. The user needs to be an AP/Device Manager or OV3600 Administrator.
Password	The password used by the Master Console OV3600 to login to the managed OV3600.
Polling Period	Determines how frequently the Master Console will poll the managed OV3600s.
Total Devices	The number of Up and Down devices. The Total devices count does not include New devices.
New Devices	The number of devices that have been discovered by the managed OV3600 but not yet added to a group.
Up	The number of managed, authorized APs that are currently responding to the managed OV3600' requests.
Down	The number of managed, authorized APs that are not currently responding to the managed OV3600' SNMP requests.
Rogue	The number of unknown APs detected on the network by the managed OV3600 with a score of five. A score of five means the rogues were discovered via wireless or wireline fingerprint scanning techniques. NOTE: A newly discovered AP is considered a Rogue if it is not a supported AP that OV3600 can manage and monitor. If the newly discovered AP is capable of being managed and monitored by OV3600 it will be classified as a New device rather than a Rogue.
Users	The number of wireless users currently associated to the wireless network via all APs managed by the managed OV3600.

Table 153 Master Console > Manage OV3600s, IP/Hostname (Continued)

Field	Description
Alerts	The number of non-acknowledged OV3600 alerts generated by user-configured triggers on the managed OV3600.
BW(kbps)	The total amount of bandwidth, in kbps, currently used by the managed OV3600.
Version	The version of OV3600 software currently running on the managed OV3600.
Last Contacted	The last time the managing OV3600 was able to connect to the managed OV3600.
Failover Status	Lists the status of Failover OV3600s. <ul style="list-style-type: none"> ● Watching—The failover server is monitoring healthy OV3600s. ● Failed Over—The monitored OV3600 failed to respond and the Failover OV3600 is currently monitoring APs.
Status	Description of any errors connecting to the managed OV3600. This is not a list of errors that have occurred on the managed OV3600.

1. To push configurations to managed groups using OV3600' global groups feature, first navigate to the Master Console's **Groups > List** page.
2. Click the **Add** button to add a new group, or click the name of the group to edit settings for an existing group.
3. 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).

Figure 146 Master Console > Groups



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. 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 Groups > Templates section of the *User Guide*, 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.

Figure 147 Master Console Groups > Basic



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.

Figure 148 *Master Console > Groups > Basic, Managed*

Group: Access Points

Basic

Name: Access Points

Missed SNMP Poll Threshold (1-100): 1

Regulatory Domain: United States

Timezone: AMP system time
For scheduling group configuration changes

Allow One-to-One NAT: Yes No

Global Groups

Use Global Group: Yes No

Global Group: globalgrouponMC (SSID: -)

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.

Figure 149 *Master Console > Groups > Basic, Managed Subscriber Group*

Group: subscribedgroup

Basic

Name: subscribedgroup

Missed SNMP Poll Threshold (1-100): 1

Regulatory Domain: United States

Timezone: AMP system time
For scheduling group configuration changes

Allow One-to-One NAT: No

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 Groups in OV3600” on page 65](#).

Introduction

This chapter describes reports in OV3600 6.2, to include standard and custom reports, report creation and scheduling, and report distribution via email and processing via XML. This chapter contains the following sections:

- [Overview of OV3600 6.2 Reports](#)
 - [Supported Report Types in OV3600 6.2](#)
 - [Reports > Definitions Page Overview](#)
 - [Reports > Generated Page Overview](#)
- [Using Daily Reports in OV3600 6.2](#)
- [Viewing Reports](#)
- [Exporting Reports to XML](#)
- [Creating and Running Custom Reports](#)
- [Emailing Reports to Smarthost](#)

Overview of OV3600 6.2 Reports

OV3600 Version 6.2 supports a wide variety of reports. These reports are powerful tools in network analysis, user configuration, device optimization, and network monitoring on multiple levels. In addition, such reports can provide an interface for multiple configurations. The following three topics provide an overview of OV3600 6.2 reports:

- [Supported Report Types in OV3600 6.2](#)
- [Reports > Definitions Page Overview](#)
- [Reports > Generated Page Overview](#)

Supported Report Types in OV3600 6.2

OV3600 6.2 supports the following report types, most of which can be custom-configured:

- Capacity Planning
- Configuration Audit
- Device Summary
- Device Uptime
- IDS Events
- Inventory
- Memory and CPU Utilization
- Network Usage
- New Rogue Devices
- New Users
- PCI Compliance
- RADIUS Authentication Issues
- User Session

See [Table 158](#) for an explanation of each.

OV3600 6.2 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 can 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 time period. They 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 has these sections:

- **Report Definitions**—This field lists all reports that are currently defined in OV3600.
- **Add**—This button launches a report definition page by which to create and schedule new reports.
- **Run**—This button allows you to run any report that has been defined.
- **Delete**—This button enables you to delete any report that has been defined.

Once reports have been created with the **Definition** page, reports appear on the **Generated** page. [Figure 150](#) illustrates the **Report > Definition** page, and [Table 154](#) describes the fields.

Figure 150 Report > Definition Page

Report definitions:

New Report Definition

Reports are available on the [Generated Reports](#) page after they have been run.

1-20 of 40 Report Definitions Page 1 of 2 > > |

<input type="checkbox"/>	Title	Type	Subject	Latest Report
<input checked="" type="checkbox"/>	802.11n Prep	Capacity Planning	All Groups, Folders and SSIDs	-
<input type="checkbox"/>	custom network usage	Network Usage	All Groups, Folders and SSIDs	custom network usage
<input type="checkbox"/>	Custom Network Usage Report	Network Usage	SSID ethersphere-wpa2	Custom Network Usage Report
<input type="checkbox"/>	Custom Network Usage Report	Network Usage	Groups Acme Corporation, Korea Regional Office, Outdoor	-
<input type="checkbox"/>	Custom New Rogue Devices Report	New Rogue Devices	All Groups and Folders	-
<input type="checkbox"/>	Custom PCI Compliance Report	PCI Compliance	All Groups, Folders and PCI Requirements	Custom PCI Compliance Report
<input type="checkbox"/>	Custom RADIUS Authentication Issues Report	RADIUS Authentication Issues	All Groups, Folders and SSIDs	-
<input type="checkbox"/>	Custom User Session Report	User Session	SSID ethersphere-wpa2	Custom User Session Report
<input type="checkbox"/>	Custom User Session Report	User Session	All Groups, Folders and SSIDs	-
<input type="checkbox"/>	Daily Capacity Planning Report	Capacity Planning	All Groups, Folders and SSIDs	Daily Capacity Planning Report
<input type="checkbox"/>	Daily Configuration Audit Report	Configuration Audit	All Groups, Folders and SSIDs	Daily Configuration Audit Report
<input type="checkbox"/>	Daily Device Summary Report	Device Summary	All Groups, Folders and SSIDs	Daily Device Summary Report
<input type="checkbox"/>	Daily Device Uptime Report	Device Uptime	All Groups, Folders and SSIDs	Daily Device Uptime Report
<input type="checkbox"/>	Daily Inventory Report	Inventory	All Groups and Folders	Daily Inventory Report
<input type="checkbox"/>	Daily Inventory Report - Detailed	Inventory	All Groups and Folders	-
<input type="checkbox"/>	Daily New Rogue Devices Report	New Rogue Devices	All Groups and Folders	Daily New Rogue Devices Report
<input type="checkbox"/>	Daily New Users Report	New Users	All Groups, Folders and SSIDs	Daily New Users Report
<input type="checkbox"/>	Daily PCI Compliance Report	PCI Compliance	All Groups, Folders and PCI Requirements	Daily PCI Compliance Report
<input type="checkbox"/>	Daily RADIUS Authentication Issues Report	RADIUS Authentication Issues	All Groups, Folders and SSIDs	Daily RADIUS Authentication Issues Report
<input type="checkbox"/>	Daily Uptime Report	Device Uptime	All Groups, Folders and SSIDs	Daily Uptime Report

Report Start	Report End	Last Run Time	Scheduled
2 months ago	now	4/17/2008 2:19 PM	-
1 day ago	now	1/12/2009 7:04 PM	-
1 day ago	now	1/15/2009 4:48 PM	-
1 month ago	now	1/19/2009 11:58 AM	-
1 day ago	now	6/13/2008 7:36 AM	-
1/5/2009	1/15/2009	1/15/2009 1:26 PM	-
2 months ago	now	6/26/2008 12:37 PM	-
1 day ago	now	1/14/2009 10:04 AM	-
2008-06-01	2008-06-30	7/2/2008 10:13 AM	-
12:00 a.m. yesterday	12:00 a.m. today	1/20/2009 12:15 AM	Daily at 12:15 am PST
12:00 a.m. yesterday	12:00 a.m. today	1/20/2009 12:15 AM	Daily at 12:15 am PST
12:00 a.m. yesterday	12:00 a.m. today	1/20/2009 12:15 AM	Daily at 12:15 am PST
12:00 a.m. yesterday	12:00 a.m. today	1/20/2009 12:15 AM	Daily at 12:15 am PST
12:00 a.m. yesterday	12:00 a.m. today	1/20/2009 12:15 AM	Daily at 12:15 am PST
-	-	12/12/2008 1:48 PM	-
12:00 a.m. yesterday	12:00 a.m. today	1/20/2009 12:15 AM	Daily at 12:15 am PST
12:00 a.m. yesterday	12:00 a.m. today	1/20/2009 12:15 AM	Daily at 12:15 am PST
12:00 a.m. yesterday	12:00 a.m. today	1/20/2009 12:15 AM	Daily at 12:15 am PST
12:00 a.m. yesterday	12:00 a.m. today	1/20/2009 12:15 AM	Daily at 12:15 am PST
12:00 a.m. yesterday	12:00 a.m. today	1/20/2009 12:15 AM	Daily at 12:15 am PST

Select All - Unselect All

Table 154 Report Definitions Page Fields and Descriptions

Field	Description
Generation Time	Displays the time OV3600 created the report.
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 Version 6.2.
Subject	Displays the scope of the report, to include groups, folders, SSIDs, or any combination of these that are included in the report.
Latest Report	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 and clicking Run .
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.
Last Run Time	Displays the date and time of the last time the report was run.
Scheduled	Displays the frequency in which the report is configured to be run.

Reports > Generated Page Overview

The **Reports > Generated** page displays reports that have been defined in the **Reports > Definitions** page. Additionally, this page enables you to display the most recent daily version of any report with a single click. 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 three primary sections, as follows:

- Generated reports configured for the current role
- Generated reports for other roles
- The option to view the latest daily reports with a single click for immediate online viewing

Figure 151 Reports > Generated Page Example

Generation Time	Title	Type	Subject	Report Start	Report End
<input type="checkbox"/> 1/19/2009 11:59 AM	Custom Network Usage Report	Network Usage	Groups Acme Corporation, Korea Regional Office, Outdoor	12/19/2008 11:58 AM	1/19/2009 11:58 AM
<input type="checkbox"/> 1/19/2009 9:02 AM	PCI Compliance Report	PCI Compliance	Folders Top > HQ, Top > Stores (and subfolders), Top > Training	1/5/2009 9:00 AM	1/19/2009 9:00 AM
<input type="checkbox"/> 1/19/2009 12:21 AM	Daily PCI Compliance Report	PCI Compliance	All Groups, Folders and PCI Requirements	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/19/2009 12:19 AM	Daily Inventory Report	Inventory	All Groups and Folders	1/19/2009 12:19 AM	-
<input type="checkbox"/> 1/19/2009 12:19 AM	Daily RADIUS Authentication Issues Report	RADIUS Authentication Issues	All Groups, Folders and SSIDs	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/19/2009 12:19 AM	Daily Device Uptime Report	Device Uptime	All Groups, Folders and SSIDs	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/19/2009 12:19 AM	Daily User Session Report	User Session	All Groups, Folders and SSIDs	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/19/2009 12:19 AM	Daily Configuration Audit Report	Configuration Audit	All Groups, Folders and SSIDs	1/19/2009 12:19 AM	-
<input type="checkbox"/> 1/19/2009 12:17 AM	Daily Device Summary Report	Device Summary	All Groups, Folders and SSIDs	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/19/2009 12:16 AM	IDS event yesterday	IDS Events	All Groups and Folders	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/19/2009 12:16 AM	Daily Capacity Planning Report	Capacity Planning	All Groups, Folders and SSIDs	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/19/2009 12:15 AM	Daily Uptime Report	Device Uptime	All Groups, Folders and SSIDs	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/19/2009 12:15 AM	Daily New Rogue Devices Report	New Rogue Devices	All Groups and Folders	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/19/2009 12:15 AM	Daily New Users Report	New Users	All Groups, Folders and SSIDs	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/19/2009 12:15 AM	Daily Wireless Network Usage Report	Network Usage	All Groups, Folders and SSIDs	1/18/2009 12:00 AM	1/19/2009 12:00 AM
<input type="checkbox"/> 1/18/2009 12:22 AM	Daily PCI Compliance Report	PCI Compliance	All Groups, Folders and PCI Requirements	1/17/2009 12:00 AM	1/18/2009 12:00 AM
<input type="checkbox"/> 1/18/2009 12:20 AM	Daily Inventory Report	Inventory	All Groups and Folders	1/18/2009 12:20 AM	-
<input type="checkbox"/> 1/18/2009 12:20 AM	Daily RADIUS Authentication Issues Report	RADIUS Authentication Issues	All Groups, Folders and SSIDs	1/17/2009 12:00 AM	1/18/2009 12:00 AM
<input type="checkbox"/> 1/18/2009 12:20 AM	Daily Device Uptime Report	Device Uptime	All Groups, Folders and SSIDs	1/17/2009 12:00 AM	1/18/2009 12:00 AM
<input type="checkbox"/> 1/18/2009 12:20 AM	Daily User Session Report	User Session	All Groups, Folders and SSIDs	1/17/2009 12:00 AM	1/18/2009 12:00 AM

Select All - Unselect All

Figure 152 Reports > Generated Page, Single-click Report Viewing Options

- Latest Capacity Planning Report
- Latest Configuration Audit Report
- Latest Device Summary Report
- Latest Device Uptime Report
- Latest IDS Events Report
- Latest Inventory Report
- Latest Memory and CPU Utilization Report
- Latest Network Usage Report
- Latest New Rogue Devices Report
- Latest New Users Report
- Latest PCI Compliance Report
- Latest RADIUS Authentication Issues Report
- Latest User Session Report



Clicking any report from the list shown in [Figure 152](#) displays the **Detail** page for the most recent version of that report.

Refer to “[Using Daily Reports in OV3600 6.2](#)” on page 238 for complete information and examples for the daily version of each report.

Viewing Reports

To display all reports that are currently configured on OV3600 6.2, navigate to the **Reports > Generated** page. You have two options for generating reports from this page, as follows:

- Use the list of generated reports on **Reports > Generated** to view details for each, or click **Add** to create new reports that appear on this page once configured. This method is described in this topic.
- Scroll to the bottom of the **Reports > Generated** page, and click any of the 13 report types to instantly view the most recent version of any given report. This method is described in “[Using Daily Reports in OV3600 6.2](#)” on page 238.

By default, the reports on the **Reports > Generated** page are sorted by **Generation Time**. Reports can be sorted by any other category (column header) in sequential or reverse sequential order. Additional guidelines for using this page are as follows:

- To view the details of a specific report, click the title of the report you wish to display. This launches the **Reports > Details** page. The content of the **Reports > Details** page varies significantly according to the type of report requested.

[Table 155](#) describes the contents and controls of the Reports > Generated page.

Table 155 Reports > Generated Fields and Descriptions

Field	Description
Device	Name of the device.
Group	The Name of the device's Group.
SNMP Uptime	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	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.

Table 155 Reports > Generated Fields and Descriptions (Continued)

Field	Description
Time Since Last Boot	The uptime as reported by the device at the end of the time period covered by the report.
Average Uptime by Group	Average uptime of all the devices in the group.
Total Average Uptime	Average uptime of all the devices OV3600 is monitoring or managing.
Rank	The devices in each section of the device Summary report are ranked by the title field of each section.
Name	Name of the device.
Unique Users	Number of unique MAC address that have associated to the device in the report period.
Max Simult.	The largest number of simultaneous users observed during the report period.
Total Traffic	Total amount of Traffic pushed during the report period in megabytes.
Average Bandwidth	The average bandwidth in kilobytes used on the device according to the device's bandwidth counters. Almost all of this is user traffic. On some devices multicast data is counted as well.
Interval	The interval is based on the amount of time covered in the report as well as the age of the data in the report. Reports over recent time periods will have much smaller intervals and contain more information than a report of similar length 6 months ago.
Connected Users	Average number of connected users during the interval.
Type	The make and model of the access point.
Version	Firmware version of the access point.
LAN IP	The IP of the Ethernet interface on the device.
LAN/RADIO MAC Address	The MAC address of the radio and interfaces.
Channel	The channel the device's radio is using.
Uptime	The uptime as reported by the device when the device Inventory report is generated. This time is independent of OV3600.
SSID	Service Set Identifier (SSID) set on the device.
Serial	Serial number of the device. Only reported for certain Proxim and Colubris APs.
Radio Serial	Radio serial number. Only reported for certain Proxim and Colubris APs.
Notes	Any notes entered into the APs/Devices > Manage interface.
Time Above x% of Capacity	The amount of time the radio or interface spent broadcasting above the capacity threshold given in the report definition.
Capacity Combined	The combined bandwidth per second for both in and out paths summed together.
Usage While > Threshold (Combined, In and Out)	The average percent usage during the time that the usage is over the defined threshold (for bandwidth in, out, and combined).
Overall Usage (Combined, In, Out)	The average percent usage during the entire time span of the report (for bandwidth in, out and combined).

Emailing and Exporting Reports

This section describes three ways in which distribute reports from OV3600 Version 6.2:

- [Emailing Reports in General Email Applications](#)
- [Emailing Reports to Smarthost](#)
- [Exporting Reports to XML](#)

Emailing Reports in General Email Applications

Perform these steps to set up email distribution of reports in OV3600 Version 6.2:

- 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 “[Creating and Running Custom Reports](#)” on page 235, and in “[Emailing Reports to Smarthost](#)” on page 234.

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

OV3600 allows users to export individual reports in XML (xhtml) form. These files may be read by an html browser or opened in Excel. Perform the following steps to export reports to XML and MS Excel:

1. Navigate to **Reports > Generated** page, and click the name of a previously defined report, or click the link for a daily report from the bottom of the page. The corresponding **Detail** page displays.
2. On the top right of the page, click **XML (XHTML) export**. The XML page appears after a moment. Allow a short period of time for the XML-compatible version of the page to display.
3. In your browser, click **File > Save as**. Define the filename and location, select **Web Page Complete**, then click **Save**. A brief **Save Webpage** status box appears to display the saving process. Allow the process some time, particularly for reports that contain a lot of links or large graphics.
4. Open MS Excel, and open the file. You may need to display **files of all type** to access the file.
5. Once the file is open in Excel, you may save it further as XML by clicking **File > Save As** and choosing XML as the file type.



This method of exporting files supports graphics and links, and prevents **Missing File C:\filename.css** error messages.

Creating and Running Custom Reports

Defining Custom Reports

OV3600 allows you to create reports 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 custom report, browse to the **Reports > Definition** page and click the **Add** button, or click the **pencil** icon to edit an existing report definition. [Figure 153](#) illustrates the **Add** report page.

Figure 153 Running a Custom Report with **Reports > Definitions, Add Button**

2. Complete the fields described in [Table 156](#) and 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 in OV3600 6.2](#)” on page 238.

Table 156 Fields and Settings of the **Report > Definitions > Add** Page

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.
Folder	All Folders	If Use selected groups is chosen, a menu with checkboxes appears, allowing you to choose the groups to include in the report.

Table 156 *Fields and Settings of the Report > Definitions > Add Page*

Field	Default	Description
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: <ul style="list-style-type: none"> • Current Local Time—Displays for reference the time of the OV3600 6.2 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	Selecting Yes for this option displays additional fields in which to specific email addresses for sender and recipients. Enter the Sender Address. The sender address is what appears in the From field of the report email. Enter recipient email addresses separated by commas when using multiple email addresses.

3. Click **Add and Run** to generate the report immediately, in addition to scheduling times that may be defined.
4. Click **Add (only)** to complete the report creation, to be run at the time scheduled.
5. Click **Cancel** to exit from the **Add** page.

Overview of Custom Reports and Scheduling Options

Table 157 describes the configurable settings for the custom report to be created.

Table 157 Report Types and Scheduling Options Supported for Custom Reports

Report Type	Can be Run by Time Period	Can be Run by Group/Folder	Description
Capacity Planning	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 (if Speed value).
Configuration Audit	No	Yes	Provides a snapshot of the configuration of all monitored access points in OV3600, at one specific point in time.
Device Summary	Yes	Yes	Summarizes user and bandwidth statistics and lists devices in OV3600.
Device Uptime	Yes	Yes	Summarizes device uptime within defined groups or folders.
IDS Events	Yes	Yes	Summarizes IDS events; can be limited to a summary of a certain number of events.
Inventory	No	Yes	Provides an audit of vendors, models and firmware versions of devices in OV3600.
Memory and CPU Utilization	Yes	Yes	Summarizes utilization for controllers for defined top number of devices; can be run with or without per-CPU details and details about device memory usage.
Network Usage	Yes	Yes	Summarizes bandwidth data and number of users.
New Rogue Devices	Yes	No	Shows new rogue devices by score, discovering AP, and MAC address vendor.
New Users	Yes	No	Provides a summary list of new users, including username, MAC address, discovering AP, and association time.
PCI Compliance	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.
RADIUS Authentication Issues	Yes	Yes	Summarizes RADIUS authentication issues by controller and by user, as well as a list of all issues.
User Session	Yes	Yes	Summarizes user data by radio mode, SSID and VLAN, as well as lists all sessions.

Using Daily Reports in OV3600 6.2

This section describes the reports supported in OV3600 Version 6.2. These reports can be accessed from the bottom of the **Reports > Generated** page, and are presented in alphabetical order as follows in [Table 158](#):

Table 158 Report Types in OV3600 6.2

Report and Links	Description
“Capacity Planning Report” on page 239	The Capacity Planning Report tracks bandwidth capacity and consumption according to thresholds for data throughput. This is a device-oriented report. To view the latest daily version of this report, see “Using the Most Recent Capacity Planning Report” on page 239 .
“Configuration Audit Report” on page 242	The Configuration Audit Report provides an inventory of network device configurations, enabling you to display information one device at a time, one folder at a time, or one device group at a time, or in complete device inventory. To view the latest daily version of this report, see “Using the Most Recent Configuration Audit Report” on page 242 .
“Device Summary Report” on page 243	The Device Summary Report identifies the most heavily used devices and the most under-used devices on the network. To view the latest daily version of this report, see “Using the Most Recent Device Summary Report” on page 243 .
“Device Uptime Report” on page 245	The Device Uptime Report monitors network performance and availability as measured by uptime. This report monitors uptime by multiple criteria, to include the following: <ul style="list-style-type: none"> • Total average uptime by SNMP and ICMP • Average uptime by device group • Average uptime by device folder To view the latest daily version of this report, see “Using the Most Recent Device Uptime Report” on page 245 .
“IDS Events Report” on page 246	The IDS Events Report lists and tracks IDS events on the network according to Access Point (AP) or controller device. To generate the latest daily version of this report, see “Using the Most Recent IDS Events Report” on page 246 .
“Inventory Report” on page 247	The Inventory Report itemizes all devices and firmware versions on the network, to include manufacturer information and graphical summary. To generate the latest daily version of this report, see “Using the Most Recent Inventory Report” on page 247 .
“Memory and CPU Utilization Report” on page 249	The Memory and CPU Utilization Report displays CPU and random access memory (RAM) utilization on the network by device and the top memory usage by device. To generate the latest daily version of this report, see “Using the Most Recent Memory and CPU Utilization Report” on page 249 .
“Network Usage Report” on page 251	The Network Usage Report contains network-wide information in three categories: <ul style="list-style-type: none"> • Bandwidth usage • Number of users by device (maximum and average) • Number of users by time period (to include average bandwidth in and out) To generate the latest daily version of this report, see “Using the Most Recent Network Usage Report” on page 251 .
“New Rogue Devices Report” on page 252	The New Rogue Devices Report summarizes rogue device information in a number of ways, to include time, associated AP, and additional parameters. To generate the latest daily version of this report, see “Using the Most Recent New Rogue Devices Report” on page 253 .

Table 158 Report Types in OV3600 6.2

Report and Links	Description
“New Users Report” on page 256	The New Users Report lists all new users that have appeared on the network during the time duration specified for the report. To generate the latest daily version of this report, see “Using the Most Recent New Users Report” on page 256 .
“PCI Compliance Report” on page 257	The PCI Compliance Report displays current PCI configurations and compliance status when OV3600 6.2 enables such monitoring on the network. To generate the latest daily version of this report, see “Using the Most Recent PCI Compliance Report” on page 257 .
“RADIUS Authentication Issues Report” on page 259	The RADIUS Authentication Issues Report contains issues that may appear with AP controllers, RADIUS Servers, and users. To generate the latest daily version of this report, see “Using the Most Recent RADIUS Authentication Issues Report” on page 259 .
“User Session Report” on page 260	The User Session Report tracks user-level activity by session. Session information can be established and tracked by multiple parameters. To generate the latest daily version of this report, see “Using the Most Recent User Session Report” on page 260 .

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. The information in this report can be sorted by any column header in sequential or reverse-sequential order by clicking the column heading.

To view the latest version of this report, refer to [“Using the Most Recent Capacity Planning Report” on page 239](#).

To create a generated report of this type, refer to [“Viewing Reports” on page 232](#).

Refer also to the [“Network Usage Report” on page 251](#) for additional bandwidth information.

Using the Most Recent Capacity Planning Report

Perform these steps to view the most recent **Reports > Generated > Capacity Planning Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Latest Capacity Report** to display **Detail** device capacity information for all devices. The ensuing **Detail** report provides multiple links to additional device configuration or information display pages.

The following figures and [Table 159](#) illustrate and describe the contents of the **Capacity Planning Report**.

Figure 154 OV3600 6.2 Capacity Planning Report, Top Section

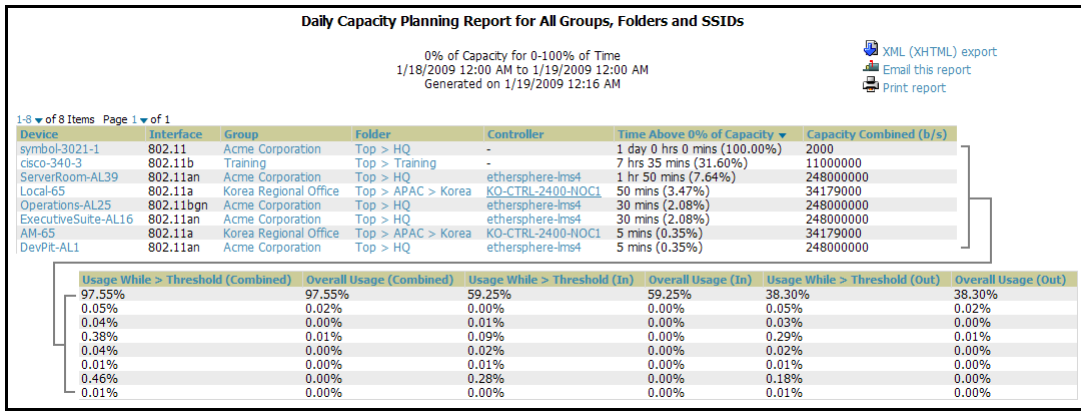


Figure 155 OV3600 6.2 Capacity Planning Report, Graphic Sections



Figure 156 OV3600 6.2 Capacity Planning Report, Bottom Section

1-20 of 2304 Items Page 1 of 116 > > |

Device	Interface	Group	Folder	Controller	Interval	Usage (Combined)	Usage (In)	Usage (Out)	MB In	MB In	MB Out
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 1:00 AM - 1/18/2009 1:05 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 1:35 AM - 1/18/2009 1:40 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:30 AM - 1/18/2009 12:35 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:55 AM - 1/18/2009 1:00 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 1:15 AM - 1/18/2009 1:20 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 1:30 AM - 1/18/2009 1:35 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:10 AM - 1/18/2009 12:15 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:25 AM - 1/18/2009 12:30 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:45 AM - 1/18/2009 12:50 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:50 AM - 1/18/2009 12:55 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 1:05 AM - 1/18/2009 1:10 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 1:10 AM - 1/18/2009 1:15 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 1:20 AM - 1/18/2009 1:25 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 1:25 AM - 1/18/2009 1:30 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:00 AM - 1/18/2009 12:05 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:05 AM - 1/18/2009 12:10 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:15 AM - 1/18/2009 12:20 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:20 AM - 1/18/2009 12:25 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:35 AM - 1/18/2009 12:40 AM	0%	0%	0%	0.00	0.00	0.00
AM-65	802.11a	Korea Regional Office	Top > APAC > Korea	KO-CTRL-2400-NOCI	1/18/2009 12:40 AM - 1/18/2009 12:45 AM	0%	0%	0%	0.00	0.00	0.00

Table 159 *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 0% 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.
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.

Table 160 *Capacity Planning Report Fields and Contents, Bottom 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.
Interval	Displays the time period in which device capacity metrics were monitored for this report.
Usage (Combined)	Displays device usage for combined incoming and outgoing data.
Usage (In)	Displays device usage for incoming data.
Usage (Out)	Displays device usage for outgoing data.
MB In	Displays the incoming data in megabytes.
MB Out	Displays the outgoing data in megabytes.

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.

To view the latest version of this report, refer to “[Using the Most Recent Configuration Audit Report](#)” on page 242.

To create a new generated report of this type, refer to “[Viewing Reports](#)” on page 232.

Using the Most Recent Configuration Audit Report

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 157](#) and [Table 161](#) illustrate and describe the general **Configuration Audit** report and related contents.

Figure 157 *Reports > Generated, Daily Configuration Audit Report, Abbreviated Example*

Daily Configuration Audit Report for All Groups, Folders and SSIDs																											
Generated on 1/19/2009 12:19 AM			XML (XHTML) export Email this report Print report																								
1-20 of 23 Items Page 1 of 2 > >																											
Name ▲	Folder	Group	Mismatches																								
1250-91:14:1a-TA20884	Top > HQ > Lab	Acme Corporation	<table border="1"> <thead> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Channel Assignment Method</td> <td>Custom</td> <td>Global</td> </tr> <tr> <td>Location</td> <td>Loc20884</td> <td>some location</td> </tr> <tr> <td>Power Level Assignment Method</td> <td>Custom</td> <td>Global</td> </tr> <tr> <td>Primary Controller</td> <td>Cisco-IWLC-1</td> <td>HQ-controller</td> </tr> <tr> <td>Radio Enabled</td> <td>No</td> <td>Yes</td> </tr> <tr> <td>Secondary Controller</td> <td>airespace-4400-1</td> <td>(empty string)</td> </tr> <tr> <td>Tertiary Controller</td> <td>Cisco2000</td> <td>(empty string)</td> </tr> </tbody> </table>		Current Device Configuration	Desired Device Configuration	Channel Assignment Method	Custom	Global	Location	Loc20884	some location	Power Level Assignment Method	Custom	Global	Primary Controller	Cisco-IWLC-1	HQ-controller	Radio Enabled	No	Yes	Secondary Controller	airespace-4400-1	(empty string)	Tertiary Controller	Cisco2000	(empty string)
	Current Device Configuration	Desired Device Configuration																									
Channel Assignment Method	Custom	Global																									
Location	Loc20884	some location																									
Power Level Assignment Method	Custom	Global																									
Primary Controller	Cisco-IWLC-1	HQ-controller																									
Radio Enabled	No	Yes																									
Secondary Controller	airespace-4400-1	(empty string)																									
Tertiary Controller	Cisco2000	(empty string)																									

Table 161 *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.

Device Summary Report

The **Device Summary Report** identifies devices that are the most or least used devices. One potential use of this report is to establish more equal bandwidth distribution across multiple devices. This report contains the following lists of such devices:

- **Most Utilized by Maximum Number of Users**—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**—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**—This list displays the 10 devices that are the least used, according to the number of users.
- **Least Utilized by Bandwidth**—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 these four categories in the **Reports > Definitions > Add** page.

The **Devices** section of this report includes a list of all devices, and can be sorted by any of the columns in the section, in order of appearance:

- 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.

To view the latest version of this report, refer to [“Using the Most Recent Device Summary Report” on page 243](#).

To create a generated or custom report of this type, refer to [“Viewing Reports” on page 232](#).

Using the Most Recent Device Summary Report

Perform these steps to view the most recent version of the 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 Reports” on page 232](#).

Figure 158 and Table 162 illustrate and describe the Reports > Generated > Device Summary Detail page.

Figure 158 Reports > Generated, Daily Device Summary Report (Shortened for Space)

Daily Device Summary Report for All Groups, Folders and SSIDs									
1/19/2009 12:00 AM to 1/20/2009 12:00 AM Generated on 1/20/2009 12:18 AM									
XML (XHTML) 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	Controller	Folder	Group
1	ethersphere-lms4	0	52	0.00	0.00	1344 Rack 2	-	Top > HQ	Acme Corporation
2	Operations-AL25	45	21	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
3	ExecutiveSuite-AL16	47	20	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
4	BaDev-AL12	54	19	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
5	DevPE-AL1	46	16	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
6	Sales-AL7	29	12	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
7	Legal-AL21	30	12	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
8	AL19	27	9	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
9	Finance-AL27	22	9	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
10	StorageRooms-AL5	25	7	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
Most Utilized by Bandwidth									
Rank ▲	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Controller	Folder	Group
1	FrontDesk-AP125-AM	0	0	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
2	FishBowlEast-AL40	4	3	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
3	11.1.5	1	0	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
4	FishBowlEast-AL400	0	0	0.00	0.00	-	ethersphere-lms4	Top > HQ	Acme Corporation
5	11.1.4	1	1	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
6	AL36	0	0	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
7	TrainingCenter-AL31	8	5	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
8	FishBowlEast-AL401	0	0	0.00	0.00	-	ethersphere-lms4	Top > HQ	Acme Corporation
9	StorageRooms-AL5	25	7	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
10	FishBowlEast-AL402	0	0	0.00	0.00	-	ethersphere-lms4	Top > HQ	Acme Corporation
Least Utilized by Maximum Number of Simultaneous Users									
Rank ▲	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Controller	Folder	Group
1	HQZ-4400-CTRL-NOC2	0	0	0.00	0.00	Nate	-	Top > HQ > Lab	Acme Corporation
2	Router	0	0	0.00	0.00	-	-	Top > Stores	Acme Corporation
3	FrontDesk-AP125-AM	0	0	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
4	SV-1252-SHIP-22:60	0	0	0.00	0.00	-	-	Top > HQ > Lab	Acme Corporation
5	TrainingCenter-AL32	0	0	0.00	0.00	-	ethersphere-lms4	Top > HQ	Acme Corporation
6	AL36	0	0	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
7	11.1.5	1	0	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
8	SV-1253-SHIP-22:00	0	0	0.00	0.00	-	ethersphere-lms4	Top > HQ	Acme Corporation
9	TrainingCenter-AL33	0	0	0.00	0.00	-	ethersphere-lms4	Top > HQ	Acme Corporation
10	symbol-4131-3	0	0	0.00	0.00	-	-	Top > HQ > Lab	Acme Corporation
Least Utilized by Bandwidth									
Rank ▲	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Controller	Folder	Group
1	FrontDesk-AP125-AM	0	0	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
2	FishBowlEast-AL40	4	3	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
3	11.1.5	1	0	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
4	SV-1252-SHIP-22:60	0	0	0.00	0.00	-	ethersphere-lms4	Top > HQ	Acme Corporation
5	11.1.4	1	1	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation
6	AL36	0	0	0.00	0.00	Not Available	ethersphere-lms4	Top > HQ	Acme Corporation

Table 162 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.
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.

Device Uptime Report

The **Device Uptime Report** monitors network performance and availability, 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

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.

To view the latest version of this report, refer to [“Using the Most Recent Device Uptime Report” on page 245](#).

To create a generated report of this type, refer to [“Viewing Reports” on page 232](#).

Using the Most Recent Device Uptime 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. You can use this report as the central starting point to improve uptime by multiple criteria.
3. To generate more reports of this type that cover a greater span of time, refer to [“Using Daily Reports in OV3600 6.2” on page 238](#).

Figure 158 and Table 162 illustrate and describe the **Reports > Generated > Device Uptime Detail** page.

Figure 159 Reports > Generated > Device Uptime Report

Daily Device Uptime Report for All Groups, Folders and SSIDs

1/19/2009 12:00 AM to 1/20/2009 12:00 AM
Generated on 1/20/2009 12:20 AM

XML (XHTML) export
Email this report
Print report

Total Average Uptime

SNMP Uptime	ICMP Uptime
75.92%	79.18%

Average Uptime by Group

1-5 of 5 Groups Page 1 of 1

Group	SNMP Uptime	ICMP Uptime
Acme Corporation	73.88%	76.66%
Korea Regional Office	100.00%	100.00%
Outdoor	100.00%	100.00%
Routers/Switches	100.00%	100.00%
Training	88.58%	99.69%

Average Uptime by Folder

1-7 of 7 Folders Page 1 of 1

Folder	SNMP Uptime	ICMP Uptime	SNMP Uptime (incl. subfolders)	ICMP Uptime (incl. subfolders)
Top > APAC > Korea	100.00%	100.00%	100.00%	100.00%
Top > HQ	88.85%	88.85%	73.49%	76.63%
Top > HQ > Lab	55.51%	62.33%	55.51%	62.33%
Top > Outdoor	62.50%	62.50%	62.50%	62.50%
Top > Stores	100.00%	100.00%	100.00%	100.00%
Top > Stores > Flagship	100.00%	100.00%	100.00%	100.00%
Top > Training	88.58%	99.69%	88.58%	99.69%

Table 163 Reports > Generated > Device Uptime Report Fields and Descriptions

Field	Description
Total Average Uptime	This section displays the average uptime for SNMP and ICMP. This information is an average across the network, accounting for all groups and folders on the network. Additional information for each group or folder is available elsewhere in this report.
Average Uptimes by Group	This section displays SNMP and ICMP uptime averages for each group on the network. Clicking any group in this section takes you to the Groups > Monitor page for additional group information.
Average Uptimes by Folder	This section displays SNMP and ICMP uptime averages according to device folders and sub-folders. Clicking any folder in this section takes you to the APs/Devices > List page for additional folder information.

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.

To view the latest version of this report, refer to “[Using the Most Recent IDS Events Report](#)” on page 246.

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 219 for additional information.

To create a generated report of this type, refer to “[Viewing Reports](#)” on page 232.

Using the Most Recent IDS Events Report

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 158](#) and [Table 162](#) illustrate and describe the **Reports > Generated > IDS Events Detail** page.

Figure 160 Reports > Generated > IDS Events Detail

IDS event yesterday for All Groups and Folders			
1/19/2009 12:00 AM to 1/20/2009 12:00 AM Generated on 1/20/2009 12:17 AM			
XML (XHTML) export Email this report Print report			
Top IDS Events by AP			
AP	Total Events ▲	First Event	Most Recent Event
FishBowEast-AL40	2	1/19/2009 5:12 PM	1/19/2009 5:12 PM
Area51-AL33	2	1/19/2009 5:11 PM	1/19/2009 5:11 PM
AL4	2	1/19/2009 5:11 PM	1/19/2009 5:11 PM
BizDev-AL12	2	1/19/2009 5:11 PM	1/19/2009 5:11 PM
FishBowWest-AL42	2	1/19/2009 9:34 AM	1/19/2009 9:34 AM
Marketing-AL10	2	1/19/2009 5:11 PM	1/19/2009 5:11 PM
AL35	2	1/19/2009 5:12 PM	1/19/2009 5:12 PM
ExecutiveSuite-AL16	2	1/19/2009 5:11 PM	1/19/2009 5:11 PM
AL36	2	1/19/2009 5:11 PM	1/19/2009 5:11 PM
Corp1344-SW-AP85	18	1/19/2009 1:44 AM	1/19/2009 10:37 PM
10 Top IDS Events by AP			
Top IDS Events by Controller			
Controller	Total Events ▲	First Event	Most Recent Event
ethersphere-lms4	49	1/19/2009 1:44 AM	1/19/2009 10:37 PM

Table 164 Reports > Generated > IDS Events Detail

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.
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.
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.

Inventory Report

The **Inventory Report** itemizes all devices and firmware versions on the network, to include manufacturer information and graphical pie-chart summaries. The primary sections of this report are as follows:

- **Vendor Summary**—Lists the manufacturers 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.

To view the latest version of this report, refer to “[Using the Most Recent Inventory Report](#)” on page 247.

To create a generated report of this type, refer to “[Viewing Reports](#)” on page 232.

Using the Most Recent Inventory Report

Perform these steps to view the most recent version of the **Inventory** report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Daily Inventory Report** to display report **Detail** information.
3. The **Details** page allows you to view device or other information by clicking the device name, IP address, MAC Address, Group, Folder, or associated controller links.

The figures that immediately follow illustrate the **Reports > Generated > Inventory Detail** page.

Figure 161 Vendor Summary Section of Reports > Generated > Inventory Report

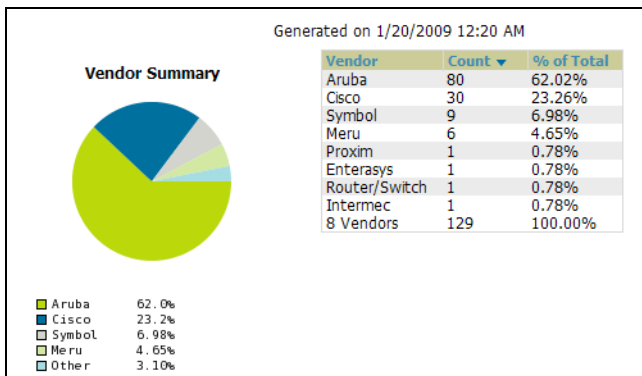


Figure 162 Model Summary Section of Reports > Generated > Inventory Report

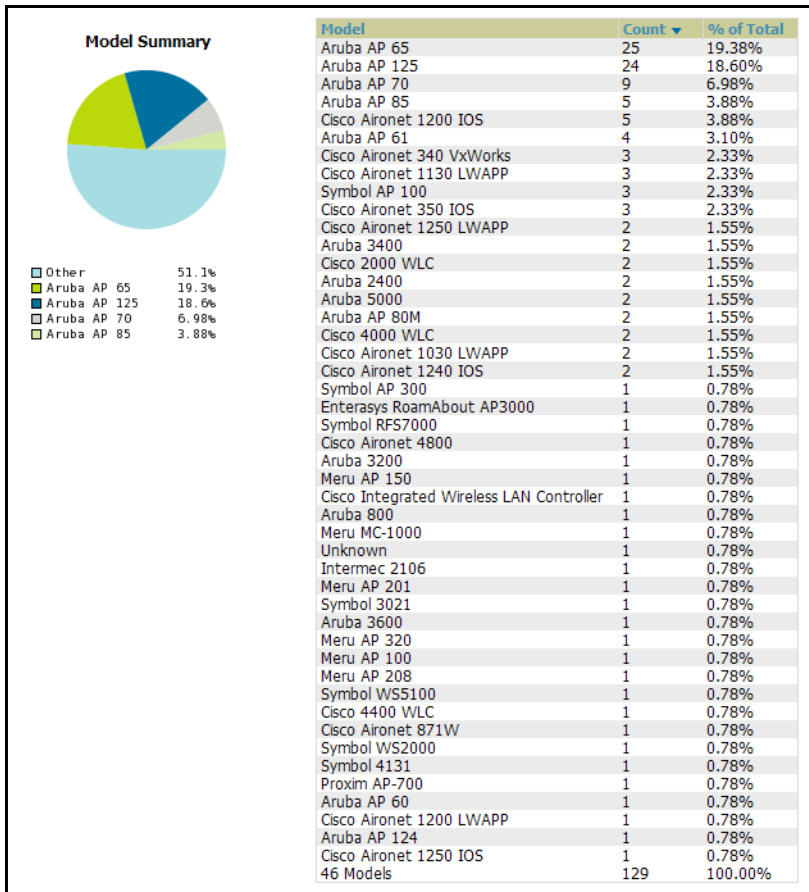


Figure 163 Firmware Version Summary Section of Reports > Generated > Inventory Report

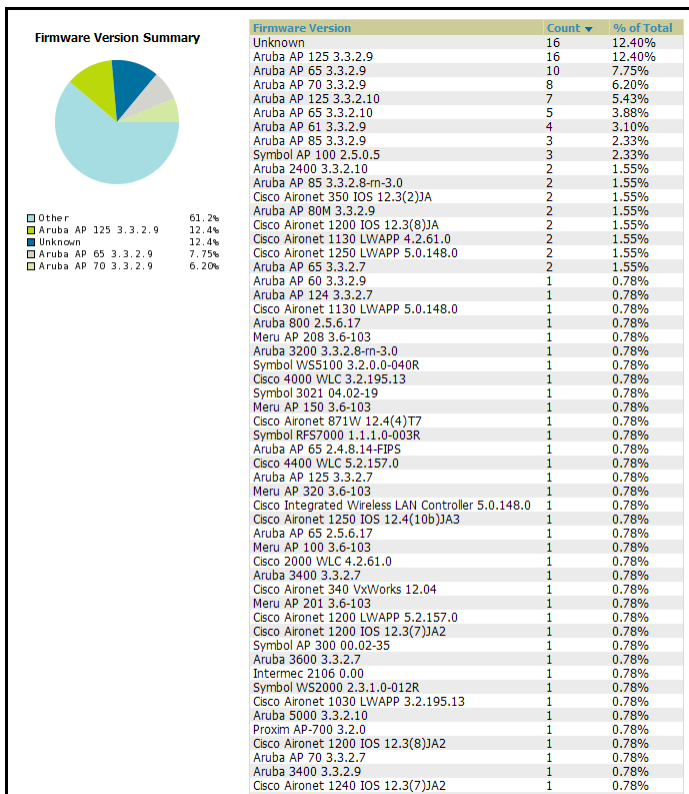


Figure 164 APs/Devices Section of Reports > Generated > Inventory Report (Split View)

APs/Devices								
1-20 of 129 APs/Devices Page 1 of 7 > >								
Name ▲	Type	Version	IP Address	LAN MAC Address	Group	Folder	Controller	
00:0b:00:0b:00:0b	Aruba AP 85	3.3.2.8-rn-3.0	11.10.10.10	00:08:00:08:00:08	Acme Corporation	Top > HQ > Lab	Aruba3200	
00:0b:86:00:0b:86	Aruba AP 65	3.3.2.10	11.10.10.21	00:08:86:00:08:86	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:cd:ce:ce:ce	Aruba AP 65	3.3.2.10	11.10.10.11	00:08:CD:CE:CE:CE	Acme Corporation	Top > HQ	ethersphere-lms4	
00:1a:1e:1a:1e:c0	Aruba AP 125	3.3.2.7	11.10.10.22	00:1A:1E:1A:1E:C0	Acme Corporation	Top > HQ > Lab	Aruba-3400	
00:0b:00:0b:00:0b	Aruba AP 124	3.3.2.7	11.10.10.12	00:08:00:08:00:08	Acme Corporation	Top > HQ > Lab	ethersphere-lms4	
00:0b:86:00:0b:86	Aruba AP 65	3.3.2.10	11.10.10.23	00:08:86:00:08:86	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:cd:ce:ce:ce	Aruba AP 65	-	11.10.10.13	00:08:CD:CE:CE:CE	Acme Corporation	Top > HQ	ethersphere-lms4	
00:1a:1e:1a:1e:c0	Aruba AP 65	-	11.10.10.24	00:1A:1E:1A:1E:C0	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:00:0b:00:0b	Aruba AP 65	-	11.10.10.14	00:1A:1E:C6:5E:58	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:86:00:0b:86	Aruba AP 65	-	11.10.10.25	00:1A:1E:C6:5E:60	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:cd:ce:ce:ce	Aruba AP 65	-	11.10.10.15	00:08:00:08:00:08	Acme Corporation	Top > HQ	ethersphere-lms4	
00:1a:1e:1a:1e:c0	Aruba AP 65	-	11.10.10.26	00:08:86:00:08:86	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:00:0b:00:0b	Aruba AP 61	3.3.2.9	11.10.10.16	00:08:CD:CE:CE:CE	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:86:00:0b:86	Aruba AP 61	3.3.2.9	11.10.10.27	00:1A:1E:1A:1E:C0	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:cd:ce:ce:ce	Aruba AP 61	3.3.2.9	11.10.10.17	00:08:00:08:00:08	Acme Corporation	Top > HQ	ethersphere-lms4	
00:1a:1e:1a:1e:c0	Aruba AP 61	3.3.2.9	11.10.10.28	00:08:86:00:08:86	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:00:0b:00:0b	Aruba AP 70	3.3.2.9	11.10.10.18	00:08:00:08:00:08	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:86:00:0b:86	Aruba AP 70	3.3.2.9	11.10.10.29	00:08:86:00:08:86	Acme Corporation	Top > HQ	ethersphere-lms4	
00:0b:cd:ce:ce:ce	Cisco Aironet 1250 LWAPP	5.0.148.0	11.10.10.19	00:08:CD:CE:CE:CE	Acme Corporation	Top > HQ > Lab	Cisco-IWLC-1	
00:1a:1e:1a:1e:c0	Cisco 4000 WLC	-	11.10.10.30	00:1A:1E:1A:1E:C0	Acme Corporation	Top > HQ > Lab	-	

Uptime	Location	Contact	Serial	First Radio MAC Address	Ch	SSID	Serial	Second Radio MAC Address	Ch	SSID	Notes
-	Not Available	-	AB0000000	00:08:86:9A:F1:20	-	-	-	00:08:86:9A:F1:28	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
5 hrs 16 mins	Not Available	-	AD0000638	00:1A:1E:1A:1E:81	0	-	-	-	-	-	-
7 hrs 47 mins	Not Available	-	AD0000000	00:1A:1E:81:B3:10	0	-	-	00:1A:1E:80:B3:80	0	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
5 hrs 8 mins	Not Available	-	A30000000	00:08:86:08:86:A1	48	-	-	-	-	-	-
5 hrs 9 mins	Not Available	-	A30000630	00:1A:1E:1A:1E:81	48	-	-	-	-	-	-
5 hrs 9 mins	Not Available	-	A30010000	00:08:86:08:86:A1	40	-	-	-	-	-	-
5 hrs 9 mins	Not Available	-	A30000063	00:1A:1E:1A:1E:81	149	-	-	-	-	-	-
5 hrs 10 mins	Not Available	-	A50040000	00:08:86:08:86:A1	6	-	-	00:08:86:08:86:A1	40	-	-
5 hrs 10 mins	Not Available	-	A50030063	00:1A:1E:1A:1E:81	6	-	-	00:1A:1E:1A:1E:81	149	-	-
6 days 12 hrs 41 mins	Loc20884	-	FTX1100001E	00:08:86:08:86:A1	11	-	-	00:08:86:08:86:A1	149	-	-
-	-	-	-	-	-	-	-	-	-	-	-

Memory and CPU Utilization Report

The **Memory and CPU Utilization Report** displays the top memory usage by device, and CPU utilization on the network by device. The usage for any given resource, whether CPU or RAM usage, is listed as a percentage.

To view the latest version of this report, refer to “Using the Most Recent Memory and CPU Utilization Report” on page 249.

To create a generated report of this type, refer to “Using Daily Reports in OV3600 6.2” on page 238.

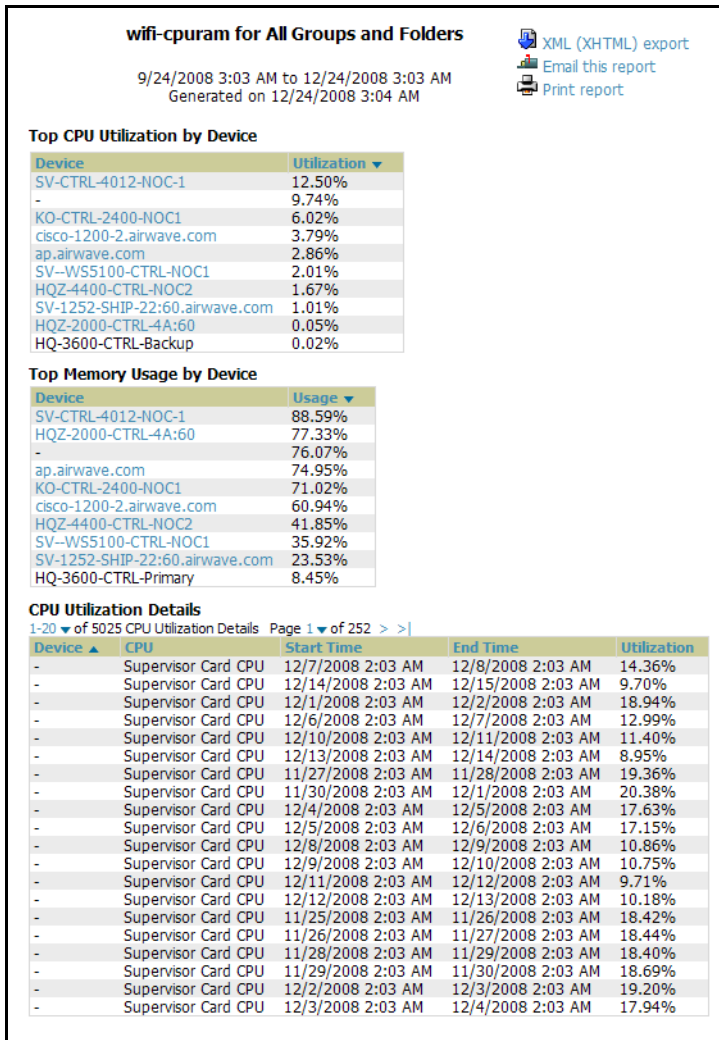
Using the Most Recent Memory and CPU Utilization Report

Perform these steps to view the most recent version of the **Memory and CPU Utilization Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Daily Memory and CPU Utilization** to display report **Detail** information.
3. The **Details** 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 165 illustrates the **Reports > Generated > Daily Memory and CPU Utilization Detail** page.

Figure 165 Reports > Generated > Daily Memory and CPU Utilization Details



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

To view the latest version of this report, refer to “[Using the Most Recent Memory and CPU Utilization Report](#)” on page 249.

To create a generated report of this type, refer to “[Using Daily Reports in OV3600 6.2](#)” on page 238.

Using the Most Recent Network Usage Report

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 **Details** page allows you to view bandwidth and device usage in three sections, illustrated below.

[Figure 165](#) illustrates the **Reports > Generated > Daily Memory and CPU Utilization Detail** page.

Figure 166 *Bandwidth Usage Information in Reports > Generated > Network Usage*

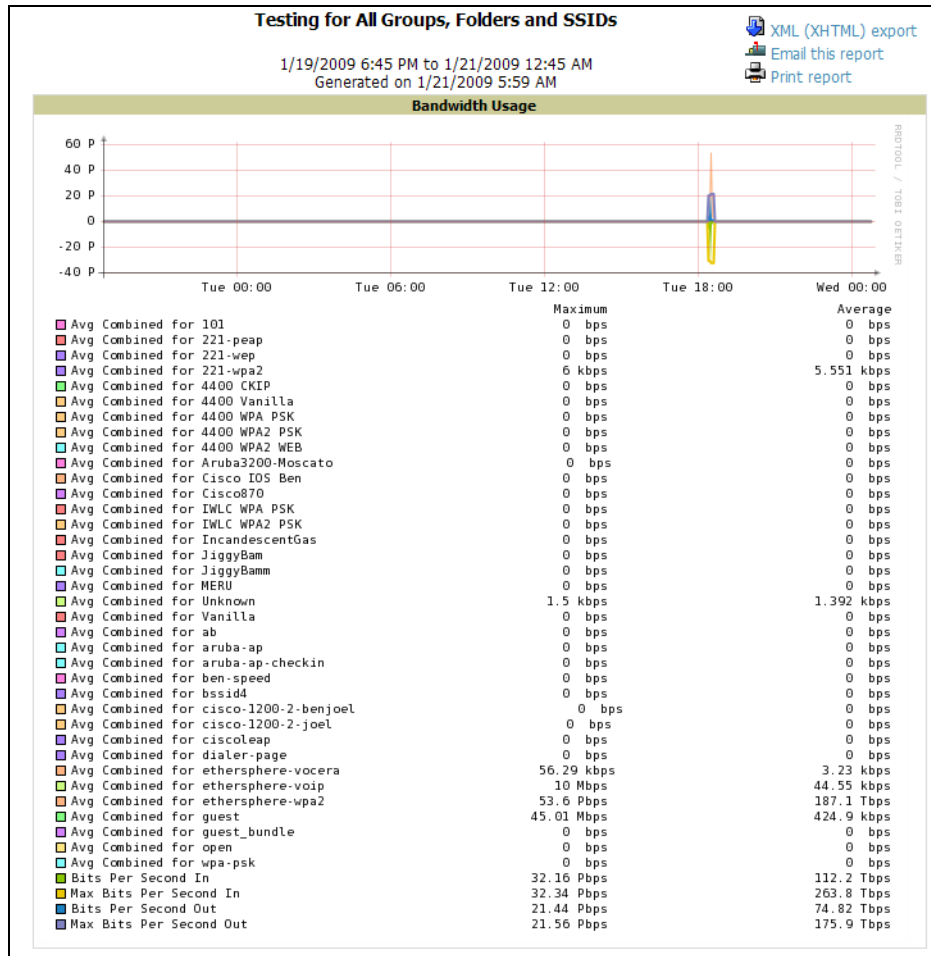


Figure 167 Number of Users Information in Reports > Generated > Network Usage

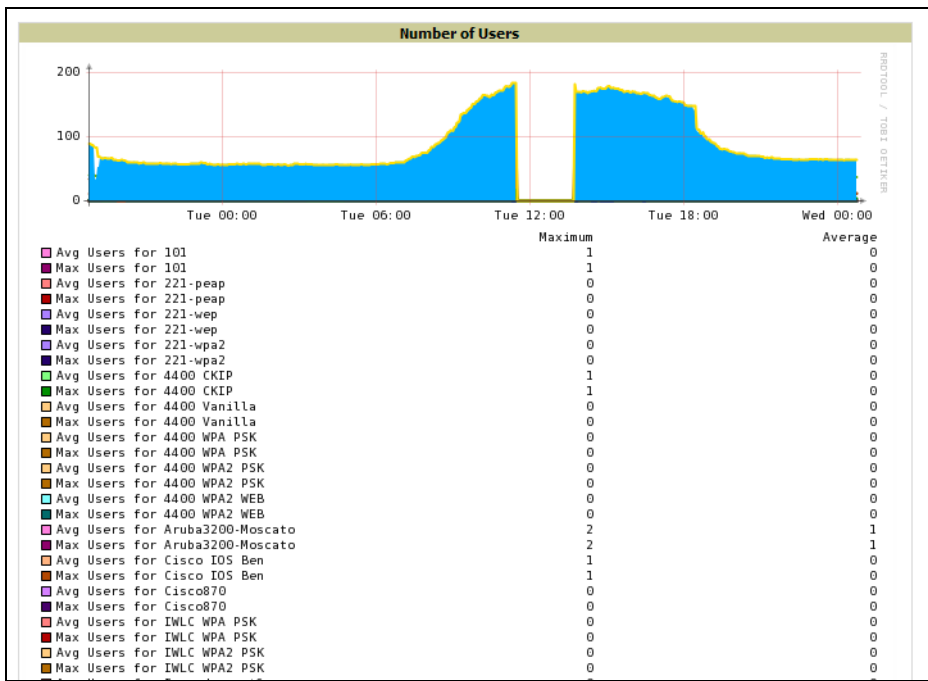


Figure 168 Number of Users and Bandwidth Usage Information by Time Period

Interval	Average Number of Users	Average Bandwidth In (kbps)	Average Bandwidth Out (kbps)
1/19/2009 6:45 PM - 1/19/2009 6:50 PM	87	281.68	492.05
1/19/2009 6:50 PM - 1/19/2009 6:55 PM	84	282.78	460.56
1/19/2009 6:55 PM - 1/19/2009 7:00 PM	82	266.45	433.86
1/19/2009 7:00 PM - 1/19/2009 7:05 PM	32	543.75	610.23
1/19/2009 7:05 PM - 1/19/2009 7:10 PM	51	7813.17	7917.09
1/19/2009 7:10 PM - 1/19/2009 7:15 PM	67	170.57	290.27
1/19/2009 7:15 PM - 1/19/2009 7:20 PM	66	65.97	187.36
1/19/2009 7:20 PM - 1/19/2009 7:25 PM	66	66.25	186.18
1/19/2009 7:25 PM - 1/19/2009 7:30 PM	66	64.49	184.99
1/19/2009 7:30 PM - 1/19/2009 7:35 PM	66	65.49	183.88
1/19/2009 7:35 PM - 1/19/2009 7:40 PM	64	77.38	189.21
1/19/2009 7:40 PM - 1/19/2009 7:45 PM	64	102.13	192.33
1/19/2009 7:45 PM - 1/19/2009 7:50 PM	62	81.16	342.63
1/19/2009 7:50 PM - 1/19/2009 7:55 PM	62	68.57	254.22
1/19/2009 7:55 PM - 1/19/2009 8:00 PM	63	66.91	204.22
1/19/2009 8:00 PM - 1/19/2009 8:05 PM	62	64.52	193.06
1/19/2009 8:05 PM - 1/19/2009 8:10 PM	61	63.83	188.02
1/19/2009 8:10 PM - 1/19/2009 8:15 PM	61	63.33	185.20
1/19/2009 8:15 PM - 1/19/2009 8:20 PM	60	63.07	185.46
1/19/2009 8:20 PM - 1/19/2009 8:25 PM	59	63.12	185.64

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:

- Graphical summary of rogue devices by score and by classification
- Rogue devices according to the AP device that discovers them and by signal strength
- Rogue devices by MAC address information
- A complete summary of the number of rogue devices, discovery events, discovery averages, and rogue device signal quality
- Rogue devices discovered by wireless scan
- Rogue devices by device name, with comprehensive device parameters

To view the latest version of this report, refer to [“Using the Most Recent New Rogue Devices Report”](#) on page 253.

To create a generated report of this type, refer to [“Viewing Reports”](#) on page 232.

Using the Most Recent New Rogue Devices Report

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 **New Rogue Devices** to display report **Detail** information.
3. The **Details** 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 169 *Reports > Generated > New Rogue Devices, Score and Classification Graphs*

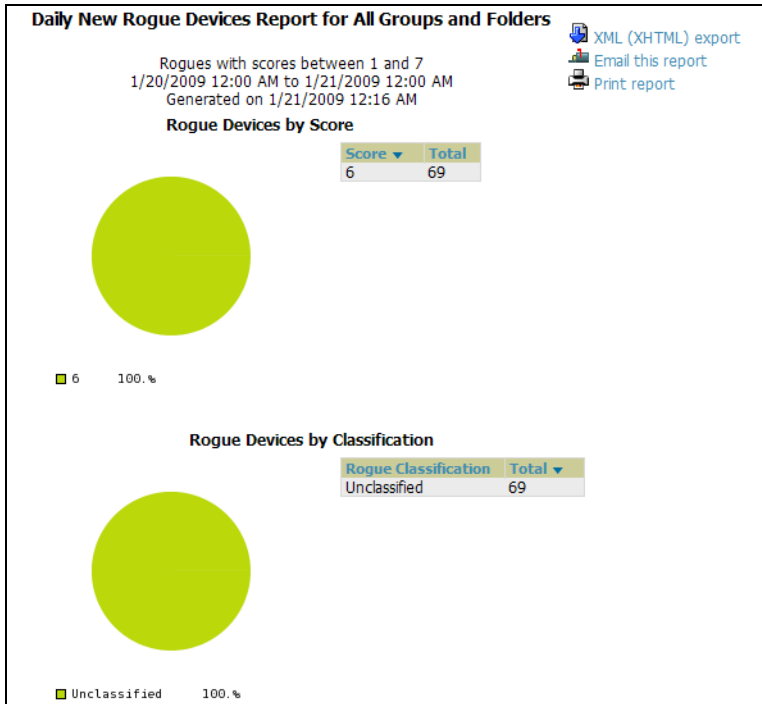


Figure 170 *Reports > Generated > New Rogue Devices, Discovering APs and Signal Strength*

Top Rogue Devices by Number of Discovering APs		Top Rogue Devices by Signal Strength	
Name	Total Discovering APs	Name	Signal
Aruba Netw-84:99:02	13	Cisco Syst-A7:B9:EE	-35
Aruba Netw-84:99:12	13	Cisco-49:08:3E	-41
Aruba Netw-84:9C:63	12	Aruba Netw-94:D1:62	-54
Aruba Netw-98:14:F3	12	Aruba Netw-98:14:E3	-56
Cisco-49:08:3E	12	Aruba Netw-84:9A:A0	-57
Cisco Syst-A7:B9:EE	11	Aruba Netw-84:99:02	-59
Aruba Netw-94:CF:12	11	Aruba Netw-84:50:E3	-59
Aruba Netw-98:14:E3	10	Aruba Netw-94:CF:02	-60
Aruba Netw-84:50:E2	10	Aruba Netw-84:50:E2	-60
Aruba Netw-84:50:F2	10	Aruba Netw-99:83:01	-62

Figure 171 Reports > Generated > New Rogue Devices, MAC Address Graphs

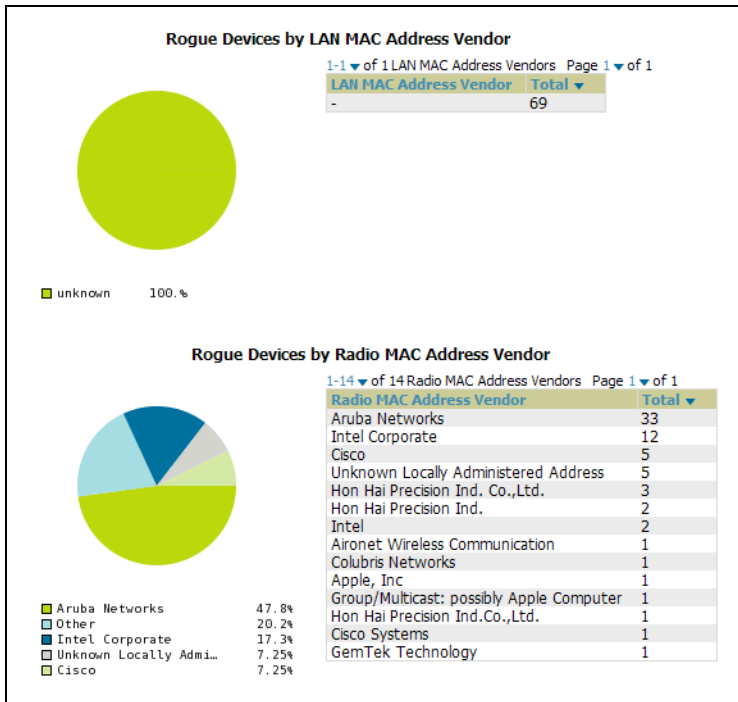


Figure 172 Reports > Generated > New Rogue Devices, Summary and Wireless Scans

Summary	
Total number of rogues:	69
Total number of discovery events:	304
Average number of discovery events per rogue:	4.41
Average signal quality:	-68.91

Rogue Devices Discovered via Wireless Scans

1-20 of 69 Rogue Devices Page 1 of 4 > >

Name	Classification	Ack	Score	First Discovered	First Discovery Method	First Discovery Agent	Last Discovering AP	Type	Operating System	IP Address	SSID	Network Type	Channel
Aruba Netw-87:EC:90	Unclassified	No	6	1/20/2009 8:56 PM	Wireless AP scan	SW-2	SW-2	-	-	-	-	AP	36
Cisco-DE:16:F1	Unclassified	No	6	1/20/2009 7:32 PM	Wireless AP scan	11.1.5	11.1.5	-	-	-	chatter	AP	11
Cisco-DE:16:F2	Unclassified	No	6	1/20/2009 7:32 PM	Wireless AP scan	11.1.5	11.1.5	-	-	-	unplugged	AP	11
Cisco-SB:F7:73	Unclassified	No	6	1/20/2009 7:32 PM	Wireless AP scan	11.1.5	11.1.5	-	-	-	roamer	AP	1
Cisco-DE:16:F0	Unclassified	No	6	1/20/2009 7:32 PM	Wireless AP scan	11.1.5	11.1.5	-	-	-	-	AP	11
Aruba Netw-61:1D:F0	Unclassified	No	6	1/20/2009 6:55 PM	Wireless AP scan	SW-2	SW-2	-	-	-	aruba-ap	AP	36
Aruba Netw-84:9C:63	Unclassified	No	6	1/20/2009 2:46 PM	Wireless AP scan	aruba-ap85-cl:ad:13	00:1a:1e:00:1a:1e	-	-	-	student19	AP	1
Colubris N-C7:D9:30	Unclassified	No	6	1/20/2009 8:53 AM	Wireless AP scan	Local-65	AM-65	-	-	-	OfficeBizk	AP	8
Aruba Netw-B0:00:58	Unclassified	No	6	1/20/2009 9:32 AM	Wireless AP scan	SW-2	SW-2	-	-	-	sw_sathish_tk	AP	149
Unknown Lo-68:67:7C	Unclassified	No	6	1/20/2009 9:09 AM	Wireless AP scan	rfs	rfs	-	-	-	-	AP	6
Unknown Lo-00:00:00	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-2	AP-2	-	-	-	-	Unknown	6
Group/Mult-FF:FF:FF	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-2	AP-2	-	-	-	-	Unknown	153
Unknown Lo-00:00:00	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-2	AP-2	-	-	-	□US □ □	Unknown	6
Unknown Lo-00:00:00	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-2	AP-2	-	-	-	-	Unknown	6
Hon Hai Pr-C7:8D:5D	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-3	AP-5	-	-	-	-	Unknown	165
Intel Corp-91:67:03	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-1	AP-2	-	-	-	-	AP	149
Intel Corp-85:B7:B3	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-3	AP-3	-	-	-	-	Unknown	40
Intel Corp-08:FF:29	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-1	AP-5	-	-	-	-	Unknown	149
Intel Corp-09:20:ED	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-3	AP-1	-	-	-	-	AP	6
Intel Corp-08:B4:AA	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-5	AP-5	-	-	-	-	AP	0

WEP	RSSI	Signal	LAN MAC Address	LAN Vendor	Radio MAC Address	Radio Vendor	Switch/Router	Port	Last Seen	Total Discovering APs	Total Discovery Events
-	-	-	-	-	00:1A:1E:00:1A:1E	Aruba Networks	-	-	1/20/2009 8:56 PM	1	1
-	13	-82	-	-	00:0F:24:00:0F:24	Cisco	-	-	1/20/2009 11:53 PM	1	2
-	13	-83	-	-	00:1A:1E:00:1A:1E	Cisco	-	-	1/20/2009 8:04 PM	1	2
-	12	-82	-	-	00:0F:24:00:0F:24	Cisco	-	-	1/20/2009 11:53 PM	1	2
-	-	-	-	-	00:1A:1E:00:1A:1E	Cisco	-	-	1/20/2009 7:32 PM	1	1
-	-	-	-	-	00:0F:24:00:0F:24	Aruba Networks	-	-	1/20/2009 6:55 PM	1	1
No	29	-63	-	-	00:1A:1E:00:1A:1E	Aruba Networks	-	-	1/21/2009 12:01 AM	12	14
-	22	-76	-	-	00:0F:24:00:0F:24	Colubris Networks	-	-	1/20/2009 11:51 PM	2	2
-	-	-	-	-	00:1A:1E:00:1A:1E	Aruba Networks	-	-	1/20/2009 9:32 AM	1	1
-	-	-	-	-	00:0F:24:00:0F:24	Unknown Locally Administered Address	-	-	1/20/2009 9:09 AM	1	1
-	-33	-	-	-	00:1A:1E:00:1A:1E	Unknown Locally Administered Address	-	-	1/20/2009 10:08 AM	1	1
-	-95	-	-	-	00:0F:24:00:0F:24	Group/Multicast: possibly Apple Computer	-	-	1/20/2009 10:08 AM	1	1
-	-47	-	-	-	00:1A:1E:00:1A:1E	Unknown Locally Administered Address	-	-	1/20/2009 10:08 AM	1	1
-	-43	-	-	-	00:0F:24:00:0F:24	Unknown Locally Administered Address	-	-	1/20/2009 10:08 AM	1	1
-	-60	-	-	-	00:1A:1E:00:1A:1E	Hon Hai Precision Ind. Co.,Ltd.	-	-	1/20/2009 10:08 AM	2	2
-	0	-	-	-	00:0F:24:00:0F:24	Intel Corporate	-	-	1/20/2009 3:15 PM	4	4
-	-82	-	-	-	00:1A:1E:00:1A:1E	Intel Corporate	-	-	1/20/2009 5:48 PM	2	2
-	-64	-	-	-	00:0F:24:00:0F:24	Intel Corporate	-	-	1/20/2009 10:08 AM	3	3
-	-74	-	-	-	00:1A:1E:00:1A:1E	Intel Corporate	-	-	1/20/2009 3:15 PM	2	2
-	-78	-	-	-	00:0F:24:00:0F:24	Intel Corporate	-	-	1/20/2009 5:48 PM	3	3

Figure 173 Reports > Generated > New Rogue Devices, Rogue Devices Inventory

Rogue Devices													
1-20 of 69 Rogue Devices Page 1 of 4 >													
Name	Classification	Ack	Score	First Discovered	First Discovery Method	First Discovery Agent	Last Discovering AP	Type	Operating System	IP Address	SSID	Network Type	Channel
Aruba Netw-87:EC:90	Unclassified	No	6	1/20/2009 8:56 PM	Wireless AP scan	SW-2	SW-2	-	-	-	-	AP	36
Cisco-DE:16:F1	Unclassified	No	6	1/20/2009 7:32 PM	Wireless AP scan	11.1.5	11.1.5	-	-	-	chatter	AP	11
Cisco-DE:16:F2	Unclassified	No	6	1/20/2009 7:32 PM	Wireless AP scan	11.1.5	11.1.5	-	-	-	unplugged	AP	11
Cisco-5B:F7:73	Unclassified	No	6	1/20/2009 7:32 PM	Wireless AP scan	11.1.5	11.1.5	-	-	-	roamer	AP	1
Cisco-DE:16:F0	Unclassified	No	6	1/20/2009 7:32 PM	Wireless AP scan	11.1.5	11.1.5	-	-	-	-	AP	11
Aruba Netw-61:1D:F0	Unclassified	No	6	1/20/2009 6:55 PM	Wireless AP scan	SW-2	SW-2	-	-	-	aruba-ap	AP	36
Aruba Netw-84:9C:63	Unclassified	No	6	1/20/2009 2:46 PM	Wireless AP scan	aruba-ap85-c1:ad:13	00:1a:1e:00:1a:1e	-	-	-	student19	AP	1
Colubris N-C7:D9:30	Unclassified	No	6	1/20/2009 8:53 AM	Wireless AP scan	Local-65	AM-65	-	-	-	OfficeBizK	AP	8
Aruba Netw-B0:00:58	Unclassified	No	6	1/20/2009 9:32 AM	Wireless AP scan	SW-2	SW-2	-	-	-	sw_sathish_tk	AP	149
Unknown Lo-68:67:7C	Unclassified	No	6	1/20/2009 9:09 AM	Wireless AP scan	rtis	rtis	-	-	-	-	AP	6
Unknown Lo-00:00:00	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-2	AP-2	-	-	-	-	Unknown	6
Group/Mult-FF:FF:FF	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-2	AP-2	-	-	-	-	Unknown	153
Unknown Lo-00:00:00	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-2	AP-2	-	-	-	□US □ □	Unknown	6
Unknown Lo-00:00:00	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-2	AP-2	-	-	-	-	Unknown	6
Hon Hai P-C7:80:5D	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-3	AP-5	-	-	-	-	Unknown	165
Intel Corp-91:67:03	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-1	AP-2	-	-	-	-	AP	149
Intel Corp-85:87:83	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-3	AP-3	-	-	-	-	Unknown	40
Intel Corp-08:FF:29	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-1	AP-5	-	-	-	-	Unknown	149
Intel Corp-09:20:ED	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-3	AP-1	-	-	-	-	AP	6
Intel Corp-08:B4:AA	Unclassified	No	6	1/20/2009 10:08 AM	Wireless AP scan	AP-5	AP-5	-	-	-	-	AP	0

WEP	RSSI	Signal	LAN MAC Address	LAN Vendor	Radio MAC Address	Radio Vendor	Switch/Router	Port	Last Seen	Total Discovering APs	Total Discovery Events
-	-	-	-	-	00:1A:1E:00:1A:1E	Aruba Networks	-	-	1/20/2009 8:56 PM	1	1
-	13	-82	-	-	00:0F:24:00:0F:24	Cisco	-	-	1/20/2009 11:53 PM	1	2
-	13	-83	-	-	00:1A:1E:00:1A:1E	Cisco	-	-	1/20/2009 8:04 PM	1	2
-	12	-82	-	-	00:0F:24:00:0F:24	Cisco	-	-	1/20/2009 11:53 PM	1	2
-	-	-	-	-	00:1A:1E:00:1A:1E	Cisco	-	-	1/20/2009 7:32 PM	1	1
No	29	-63	-	-	00:1A:1E:00:1A:1E	Aruba Networks	-	-	1/20/2009 6:55 PM	1	1
-	22	-76	-	-	00:0F:24:00:0F:24	Colubris Networks	-	-	1/21/2009 12:01 AM	12	14
-	-	-	-	-	00:0F:24:00:0F:24	Colubris Networks	-	-	1/20/2009 11:51 PM	2	2
-	-	-	-	-	00:1A:1E:00:1A:1E	Aruba Networks	-	-	1/20/2009 9:32 AM	1	1
-	-	-	-	-	00:0F:24:00:0F:24	Unknown Locally Administered Address	-	-	1/20/2009 9:09 AM	1	1
-	-33	-	-	-	00:1A:1E:00:1A:1E	Unknown Locally Administered Address	-	-	1/20/2009 10:08 AM	1	1
-	-95	-	-	-	00:0F:24:00:0F:24	Group/Multicast: possibly Apple Computer	-	-	1/20/2009 10:08 AM	1	1
-	-47	-	-	-	00:1A:1E:00:1A:1E	Unknown Locally Administered Address	-	-	1/20/2009 10:08 AM	1	1
-	-43	-	-	-	00:0F:24:00:0F:24	Unknown Locally Administered Address	-	-	1/20/2009 10:08 AM	1	1
-	-60	-	-	-	00:1A:1E:00:1A:1E	Hon Hai Precision Ind. Co., Ltd.	-	-	1/20/2009 10:08 AM	2	2
-	0	-	-	-	00:0F:24:00:0F:24	Intel Corporate	-	-	1/20/2009 3:15 PM	4	4
-	-82	-	-	-	00:1A:1E:00:1A:1E	Intel Corporate	-	-	1/20/2009 5:48 PM	2	2
-	-64	-	-	-	00:0F:24:00:0F:24	Intel Corporate	-	-	1/20/2009 10:08 AM	3	3
-	-74	-	-	-	00:1A:1E:00:1A:1E	Intel Corporate	-	-	1/20/2009 3:15 PM	2	2
-	-78	-	-	-	00:0F:24:00:0F:24	Intel Corporate	-	-	1/20/2009 5:48 PM	3	3

The detailed device inventories that comprise parts of this report contain the following fields, described in Table 165.

Table 165 Fields in the New Rogue Devices Report

Field	Description
Name	Displays the device name, as able to be determined.
Classification	Displays the rogue classification, when supported.
Ack	Displays whether the device has been acknowledged with the network.
Score	Displays the rogue score for this device.
First Discovered	Displays the date and time that the rogue device was first discovered on the network.
First Discovery Method	Displays the method by which the rogue device was discovered.
First Discovery Agent	Displays the network device that first discovered the rogue device.
Last Discovering AP	Displays the network device that most recently discovered the rogue device.
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.

Table 165 Fields in the **New Rogue Devices Report** (Continued)

Field	Description
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.
Radio Vendor	Displays the manufacturer information for the radio device when known.
Switch/Router	Displays the switch or router associated with the rogue 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.

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.

- To view the latest version of this report, refer to [“Using the Most Recent New Users Report”](#) on page 256.
- To create a generated report of this type, refer to [“Viewing Reports”](#) on page 232.

Using the Most Recent New Users Report

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 **Details** page allows you to view information for new users that have appeared on the network during the time period defined for the report.

[Figure 174](#) illustrates the fields and information in the **New Users Report**.

Figure 174 Reports > Generated > New Users Report

Daily New Users 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 12:16 AM						
XML (XHTML) 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 166 *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.

PCI Compliance Report

OV3600 Version 6.2 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.

Refer to the “[Overview of PCI Compliance in OV3600 6.2](#)” on page 184 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.

- To view the latest version of this report, refer to “[Using the Most Recent New Users Report](#)” on page 256.
- To create a generated report of this type, refer to “[Viewing Reports](#)” on page 232.

Using the Most Recent PCI Compliance Report

Perform these steps to view the most recent version of the **PCI Compliance Report**.

1. Verify that OV3600 6.2 is enabled to monitor compliance with PCI requirements, as described in the “[Overview of PCI Compliance in OV3600 6.2](#)” on page 184.
2. Navigate to the **Reports > Generated** page.
3. Scroll to the bottom, and click **PCI Compliance** to display **Detail** information.

[Figure 175](#) illustrates the fields and information in the most recent **PCI Compliance Report**.

Refer also to the section titled “[Overview of PCI Compliance in OV3600 6.2](#)” on page 184.

Figure 175 Reports > Generated > PCI Compliance Report Details

Daily PCI Compliance Report for All Groups, Folders and PCI Requirements

1/20/2009 12:00 AM to 1/21/2009 12:00 AM
Generated on 1/21/2009 12:23 AM

This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.2 requirements that are relevant to security in your network. PCI DSS standard requirements are available at <https://www.pcisecuritystandards.org>.

Disclaimer: The PCI Compliance Report must be completed by an authorized QSA. The sole purpose of this report is to provide IT administrators with an on-demand internal audit of components which are visible to AirWave Wireless Management Suite.

XML (XHTML) export
Email this report
Print report

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

Defining and Generating PCI Compliance Reports

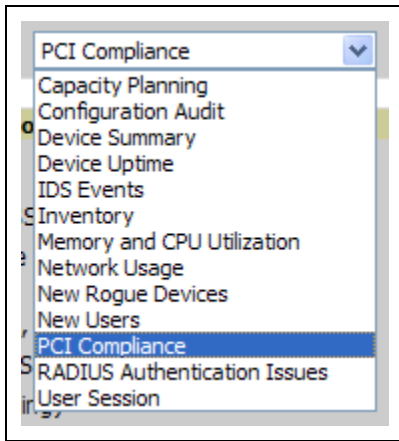
Perform these steps to define and generate PCI Compliance generated reports in OV3600 6.2. These steps are a modification to general report creation procedures, with an emphasis on PCI requirements.



Only **Admin** users have complete access to complete PCI Compliance information. The OV3600 6.2 reports and online displays of information can vary with configuration, User Roles, and Folders.

1. Navigate to the **Reports > Definitions** page, and click the **Add New Report Definition** button. The **Report Definitions** page appears.
2. Complete the **Report Definition** section.
 - a. In the **Title** field, provide a name for this PCI compliance report. Useful terms to include in a title might be include the report frequency, such **Daily**, **Weekly**, or **Monthly**.
 - b. In the **Type** field, select **PCI Compliance** in the drop-down menu. The **Definitions** page changes to PCI-specific configurations once you select this report type.

Figure 176 Report Type Drop-down Menu in Reports > Definitions > Add



3. Use the **Group** and **Folder** sections to define the scope of the PCI Compliance report. These report parameters apply to any OV3600 6.2 report that supports groups.
 - a. If you choose **Use selected Groups** in the **Group** down-down menu, then all groups that have been defined in the **Groups** page appear, and you can select the specific group or groups for which to generate PCI Compliance data. Refer to [“Group Configuration Overview” on page 66](#) for additional information.
 - b. If you choose **Use selected Folders** in the **Folders** drop-down menu, then all folders that have been defined appear, and you can select the specific folder or folders for which to generate PCI Compliance data. Refer to [“Using Device Folders \(Optional\)” on page 165](#) for additional information.
4. Use the **PCI Requirements** section to define the PCI Compliance standards to include in tracking and reports generation. [Table 130](#) describes each standard, and you have the option of including these explanations in reports by clicking **Yes** in the **Include Details...** field.
5. Specify the **Scheduling Options** to establish how often and over what period of time a report is to include data.
6. Specify the **Report Visibility** settings, to generate report information by role or by subject.
7. Specify the **Email Option** settings as required.
8. Complete the remainder of this **Definitions** page and specify report details.
9. Click **Add** or **Add and Run** to complete the configuration of the PCI compliance report, and repeat these steps as desired to create as many PCI Compliance reports as desired.

RADIUS Authentication Issues Report

The **RADIUS Authentication Issues Report** contains issues that may appear with AP controllers, RADIUS Servers, and users.

To view the latest version of this report, refer to [“Using the Most Recent RADIUS Authentication Issues Report” on page 259](#).

To create a generated report of this type, refer to [“Viewing Reports” on page 232](#).

Using the Most Recent RADIUS Authentication Issues Report

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 **Details** page allows you to view information for RADIUS issues that have appeared on the network during the time period defined for the report.

Figure 177 illustrates the fields and information in the **RADIUS Authentication Issues Report**.

Figure 177 Reports > Generated > RADIUS Authentication Issues Details

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
 Email this report
 Print report

Top 10 RADIUS Authentication Issues by Controller

Controller	Total Failures	First Event	Most Recent Event
ethersphere-lms4	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:8F:00:1C:8F	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	Controller	AP	Radio
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:59 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:59 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:58 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:58 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:57 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:57 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:56 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:56 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:55 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:55 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:55 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:54 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:54 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:53 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:53 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:52 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:52 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:51 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:51 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:50 PM	ethersphere-lms4	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	-	1/20/2009 11:50 PM	ethersphere-lms4	-	-

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. Session information can be established and tracked by multiple parameters, to include the following:

- Connection mode and multifaceted parameters in this category
- SSID session data
- VLAN session data
- Cipher data
- more

To view the latest version of this report, refer to “Using the Most Recent User Session Report” on page 260.

To create a generated report of this type, refer to “Viewing Reports” on page 232.

Using the Most Recent 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 **Details** 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 178 Reports > Generated > User Session Detail, Connection Mode Information

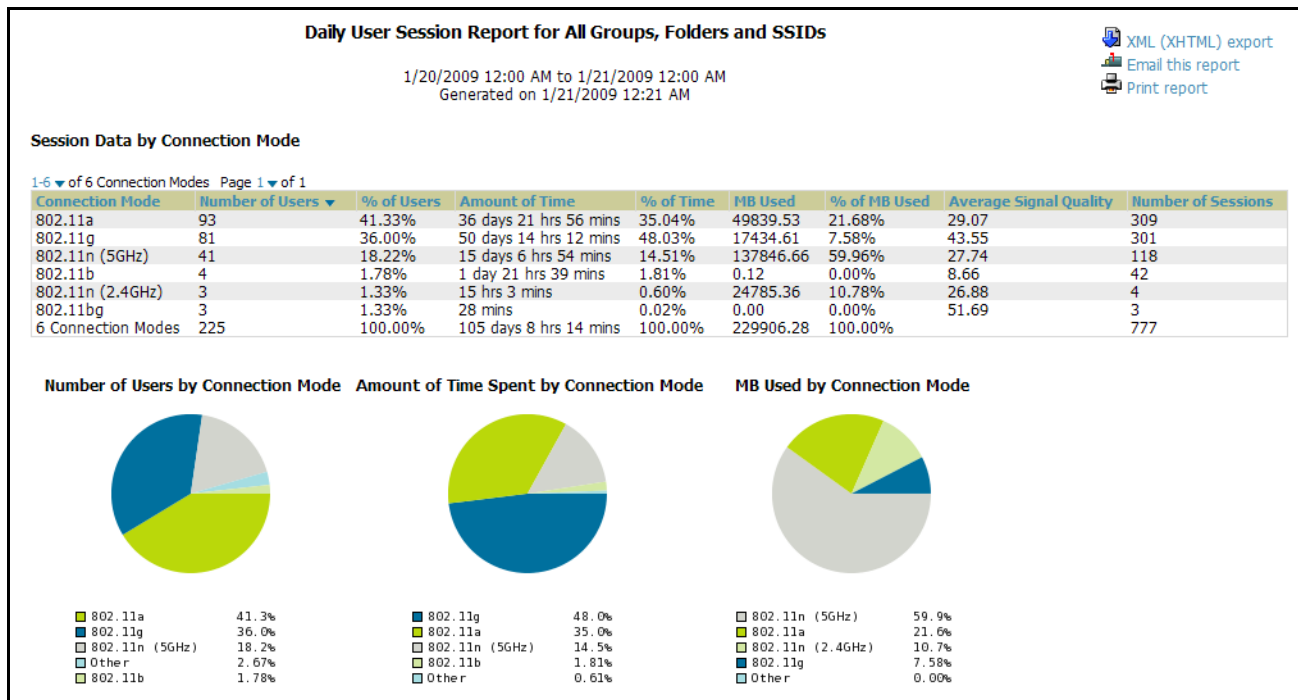


Figure 179 Reports > Generated > User Session Detail, SSID Information

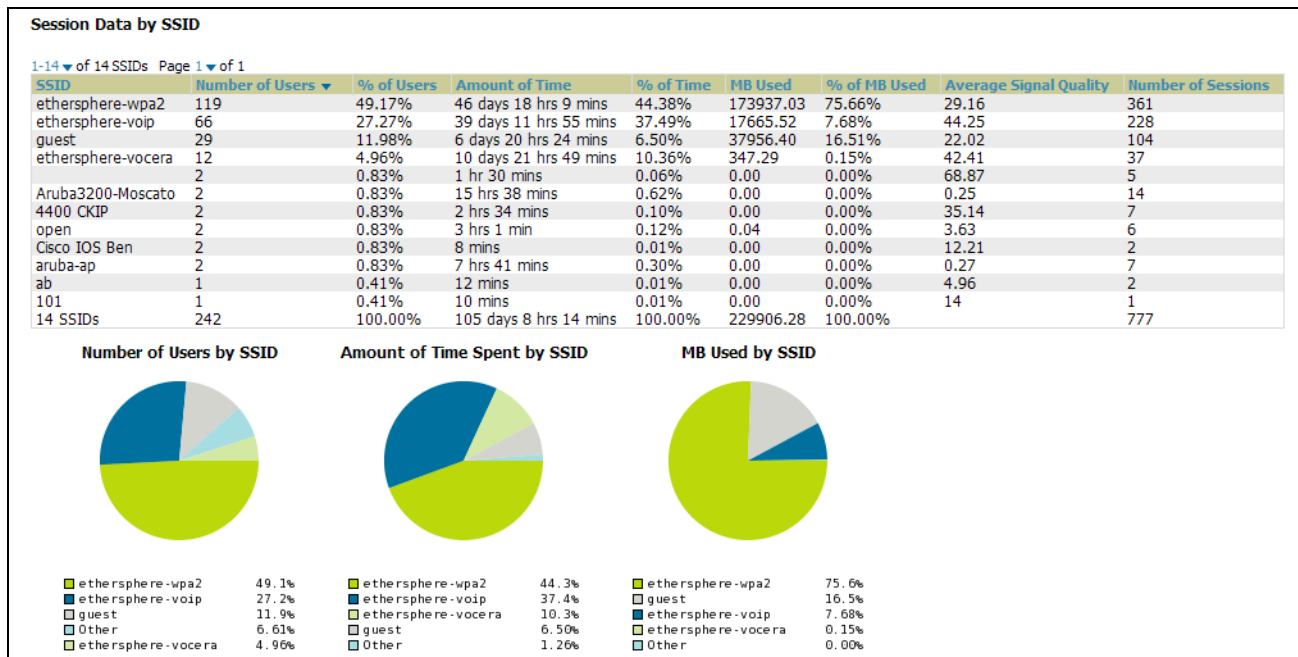


Figure 180 Reports > Generated > User Session Detail, VLAN Information

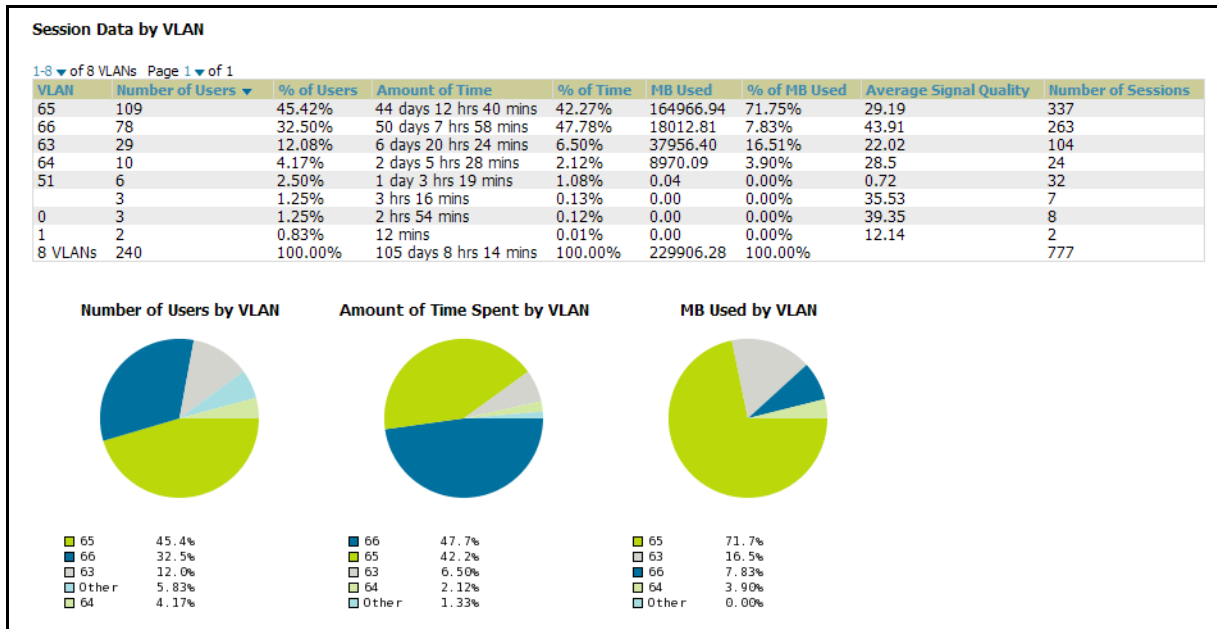


Figure 181 Reports > Generated > User Session Detail, Cipher Information

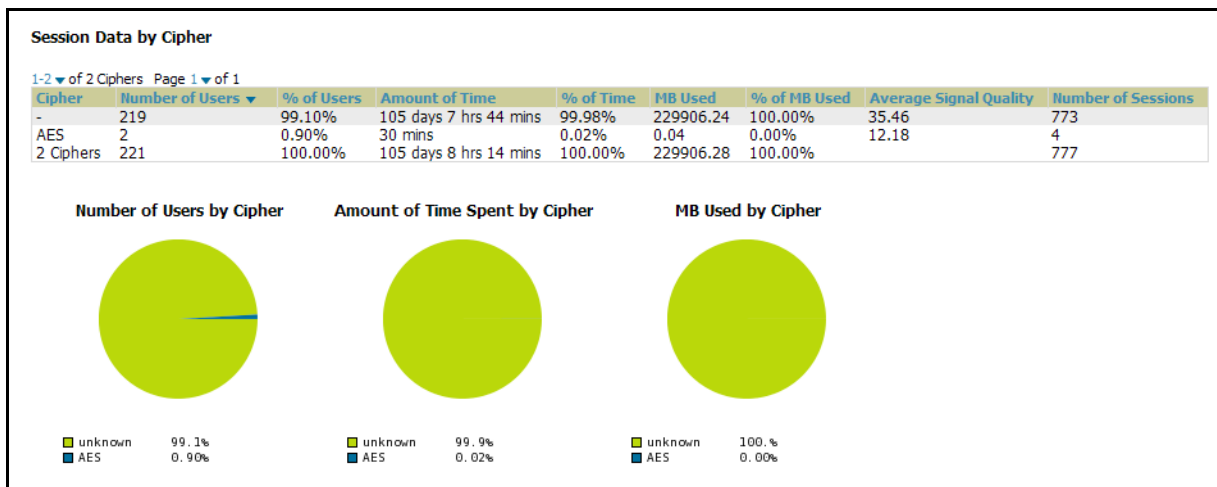


Figure 182 Reports > Generated > User Session Detail, Summary and User Information

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

Session Data by User

1-20 of 220 Users Page 1 of 11 >>

MAC Address	Username	Roles	Amount of Time	MB Used	Avg Bandwidth (kbps)	Average Signal Quality	Vendor	Connection Modes	VLANs	SSIDs	Guest User
00:03:2A:02:4F:95	wifiphone	employee	23 hrs 59 mins	0.43	0.04	49.24	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
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	66	ethersphere-voip	No
00:03:2A:02:52:8C	wifiphone	employee	23 hrs 59 mins	7.35	0.7	50.65	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
00:03:2A:02:5F:B4	-	VoFi	5 hrs 34 mins	0.12	0.05	44.74	UniData Communication Systems, Inc.	802.11b	63	guest	No
00:03:2A:02:67:FD	wifiphone	employee	14 hrs 58 mins	0.15	0.02	46.99	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
00:03:2A:02:69:7A	azindel	employee	23 hrs 59 mins	5.65	0.54	40.53	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
00:03:2A:02:69:88	wifiphone	employee	23 hrs 59 mins	8382.05	794.75	44.87	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
00:03:2A:02:69:C9	wifiphone	employee	23 hrs 59 mins	16.70	1.58	41.3	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
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	66	ethersphere-voip	No
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	66	ethersphere-voip	No
00:03:2A:02:6A:05	wifiphone	employee	23 hrs 59 mins	0.45	0.04	47.31	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
00:03:2A:02:6A:0B	wifiphone	employee	23 hrs 59 mins	3.68	0.35	50.34	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
00:03:2A:02:6A:0C	wifiphone	employee	23 hrs 59 mins	0.46	0.04	42.12	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
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	66	ethersphere-voip	No
00:03:2A:02:6A:61	wifiphone	employee	23 hrs 59 mins	0.39	0.04	46.13	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
00:03:2A:02:6A:62	wifiphone	employee	23 hrs 59 mins	0.43	0.04	42.36	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
00:03:2A:02:6A:63	wifiphone	employee	23 hrs 59 mins	1.17	0.11	46.36	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
00:03:2A:02:6A:65	wifiphone	employee	23 hrs 59 mins	0.39	0.04	51.69	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No
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	66	ethersphere-voip	No
00:03:2A:02:6A:D3	wifiphone	employee	23 hrs 59 mins	0.37	0.04	42.15	UniData Communication Systems, Inc.	802.11g	66	ethersphere-voip	No

Introduction

This chapter presents the functions, configuration, and use of the OV3600 **Helpdesk**. This chapter contains the following sections:

- [Introduction](#)
- [OV3600 Helpdesk Overview](#)
- [Monitoring Incidents with Helpdesk](#)
- [Creating a New Incident with Helpdesk](#)
- [Creating New Snapshots or Incident Relationships](#)
- [Using the Helpdesk Tab with an Existing Remedy Server](#)

OV3600 Helpdesk Overview

The Helpdesk module of the OmniVista 3600 Air Manager allows front-line technical support staff to take full advantage of the data available in the OmniVista 3600 Air Manager. The OV3600 Helpdesk includes the following features and functions, in addition to more functions 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.
- The 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.
- The OV3600 Helpdesk includes the ability to document incidents associated with users on the network.
- If an external Remedy installation is available, the Helpdesk functionality can be disabled, and the OV3600 can be used as an interface to create, view and edit incidents on the existing Remedy server. Snapshots can also be associated with Remedy incidents and stored locally on the OV3600 server. By default, the option to use an external Remedy server is disabled; navigate to the **Helpdesk > Setup** page to enable Remedy. Refer to [“Using the Helpdesk Tab with an Existing Remedy Server” on page 267](#) for more information on how to configure OV3600 to integrate with a Remedy server.

Monitoring Incidents with Helpdesk

For a complete list of incidents, or to open a new incident, navigate to the **Helpdesk > Incidents** page. Figure 183 illustrates the components of the OV3600 **Helpdesk Incidents** page.

Figure 183 *Helpdesk > Incidents*

State	Last 2 Hours	Last Day	Total
Open	0	0	80
Closed	0	0	1
Total	0	0	81

New Incident

1-20 ▼ of 81 Incidents Page 1 ▼ of 4 > > |

	ID	Summary	State	Opened By	Related	Created	Updated
<input type="checkbox"/>	139	brian's problem	Open	aruba-se	0	1/29/2009 2:25 PM	1/29/2009 2:25 PM
<input type="checkbox"/>	138	Robert's connectivity problem	Open	mbruno	1	1/28/2009 8:16 AM	1/28/2009 8:17 AM
<input type="checkbox"/>	136	incident	Open	jason	0	1/22/2009 1:42 PM	1/22/2009 1:42 PM
<input type="checkbox"/>	135	Kaveh's wireless issue	Open	david	0	1/19/2009 11:32 AM	1/19/2009 11:32 AM
<input type="checkbox"/>	134	Ezra can't see the network	Closed	katie	0	1/13/2009 9:23 AM	1/13/2009 9:23 AM
<input type="checkbox"/>	133	Can't connect	Open	jason	1	1/12/2009 12:00 PM	1/12/2009 12:01 PM
<input type="checkbox"/>	132	Oak Grove Guest Issue	Open	paul	0	1/9/2009 6:53 AM	1/9/2009 6:53 AM
<input type="checkbox"/>	131	Patricks Wireless Issue	Open	patrick	0	12/23/2008 5:31 PM	12/23/2008 5:31 PM
<input type="checkbox"/>	129	peter problem	Open	aruba-se	0	12/18/2008 11:54 PM	12/18/2008 11:54 PM
<input type="checkbox"/>	126	damien's connectivity issue	Open	aruba-se	0	12/12/2008 12:12 AM	12/12/2008 12:12 AM
<input type="checkbox"/>	125	Sergio wireless issues 29/7	Open	patrick	0	7/28/2008 2:38 PM	7/28/2008 2:38 PM
<input type="checkbox"/>	124	User cannot login	Open	dan	0	7/28/2008 7:06 AM	7/28/2008 7:07 AM
<input type="checkbox"/>	123	Kaveh's Wireless issues - 28/7	Open	patrick	0	7/27/2008 2:33 PM	7/27/2008 2:33 PM
<input type="checkbox"/>	122	patrick's wireless issue	Open	patrick	0	7/24/2008 11:04 AM	7/24/2008 11:04 AM
<input type="checkbox"/>	121	Sergio wireless issues	Open	patrick	0	7/22/2008 12:32 PM	7/22/2008 12:32 PM
<input type="checkbox"/>	120	Kevin's low signal issue	Open	aruba-se	0	7/22/2008 1:47 AM	7/22/2008 1:47 AM
<input type="checkbox"/>	119	patrick's issues	Open	patrick	0	7/18/2008 9:28 AM	7/21/2008 7:31 AM
<input type="checkbox"/>	118	Katie's wireless issue	Open	patrick	0	7/14/2008 1:33 PM	7/14/2008 1:33 PM
<input type="checkbox"/>	117	Rogue device	Open	dkennison	0	7/9/2008 4:50 PM	7/9/2008 4:50 PM
<input type="checkbox"/>	116	Katie's Wireless Issues	Open	patrick	0	7/9/2008 10:02 AM	7/9/2008 10:02 AM

Select All - Unselect All

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 167 *Helpdesk > Incidents, Topmost Table*

Column	Description
State	Displays three states as they apply, as follows: <ul style="list-style-type: none"> ● Open (currently under investigation) ● Closed (resolved) ● The total incident count
Period of time	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 168](#) below, summarizes the incidents that have been reported so far. Clicking the **pencil** icon next to any incident opens an edit page where the incident can be modified. An incident can be deleted by selecting the check box next to it and clicking the **Delete** button at the bottom of the table.

Table 168 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. The 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.
Creation Date	Displays the time and date the incident was created.
Last Update Time	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 184](#). The contents of this page are described in [Table 169](#).

Figure 184 *Incident Edit*

Table 169 *Helpdesk Incident Edit*

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.





Helpdesk icons appear at the top of other OV3600 pages, allowing graphical snapshots and other records to be associated to existing incidents. These appear in the upper right-hand corner next to the **Help** link. Refer to [Figure 185](#).

Figure 185 *Helpdesk Icons on Additional Pages*



[Table 170](#) describes the Helpdesk icon components.

Table 170 *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 170](#)) 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 186](#) illustrates these GUI tools.

Figure 186 Relationships and Snapshots on the *Incident Edit* Page

The screenshot shows the 'Incident Edit' page. At the top, there is a header 'Incident'. Below it, the 'Summary' field contains 'Patricks Wireless Issue'. The 'State' is set to 'Open'. The 'Description' field contains 'notes'. There are 'Save' and 'Cancel' buttons. Below the incident details, there is a 'Snapshots' section. It shows '1-2 of 2 Incident Snapshots Page 1 of 1'. A table lists two snapshots:

Description	Created
<input type="checkbox"/> Snapshot 261	12/23/2008 5:31 PM
<input type="checkbox"/> Snapshot 262	12/23/2008 5:31 PM

Below the table, there is a 'Select All - Unselect All' link and a 'Delete' button.

Using the Helpdesk Tab with an Existing Remedy Server

If an external Remedy server exists, the OV3600 **Helpdesk** tab can be used 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**. Refer to the prior topic for more details on their operation. [Figure 187](#) illustrates this appearance, and [Table 171](#) describes the components.

Figure 187 *Helpdesk > Setup with Remedy Enabled*

The screenshot shows the 'BMC Remedy Setup' page. It has a header 'BMC Remedy Setup' and a sub-header 'Set up your integration with BMC Remedy.'. The 'Remedy Enabled:' field has radio buttons for 'Yes' (selected) and 'No'. The 'Middle Tier Host:' field contains 'remedy.dev.airwave.com'. The 'Port:' field contains '8080'. The 'SOAP URL:' field contains 'arsys/services/ARService'. The 'Server:' field contains 'remedy'. The 'Timeout (Greater than or equal to 0 seconds):' field contains '60'. The 'Username:' field contains 'appadmin'. The 'Password:' and 'Confirm Password:' fields are empty. There are 'Save' and 'Revert' buttons at the bottom.

Table 171 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.
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, the OV3600 **Helpdesk** functionality is disabled. OV3600 then displays incident data pulled from the **Remedy** server and push changes back. With the exception of snapshots, OV3600 does not store any Remedy data locally.

To view **Remedy** incidents in OV3600, navigate to the **Helpdesk > Incidents** tab. [Figure 188](#) illustrates the appearance and [Table 172](#) describes the components of this page.

Figure 188 *Helpdesk > Incidents* with Remedy Enabled

Incident Number	Summary	Status	Assignee	Urgency
INC000000000063	Repeatedly dropped from the network	Assigned	-	1-Critical

Table 172 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: <ul style="list-style-type: none"> • New • Assigned • In Progress • Pending • Resolved • Closed • Cancelled

Table 172 Components of **Helpdesk > Incidents** with Remedy Enabled

Field	Description
Assignee	Assigned by Remedy installation; cannot be changed in OV3600.
Urgency	Displays the urgency level, as chosen by the OV3600 or Remedy User: <ul style="list-style-type: none"> ● 1 - Critical ● 2 - High ● 3 - Medium ● 4 - Low.

To change the current incident in the **Helpdesk** header, click the **Unsettle 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 189](#) and [Table 173](#) for additional illustration and explanation.

Figure 189 **Helpdesk > Incidents**, Add a New **Remedy Incident**

Table 173 Components of **Helpdesk > Incidents**, Add a New **Remedy Incident**

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	<ul style="list-style-type: none"> ● 1 - Extensive/Widespread (default) ● 2 - Significant/Large ● 3 - Moderate/Limited ● 4- Minor/Localized
Urgency	<ul style="list-style-type: none"> ● 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.

This brief chapter describes the Yum packaging management system, and provides advisories on alternative methods that may cause issues with OV3600 6.2.

Yum for OV3600 6.2

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 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 6.2.

To run Yum on a CentOS 4 machine, use the steps below; for a CentOS 5 machine, yum-cron is also required.

1. Before Yum is run for the first time, you need to install the GPG key. The GPG key is used to validate the authenticity 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 Enterprise Support at support@ind.alcatel.com for further assistance.

Package Management System Advisories for OV3600 6.2



Alcatel-Lucent does not support Yum or Up2date on Red Hat 8 or 9. Running Yum on RH8 or RH9 will cause serious problems

Overview

Cisco WLSE functions as an integral part of the Cisco 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 174](#) describes these components.

Table 174 Cisco SWAN Architecture Components

SWAN Component	Requirements
WDS	<ul style="list-style-type: none"> WDS Name Primary and backup IP address for WDS devices (IOS AP or WLSM) WDS Credentials APs within WDS Group <p>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.</p>
WLSE	<ul style="list-style-type: none"> IP Address Login
ACS	<ul style="list-style-type: none"> IP Address Login
APs	<ul style="list-style-type: none"> APs within WDS Group

Helpful Cisco Links

- Ciscoworks WLSE
<http://www.cisco.com/en/US/products/sw/cscowork/ps3915/>
- Cisco WLSE Release Notes
http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_release_notes_list.html
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/

Performing Initial WLSE Configuration

Use the following instructions to configure a WLSE.

Adding an ACS Server

- Navigate to the **Devices > Discover > AAA Server** page.
- Select **New** from the pull down list.
- Enter the **Server Name**, **Server Port** (default 2002), **Username**, **Password**, and **Secret**.
- Click the **Save** button.

Enabling Rogue Alerts

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

Configuring WLSE to Communicate with APs

1. Navigate to the **Device > 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:

- CDP
- Import from a file.
- Import 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.

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

Use these pages to make such configurations:

1. 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's 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

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 (Optional)

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.

Bluesocket Integration (Optional)

Requirements

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 Bluesocket security scheme:

1. Login into the Bluesocket Server via HTTP with proper user credentials.
2. Navigate to **Users > External Accounting Servers**.
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 OV3600's shared secret).
9. Enter Notes (optional).
10. Click the **Save** button.
11. If you are using an External LDAP Server, ensure that the accounting records are forwarding to OV3600 upon authentication.
12. Navigate to **Users > External Authentication Servers**.
13. Modify the LDAP server.
14. Ensure under the Accounting server matches the server entered in step 5.
15. 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 (Optional)

Requirements

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 OV3600 with a RADIUS Accounting Server \(Optional\)”](#) on page 53.

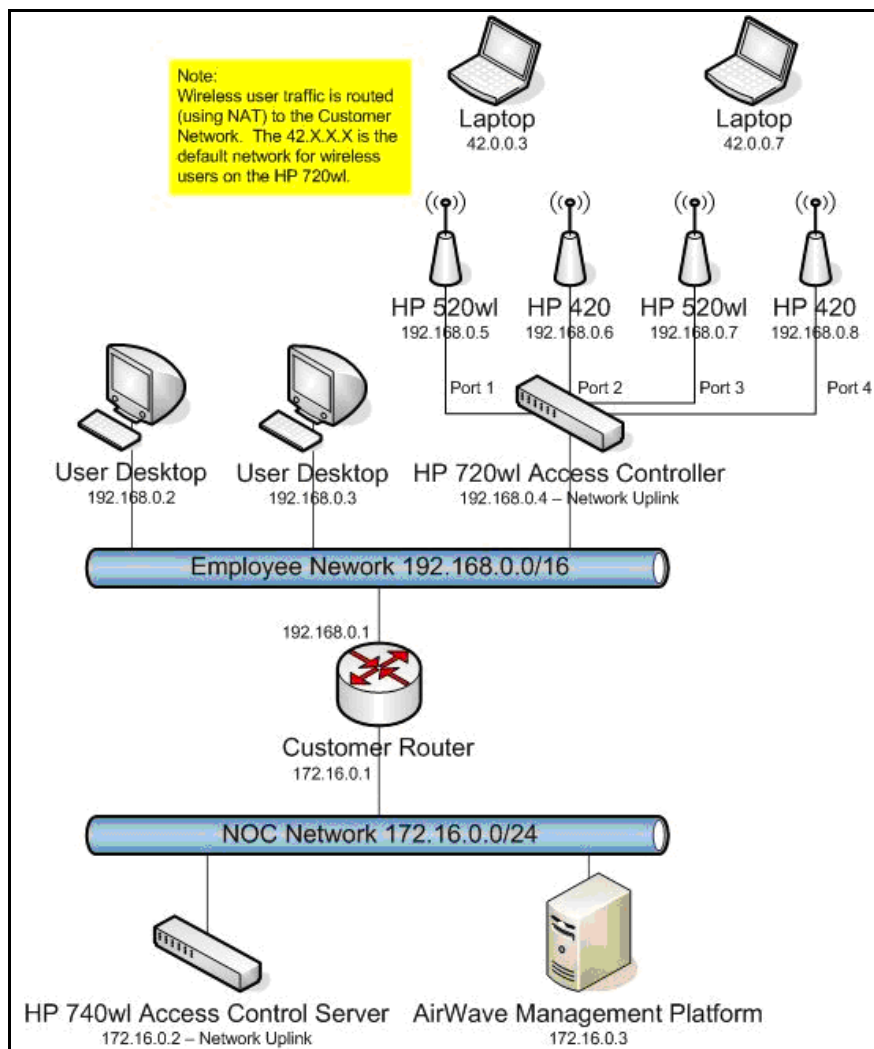
ReefEdge Configuration

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 OV3600's 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 (Optional)

Figure 190 Diagram of HP ProCurve Network Architecture



Requirements

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 OV3600 with a RADIUS Accounting Server \(Optional\)”](#) on page 53.

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 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's IP Address**.
8. Enter **Shared Secret**.
9. Enter **Port - 1812**.
10. Enter the **Shared Secret** and **Confirm** (matching OV3600's 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.

Resetting Cisco (VxWorks) Access Points

Introduction

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 **:reseta11** 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.

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 yourdomain.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 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 OV3600's 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.

Requirements

Integrations of Cisco Clean Access into the OV3600 deployment has the following prerequisites:

- Clean Access Software 3.5 or higher
- OV3600 version 3.4.0 or higher
- Completion 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 OV3600's 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"
```



NOTE

These attribute element pairs are mandatory for username display within OV3600.

Perform the following steps to install HP/Compaq Insight Manager on the OV3600:

1. Use SCP to move the two files over to the server:

```
hpsasm-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 hpsasm-7.8.0-88.rhel4.i386.rpm` at the command line interface.
3. Type `hpsasm 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 erroring on CentOS, as opposed to RedHat. This rpm *must* be run after the hpsasm 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 'o'.

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/hpsasm 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
rocommunity 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.

Symbol controllers (5100 and 2000) can be configured in OV3600 using templates. A sample running-configuration file template is provided below for reference. A template can be fetched from a "model" device using the procedure described earlier in the section on configuring templates for Cisco IOS devices. Certain parameters like hostname and location are turned into variables with the "%" tags so that device-specific values can be read off of the individual manage pages and inserted.

There is an option on the **Group > Templates** page to reboot the device after pushing a configuration. Certain settings have now integrated variables, including ap-license and adoption-preference-id. The radio preamble has now been template-integrated as well. OV3600 supports Symbol 5100 firmware upgrades for 3.x to 3.x.

```
//
// 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%

```


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 the OV3600 install on a VMware virtual machine can be done in one of three typical ways:

1. Write 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. Copy 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. Use 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 *Alcatel-Lucent 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's smartd service will fail at startup.

The service can be prevented from starting at boot by running the following commands at the OV3600's 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.

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.

OV3600 contains some software provided by third parties (both commercial and open-source licenses).

Copyright Notices

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 acknowledgment: 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

- A**
- Alcatel-Lucent 3, 23, 24, 25, 27, 32, 128, 201
 - contacting15, 21
 - documentation18
 - leading wireless vendor16
- C**
- Cisco
 - configuring IOS templates137
 - IOS config template133
 - Cisco IOS128
 - Colubris94, 117
 - CSV File148
- D**
- date and time
 - configuring20
 - devices141
- E**
- Enterasys R294
- F**
- firmware
 - loading device firmware60
- H**
- Hirschmann128
 - HP ProCurve128
 - HP ProCurve 42091
- I**
- installation
 - completing23
- L**
- Lancom128
 - Linux CentOS 5
 - installing19
- M**
- Master Console225
- N**
- Nomdix128
- O**
- OmniVista 3600 Air Manager16
 - OV3600
 - A Unified Wireless Network Command Center 15
 - adding access points, routers and switches with a CSV File148
 - Adding Templates130
 - additional interfaces and tools187
 - assigning host name22
 - assigning IP address22
 - assigning newly discovered devices to groups 150
 - backups222
 - changing default root password23
 - changing multiple group configurations 121
 - checking installation21
 - completing installation23
 - configuring a global template139
 - configuring and using groups with65
 - configuring and using security173
 - configuring basic group settings68
 - configuring Cisco IOS templates137
 - configuring Cisco WLC radio settings ... 95
 - configuring Colubris advanced settings . 117
 - configuring communication settings for discovered devices57
 - configuring date and time20
 - configuring group AAA servers86
 - configuring group MAC access control lists 119
 - configuring group PTMP/WiMAX settings 111
 - configuring group radio settings88
 - configuring group security settings74
 - configuring group SSIDs and VLANs .. 80
 - configuring group templates128
 - configuring groups66
 - configuring LWAPP AP settings110
 - configuring mesh radio settings115
 - configuring port consumption24
 - configuring TACACS+ integration47
 - core components16
 - creating a new incident with Helpdesk .. 265
 - creating and running custom reports235
 - creating new groups121
 - creating new snapshots and incident relationships 266
 - creating user roles42
 - creating users44
 - creating, running, and emailing reports .. 229
 - defining a scan144

defining credentials for scanning	143	Activity	29
defining network settings	40	Adding a RADIUS or TACACS+ Server	86
deleting a group	121	APs/Devices	28
deploying RAPIDS	173	APs/Devices > Audit	155
discovering, managing, and troubleshooting		APs/Devices > List	151
individual devices	141	APs/Devices > Manage, Device Communication	154
enabling AP automatic discovery	142	APs/Devices > New	150
enabling to nmanage your devices	57	Authentication Dialog Box	32
executing a scan	145	Authentication Failures Summary	152
getting started with	32	Buttons and Icons	29
Groups overview	65	Cisco WLC Security Attacks	152
hardware requirements	18	Configuration Change Confirmation	122
Helpdesk	263	Device Setup	28
initial login	32	Device Setup > Add	146
installation media	18	Device Setup > Add (from CSV)	149
installing	19	Device Setup > Communication	57
integrating ACS	50	Device Setup > Communication, Colubris	
integrating into network	17	Administration Options	59
integrating with existing network management		Device Setup > Communication, Concurrent	
solution	51	Process Limits	59
integrating with RADIUS authentication server		Device Setup > Communication, HTTP Discover	
53		Settings	58
integrating with WLSE rogue scanning ..	48	Device Setup > Communication, ICMP Settings	59
loading device firmware onto	60	Device Setup > Communication, SNMP 58	
managing devices with	57	Device Setup > Communication, SNMP Settings	58
manually adding individual devices	146	Device Setup > Communication, Telnet/SSH	58
modifying multiple devices	123	Device Setup > Communication, Telnet/SSH	58
monitoring incidents with Helpdesk	264	Settings	58
naming the network administration system	22	Device Setup > Communications	60
Package Management	271	Device Setup > Discover, Discovery Execution	145
performing backups	222	Device Setup > Discover, New Credentials	143
protocol and port diagram	24	Device Setup > Firmware Files	60, 61
Replacing a Broken Device	154	Failover	223
replacing a broken device	154	flash graphs	26
specifying general server settings	33	Global Template Variables	139
specifying minimum firmware versions for APs in		Group > Basic > Symbol/Intel	73
a group	120	Group > Basic, Automatic Static IPO Assignment	70
Template Variables	139	Group > Basic, Cisco WLC	72
troubleshooting a newly discovered device with		Group > Basic, HP ProCurve 420	73
down status	153	Group > Basic, Proxim/Avaya	72
using global groups for group configuration	124	Group > Templates, Add	139
using the Helpdesk tab with an existing remedy		Group SNMP Polling Period	69
server	267	Groups	27
verifying that devices are successfully added to a		Groups > Basic	68, 69, 125
group	151		
verifying the device configuration status	155		
viewing all defined device groups	66		
viewing defined device groups	66		
Watched OV3600 stations	223		
OV3600 interface			

Groups > Basic, Cisco IOS/VxWorks	71	Master Console Groups > Basic	227
Groups > Basic, Group Display Options	70	Navigation Section	27
Groups > Basic, Notes	70	RAPIDS	28
Groups > Basic, NTP	71	RAPIDS > Overview	174
Groups > Basic, Spanning Tree Protocol Configuration	71	RAPIDS > Rogue APs	175
Groups > Colubris	118	RAPIDS > Rogue APs (Detail), Score Override 182	
Groups > Firmware	120	RAPIDS > Score Override	182
Groups > List	66	RAPIDS > Setup, Basic Configuration ..	179
Groups > LWAPP AP Settings	110	RAPIDS > Setup, Operating System	181
Groups > MAC ACL	119	Reports	28
Groups > PTMP/WiMAX	111	Reports > Definitions	231
Groups > PTMP/WiMAX Configuring Packet Identification Rules	112	Reports > Definitions, Add	235
Groups > PTMP/WiMAX Configuring Service Flow Classes	113	Setup	28
Groups > PTMP/WiMAX Configuring Subscriber Station Classes	114	Setup > ACS	50
Groups > Radio	88	Setup > General Server Settings	34
Groups > Security	74	Setup > General, Auto Discovery	142
Groups > Security Configure Local Net Users	75	Setup > General, Default Firmware Upgrade Options	38
Groups > Security, Enable VLAN Tagging	79	Setup > Network Interface Activity	40
Groups > SSIDS	80	Setup > Network, External Syslog	41
Groups > Templates	129	Setup > NMS	51, 52
Groups > Templates Edit	140	Setup > NMS, Options	52
Groups > Templates, Add Template	130	Setup > RADIUS Accounting	53
Groups > WLC Radio	98	Setup > Roles	42, 193
Groups > WLC Radio Settings	97	Setup > TACACS Configuration	47
GRUB screen	20	Setup > Users	44
Help	29	Setup > WLSE	48
Helpdesk > Incidents	264, 268	Status Section	26
Helpdesk > Setup	267	System	28, 202
Home	27, 196	System > Alerts	221
Home > Documentation	18, 201	System > Backups	222
Home > License	198	System > Configuration Change Jobs ...	203
Home > Overview	196, 225	System > Event Logs	204
Home > Search	200	System > Performance	205
Home > User Info	201	System > Status	202
Home > Watched	224	System > Status Log	203
Home Overview	26	System > Trigger Detail	209
Incident Edit	267	System > Triggers	208
Master Console	29, 225	Triggers and Alerts	207
Master Console > Groups	227	User Interface—Basic Sections	25
Master Console > Groups > Basic, Managed	228	Users	28, 188
Master Console > Groups > Basic, Managed Subscriber Group	228	Users > Connected	188
Master Console > Manage AMPs, IP/Hostname 226		Users > Detail	191
Master Console > Manage OV3600s	226	Users > Diagnostics	191
Master Console and Failover	17	Users > Guest Users	194
		Users > Tags	195
		View AP Credentials	153
		VisualRF	29

P	
password	
changing default root	23
PCI Compliance	
Default Credential Compliance	186
PCI Requirements	184
port consumption	
configuring	24
Proxim 4900	93
R	
RAPIDS	28, 173, 175
RAPIDs	17
reports	229
rogue APs	175
S	
security	173
Smarthost	234
Symbol	94, 128
T	
Trapeze	128
V	
VisualRF	16, 29
W	
Wireless LAN	
components	18
Y	
Yum	271