

OmniVista 3600 Air Manager (OV3600)

Version 6.4



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.

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 Version 6.4.0*

| Enhancement | Document Section | Description |
|--|--|---|
| OV3600 Version 6.4 Enhancements | <ul style="list-style-type: none">General document | Document consolidates GUI, procedural, and feature-oriented enhancements, and implements several additional corrections. For detailed information about the new Alcatel-Lucent Configuration feature, refer to the new <i>Alcatel-Lucent Configuration Guide</i> . |
| CDP Device Discovery | <ul style="list-style-type: none">Chapter 5, "Discovering, Adding, and Managing Devices" on page 122 | OV3600 6.4 can discover CDP neighbors of an AP device when the IP address for that device is known. |
| General Device Discovery | <ul style="list-style-type: none">Chapter 5, "Discovering, Adding, and Managing Devices" on page 121 | Updated the chapter to support changes in OV3600 6.4. |
| Exporting Reports to XML | <ul style="list-style-type: none">Chapter 9, "Creating, Running, and Emailing Reports" on page 278 | Revised the procedure to account for changes in more recent versions of MS Excel. |
| Rogue Device Classification and RAPIDS Rules | <ul style="list-style-type: none">Chapter 7, "Using RAPIDS and Rogue Classification" on page 183 | OV3600 6.4 introduces significant enhancements to the RAPIDS module, to include changes in classification of rogue devices and introduction of RAPIDS rules that define rogue classification. |
| Downgrade Advisory | <ul style="list-style-type: none">Chapter 2, "Installing the OmniVista Air Manager (OV3600)" | Downgrade from Version 6.4 may result in data loss and other risks. Refer to Chapter 2, "Installing the OmniVista Air Manager (OV3600)" . |
| "OV3600 Setup" and general configuration | <ul style="list-style-type: none">Chapter 3, "Configuring the OmniVista Air Manager (OV3600)" on page 31 | <ul style="list-style-type: none">Overhauled topics to describe enhancements in the OV3600 Setup section through OV3600 Version 6.4.Moved information about the OV3600 Setup > PCI Compliance instructions to this chapter.Moved initial device configuration information to this chapter. |
| Cisco WLSE | <ul style="list-style-type: none">Chapter 3, "Configuring the OmniVista Air Manager (OV3600)" on page 58 | Consolidated topics supporting Cisco WLSE in OV3600. |

Table 2 summarizes content changes to this document after initial release of OV3600 Version 6.4.x. These changes are of the following types:

- enhancements to information in support of OV3600 6.4 features
- features from earlier OV3600 versions that were not described at the time of their original availability
- revisions to product or document bugs between major feature releases
- revisions derived from customer feedback or alternate sources

Table 2 *User Guide Document Revisions, OV3600 Version 6.4*

| Enhancement or Change | Document Section | Description |
|------------------------------------|---|--|
| Reports in O V3600 | <ul style="list-style-type: none">"Creating, Running, and Emailing Reports" on page 247 | Chapter "Introduction" cites three additional and lesser-known report options that are separate from the Reports pages in OV3600. |
| Users > Guest Users page | <ul style="list-style-type: none">"Configuring Your Own User Information with the Home > User Info Page" on page 235 | Topic cites additional information about using this page. |

Table 2 *User Guide Document Revisions, OV3600 Version 6.4 (Continued)*

| Enhancement or Change | Document Section | Description |
|--|--|--|
| Users > Tags page | <ul style="list-style-type: none">"Supporting Users on Thin AP Networks With the Users > Tags Page" on page 221 | Topic cites additional information about RFID tags. |
| Web Auth Bundle information supporting Cisco WLAN switches | <ul style="list-style-type: none">"Using Web Auth Bundles in OV3600" on page 53 | Chapter adds a new procedure to support the Web Auth Bundle feature on the Device Setup > Upload Files page. |
| Authentication Type | <ul style="list-style-type: none">"Using the OV3600 APs/ Devices Pages for AP Communication Settings" on page 153 (Table 91) | Increased certain details about authentication types reported in OV3600. |
| Backing Up OV3600 | <ul style="list-style-type: none">"Backing Up OV3600" on page 242 | Updated graphics and information for backups of OV3600 Version 6.3.2 and later OV3600 versions. |

| | | |
|------------------|---|-----------|
| | Document Organization | 91 |
| Preface | | 7 |
| | Document Organization | 7 |
| | Text Conventions | 8 |
| | Contacting Alcatel-Lucent | 9 |
| Chapter 1 | Introduction to the OmniVista Air Manager (OV3600) | 11 |
| | OV3600—A Unified Wireless Network Command Center | 11 |
| | VisualRF™ | 11 |
| | RAPIDS™ | 12 |
| | Master Console and Failover | 12 |
| | Integrating OV3600 into the Network and Organizational Hierarchy | 12 |
| Chapter 2 | Installing the OmniVista Air Manager (OV3600) | 15 |
| | Introduction | 15 |
| | OV3600 Hardware Requirements and Installation Media | 15 |
| | Installing Linux CentOS 5 (Phase 1) | 16 |
| | Installing OV3600 Software (Phase 2) | 16 |
| | Getting Started | 16 |
| | Step 1: Configuring Date and Time, Checking for Prior Installations | 16 |
| | Step 2: Installing OV3600 Software, Including OV3600 | 18 |
| | Step 3: Checking the OV3600 Installation | 18 |
| | Step 4: Assigning an IP Address to the OV3600 System | 18 |
| | Step 5: Naming the OV3600 Network Administration System | 19 |
| | Step 6: Assigning a Host Name to the OV3600 | 19 |
| | Step 7: Changing the Default Root Password | 19 |
| | Completing the Installation | 19 |
| | Configuring and Mapping Port Usage for OV3600 | 20 |
| | OV3600 Navigation Basics | 21 |
| | Status Section | 22 |
| | Navigation Section | 23 |
| | Activity Section | 25 |
| | Help Links in the GUI | 25 |
| | Common List Settings | 26 |
| | Buttons and Icons | 27 |
| | Getting Started with OV3600 | 29 |
| | Completing Initial Login | 29 |
| Chapter 3 | Configuring the OmniVista Air Manager (OV3600) | 31 |
| | Defining General OV3600 Server Settings | 32 |
| | Defining OV3600 Network Settings | 38 |
| | Creating OV3600 Users | 40 |
| | Creating OV3600 User Roles | 42 |
| | Enabling OV3600 to Manage Your Devices | 44 |

| | | |
|------------------|--|------------|
| | Configuring Communication Settings for Discovered Devices | 46 |
| | Loading Device Firmware onto OV3600 (Optional) | 49 |
| | Configuring TACACS+ and RADIUS Authentication | 53 |
| | Configuring TACACS+ Authentication | 53 |
| | Configuring RADIUS Authentication and Authorization | 55 |
| | Integrating a RADIUS Accounting Server | 57 |
| | Configuring Cisco WLSE and WLSE Rogue Scanning | 58 |
| | Introduction to Cisco WLSE | 58 |
| | Configuring WLSE Initially in OV3600 | 58 |
| | Configuring IOS APs for WDS Participation | 60 |
| | Configuring ACS for WDS Authentication | 61 |
| | Configuring Cisco WLSE Rogue Scanning | 61 |
| | Configuring ACS Servers | 64 |
| | Integrating OV3600 with an Existing Network Management Solution (NMS) | 65 |
| | Auditing PCI Compliance on the Network | 67 |
| | Introduction to PCI Requirements | 67 |
| | PCI Auditing in the OV3600 Interface | 67 |
| | Enabling or Disabling PCI Auditing | 68 |
| | Deploying WMS Offload | 70 |
| | Overview of WMS Offload in OV3600 | 70 |
| | General Configuration Tasks Supporting WMS Offload in OV3600 | 70 |
| | Additional Information Supporting WMS Offload | 71 |
| Chapter 4 | Configuring and Using Device Groups in OV3600 | 73 |
| | OV3600 Group Overview | 74 |
| | Important Group Concepts | 74 |
| | Viewing All Defined Device Groups | 75 |
| | Editing Columns on the Groups > List Page and Additional Pages | 76 |
| | Configuring Basic Group Settings | 77 |
| | What Next? | 85 |
| | Configuring Group Security Settings | 85 |
| | Configuring Group SSIDs and VLANs | 87 |
| | Adding and Configuring Group AAA Servers | 92 |
| | Configuring Radio Settings for Device Groups | 93 |
| | An Overview of Cisco WLC Configuration | 100 |
| | Accessing Cisco WLC Configuration | 100 |
| | Navigating Cisco WLC Configuration | 100 |
| | Configuring WLANs for Cisco WLC Devices | 101 |
| | Defining and Configuring LWAPP AP Groups for Cisco Devices | 103 |
| | Configuring Cisco Controller Settings | 104 |
| | Configuring Wireless Parameters for Cisco Controllers | 104 |
| | Configuring Security Parameters and Functions | 104 |
| | Configuring Management Settings for Cisco Controllers | 105 |
| | Configuring Group PTMP/WiMAX Settings | 105 |
| | Configuring Proxim Mesh Radio Settings | 109 |
| | Configuring Group MAC Access Control Lists | 111 |
| | Specifying Minimum Firmware Versions for APs in a Group | 112 |
| | Comparing Device Groups | 113 |
| | Deleting a Group | 114 |
| | Changing Multiple Group Configurations | 114 |
| | Modifying Multiple Devices | 115 |
| | Using Global Groups for Group Configuration | 117 |

| | | |
|------------------|---|------------|
| Chapter 5 | Discovering, Adding, and Managing Devices | 121 |
| | Introduction | 121 |
| | Discovery of Devices Overview | 122 |
| | Defining Networks for SNMP/HTTP Scanning | 122 |
| | Adding Networks for SNMP/HTTP Scanning | 123 |
| | Defining Credentials for SNMP/HTTP Scanning | 124 |
| | Defining a SNMP/HTTP Scan Set | 124 |
| | Executing a Scan by Running a Scan Set | 126 |
| | Manually Adding Individual Devices | 129 |
| | Adding Devices with the Device Setup > Add Page | 129 |
| | Adding Access Points, Routers and Switches with a CSV File | 131 |
| | Adding Universal Devices | 133 |
| | Assigning Newly Discovered Devices to Groups | 134 |
| | Overview | 134 |
| | Adding a Newly Discovered Device to a Group | 134 |
| | Verifying That Devices Are Added to a Group | 136 |
| | Troubleshooting a Newly Discovered Device with Down Status | 141 |
| | Replacing a Broken Device | 143 |
| | Verifying the Device Configuration Status | 143 |
| | Moving a Device from Monitor Only to Manage Read/Write Mode | 144 |
| | Configuring Individual Device Settings | 145 |
| | Overview of Individual Device Configuration | 145 |
| | Configuring AP Settings | 145 |
| | Configuring Device Interfaces | 151 |
| | Configuring AP Communication Settings | 151 |
| | Using the OV3600 APs/Devices Pages for AP Communication Settings | 153 |
| Chapter 6 | Creating and Using Templates | 163 |
| | Group Templates | 164 |
| | Supported Device Templates | 164 |
| | Template Variables | 164 |
| | Viewing and Adding Templates | 164 |
| | Configuring General Template Files and Variables | 169 |
| | Configuring General Templates | 169 |
| | Using Template Syntax | 171 |
| | Using Directives to Eliminate Reporting of Configuration Mismatches | 171 |
| | Using Conditional Variables in Templates | 172 |
| | Using Substitution Variables in Templates | 172 |
| | Using AP-Specific Variables | 173 |
| | Configuring Cisco IOS Templates | 175 |
| | Applying Startup-config Files | 175 |
| | WDS Settings in Templates | 175 |
| | SCP Required Settings in Templates | 176 |
| | Supporting Multiple Radio Types via a Single IOS Template | 176 |
| | Configuring Single and Dual-Radio APs via a Single IOS Template | 176 |
| | Configuring Symbol Controller / HP WESM Templates | 177 |
| | Configuring Clustering and Redundancy | 179 |
| | Changing Redundancy Configuration | 179 |
| | Adding Clustering Members | 180 |
| | Configuring a Global Template | 180 |
| Chapter 7 | Using RAPIDS and Rogue Classification | 183 |
| | Overview | 183 |
| | RAPIDS Tabs | 183 |

| | | |
|------------------|--|------------|
| | Additional Rogue Device Resources | 184 |
| | Additional Security-Related Topics | 184 |
| | Monitoring Rogue AP Devices | 184 |
| | Viewing a Rogue AP | 186 |
| | Viewing Ignored Rogue Devices | 189 |
| | Using RAPIDS Workflow to Process Rogue Devices | 190 |
| | Configuring RAPIDS | 190 |
| | Using the Basic Configuration Section | 190 |
| | Configuring Additional RAPIDS Settings in OV3600 | 192 |
| | RAPIDS Rules | 193 |
| | Controller Classification with WMS Offload | 193 |
| | Device OUI Score | 193 |
| | Rogue Device Threat Level | 194 |
| | Viewing and Configuring RAPIDS Rules | 194 |
| | Common RAPIDS Rules Enabled by Default | 198 |
| | Using RAPIDS Rules with Additional OV3600 Functions | 198 |
| | The RAPIDS OUI Score Override | 198 |
| Chapter 8 | Performing Daily Administration in OV3600 | 201 |
| | Introduction | 201 |
| | Creating and Using Triggers and Alerts | 202 |
| | Overview of Triggers and Alerts | 202 |
| | Viewing Triggers | 202 |
| | Creating New Triggers | 202 |
| | Delivering Triggered Alerts | 213 |
| | Viewing Alerts | 214 |
| | Responding to Alerts | 215 |
| | Monitoring and Supporting WLAN Users | 215 |
| | Overview of the Users Pages | 216 |
| | Monitoring WLAN Users With the Users > Connected and Users > All Pages | 216 |
| | Supporting Guest WLAN Users With the Users > Guest Users Page | 218 |
| | Supporting Users on Thin AP Networks With the Users > Tags Page | 221 |
| | Evaluating and Diagnosing User Status and Issues | 222 |
| | Evaluating User Status with the Users > User Detail Page | 222 |
| | Using the Deauthenticate User Feature | 223 |
| | Evaluating User Status with the Users > Diagnostics Page | 223 |
| | Supporting OV3600 Stations with the Master Console | 227 |
| | Adding a Managed OV3600 with the Master Console | 227 |
| | Monitoring and Supporting OV3600 with the Home Pages | 229 |
| | Overview of the Home Pages | 229 |
| | Monitoring OV3600 with the Home > Overview Page | 229 |
| | Viewing and Updating License Information with the Home > License Page | 232 |
| | Searching OV3600 with the Home > Search Page | 232 |
| | Accessing OV3600 Documentation with the Home > Documentation Page | 234 |
| | Configuring Your Own User Information with the Home > User Info Page | 235 |
| | Monitoring and Supporting OV3600 with the System Pages | 236 |
| | Using the System > Status Page | 236 |
| | Using the System > Event Logs Page | 238 |
| | Using the System > Configuration Change Jobs Page | 239 |
| | Using the System > Performance Page | 239 |
| | Upgrading OV3600 | 242 |
| | Upgrade Instructions | 242 |
| | Upgrading Without Internet Access | 242 |
| | Backing Up OV3600 | 242 |
| | Overview of Backups | 242 |

| | | |
|-------------------|--|------------|
| | Viewing and Downloading Backups | 242 |
| | Running Backup on Demand | 243 |
| | Restoring from a Backup | 243 |
| | OV3600 Failover | 243 |
| | Adding Watched OV3600 Stations | 244 |
| Chapter 9 | Creating, Running, and Emailing Reports | 247 |
| | Introduction | 247 |
| | Overview of OV3600 Reports | 248 |
| | Supported Report Types in OV3600 | 248 |
| | Reports > Definitions Page Overview | 249 |
| | Reports > Generated Page Overview | 251 |
| | Using Daily Reports | 252 |
| | Viewing Generated Reports | 252 |
| | Using Custom Reports | 253 |
| | Using the Capacity Planning Report | 254 |
| | Using the Configuration Audit Report | 255 |
| | Using the Device Summary Report | 257 |
| | Using the Device Uptime Report | 259 |
| | Using the IDS Events Report | 261 |
| | Using the Inventory Report | 262 |
| | Using the Memory and CPU Utilization Report | 263 |
| | Using the Network Usage Report | 264 |
| | Using the New Rogue Devices Report | 265 |
| | Using the New Users Report | 267 |
| | Using the PCI Compliance Report | 268 |
| | Using the RADIUS Authentication Issues Report | 270 |
| | Using the User Session Report | 271 |
| | Defining Reports | 274 |
| | Emailing and Exporting Reports | 278 |
| | Emailing Reports in General Email Applications | 278 |
| | Emailing Reports to Smarthost | 278 |
| | Exporting Reports to XML | 278 |
| Chapter 10 | Using the OV3600 Helpdesk | 279 |
| | Introduction | 279 |
| | OV3600 Helpdesk Overview | 279 |
| | Monitoring Incidents with Helpdesk | 280 |
| | Creating a New Incident with Helpdesk | 281 |
| | Creating New Snapshots or Incident Relationships | 282 |
| | Using the Helpdesk Tab with an Existing Remedy Server | 283 |
| Appendix A | Package Management for OV3600 | 287 |
| | Yum for OV3600 | 287 |
| | Package Management System Advisories for OV3600 | 287 |
| Appendix B | Third-Party Security Integration for OV3600 | 289 |
| | Introduction | 289 |
| | Bluesocket Integration | 289 |
| | ReefEdge Integration | 290 |
| | HP ProCurve 700wl Series Secure Access Controllers Integration | 290 |
| | Requirements | 290 |
| | Example Network Configuration | 290 |
| | HP ProCurve 700wl Series Configuration | 291 |
| Appendix C | Access Point Notes | 293 |

| | | |
|-------------------|---|------------|
| | Resetting Cisco (VxWorks) Access Points | 293 |
| | Introduction | 293 |
| | Connecting to the AP | 293 |
| | Determining the Boot-Block Version | 293 |
| | Resetting the AP (for Boot-Block Versions from 1.02 to 11.06) | 294 |
| | Resetting the AP (for Boot-Block Versions 11.07 and Higher) | 294 |
| | IOS Dual Radio Template | 295 |
| | Speed Issues Related to IOS Firmware Upgrades | 296 |
| | OV3600 Firmware Upgrade Process | 296 |
| Appendix D | Initiating a Support Connection | 297 |
| | Network Requirements | 297 |
| | Procedure | 297 |
| Appendix E | Cisco Clean Access Integration (Perfigo) | 299 |
| | Requirements | 299 |
| | Adding OV3600 as RADIUS Accounting Server | 299 |
| | Configuring Data in Accounting Packets | 299 |
| Appendix F | HP Insight Install Instructions for OV3600 Servers | 301 |
| Appendix G | Installing OV3600 on VMware ESX (3i v. 3.5) | 303 |
| | Creating a New Virtual Machine to Run OV3600 | 303 |
| | Installing OV3600 on the Virtual Machine | 303 |
| | OV3600 Post-Installation Issues on VMware | 304 |
| Appendix H | Third-Party Copyright Information | 305 |
| | Copyright Notices | 305 |
| | Packages | 305 |

This preface provides an overview of this document, a list of general documentation supporting OV3600 Version 6.4, and contact information for Alcatel-Lucent with 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 Air Manager (OV3600), Version 6.4. This includes wide deployment of wireless access points (APs), device administration, rogue detection and classification, wireless controller devices, security, reports, and additional features of OV3600 6.4.

Table 1 *Document Organization and Purposes*

| Chapter | Description |
|---|---|
| Chapter 1, "Introduction to the OmniVista Air Manager (OV3600)" | Introduces and presents the OmniVista Air Manager (OV3600), Version 6.4, OV3600 components, and general network functions. |
| Chapter 2, "Installing the OmniVista Air Manager (OV3600)" | Describes system and network requirements, Linux OS installation, and OV3600 installation. |
| Chapter 3, "Configuring the OmniVista Air Manager (OV3600)" | Describes the primary and required configurations for startup and launch of OV3600 6.4, with frequently used optional configurations. |
| Chapter 4, "Configuring and Using Device Groups in OV3600" | Describes configuration and deployment for group device profiles. |
| Chapter 5, "Discovering, Adding, and Managing Devices" | Describes how to discover and manage devices on the network. |
| Chapter 6, "Creating and Using Templates" | Describes and illustrates the use of templates in group and global device configuration. |
| Chapter 7, "Using RAPIDS and Rogue Classification" | Describes the RAPIDS module of OV3600, and enhanced rogue classification supported in OV3600 6.4. |
| Chapter 8, "Performing Daily Administration in OV3600" | Describes common daily operations and tools in OV3600 6.4, to include general user administration, the use of triggers and alerts, network monitoring, and backups. |
| Chapter 9, "Creating, Running, and Emailing Reports" | Describes OV3600 reports, scheduling and generation options, and distribution of reports from OV3600 6.4. |
| Chapter 10, "Using the OV3600 Helpdesk" | Describes how to use the OV3600 6.4 Helpdesk GUI and related functions. |
| Appendix A, "Package Management for OV3600" | Describes the Yum packaging management system, and provides advisories on alternative methods that may cause issues with OV3600. |
| Appendix B, "Third-Party Security Integration for OV3600" | Describes additional and optional security configurations in OV3600 Version 6.4. |

Table 1 Document Organization and Purposes

| Chapter | Description |
|--|---|
| Appendix C, "Access Point Notes" | Provides guidelines and suggestions for Access Point devices in OV3600. |
| Appendix D, "Initiating a Support Connection" | Provides instructions about how to create and use a support connection between OV3600 and Alcatel-Lucent Wireless Support. |
| Appendix E, "Cisco Clean Access Integration (Perfigo)" | Provides instructions for integrating Cisco Clean Access within OV3600. |
| Appendix F, "HP Insight Install Instructions for OV3600 Servers" | Provides instructions for installing HP Insight on OV3600 6.4 servers. |
| Appendix G, "Installing OV3600 on VMware ESX (3i v. 3.5)" | Provides instructions for an alternative installation option on VMware ESX for OV3600 Version 6.4. |
| Appendix H, "Third-Party Copyright Information" | Presents multiple copyright statements from multiple equipment vendors that interoperate with OV3600 Version 6.4. |
| Index | Provides extensive citation of and links to document topics, with emphasis on the OV3600 6.4 GUI and tasks relating to OV3600 6.4 installation and operation. |

Text Conventions

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

Table 2 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 | http://service.esd.alcatel-lucent.com |
| Alcatel-Lucent Enterprise Service and OmniVista 3600 Email Support | Esd.support@alcatel-lucent.com |

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

This *User Guide* provides instructions for the installation, configuration, and operation of the OmniVista Air Manager (OV3600). This chapter contains the following topics:

- [OV3600—A Unified Wireless Network Command Center](#)
- [VisualRF™](#)
- [RAPIDS™](#)
- [Master Console and Failover](#)
- [Integrating OV3600 into the Network and Organizational Hierarchy](#)

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

OV3600—A Unified Wireless Network Command Center

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

The OmniVista Air Manager (OV3600) supports hardware from leading wireless vendors, including Alcatel-Lucent, Aruba Networks, Avaya, Cisco (Aironet and WLC), Colubris Networks, Enterasys, Juniper Networks, LANCOM Systems, Meru, Nomadix, Nortel, ProCurve by HP, Proxim, Symbol, Trapeze, Tropos, and many others.

The components of the OmniVista Air Manager (OV3600) are as follows:

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

VisualRF™

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

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

RAPIDS™

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

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

Master Console and Failover

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

- Provides network-wide visibility, even when the WLAN grows to 50,000+ devices.
- Executive Portal allows executives to view high-level usage and performance data.
- Aggregated Alerts
- Failover
 - Many-to-one failover
 - One-to-one failover
- The **Master Console** and **Failover** servers can be configured with a **Device Down** trigger that generates an alert if communication is lost. In addition to generating an alert, the **Master Console** or **Failover** server can also send email or NMS notifications about the event. See [“Using Triggers and Alerts” on page 232](#).

Integrating OV3600 into the Network and Organizational Hierarchy

OV3600 generally resides in the NOC and communicates with various components of your WLAN infrastructure. In basic deployments, OV3600 communicates solely with indoor wireless access points and WLAN controllers over the wired network. In more complex deployments OV3600 seamlessly integrates and communicates with authentication servers, accounting servers, TACACS+ servers, routers, switches, network management servers, wireless IDS solutions, help systems, indoor wireless access points, mesh devices, and WiMAX devices.

OV3600 has the flexibility to manage devices on local networks, remote networks, and networks using Network Address Translation (NAT). OV3600 communicates over-the-air or over-the-wire utilizing a variety of protocols.

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

Table 1 *Components of a Wireless LAN*

| Component | Description |
|-------------------|---|
| Autonomous AP | Standalone device which performs radio and authentication functions |
| Thin AP | Radio-only device coupled with WLAN Controller to perform authentication |
| WLAN Controller | Used in conjunction with Thin APs to coordinate authentication and roaming |
| NMS | Network Management Systems and Event Correlation (OpenView, Tivoli, and so forth) |
| RADIUS Auth. | RADIUS Authentication servers (Funk, FreeRADIUS, ACS, or IAS) |
| RADIUS Accounting | OV3600 itself serves as a RADIUS accounting client |
| Wireless Gateways | Provide HTML redirect and/or wireless VPNs |
| TACACS+ | Used to authenticated OV3600 administrative users |
| Routers/Switches | Provide OV3600 with data for user information and AP and Rogue discovery |
| Help Desk Systems | Remedy EPICOR |
| 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 give read-only access to monitoring all devices from the **Master Console**.

Introduction

This chapter contains information and procedures to install and launch the OmniVista Air Manager (OV3600). This chapter contains the following topics:

OV3600 Hardware Requirements and Installation Media

Installing Linux CentOS 5 (Phase 1)

Installing OV3600 Software (Phase 2)

- Step 1: Configuring Date and Time, Checking for Prior Installations
- Step 2: Installing OV3600 Software, Including OV3600
- Step 3: Checking the OV3600 Installation
- Step 4: Assigning an IP Address to the OV3600 System
- Step 5: Naming the OV3600 Network Administration System
- Step 6: Assigning a Host Name to the OV3600
- Step 7: Changing the Default Root Password
- Completing the Installation

Configuring and Mapping Port Usage for OV3600

OV3600 Navigation Basics

- Status Section
- Navigation Section
- Activity Section
- Help Links in the GUI
- Buttons and Icons

Getting Started with OV3600

- Completing Initial Login



NOTE

OV3600 does not support downgrading to older versions of the code. Significant data would be lost or compromised in such a downgrade.

In unusual circumstances involving return to a prior OV3600 version, the recommended approach is to perform a fresh installation of the prior OV3600 version, then to restore data from a pre-upgrade backup.

OV3600 Hardware Requirements and Installation Media

The OV3600 installation CD includes all software (including the Linux OS) required to complete the installation of the OmniVista Air Manager (OV3600). 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 Support at Esd.support@alcatel-lucent.com.

Installing Linux CentOS 5 (Phase 1)

Perform the following steps to install the Linux CentOS 5 operating system. The Linux installation is a prerequisite to installing OV3600 Version 6.4 on the network management system.



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**.



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

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

The following message appears on the screen.

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

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

boot:

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

1. Allow the installation process to continue in automatic fashion. Installing the CentOS software (Phase I) takes 10 to 20 minutes to complete. This process formats the hard drive and launches Anaconda to install all necessary packages. Anaconda gauges the progress of the installation. Upon completion, the system automatically reboots and ejects the installation CD.
2. Remove the CD from the drive and store in a safe location.

Installing OV3600 Software (Phase 2)

Getting Started

After the reboot, the **GRUB** screen appears.

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

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

Date and Time

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

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

2) Change Time Zone

0) Finish

Ensure that you enter the accurate date and time during this process. *Errors will arise later in the installation if the specified date varies significantly from the actual date.*

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



Changing these settings after the installation can cause a loss of graphical data, and you should avoid delayed configuration.

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

Previous OV3600 Installations

The following message appears after date and time are set.

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

If a previous version of OV3600 software is not discovered, the installation program automatically proceeds to [“Step 2: Installing OV3600 Software, Including OV3600” on page 18](#). If a previous version of the software is discovered, the following message appears on the screen.

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

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



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

Step 2: Installing OV3600 Software, Including OV3600

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

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

This step requires no user input, but you have the option of monitoring progress in more detail should you wish to do so:

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

Step 3: Checking the OV3600 Installation

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

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

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

Step 4: Assigning an IP Address to the OV3600 System

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

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

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

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

9) Commit Changes
0) Exit (discard changes)
```

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

1. Enter the network information.



The Secondary DNS setting is an optional field.

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

Step 5: Naming the OV3600 Network Administration System

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

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

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

Step 6: Assigning a Host Name to the OV3600

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

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

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

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

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

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

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

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

Proceed to the next step as the system prompts you.

Step 7: Changing the Default Root Password

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

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

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

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

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

Completing the Installation

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

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

- To view the Phase 1 installation log file, type **cat /root/install.log**.
- To view the Phase 2 installation log file, type **cat /tmp/OV3600-install.log**.
- To access the OV3600 GUI, enter the OV3600 IP address in the address bar of any 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 [“Supporting OV3600 Stations with the Master Console”](#) on page 227 for additional information.

Configuring and Mapping Port Usage for OV3600

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

Table 2 *OV3600 Protocol and Port Chart*

| Port | Type | Protocol | Description | Dataflow Direction | Device Type |
|------|------|----------|---------------------------------------|--------------------|-------------------------------------|
| 21 | TCP | FTP | Configure devices and FW distribution | > | Legacy AP (Cisco 4800) |
| 22 | TCP | SSH | Configure devices | > | APs or controllers |
| 22 | TCP | SSH | Configure OV3600 from CLI | < | Laptop or workstation |
| 22 | TCP | VTUN | Support connection (optional) | > | Alcatel-Lucent support home office |
| 22 | TCP | SCP | Transfer configuration files or FW | < | APs or controllers |
| 23 | TCP | Telnet | Configure devices | > | APs or controllers |
| 23 | TCP | VTUN | Support connection (Optional) | > | Alcatel-Lucent support home office |
| 25 | TCP | SMTP | Support email (optional) | > | Alcatel-Lucent support email server |
| 49 | UDP | TACACS | OV3600 Administrative Authentication | > | Cisco TACACS+ |
| 53 | UDP | DNS | DNS lookup from OV3600 | > | DNS Server |
| 69 | UDP | TFTP | Transfer configuration files or FW | < | APs or Controllers |
| 80 | TCP | HTTP | Configure devices | > | Legacy APs |
| 80 | TCP | HTTP | Firmware upgrades | < | Colubris devices |
| 80 | TCP | VTUN | Support connection (optional) | > | Alcatel-Lucent support home office |
| 161 | UDP | SNMP | Get and Set operations | > | APs or controllers |
| 162 | UDP | SNMP | Traps from devices | < | APs or controllers |
| 162 | UDP | SNMP | Traps from OV3600 | > | NMS |
| 443 | TCP | HTTPS | Web management | < | Laptop or workstation |
| 443 | TCP | HTTPS | WLSE polling | > | WLSE |
| 443 | TCP | VTUN | Support connection (optional) | > | Alcatel-Lucent support home office |

Table 2 OV3600 Protocol and Port Chart (Continued)

| Port | Type | Protocol | Description | Dataflow Direction | Device Type |
|------|------|----------|---|--------------------|-------------------------|
| 1701 | TCP | HTTPS | AP and rogue discovery | > | WLSE |
| 1741 | TCP | HTTP | WLSE polling | > | WLSE |
| 1813 | UDP | RADIUS | Retrieve client authentication info | < | Accounting Server |
| 1813 | UDP | RADIUS | Retrieve client authentication info | < | AP or Controllers |
| 1813 | UDP | RADIUS | Outbound from OV3600 to a RADIUS server for OV3600 administrator authentication | > | RADIUS server |
| 2002 | TCP | HTTPS | Retrieve client authentication info | > | ACS |
| 5050 | UDP | RTLS | Real Time Location Feed | < | Alcatel-Lucent thin APs |
| 8211 | UDP | PAPI | Real Time Feed | < > | WLAN switches |
| | | ICMP | Ping Probe | > | APs or controllers |

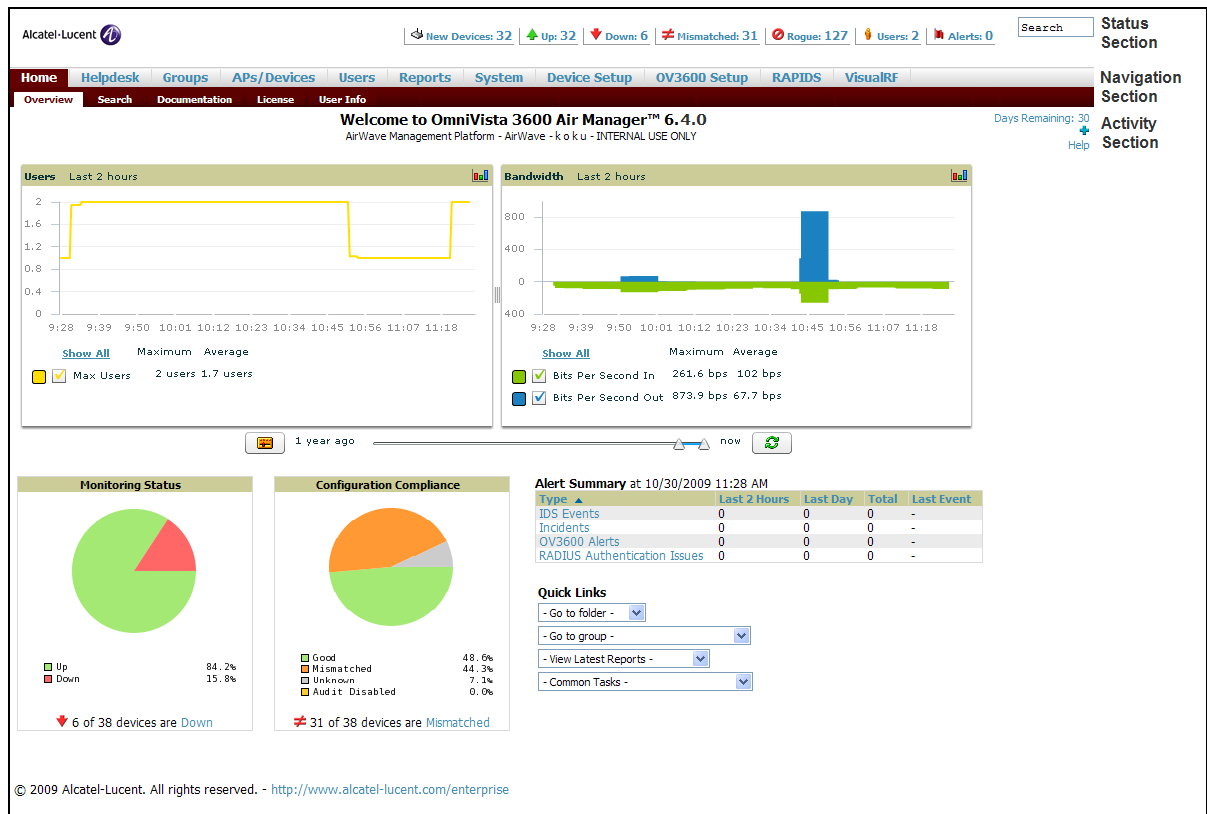
OV3600 Navigation Basics

Every OV3600 page contains three basic sections, as follows:

- Status Section
- Navigation Section
- Activity Section

The OV3600 pages also contain **Help** links with GUI-specific help information and certain standard action buttons. [Figure 1](#) illustrates these sections.

Figure 1 Home > Overview Page Illustration



Status Section

The **Status** section provides a snapshot view of overall WLAN performance and provides direct links for immediate access to key system components. The Status section remains at the top of all pages in the OV3600 and RAPIDS modules. OV3600 6.4 introduces the ability to customize the contents of the Status section from the **Home > User Info** page, to include support for both wireless and wired network components. Refer to [“Configuring Your Own User Information with the Home > User Info Page” on page 235](#).

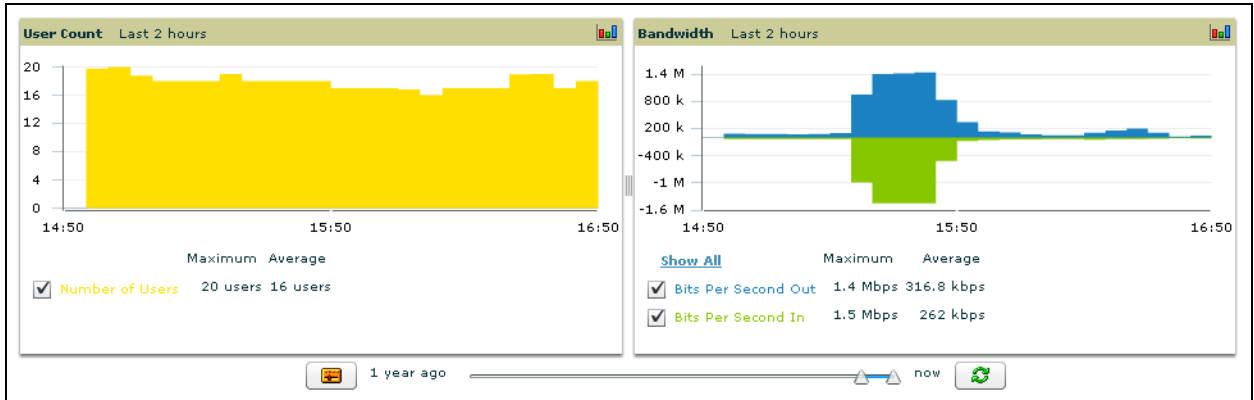
The table below describes these elements in further detail.

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

| Field | Description |
|--|--|
| New Devices | The number of wireless APs or wireless LAN switches/controllers that have been discovered by OV3600 but not yet managed by network administrators. When you click this link, OV3600 directs you to a page that displays a detailed list of devices awaiting authorization. |
| Up (Wired, Wireless, and combined) | The number of managed, authorized devices that are currently responding to OV3600 requests. When you click this link, OV3600 will direct you to a page that displays a detailed list of all Up devices. |
| Down (Wired, Wireless, and combined) | The number of managed, authorized devices that are not currently responding to OV3600 SNMP requests. When you click this link, OV3600 will direct you to a page that displays a detailed list of all "Down" devices. |
| Mismatched | The total number of Mismatched devices. A device is considered mismatched when the desired configuration in OV3600 does not match the actual device configuration read from the device. |
| Rogue | The number of devices that have been classified by the RAPIDS rules engine above the threshold defined on the Home > User Info page. |
| Users | The number of wireless users currently associated to the wireless network via all the APs managed by OV3600. When you click this link, OV3600 directs you to a page that contains a list of users that are associated. |
| Alerts | Displays the number of non-acknowledged OV3600 alerts generated by user-configured triggers. When you click this link, OV3600 directs you to a page containing a detailed list of active alerts. |
| Severe Alerts (conditional) | When triggers are given a severity of Critical , they generate Severe Alerts . When a Severe Alert exists, a new component appears at the right of the Status field in bold red font. Only users configured on the Home > User Info page to be enabled to view critical alerts can see Severe Alerts. The functionality of Severe Alerts is the same as that described above for Alerts. However, unlike Alerts, the Severe Alerts section is hidden if there are no Severe Alerts. |
| Device Types to Include in Header Stats | You can support statistics for any combination of the following device types: <ul style="list-style-type: none"> ● Autonomous APs ● Controllers ● Routers/Switches ● Thin APs ● Universal Devices Refer to “Configuring Your Own User Information with the Home > User Info Page” on page 235 . |
| 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 to change graph attributes, as shown in Figure 2.

Figure 2 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 checkboxes to change the data displayed on each graph. The button with green arrows refreshes data on the graph.
- The **Show All** link displays all of the available checkboxes supporting the flash graphs.
- Once a change to the slider bars or to the display boxes has been made, the same change can be applied to all other flash graphs with an **apply** button (appears on mouse-over only).
- For non-flash graphs, click the graph to open a popup window that shows historical data.

A non-flash version of the OV3600 user page is available if desired; instead of flash it uses the RRD graphs that were used in OV3600 through the 5.3 Version. Contact Alcatel-Lucent support for more information on activating this feature in the OV3600 database.

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 pages provide 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 “Monitoring and Supporting OV3600 with the Home Pages” on page 229.</p> | <ul style="list-style-type: none"> • Overview • Search • Documentation • License • User Info |
| Helpdesk | <p>The Helpdesk pages provide an interface for support and diagnostic tools.</p> <p>For additional information refer to Chapter 10, “Using the OV3600 Helpdesk” on page 279.</p> | <ul style="list-style-type: none"> • Incidents • Setup |

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

| Main Tab | Description | Sub-Menus |
|--------------------|---|---|
| Groups | <p>The Groups pages provide information on the logical "groups" of devices that have been established for efficient monitoring and configuration. For additional information, see Chapter 4, "Configuring and Using Device Groups in OV3600" on page 73.</p> <p>NOTE: Some of the focused sub-menus will not appear for all groups. Focused sub-menus are visible based on the device type field on the Groups > Basic page. This sub-menu is the first page to appear when adding or editing groups.</p> <p>NOTE: When individual device configurations are specified, device-level settings override the Group-level settings to which a device belongs.</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 Ⓢ Alcatel-Lucent Config Ⓢ Cisco WLC Config Ⓢ PTMP/WiMAX Ⓢ Proxim Mesh Ⓢ Colubris Ⓢ MAC ACL Ⓢ Firmware Ⓢ Compare (Master Console Only) |
| APs/Devices | <p>The APs/Devices pages provide detailed information about all authorized APs and wireless LAN switches or controllers on the network, including all configuration and current monitoring data.</p> <p>These pages interact with several additional pages in OV3600. One chapter to emphasize the APs/Devices pages is Chapter 5, "Discovering, Adding, and Managing Devices" on page 121.</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 Ⓢ Interfaces (Router/Switch only) |
| Users | <p>The Users pages provide detailed information about all client devices and users currently associated to the WLAN. For additional information, refer to "Monitoring and Supporting WLAN Users" on page 215.</p> | <ul style="list-style-type: none"> ● Connected ● All ● Guest Users ● User Detail ● Diagnostics ● Tags |
| Reports | <p>The Reports pages list all the standard and custom reports generated by OV3600. OV3600 supports 13 reports in the OV3600 module. For additional information, refer to Chapter 9, "Creating, Running, and Emailing Reports" on page 247.</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 "Monitoring and Supporting OV3600 with the System Pages" on page 236.</p> | <ul style="list-style-type: none"> ● Status ● Event Log ● Triggers ● Alerts ● Configuration Change Jobs ● Firmware Upgrade Jobs ● Performance |

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

| Main Tab | Description | Sub-Menus |
|---------------------|---|---|
| Device Setup | The Device Setup pages provide the ability to add, configure, and monitor devices, to include setting AP discovery parameters, performing firmware management, defining VLANs, and so forth. For additional information, refer to “Enabling OV3600 to Manage Your Devices” on page 44. | <ul style="list-style-type: none"> ● Discover ● Add ● Communication ● Alcatel-Lucent Configuration ● Upload Files |
| OV3600 Setup | The OV3600 Setup pages provide all information relating to the configuration of OV3600 itself and its connection to your network. This page entails several processes, configurations, or tools in OV3600. For additional information, start with Chapter 3, “Configuring the OmniVista Air Manager (OV3600)” on page 31. NOTE: The OV3600 Setup pages may not be visible, depending on the role and license set in OV3600. | <ul style="list-style-type: none"> ● General ● Network ● Users ● Roles ● Authentication ● WLSE ● ACS ● NMS ● RADIUS Accounting ● PCI Compliance |
| RAPIDS | The RAPIDS pages provide all information relating to rogue access points, including methods of discovery and lists of discovered and possible rogues. For additional information, refer to Chapter 7, “Using RAPIDS and Rogue Classification” on page 183. NOTE: The RAPIDS pages may not be visible, depending on the role and license set in OV3600. | <ul style="list-style-type: none"> ● Overview ● Rogue APs ● Setup ● Rules ● Score Override |
| VisualRF | VisualRF pages provide graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network. For additional information, refer to the <i>VisualRF User Guide</i> . NOTE: VisualRF may not be visible, depending on the role and license set in OV3600. | <ul style="list-style-type: none"> ● Overview ● Floor Plans ● Campus/Building ● Setup ● Import |



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

Activity Section

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

Help Links in the GUI

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



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

Common List Settings

All of the lists in OV3600 have some common options. All lists are paginated with a configurable number of items per page, as shown in [Figure 3](#).

Figure 3 Example of Common List Settings Configurable Attributes

| Username | Role | MAC Address | AP/Device | Location | SSID |
|----------|------|-------------------|----------------------|----------|-------------------------------|
| - | - | 00:22:FA:BA:B7:62 | CiscoIOS1100-12.3(2) | - | muirtest1200 |
| - | - | 00:24:2C:05:BB:C3 | CiscoIOS1100-12.3(2) | - | muirtest1200 |
| - | - | 00:1C:B3:05:44:1E | RoamAbout AP | - | RoamAbout Default Network Nam |
| - | - | 00:23:12:DF:D8:F5 | CiscoIOS1100-12.3(2) | - | muirtest1200 |
| - | - | 00:22:41:0C:40:39 | ag-2100 | - | - |

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

Clicking on the left most down arrow allows you to set how many rows appear on one page of the list. The next down arrow is used to jump to a specific page in the list. Clicking it will bring up a drop down menu that allows you to select the exact page you would like to view, as shown in [Figure 4](#).

Figure 4 Common List Settings Choose Columns Illustration

| Username | Role | MAC Address | AP/Device | Location | SSID |
|----------|------|-------------------|-----------|----------|----------------------------------|
| - | - | 00:22:FA:BA:B7:62 | Cisco | | muirtest1200 |
| - | - | 00:24:2C:05:BB:C3 | Cisco | | muirtest1200 |
| - | - | 00:1C:B3:05:44:1E | Roam | | RoamAbout Default Network Name 0 |
| - | - | 00:23:12:DF:D8:F5 | Cisco | | muirtest1200 |
| - | - | 00:22:41:0C:40:39 | ag-2 | | - |

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

Save | Cancel

- Username ↑↓
- Role ↑↓
- MAC Address ↑↓
- AP/Device ↑↓
- Location ↑↓
- SSID ↑↓
- VLAN ↑↓
- AP Radio ↑↓
- Connection Mode ↑↓
- Ch BW ↑↓
- Association Time ↑↓
- Duration ↑↓
- LAN IP Address ↑↓
- LAN Hostname ↑↓
- Guest User ↑↓
- VPN IP Address ↑↓
- VPN Hostname ↑↓

1-5 of 5 Users Page 1 of 1

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

| Type ▲ | Last 2 Hours | Event |
|------------------------------|--------------|-------|
| Incidents | 0 | |
| OV3600 Alerts | 0 | |
| RADIUS Authentication Issues | 0 | |

The **Choose Columns** option allows you to configure the columns that are presented in the list and the order in which they are presented. To disable a column simply uncheck the checkbox. To reorder the columns, click and drag a specific row to the appropriate new position. When you are satisfied with the enabled columns and their order, click on the save button.

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

Buttons and Icons

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

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

















| Buttons and Icons | Appearance ^a | Description |
|----------------------|---|---|
| Acknowledge | | Acknowledges and clears an OV3600 alert. |
| Add | | Adds the object to both OV3600' database and the onscreen display list. |
| Add Folder |  | Adds a new folder to hierarchically organize APs. |
| Alert |  | Indicates an alert. |
| Apply | | Applies all "saved" configuration changes to devices on the WLAN. |
| Attach |  | Attaches a snapshot of an OV3600 screen to a Helpdesk incident. |
| Audit | | Reads device configuration, compare to desired, and update status. |
| Bandwidth |  | Displays current bandwidth for group. |
| Choose |  | Chooses a new Helpdesk incident to be the Current Incident. |
| Create |  | Creates a new Helpdesk incident. |
| Customize | | Ignores selected settings when calculating the configuration status. |
| Delete |  | Deletes an object from OV3600' database. |
| Down |  | Indicates down devices and radios. |
| Drag and Drop |  | Dragging and dropping objects with this icon changes the sequence of items in relation to each other. Refer to "Using RAPIDS and Rogue Classification" on page 183 as one example of drag-and-drop. |
| Duplicate |  | Duplicates or makes a copy of the configuration of an OV3600 object. |
| Edit |  | Edits the object properties. |
| Email |  | Links to email reports. |
| Filter | | Filters rogue list by score and/or ad hoc status. |
| Google Earth |  | Views device's location in Google Earth (requires plug-in). |
| Manage |  | Manages the object properties. |
| Mismatched |  | Indicates mismatched device configuration, in which the most recent configuration in OV3600 and the current configuration on a device are mismatched. |
| Monitor |  | Indicates an access point is in "monitor only" mode. |

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

| Buttons and Icons | Appearance ^a | Description |
|---------------------------------|---|--|
| Ignore | | Ignores specific device(s) - devices selected with check boxes. |
| Import | | Updates a Group's desired settings to match current settings. |
| Mismatched | | Indicates mismatched access points. |
| New Devices |  | Indicates new access points and devices. |
| Poll Now | | Polls device (or controller) immediately, override group polling settings. |
| Preview | | Displays a preview of changes applicable to multiple groups. |
| Print |  | Prints the report. |
| Reboot | | Reboots devices or OV3600. |
| Refresh |  | Refreshes the display of flash graphs when settings have changed. |
| Relate |  | Relates an AP, Group or Client to a Helpdesk incident. |
| Replace Hardware | | Confers configuration and history of one AP to a replacement device. |
| Revert | | Returns all configurable data on the screen to its original status. |
| Rogue |  | Indicates a rogue access point. |
| Run | | Runs a new user-defined report. |
| Save | | Saves the information on the page in the OV3600 database. |
| Save & Apply | | Saves changes to OV3600' database and apply all changes to devices. |
| Scan | | Scans for devices and rogues using selected networks. |
| Schedule | | Schedules a window for reports, device changes, or maintenance. |
| Search |  | Searches OV3600 for the specified name, MAC or IP address. |
| Set Time Range |  | Sets the time range for flash graphs to the range specified with the time-range bar. |
| Up |  | Indicates access points which are in the up status. |
| Update Firmware | | Applies a new firmware image to an AP/device. |
| User |  | Indicates a user. |
| View Graph in New Window |  | Displays flash graphs in a new window. |
| VisualRF |  | Links to VisualRF - real time visualization. |
| XML |  | Links to export XHTML versions of reports. |

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

Getting Started with OV3600

This topic describes how to perform an initial launch of the OV3600 network management solution. This topic requires successful completion of installation, as described earlier in this chapter. This topic prepares the administrator for wider deployment and device support and operations once initial startup is complete.

Completing Initial Login

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

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

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

Required or Important Configurations

- Defining General OV3600 Server Settings
- Defining OV3600 Network Settings
- Creating OV3600 Users
- Creating OV3600 User Roles
- Enabling OV3600 to Manage Your Devices

Additional and Advanced Configurations

- Configuring TACACS+ and RADIUS Authentication
- Configuring Cisco WLSE and WLSE Rogue Scanning
- Configuring ACS Servers
- Integrating OV3600 with an Existing Network Management Solution (NMS)
- Integrating a RADIUS Accounting Server
- Auditing PCI Compliance on the Network
- Deploying WMS Offload
 - Overview of WMS Offload in OV3600
 - General Configuration Tasks Supporting WMS Offload in OV3600
 - Additional Information Supporting WMS Offload



Additional configurations of multiple types are available after basic configurations in this chapter are complete.

Defining General OV3600 Server Settings

The first step in configuring OV3600 is to specify the general settings for the OV3600 server. Figure 6 illustrates the **OV3600 Setup > General** page, enhanced in OV3600 6.4:

Figure 6 **OV3600 Setup > General Page Illustration**

| General | | Historical Data Retention | |
|--|--|---|---|
| System Name: | <input type="text" value="OV3600 Server Name"/> | Inactive User Data (2-1500 days): | <input type="text" value="60"/> |
| Automatically Monitor/Manage New Devices: | <input type="button" value="No"/> | User Association History (2-550 days): | <input type="text" value="14"/> |
| Default Group: | <input type="button" value="Access Points (SSID: alcatel-lucent-ap)"/> | Tag History (2-550 days): | <input type="text" value="14"/> |
| Device Configuration Audit Interval: | <input type="button" value="Daily"/> | Rogue AP Discovery Events (2-550 days): <small>Cannot be smaller than the 'Delete Rogues not detected for' window (0) configured on the RAPIDS Setup page.</small> | <input type="text" value="14"/> |
| Automatically Repair Misconfigured Devices: | <input type="radio"/> Yes <input checked="" type="radio"/> No | Reports (2-550 days): | <input type="text" value="60"/> |
| Send Debugging Messages to Alcatel-Lucent: | <input checked="" type="radio"/> Yes <input type="radio"/> No | Automatically Acknowledge Alerts (0-550 days, zero disables): | <input type="text" value="14"/> |
| Nightly Maintenance Time (00:00 - 23:59): | <input type="text" value="04:15"/> | Acknowledged Alerts (2-550 days): | <input type="text" value="60"/> |
| OV3600 User Authorization Lifetime (0-240 min): | <input type="text" value="0"/> | Traps from Managed Devices (0-550 days, zero disables): | <input type="text" value="14"/> |
| Top Header Stats | | Archived Device Configurations (1-100): | <input type="text" value="10"/> |
| Stats: | <input checked="" type="checkbox"/> New Devices <input checked="" type="checkbox"/> Up (Wired & Wireless) <input type="checkbox"/> Up (Wired) <input type="checkbox"/> Up (Wireless) <input checked="" type="checkbox"/> Down (Wired & Wireless) <input type="checkbox"/> Down (Wired) <input type="checkbox"/> Down (Wireless) <input checked="" type="checkbox"/> Mismatched <input checked="" type="checkbox"/> Rogues <input checked="" type="checkbox"/> Users <input checked="" type="checkbox"/> Alerts <input type="button" value="Select All - Unselect All"/> | Guest Users (0-550 days, zero disables): | <input type="text" value="30"/> |
| Include Device Types: | <input checked="" type="checkbox"/> Autonomous APs <input checked="" type="checkbox"/> Controllers <input checked="" type="checkbox"/> Routers/Switches <input checked="" type="checkbox"/> Thin APs <input checked="" type="checkbox"/> Universals <input type="button" value="Select All - Unselect All"/> | Closed Helpdesk Incidents (0-550 days, zero disables): | <input type="text" value="30"/> |
| Display Options | | Inactive SSIDs (0-550 days, zero disables): | <input type="text" value="425"/> |
| Use Fully Qualified Domain Names: Cisco IOS/Aruba/Alcatel-Lucent only | <input type="radio"/> Yes <input checked="" type="radio"/> No | Default Firmware Upgrade Options | |
| Show Vendor-Specific Device Settings For: | <input type="button" value="Only devices on this OV3600"/> | Allow Firmware Upgrades in Monitor-Only Mode: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Selected Device Types: | 3Com 8750, Alcatel-Lucent, Aruba, Cisco IOS, Cisco VxWorks, Cisco WLC, Enterasys RoamAbout AP3000/AP4102, HP ProCurve 420, HP ProCurve 530, Nomadix, Proxim, Proxim MP.11, Symbol, Symbol Wireless Switch, Trapeze | Simultaneous Jobs (1-20): | <input type="text" value="20"/> |
| Look up Wireless User Hostnames: | <input checked="" type="radio"/> Yes <input type="radio"/> No | Simultaneous Devices per Job (1-1000): | <input type="text" value="20"/> |
| DNS Hostname Lifetime: | <input type="button" value="1 hour"/> | Failures Before Stopping (0-20, zero disables): | <input type="text" value="1"/> |
| AP Troubleshooting Hint: Displayed along with the 'Down' reason if a device's upstream device is up. | <input type="text"/> | Additional OV3600 Services | |
| Configuration Options | | Enable FTP Server: required to manage Cisco WLC and Aironet 4800 APs; optional for FTP upgrades on supported devices. | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Allow Guest User Configuration in Monitor-Only Mode: | <input type="radio"/> Yes <input checked="" type="radio"/> No | Enable RTLS Collector: Aruba/Alcatel-Lucent only | <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 | Use Embedded Mail Server: | <input checked="" type="radio"/> Yes <input type="radio"/> No <input type="button" value="Send Test Email"/> |
| Allow Disconnecting Users While in Monitor-Only Mode: | <input type="radio"/> Yes <input checked="" type="radio"/> No | Process User Roaming Traps From Cisco WLC: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Keep Unreferenced Alcatel-Lucent Configuration: | <input type="radio"/> Yes <input checked="" type="radio"/> No | Performance Tuning | |
| External Syslog | | Monitoring Processes (1-2): | <input type="text" value="2"/> |
| Include Event Log Messages: | <input type="radio"/> Yes <input checked="" type="radio"/> No | Maximum Number Of Configuration Processes (1-10): | <input type="text" value="5"/> |
| Include Audit Log Messages: | <input type="radio"/> Yes <input checked="" type="radio"/> No | Maximum Number Of Audit Processes (1-10): | <input type="text" value="3"/> |
| | | Verbose Logging Of SNMP Configuration: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| | | SNMP Rate Limiting for Monitored Devices: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| | | RAPIDS Processing Priority: <small>When OV3600 is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (e.g. client connections and bandwidth) is not adversely impacted.</small> | <input type="button" value="Low"/> |
| | | <small>The default priority is Low. You can also tune your system performance by changing group poll periods.</small> | |
| | | <input type="button" value="Save"/> <input type="button" value="Revert"/> | |

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 described in [Table 6:](#)

Table 6 OV3600 Setup > General > General Section Fields and Default Values

| Setting | Default | Description |
|---|----------|--|
| System Name | OV3600 | Defines your name for the OV3600 server, with a maximum limit of 20 alphanumeric characters. |
| Automatically Monitor/Manage New Devices | No | <p>Launches a drop-down menu that specifies the behavior OV3600 should follow when it discovers a new device. Devices are placed in the default group which is defined in the next field.</p> <ul style="list-style-type: none"> When devices are in Monitor Only mode, OV3600 compares the current configuration with the policy, and displays any discrepancies on the APs/Devices > Audit page, but does not change the configuration of the device. When devices are in Manage Read/Write mode, OV3600 compares the device's current configuration settings with the Group configuration settings and automatically updates the device's configuration to match the Group policy. Automatically placing devices in Managed Read/Write mode will overwrite the configuration with the desired configuration in OV3600, and should only be used when you are certain OV3600 has the correct configuration. This can be risky, and generally, devices should be placed in Monitor Only mode as the default. |
| Default Group | NA | Sets the device group that this OV3600 server uses as the default for device-level configuration. Select a device group from the drop-down menu. A group must first be defined on the Groups > List page to appear in this drop-down menu. For additional information, refer to Chapter 4, "Configuring and Using Device Groups in OV3600" on page 73. |
| Device Configuration Audit Interval | Daily | <p>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.</p> <p>Alcatel-Lucent recommends enabling this feature with a frequency of Daily or more frequently to ensure that your AP configurations comply with your established policies.</p> |
| Automatically Repair Misconfigured Devices | Disabled | If enabled, this setting automatically reconfigures the settings on the device when the device is in Manage mode and OV3600 detects a variance between actual device settings and the Group configuration policy in the OV3600 database. |
| Send Debugging Messages to Alcatel-Lucent | Enabled | If enabled, OV3600 automatically emails any system errors to the Alcatel-Lucent Support Center to assist in debugging. |
| Nightly Maintenance Time (00:00 - 23:59) | 04:15 | Specifies the time of day OV3600 should perform daily maintenance. During maintenance, OV3600 cleans the database, performs backups, and completes a few other housekeeping tasks. Such processes should not be performed during peak hours of demand. |
| OV3600 User Authorization Lifetime (0-240 min) | 120 | Sets the amount of time, in minutes, that an OV3600 user session lasts before the user must authenticate when a new browser window is opened. Setting the lifetime to 0 requires the user to log in every time a new browser window is opened. |
| Check Updates from Alcatel-Lucent | Yes | Enables OV3600 to check automatically for multiple update types. Check daily for OV3600 updates, to include enhancements, device template files, important security updates, and other important news. This setting requires a direct internet connection via OV3600. |

2. Select the **Top Header Stats** by checking the corresponding check box. The selected options will be displayed at the top of GUI. For more detailed information about each option, refer to [Table 3 on page 22](#).
3. On the **OV3600 Setup > General** page, locate the **Display Options** section and adjust settings as required. The **Display Options** section configures which **Group** tabs and options appear by default in new device groups.



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

[Table 7](#) describes the settings and default values in this section.

Table 7 *OV3600 Setup > General > Display Options Section Fields and Default Values*

| Setting | Default | Description |
|--|-------------|---|
| Use Fully Qualified Domain Names | No | Sets OV3600 to use fully qualified domain names for APs instead of the AP name. For example, "testap.yourdomain.com" would be used instead of "testap." This option is supported only for Cisco IOS, Aruba, and Alcatel-Lucent devices. |
| Show Vendor-Specific Device Settings For | All Devices | Displays a drop-down menu that determines which Group tabs and options are viewable by default in new groups, and selects the device types that use fully qualified domain names. This field has three options, as follows: <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, a new field appears listing many device types. This option allows you to specify the device types for which OV3600 displays group settings. You can override this setting at the individual group level. |
| Look Up Wireless User Hostnames | Yes | Enables OV3600 to look up automatically the DNS for new user hostnames. This setting can be turned off to troubleshoot performance issues. |
| DNS Hostname Lifetime | 24 hours | Defines the length of time, in hours, for which a DNS server hostname remains valid on OV3600, after which OV3600 refreshes DNS lookup. Select a time duration from the drop-down menu. Options are as follows: <ul style="list-style-type: none"> • 1 hour • 2 hours • 4 hours • 12 hours • 24 hours |
| AP Troubleshooting Hint | N/A | The message included in this field is displayed along with the Down if a device's upstream device is up. This applies to all APs and controllers but not to routers and switches. |

4. On the **OV3600 Setup > General** page, locate the **Configuration Options** section and adjust settings as required. The settings in this field configure whether certain changes can be pushed to devices in **Monitor Only** mode. [Table 8](#) describes the settings and default values of this section.

Table 8 OV3600 Setup > General > Configuration Options Section Fields and Default Values

| Setting | Default | Description |
|--|---------|--|
| Allow Guest User Configuration in Monitor Only Mode | No | When Yes is selected, new Cisco WLC and Aruba/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 Aruba/Alcatel-Lucent devices only) | No | When Yes is selected, you can enable the Aruba/Alcatel-Lucent WMS offload feature on the Groups > Basic page for WLAN switches in Monitor Only mode. Enabling WMS offload does not cause a controller to reboot. |
| Keep Unreferenced Alcatel-Lucent Configuration | No | Allows OV3600 to retain unused Aruba/Alcatel-Lucent OS configuration profiles. You can define profiles on an WLAN switch but it is not necessary to reference them from a virtual AP configuration or other component of Aruba/Alcatel-Lucent Configuration. Normally OV3600 deletes unreferenced profiles, but this setting retains them when enabled with Yes . NOTE: If this setting is enabled with Yes, then all profiles are pushed to all controllers. In this case, you cannot have different configurations for different controllers. |

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

Table 9 OV3600 Setup > General > External Syslog Section Fields and Default Values

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

- On the **OV3600 Setup > General** page, locate the **Historical Data Retention** section and specify the number of days you wish to keep client session records and rogue discovery events. [Table 10](#) describes the settings and default values of this section.

Table 10 OV3600 Setup > General > Historical Data Retention Fields and Default Values

| Setting | Default | Description |
|--|---------|--|
| Inactive User Data (2-1500 days) | 60 | Defines the number of days OV3600 stores basic information about inactive users. Alcatel-Lucent recommends a shorter setting of 60 days for customers with high user turnover such as hotels or convention centers. The longer you store inactive user data, the more hard disk space you require. |
| User Association History (2-550 days) | 14 | Defines the number of days OV3600 stores client session records. The longer you store client session records, the more hard disk space you require. |
| Tag History (2-550 days) | 14 | Sets the number of days OV3600 retains location history for Wi-Fi tags. |
| Rogue AP Discovery Events (2-550 days) | 14 | Defines the number of days OV3600 stores Rogue Discovery Events. The longer you store discovery event records, the more hard disk space you require. |
| Reports (2-550 days) | 60 | Defines the number of days OV3600 stores Reports. Large numbers of reports, over 1000, can cause the Reports > List page to be slow to respond. |
| Automatically Acknowledged Alerts (0-550 days) | 14 | Defines automatically acknowledged alerts as the number of days OV3600 retains alerts that have been automatically acknowledged. Setting this value to 0 disables this function. |
| 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) | 14 | Defines the number of days OV3600 retains information about SNMP traps from Managed Devices. Setting this value to 0 disables this function. |
| Archived Device Configurations (1-100) | 10 | Sets the number of archived configurations to retain for each device. |
| Guest Users (0-550 days) | 30 | Sets the number of days that OV3600 is to support any guest user. Setting this value to 0 disables this function. |
| Closed Helpdesk Incidents | 30 | Sets the number of days that OV3600 is to retain records of closed Helpdesk incidents once closed. Setting this value to 0 disables this function. |
| Inactive SSIDs | 425 | Sets the number of days OV3600 retains historical information after OV3600 last saw a client on a specific SSID. Settings this value to 0 disables this function. |

7. On the **OV3600 Setup > General** page, locate the **Default Firmware Upgrade Options** section and adjust settings as required. This section allows you to configure the default firmware upgrade behavior for OV3600. [Table 11](#) describes the settings and default values of this section.

Table 11 OV3600 Setup > General > Default Firmware Upgrade Options Fields and Default Values

| Setting | Default | Description |
|---|---------|---|
| Allow Firmware upgrades in Monitor Only mode | No | If yes is selected, OV3600 upgrades the firmware for APs in Monitor Only mode. When OV3600 upgrades the firmware in this mode, the desired configuration are not be pushed to OV3600. Only the firmware is applied. The firmware upgrade may result in configuration changes. OV3600 does not correct those changes when the AP is in Monitor Only mode. |
| Simultaneous Jobs (1-20) | 20 | Defines the number of jobs OV3600 runs at the same time. A job can include multiple APs. |
| Simultaneous Devices per Job (1-1000) | 20 | Defines the number of devices that can be in the process of upgrading at the same time. OV3600 only runs one TFTP transfer at a time. As soon as the transfer to a device has completed, the next transfer begins, even if the first device is still in the process of rebooting or verifying configuration. |
| Failures Before Stopping (0-20) | 1 | Sets the default number of upgrade failures before OV3600 pauses the upgrade process. User intervention is required to resume the upgrade process. Setting this value to 0 disables this function. |

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

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

| Setting | Default | Description |
|---|---------|--|
| Enable FTP Server | No | Enables or disables the FTP server on OV3600. The FTP server is only used to manage Cisco Aironet 4800 APs. Alcatel-Lucent recommends disabling the FTP server if you do not have any Cisco Aironet 4800 APs in the network. |
| Enable RTLS Collector | No | Enables or disables the RTLS Collector, which is used to allow AOS controllers to send RTLS packets to VisualRF. The RTLS server IP address must be configured on each controller. This function is used for VisualRF to improve location accuracy and to locate chirping asset tags. This function is supported only for Aruba and Alcatel-Lucent devices. With selection of Yes , the following additional fields appear: <ul style="list-style-type: none"> ● RTLS Port—Specify the port for the RTLS server. ● RTLS Username—Enter the user name supported by the RTLS server. ● RTLS Password—Enter the RTLS server password. |
| Use Embedded Mail Server | Yes | Enables or disables the embedded mail server that is included with OV3600. This field supports a Send Test Email button for testing server functionality. Clicking this button prompts you with a To and From field in which you must enter valid email addresses, and a button to send a test email. |
| Process User Roaming Traps from Cisco WLC | Yes | OV3600 now parses client association and authentication traps from Cisco WLC controllers to give real time information on users connected to the wireless network. |

9. On the **OV3600 Setup > General** page, locate the **Performance Tuning** section. Performance tuning is unlikely to be necessary for many OV3600 implementations, and likely provides the most improvements for customers with extremely large Pro or Enterprise installations. Please contact Alcatel-Lucent support if you think you might need to change any of these settings. [Table 13](#) describes the settings and default values of this section.

Table 13 OV3600 Setup > General > Performance Tuning Fields and Default Values

| Setting | Default | Description |
|--|--|---|
| Monitoring Processes | Based on the number of cores for your server | Optional setting configures the throughput of monitoring data. Increasing this setting allows OV3600 to process more data per second, but it can take resources away from other OV3600 processes. Please contact Alcatel-Lucent Support if you think you might need to increase this setting for your network. |
| Maximum Number of Configuration Processes | 5 | Increases the number of processes that are pushing configurations to your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Please contact Alcatel-Lucent Support if you think you might need to increase this setting for your network. |
| Maximum Number of Audit Processes | 3 | Increases the number of processes that audit configurations for your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Contact Alcatel-Lucent Support if you are considering increasing this setting for your network. |
| Verbose Logging of SNMP Configuration | No | Enables or disables logging detailed records of SNMP configuration information. |
| SNMP Rate Limiting for Monitored Devices | No | Enables or disables a maximum bandwidth consumption threshold for each port for monitored devices. This setting prevents unnecessary SNMP traffic from compromising device performance. Alcatel-Lucent recommends enabling this setting when monitoring WLAN switches. |
| RAPIDS Processing Priority | Low | Defines the processing and system resource priority for RAPIDS in relation to OV3600 as a whole. When OV3600 is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (such as client connections and bandwidth) are not adversely impacted. The default priority is Low . You can also tune your system performance by changing group poll periods. |

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

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel-Lucent Support remains available to you for any phase of OV3600 installation. Refer to [“Contacting Alcatel-Lucent” on page 9.](#)

Defining OV3600 Network Settings

The next step in configuring OV3600 is to confirm the OV3600 network settings. Define these settings by navigating to the **OV3600 Setup > Network** page. [Figure 7](#) illustrates the contents of this page.

Figure 7 *OV3600 Setup > Network Page Illustration*

Perform the following steps to define the OV3600 network settings:

1. Locate the **Primary** and **Secondary Network Interface** sections. The information in these sections should match what you defined during initial network configuration and should not require changes. [Table 14](#) describes the settings and default values.

Table 14 *OV3600 Setup > Network > Primary and Secondary Network Interface Fields and Default Values*

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

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



Specifying NTP servers is optional. NTP servers synchronize the time on the OV3600 server, not on individual access points. Secondary network interface options may include multiple telnet terminal configurations, DHCP/BOOTP auto-configuration, time zone offsets, daylight savings time, and NTP addressing modes such as unicast, broadcast, and multicast. Secondary NTP information is only supported on OV3600s with multiple interfaces.

To disable NTP services, clear both the **Primary** and **Secondary** NTP server fields. Any problem related to communication between OV3600 and the NTP servers creates an entry in the event log.

[Table 15](#) describes the settings and default values in more detail.

Table 15 OV3600 Setup > Network > Secondary Network Fields and Default Values

| Setting | Default | Description |
|------------------|---------------------|---|
| Primary | ntp1.yourdomain.com | Sets the IP address or DNS name for the primary Network Time Protocol server. |
| Secondary | ntp2.yourdomain.com | Sets the IP address or DNS name for the secondary Network Time Protocol server. |

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



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

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

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel-Lucent Support remains available to you for any phase of OV3600 installation. Refer to [“Contacting Alcatel-Lucent”](#) on page 9.

Creating OV3600 Users

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

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

For each general user that you add, you define a **Username**, **Password** and a **Role**. You use the username and password when logging into OV3600. It is helpful to use unique and meaningful user names as they are recorded in the log files when you or other users make changes in OV3600.



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

The **user role** defines the user type, access level, and the top folder for that user. User roles are defined on the **OV3600 Setup > Roles** page. Refer to the next procedure in this chapter for additional information, “Creating OV3600 User Roles” on page 42.

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

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

1. Navigate to the **OV3600 Setup > Users** page. This page displays all users currently configured in OV3600. [Figure 8](#) illustrates the contents and layout of this page.

Figure 8 *OV3600 Setup > Users Page Illustration*

| | Username | Role | Enabled | Type | Access Level | Top Folder | Name | Email Address | Phone | Notes |
|--------------------------|----------|----------------|---------|---------------|--------------|------------|------|---------------|-------|-------|
| <input type="checkbox"/> | admin | Administration | Yes | Administrator | - | Top | - | - | - | - |

2. Click **Add** to create a new user, click the pencil icon to edit an existing user, or select a user and click **Delete** to remove that user from OV3600. When you click **Add** or the edit icon, the **Add User** page appears, illustrated in [Figure 9](#).

Figure 9 *OV3600 Setup > Users > Add/Edit User Page Illustration*

User

Username:

Role:

Password:

Confirm Password:

Name:

Email Address:

Phone:

Notes:

3. Enter or edit the settings on this page. [Table 16](#) describes these settings in additional detail.

Table 16 *OV3600 Setup > User > Add/Edit User Fields and Default Values*

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

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

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



In prior OV3600 versions, user roles could be assigned only to a single top folder, such as "West Coast" or "European Stores", for example. User roles can now be restricted to multiple folders within the overall hierarchy, even if they do not share the same top-level folder. Non-administrator users are only able to see data and users for devices within their assigned subset of folders.

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel-Lucent Support remains available to you for any phase of OV3600 installation. Refer to "[Contacting Alcatel-Lucent](#)" on page 9.

Creating OV3600 User Roles

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

Users can also see any building that contains a visible floor plan, and any campus that contains a visible building. When a new role is added to OV3600, VisualRF must be restarted for the new user to be enabled. Refer to the *VisualRF User Guide* for additional information.

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

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

1. Navigate to the **OV3600 Setup > Roles** page. This page displays all roles currently configured in OV3600. [Figure 10](#) illustrates the contents and layout of this page.

Figure 10 OV3600 Setup > Roles Page Illustration

| | Name ▲ | Enabled | Type | Access Level | Top Folder | Visible Groups | RAPIDS | VisualRF | Helpdesk |
|--------------------------|---------------------------------|---------|----------------------|-------------------|------------|----------------|------------|------------|----------|
| <input type="checkbox"/> | My role | Yes | Guest Access Sponsor | - | Top | - | None | Read Only | No |
| <input type="checkbox"/> | Administration | Yes | Administrator | | Top | All | Read/Write | Read/Write | Yes |
| <input type="checkbox"/> | Read-Only Monitoring & Auditing | Yes | AP/Device Manager | Audit (Read Only) | Top | All | None | Read Only | No |

2. Click **Add** to create a new role, click the pencil icon to edit an existing role, or select a role and click **Delete** to remove that role from OV3600. When you click **Add** or the edit icon, the **Add Role** page appears, illustrated in [Figure 11](#).

Figure 11 OV3600 Setup > Roles > Add/Edit Role Page Illustration

Role

Name:

Enabled: Yes No

Type:

AP/Device Access Level:

Top Folder:

RAPIDS:

Helpdesk: Yes No

Enable Adobe Flash: Yes No

3. Enter or edit the settings on this page. [Table 16](#) describes these settings in additional detail.

As explained earlier in this section, **Roles** define the type of user-level access, the user-level privileges, and the user viewability for device groups and devices in OV3600. [Table 17](#) describes the settings and default values of this section.

Table 17 OV3600 Setup > Roles > Add/Edit Roles Fields and Default Values

| Setting | Default | Description |
|-------------------------------|-------------------|--|
| Name | None | Sets the administrator-definable string that names the role. Alcatel-Lucent recommends that the role name give an indication of the devices and groups that are viewable, as well as the privileges granted to that role. |
| Enabled | Yes | Disables or enables the role. Disabling a role prevents all users of that role from logging in to OV3600. |
| Type | AP/Device Manager | <p>Defines the type of role. OV3600 supports the following role types:</p> <ul style="list-style-type: none"> ● OV3600 Administrator—The OV3600 Administrator has full access to OV3600 and all of the devices. The administrator can view and edit all settings and all APs in OV3600. Only the OV3600 Administrator can create new Users or access the OV3600 Setup page. ● AP/Device Manager—AP/Device Managers have access to a limited number of devices and groups based on the Top folder and varying levels of control based on the Access Level. ● Alcatel-Lucent Management Client—Defines the OV3600 user. The user information defined in AMC must match the user with the Alcatel-Lucent Management Client type. ● Guest Access Sponsor—Limited-functionality role to allow helpdesk or reception desk staff to grant wireless access to temporary personnel. This role only has access to the defined top folder of APs. |
| AP/Device Access Level | None | <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 cannot view the APs/Devices > Audit page which may contain sensitive information, including AP passwords. Monitor-only users also have read-only access to VisualRF. |
| Top Folder | None | <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 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 6.3, OV3600 user roles could be assigned only to a single top folder, such as "West Coast" or "European Stores", for example. User roles can now be restricted to multiple folders within the overall hierarchy, even if they do not share the same top-level folder. Non-administrator users are only able to see data and users for devices within their assigned subset of folders.</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"> ● None—Cannot view the RAPIDS tab or any Rogue APs. ● Read Only—The user can view the RAPIDS pages but cannot make any changes to rogue APs or perform OS scans. ● Read/Write—The user may ignore, delete, override scores and perform OS scans. |

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

| Setting | Default | Description |
|---------------------------|---------|--|
| Helpdesk | No | Sets the role to support helpdesk users, with parameters that are specific to the needs of helpdesk personnel supporting users on a wireless network. |
| Enable Adobe Flash | Yes | Enables the Adobe Flash application for all users who are assigned this role. Adobe Flash supports dynamic graphics on the Home > Overview page, VisualRF, Quickview functions, and additional OV3600 pages. NOTE: This field is only visible if a specific flag is set in the OV3600 database. By default this option is hidden and flash is enabled for all users. |

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel-Lucent Support remains available to you for any phase of OV3600 installation. Refer to “[Contacting Alcatel-Lucent](#)” on page 9.

Enabling OV3600 to Manage Your Devices

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

This section contains the following procedures:

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

Configuring Communication Settings for Discovered Devices

To configure OV3600 to communicate with your devices, to define the default shared secrets, and to set SNMP polling information, navigate to the **Device Setup > Communication** page, illustrated in [Figure 12](#).

Figure 12 *Device Setup > Communication Page Illustration*

| Default Credentials | |
|---|---|
| The credentials below are used to communicate with devices that are discovered by OV3600 (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. | |
| 3Com | Edit View |
| 3Com 8750 | Edit View |
| Alcatel-Lucent | Edit View |
| Apple AirPort Graphite Base Station | Edit View |
| Aruba | Edit View |
| Avaya | Edit View |
| BelAir | Edit View |
| Cisco Aironet 4800 | Edit View |
| Cisco IOS | Edit View |
| Cisco Switch | Edit View |
| Cisco VxWorks | Edit View |
| Cisco WLC | Edit View |
| Colubris | Edit View |
| Compaq WL400 | Edit View |
| Custom Device | Edit View |
| Enterasys | Edit View |
| Enterasys RoamAbout AP2000 | Edit View |
| Enterasys RoamAbout AP3000/AP4102 | Edit View |
| Enterasys RoamAbout R2 | Edit View |
| Foundry | Edit View |
| Funkwerk Artem W-1000 | Edit View |
| HP | Edit View |
| HP ProCurve 420 | Edit View |
| HP ProCurve 520WL | Edit View |
| HP ProCurve 530 | Edit View |
| HP Wireless Service Module | Edit View |
| Hirschmann | Edit View |
| Intel | Edit View |
| Intermec | Edit View |
| Juniper NetScreen SGT | Edit View |
| LANCOM | Edit View |
| Lucent/ORINOCO | Edit View |
| Meru | Edit View |
| Motorola | Edit View |
| NEC | Edit View |
| Nomadix | Edit View |
| Nortel | Edit View |
| Proxim MP.11 | Edit View |
| Proxim WiMAX | Edit View |
| Router/Switch | Edit View |
| Siemens Scalance W788 PRO | Edit View |
| Symbol | Edit View |
| Symbol Wireless Switch | Edit View |
| Systimax AirSpeed AP542 | Edit View |
| Teklogix | Edit View |
| Trapeze | Edit View |
| Tropos | Edit View |
| Universal Network Device | Edit View |
| Vivato | Edit View |

| SNMP Settings | |
|--------------------------|--------------------------------|
| SNMP Timeout (3-60 sec): | <input type="text" value="3"/> |
| SNMP Retries (1-20): | <input type="text" value="3"/> |

| Telnet/SSH Settings | |
|---------------------------------|---------------------------------|
| Telnet/SSH Timeout (3-120 sec): | <input type="text" value="10"/> |

| HTTP Discovery Settings | |
|---------------------------|--------------------------------|
| HTTP Timeout (3-120 sec): | <input type="text" value="5"/> |

| ICMP Settings | |
|---|---|
| Attempt to ping devices that were unreachable via SNMP: | <input checked="" type="radio"/> Yes <input type="radio"/> No |

| Colubris Administration Options | |
|--|--|
| <input checked="" type="radio"/> Do not modify security/HTTPS settings | |
| <input type="radio"/> Replace existing user with specified user | |

| Cisco Aironet VxWorks User Creation Options | |
|---|--|
| <input checked="" type="radio"/> Do not modify security/SNMP settings | |
| <input type="radio"/> Create and use a specified user | |

| Symbol 4131/Intel 2011B, Cisco Aironet IOS and Nomadix AG2000w SNMP Initialization | |
|--|--|
| Upon authorization into read-write manage mode, OV3600 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. | |
| <input checked="" type="radio"/> Do not modify SNMP settings | |
| <input type="radio"/> Enable read-write SNMP | |

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

1. On the **Device Setup > Communication** page, locate the **Default Credentials** area. Enter the credentials for each device model on your network. The default credentials are assigned to all newly discovered APs.
The **Edit** button edits the default credentials for newly discovered devices. To modify the credentials for existing devices, use the **APs/Devices > Manage** page or the **Modify Devices** link on the **APs/Devices > List** page.



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

2. Browse to the **Device Setup > Communication** page, locate the **SNMP Settings** area, and enter or revise the following information. [Table 18](#) lists the settings and default values.

Table 18 *Device Setup > Communication > SNMP Settings Fields and Default Values*

| Setting | Default | Description |
|---------------------|---------|--|
| SNMP Timeout | 3 | Sets the time, in seconds, that OV3600 waits for a response from a device after sending an SNMP request. |
| SNMP Retries | 3 | Sets the number of times OV3600 tries to poll a device when it does not receive a response within the SNMP Timeout period. If OV3600 does not receive an SNMP response from the device after the specified number of retries, OV3600 classifies that device as <code>Down</code> . |

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

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

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

4. On the **Device Setup > Communication** page, locate the **HTTP Discovery Settings** section. Complete or revise the default values for the settings in this section. [Table 20](#) lists these settings and default values.

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

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

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

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

| Setting | Default | Description |
|-------------------------------------|---------|--|
| Attempt to ping down devices | Yes | <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 **Colubris Administration Options** section. You only need to provide this information if you use Colubris APs on your network. Select one of the options listed. [Figure 13](#) illustrates this section and [Table 22](#) explains related fields.

Figure 13 *Device Setup > Communication > Colubris Administration Options Section Illustration*

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

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

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

- Aironet 340
- Aironet 350
- Aironet 1200

Select one of the three options listed. [Table 23](#) describes the settings and default values of this section.

Table 23 Device Setup > Communication > Cisco Aironet VxWorks User Creation Options Fields and Default Values

| Setting | Default | Description |
|---|---------|---|
| Do Not Modify Security/SNMP Settings | N/A | Enables OV3600 using only an existing user account on the AP, as defined in the Cisco VxWorks Username/Password section in the Default Secrets area. This user account must have all permissions set. |
| Create and Use Specified User | N/A | Enables OV3600 to create a new user account, specified below, on each AP, with all permissions enabled. |

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

Table 24 Device Setup > Communications Fields and Default Values

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

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

Table 25 Device Setup > Communications Fields and Default Values

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

Loading Device Firmware onto OV3600 (Optional)

Overview of the Device Setup > Upload Files Page

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

Figure 14 illustrates the **Upload Files** page, which lists all firmware files on OV3600 with file information. This page also enables you to add new firmware files, to delete firmware files, and to add **New Web Auth Bundle** files.

The following additional pages support firmware file information:

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

Figure 14 *Device Setup > Upload Files Page Illustration*

| Type | Owner Role | Description | Server Protocol | Use Group File Server | Firmware Filename | Firmware Version |
|------------|--------------------|--|-----------------|-----------------------|----------------------------------|------------------|
| Aruba 3xxx | AMP Administration | Aruba OS version 3.3.2.10 for Aruba 3xxx | TFTP | Disabled | ArubaOS_MMC_3_3_2_10_20355_0.bin | 3.3.2.10 |
| Avaya AP-3 | AMP Administration | - | TFTP | Disabled | AV_AP3_bin_0 | 2.3.3 |
| Avaya AP-3 | AMP Administration | - | TFTP | Disabled | AV_AP3_R245_bin_0 | 2.4.5 |
| Avaya AP-3 | AMP Administration | - | TFTP | Disabled | AV_AP3_2_1_0_bin_0 | 2.1.0 |
| Avaya AP-3 | AMP Administration | - | TFTP | Disabled | OR_AP2K_bin_0.bin | 2.4.4 |

| Firmware MD5 Checksum | Firmware File Size | HTML Filename | HTML Version | HTML MD5 Checksum | HTML File Size | Desired Firmware File for Specified Group |
|----------------------------------|--------------------|---------------|--------------|-------------------|----------------|---|
| 662ee818feb4bbcd279ec9c7b3cccdad | 31,616,820 bytes | - | - | - | - | - |
| fc965b8c3cd8191d51deeb31000a8e39 | 1,485,568 bytes | - | - | - | - | - |
| 6ff4d266dbd76e787ad5c6c7a0211b16 | 1,780,992 bytes | - | - | - | - | Acme Corporation, Global Corporate Po |
| cd72cd99de90550cee1f41adede0c365 | 3,681,741 bytes | - | - | - | - | - |
| f59bd897f9415a37ce1419b2a817639c | 1,781,760 bytes | - | - | - | - | - |

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

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

| Setting | Default | Description |
|------------------------------|---------|--|
| Type | None | Displays a drop-down list of the primary AP makes and models that OV3600 supports with automated firmware distribution. |
| Owner Role | None | Displays the user role that uploaded the firmware file. This is the role that has access to the file when an upgrade is attempted. |
| Description | None | Displays a user-configurable text description of the firmware file. |
| Server Protocol | None | Displays the file transfer protocol by which the firmware file was obtained from the server. |
| Use Group File Server | None | Displays the name of the file server supporting the group. |

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

| Setting | Default | Description |
|---|---------|---|
| Firmware Filename | None | Displays the name of the file that was uploaded to OV3600 and to be transferred to an AP when the file is used in an upgrade. |
| Firmware Version | None | Displays the firmware version number. This is a user-configurable field. |
| Firmware MD5 Checksum | None | Displays the MD5 checksum of the file after it was uploaded to OV3600. The MD5 checksum is used to verify that the file was uploaded to OV3600 without issue. The checksum should match the checksum of the file before it was uploaded. |
| Firmware File Size | None | Displays the size of the firmware file in bytes. |
| HTML Filename | None | Supporting HTML, displays the name of the file that was uploaded to OV3600 and to be transferred to an AP when the file is used in an upgrade. |
| HTML Version | None | Supporting HTML, displays the version of HTML used for file transfer. |
| HTML MD5 Checksum | None | Supporting HTML, displays the MD5 checksum of the file after it was uploaded to OV3600. The MD5 checksum is used to verify that the file was uploaded to OV3600 without issue. The checksum should match the checksum of the file before it was uploaded. |
| HTML File Size | None | Supporting HTML, displays the size of the file in bytes. |
| Desired Firmware File for Specified Groups | None | The firmware file is set as the desired firmware version on the Groups > Firmware Files page of the specified groups. You cannot delete a firmware file that is set as the desired firmware version for a group. |

Loading Firmware Files to OV3600

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

1. Browse to the **Device Setup > Upload Files** page.
2. From the **Upload Files** page, click the **Add** button. The **Add Firmware File** dialog box appears. [Figure 15](#) illustrates this page.

Figure 15 Device Setup > Upload Files > Add New Firmware Page Illustration

3. Click the **Supported Firmware Versions and Features** link to view a list of supported firmware versions.



Unsupported and untested firmware may cause device mismatches and other problems. Please contact Alcatel-Lucent Support before installing non-certified firmware. Refer to [“Contacting Alcatel-Lucent” on page 9](#).

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

Table 27 Supported Firmware Versions and Features Fields and Default Values

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



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

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



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

Using Web Auth Bundles in OV3600

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

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

1. Navigate to the **Device Setup > Upload Files** page. This page displays any existing Web Auth bundles that are currently configured in OV3600, and allows you to add or delete Web Auth bundles.
2. Scroll to the bottom of the page. Click **Add New Web Auth Bundle** to create a new Web Auth bundle, or click the pencil icon next to an existing bundle to edit. You may also delete Web Auth bundles by selecting that bundle with the checkbox, and clicking **Delete**.

When you add or edit a Web Auth bundle, the **Web Auth Bundle** page appears, as illustrated in [Figure 16](#).

Figure 16 Add Web Auth Bundle Page Illustration

The screenshot shows a web form titled "Web Auth Bundle". It has two input fields: "Description:" and "Web Auth Bundle:". The "Web Auth Bundle:" field has a "Browse..." button next to it. At the bottom of the form, there are two buttons: "Add" and "Cancel".

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

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

- Wireless LAN Controller Web Authentication Configuration Example, Document ID: 69340
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008067489f.shtml

Configuring TACACS+ and RADIUS Authentication

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

- [Configuring TACACS+ Authentication](#)
- [Configuring RADIUS Authentication and Authorization](#)
- [Integrating a RADIUS Accounting Server](#)

Configuring TACACS+ Authentication

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

1. Navigate to the **OV3600 Setup > Authentication** page. This page displays current status of TACACS+. [Figure 17](#) illustrates this page when neither TACACS+ nor RADIUS authentication is enabled in OV3600.

Figure 17 *OV3600 Setup > Authentication Page Illustration*

The screenshot shows the 'Authentication' configuration page in the OV3600 interface. It is divided into two main sections: 'TACACS+ Configuration' and 'RADIUS Configuration'. Each section has a header and a form with various fields and radio buttons.

TACACS+ Configuration

- Enable TACACS+ Authentication and Authorization: Yes No
- Primary Server Hostname/IP Address:
- Primary Server Port:
- Primary Server Secret:
- Confirm Primary Server Secret:
- Secondary Server Hostname/IP Address:
- Secondary Server Port:
- Secondary Server Secret:
- Confirm Secondary Server Secret:

RADIUS Configuration

- Enable RADIUS Authentication and Authorization: Yes No
- Primary Server Hostname/IP Address:
- Primary Server Port:
- Primary Server Secret:
- Confirm Primary Server Secret:
- Secondary Server Hostname/IP Address:
- Secondary Server Port:
- Secondary Server Secret:
- Confirm Secondary Server Secret:

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

Table 28 *OV3600 Setup > Authentication Fields and Default Values*

| Field | Default | Description |
|------------------------------------|---------|--|
| Primary Server Hostname/IP Address | N/A | Enter the IP address or the hostname of the primary TACACS+ server. |
| Primary Server Port | 49 | Enter the TCP port for the primary TACACS+ server. |
| Primary Server Secret | N/A | Specify the primary shared secret for the primary TACACS+ server, and confirm in the Confirm field. |

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

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

3. Click **Save** to retain these configurations, and continue with additional steps.
4. To configure Cisco ACS to work with OV3600, you must define a new service named **OV3600** that uses https on the ACS server.
 - The OV3600 https service is added to the **TACACS+** (Cisco) interface under the **Interface Configuration** tab.
 - Select a checkbox for a new service.
 - Enter **OV3600** in the service column and **https** in the protocol column.
 - Click **Save**.
5. Edit the existing groups or users in TACACS to use the "OV3600 service" and define a role for the group or user.
 - The role defined on the **Group Setup** page in ACS must match the exact name of the role defined on the **OV3600 Setup > Roles** page.
 - The defined role should use the following format: `role=<name_of_OV3600_role>`. One example is as follows:

```
role=DormMonitoring
```
6. OV3600 also needs to be configured as an AAA client.
 - On the **Network Configuration** page, click **Add Entry** to add an AAA client.
 - Enter the IP address of OV3600 as the **AAA Client IP Address**.
 - The secret should be the same value that was entered on the **OV3600 Setup > TACACS+** page.
7. Select **TACACS+** (Cisco IOS) in the **Authenticate Using** drop down menu and click **submit + restart**.



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

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel-Lucent Support remains available to you for any phase of OV3600 installation. Refer to [“Contacting Alcatel-Lucent”](#) on page 9.

Configuring RADIUS Authentication and Authorization

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

1. Navigate to the **OV3600 Setup > Authentication** page. This page displays current status of RADIUS. [Figure 18](#) illustrates this page when neither TACACS+ nor RADIUS authentication is enabled in OV3600.

Figure 18 *OV3600 Setup > Authentication Page Illustration*

The screenshot shows two configuration sections: TACACS+ Configuration and RADIUS Configuration. Each section has a radio button to enable or disable authentication and authorization, followed by fields for Primary and Secondary server Hostname/IP Address, Port, and Secret (with a Confirm field for the secret).

| Section | Field | Value |
|-----------------------|--|---|
| TACACS+ Configuration | Enable TACACS+ Authentication and Authorization: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| | Primary Server Hostname/IP Address: | tacacs.aire.com |
| | Primary Server Port: | 49 |
| | Primary Server Secret: | |
| | Confirm Primary Server Secret: | |
| | Secondary Server Hostname/IP Address: | |
| | Secondary Server Port: | 49 |
| RADIUS Configuration | Enable RADIUS Authentication and Authorization: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| | Primary Server Hostname/IP Address: | 10.200.200.200 |
| | Primary Server Port: | 1645 |
| | Primary Server Secret: | |
| | Confirm Primary Server Secret: | |
| | Secondary Server Hostname/IP Address: | |
| | Secondary Server Port: | 1812 |

2. Click **No** to disable or **Yes** to enable TACACS+ nor RADIUS authentication. If you click **Yes**, several new fields appear. Complete the fields described in [Table 29](#).

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

| Field | Default | Description |
|--------------------------------------|---------|---|
| Primary Server Hostname/IP Address | N/A | Enter the IP address or the hostname of the primary RADIUS server. |
| Primary Server Port | 49 | Enter the TCP port for the primary RADIUS server. |
| Primary Server Secret | N/A | Specify the primary shared secret for the primary RADIUS server, and confirm in the Confirm field. |
| Secondary Server Hostname/IP Address | N/A | Enter the IP address or the hostname of the secondary RADIUS server. |
| Secondary Server Port | 49 | Enter the TCP port for the secondary RADIUS server. |
| Secondary Server Secret | N/A | Enter the shared secret for the secondary RADIUS server. |

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

Integrating a RADIUS Accounting Server



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

As an optional configuration, OV3600 supports RADIUS server accounting. Use the **OV3600 Setup > RADIUS Accounting** page enables this configuration. This capability is not required for basic OV3600 operation, but can increase the user-friendliness of OV3600 administration in large networks. [Figure 19](#) illustrates the settings of this optional configuration interface.

Perform the following steps and configurations to enable OV3600 to receive accounting records from a separate RADIUS server. [Figure 19](#) illustrates the display of RADIUS accounting clients already configured, and [Figure 20](#) illustrates the **Add RADIUS Accounting Client** page.

Figure 19 *OV3600 Setup > RADIUS Accounting Page Illustration*

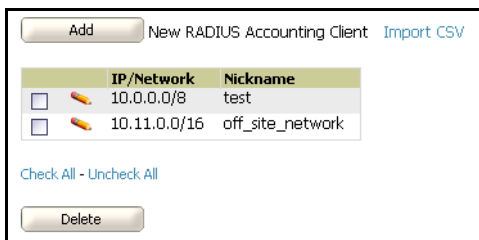
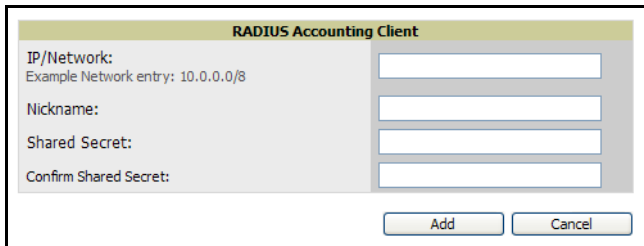


Figure 20 *OV3600 Setup > RADIUS > Add RADIUS Accounting Client Page Illustration*



1. To specify the RADIUS authentication server or network, browse to the **OV3600 Setup > RADIUS Accounting** page and click **Add**, illustrated in [Figure 20](#), and provide the information described in [Table 30](#).

Table 30 *OV3600 Setup > Radius Accounting Fields and Default Values*

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

2. Click **Add**.

What Next?

- For additional information about configuring WLAN Gateways or WLAN Controllers such as BlueSocket, ReefEdge, or ProCurve wireless gateways, refer to [“Third-Party Security Integration for OV3600” on page 289](#).
- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel-Lucent Support remains available to you for any phase of OV3600 installation. Refer to [“Contacting Alcatel-Lucent” on page 9](#).

Configuring Cisco WLSE and WLSE Rogue Scanning

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

- [Introduction to Cisco WLSE](#)
- [Configuring WLSE Initially in OV3600](#)
- [Configuring IOS APs for WDS Participation](#)
- [Configuring ACS for WDS Authentication](#)
- [Configuring Cisco WLSE Rogue Scanning](#)

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

Introduction to Cisco WLSE

Cisco WLSE functions as an integral part of the Cisco Structured Wireless-Aware Network (SWAN) architecture, which includes IOS Access Points, a Wireless Domain Service, an Access Control Server, and a WLSE. In order for OV3600 to obtain Rogue AP information from the WLSE, all SWAN components must be properly configured. [Table 31](#) describes these components.

Table 31 Cisco SWAN Architecture Components

| SWAN Component | Requirements |
|-------------------------------------|--|
| WDS (Wireless Domain Services) | <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 (Wireless LAN Solution Engine) | <ul style="list-style-type: none">• IP Address• Login |
| ACS (Access Control Server) | <ul style="list-style-type: none">• IP Address• Login |
| APs | <ul style="list-style-type: none">• APs within WDS Group |

Configuring WLSE Initially in OV3600

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

- [Adding an ACS Server for WLSE](#)
- [Enabling Rogue Alerts for Cisco WLSE](#)
- [Configuring WLSE to Communicate with APs](#)
- [Discovering Devices](#)
- [Managing Devices](#)
- [Inventory Reporting](#)
- [Defining Access](#)
- [Grouping](#)
- [WDS Participation](#)

- Primary or Secondary WDS

Adding an ACS Server for WLSE

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

Enabling Rogue Alerts for Cisco WLSE

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

Additional information about rogue device detection is available in “Configuring Cisco WLSE Rogue Scanning” on page 61.

Configuring WLSE to Communicate with APs

1. Navigate to the **Device Setup > Discover** page.
2. Configure **SNMP Information** ([click for additional information](#)).
3. Configure **HTTP Information** ([click for additional information](#)).
4. Configure **Telnet/SSH Credentials** ([click for additional information](#)).
5. Configure **HTTP ports for IOS access points** ([click for additional information](#)).
6. Configure **WLCCP credentials** ([click for additional information](#)).
7. Configure **AAA information** ([click for additional information](#)).

Discovering Devices

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

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

Perform these steps to discover access points.

1. Navigate to the **Device > Managed Devices > Discovery Wizard** page.
2. Import devices from a file ([click for additional information](#)).
3. Import devices from Cisco Works ([click for additional information](#)).
4. Import using CDP ([click for additional information](#)).

Managing Devices

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



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

Use these pages to make such configurations:

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

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

Inventory Reporting

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

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

Defining Access

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

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

Grouping

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

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

Configuring IOS APs for WDS Participation

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

- Primary WDS
- Backup WDS
- WDS Member

OV3600 monitors the AP's WDS role and displays this information on AP Monitoring page.



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

WDS Participation

Perform these steps to configure WDS participation.

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

Primary or Secondary WDS

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

1. Navigate to the **Wireless Services > WDS > General Setup** page.
2. If the AP is the Primary or Backup WDS, select **Use the AP as Wireless Domain Services**.

- Select **Priority** (set **200** for Primary, **100** for Secondary).
 - Configure the **Wireless Network Manager** (configure the IP address of WLSE).
3. If the AP is Member Only, leave all options unchecked.
 4. Navigate to the **Security > Server Manager** page.
 5. Enter the **IP address** and **Shared Secret** for the ACS server.
 6. Click the **Apply** button.
 7. Navigate to the **Wireless Services > WDS > Server Group** page.
 8. Enter the WDS Group of AP.
 9. Select the **ACS server** in the **Priority 1** drop- down menu.
 10. Click the **Apply** button.

Configuring ACS for WDS Authentication

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

1. Login to the ACS.
2. Navigate to the **System Configuration > ACS Certificate Setup** page.
3. Install a New Certificate by clicking the **Install New Certificate** button, or skip to the next step if the certificate was previously installed.
4. Click the **User Setup** button in the left frame.
5. Enter the **Username** that will be used to authenticate into the WDS and click **Add/Edit** button.
6. Enter the **Password** that will be used to authenticate into the WDS and click the **Submit** button.
7. Navigate to the **Network Configuration > Add AAA Client** page.
8. Add **AP Hostname**, **AP IP Address**, and **Community String** (for the key).
9. Enter the **Password** that will be used to authenticate into the WDS and click the **Submit** button.

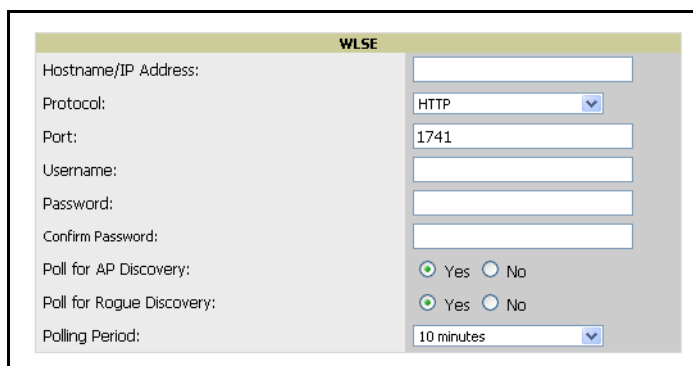
For additional and more general information about ACS, refer to “[Configuring ACS Servers](#)” on page 64.

Configuring Cisco WLSE Rogue Scanning

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

[Figure 21](#) illustrates and itemizes the OV3600 settings for communication that is enabled between OV3600 and WLSE.

Figure 21 *OV3600 Setup > WLSE > Add WLSE Page Illustration*



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

1. To add a Cisco WLSE server to OV3600, navigate to the **OV3600 Setup > WLSE** page and click **Add**. Complete the fields in this page. [Table 32](#) describes the settings and default values.

Table 32 *OV3600 Setup > WLSE Fields and Default Values*

| Setting | Default | Description |
|--|------------|--|
| Hostname/IP Address | None | Designates the IP address or DNS Hostname for the WLSE server, which must already be configured on the Cisco WLSE server. |
| Protocol | HTTP | Specifies the protocol to be used when polling the WLSE. |
| Port | 1741 | Defines the port OV3600 uses to communicate with the WLSE server. |
| Username | None | Defines the username OV3600 uses to communicate with the WLSE server. The username and password must be configured the same way on the WLSE server and on OV3600. The user needs permission to display faults to discover rogues and inventory API (XML API) to discover manageable APs. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow OV3600 to pull the necessary XML APIs. |
| Password | None | Defines the password OV3600 uses to communicate with the WLSE server. The username and password must be configured the same way on the WLSE server and on OV3600. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow OV3600 to pull the necessary XML APIs. |
| Poll for AP Discovery; Poll for Rogue Discovery | Yes | Sets the method by which OV3600 uses WLSE to poll for discovery of new APs and/or new rogue devices on the network. |
| Last Contacted | None | Displays the last time OV3600 was able to contact the WLSE server. |
| Polling Period | 10 minutes | Determines how frequently OV3600 polls WLSE to gather rogue scanning data. |

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

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel-Lucent Support remains available to you for any phase of OV3600 installation. Refer to [“Contacting Alcatel-Lucent”](#) on page 9.

Configuring ACS Servers

This is an optional configuration. The **OV3600 Setup > ACS** page allows OV3600 to poll one or more Cisco ACS servers for wireless username information. When you specify an ACS server, OV3600 gathers information about your networks wireless users. Refer to the “[Configuring TACACS+ and RADIUS Authentication](#)” on page 53 section if you want to use your ACS server to manage your OV3600 users.

Perform these steps to configure ACS servers:

1. Navigate to the **OV3600 Setup > ACS** page. This page displays current ACS information, as illustrated in [Figure 22](#).

Figure 22 *OV3600 Setup > ACS Page Illustration*

The screenshot shows the 'ACS Servers' configuration page. At the top, there is an 'Add' button and the text 'New ACS Server'. Below this, it says 'Enter one or more Cisco ACS servers to be polled for wireless username information.' There is a pagination indicator '1-1 of 1 ACS Servers Page 1 of 1'. A table lists the configured ACS servers with columns: Hostname/IP Address, Protocol, Port, Username, Polling Period, Last Contacted, and Errors. One server is listed with Hostname/IP Address: 10.1.11.1, Protocol: HTTP, Port: 2002, Username: stuff, Polling Period: 10 minutes, Last Contacted: 5/14/2009 6:37 AM. Below the table, there is a 'Select All - Unselect All' link and a 'Delete' button.

2. Click **Add** to create a new ACS server, or click a pencil icon to edit an existing server. To delete an ACS server, select that server and click **Delete**. When clicking **Add** or edit, the **Details** page appears, as illustrated in [Figure 23](#).

Figure 23 *OV3600 Setup > ACS > Add/Edit Details Page Illustration*

The screenshot shows the 'ACS Server' details form. It has the following fields: Hostname/IP Address (text input), Protocol (dropdown menu set to HTTP), Port (text input set to 2002), Username (text input), Password (text input), Confirm Password (text input), and Polling Period (dropdown menu set to 10 minutes). At the bottom, there are 'Add' and 'Cancel' buttons.

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

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

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

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

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

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

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel-Lucent Support remains available to you for any phase of OV3600 installation. Refer to [“Contacting Alcatel-Lucent”](#) on page 9.

Integrating OV3600 with an Existing Network Management Solution (NMS)

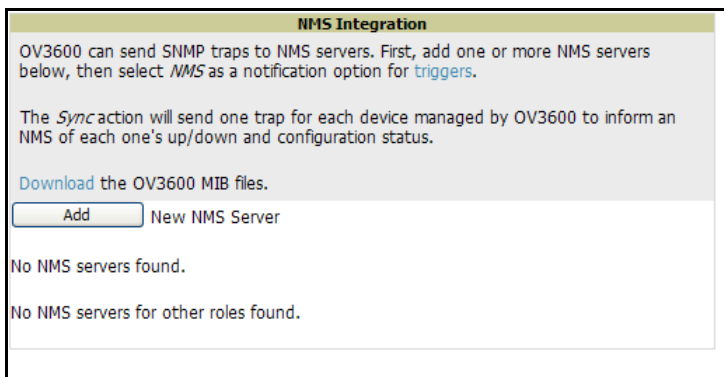
This is an optional configuration. The **OV3600 Setup > NMS** configuration page allows OV3600 to integrate with other Network Management Solution (NMS) consoles. This configuration enables advanced and interoperable functionality as follows:

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

Perform these steps to configure NMS support in OV3600:

1. Navigate to the **OV3600 Setup > NMS** page, illustrated in [Figure 24](#).

Figure 24 *OV3600 Setup > NMS Integration Page Illustration*



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

Figure 25 *OV3600 Setup > NMS Integration Add/Edit Page Illustration*

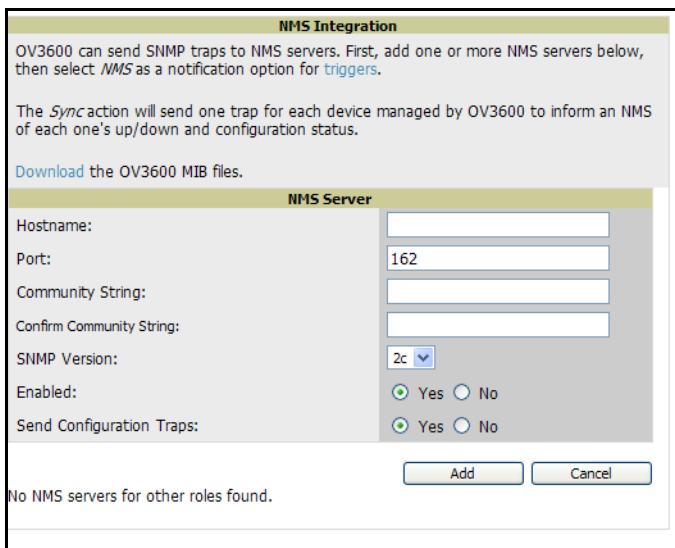


Table 34 *OV3600 Setup > NMS Integration Add/Edit Fields and Default Values*

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

Table 34 OV3600 Setup > NMS Integration Add/Edit Fields and Default Values (Continued)

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

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

What Next?

- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel-Lucent Support remains available to you for any phase of OV3600 installation. Refer to “[Contacting Alcatel-Lucent](#)” on page 9.

Auditing PCI Compliance on the Network

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

- [Introduction to PCI Requirements](#)
- [PCI Auditing in the OV3600 Interface](#)
- [Enabling or Disabling PCI Auditing](#)

Introduction to PCI Requirements

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

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

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

PCI Auditing in the OV3600 Interface

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

- The **OV3600 Setup > PCI Compliance** page enables or disables PCI Compliance monitoring on the network, and displays the current compliance status on the network. See [“Enabling or Disabling PCI Auditing” on page 68](#).
- The **Reports > Definitions** page allows you to create custom-configured and custom-scheduled PCI Compliance reports. See [“Reports > Definitions Page Overview” on page 249](#).
- The **Reports > Generated** page lists PCI Compliance reports currently available, and allows you to generate the latest daily version of the PCI Compliance Report with a single click. Refer to [“Reports > Generated Page Overview” on page 251](#).
- The **APs/Devices > PCI Compliance** page enables you to analyze PCI Compliance for any specific device on the network. This page is accessible when you select a specific device from the **APs/Devices > Monitor** page. First, you must enable this function through **OV3600 Setup**. See [“Enabling or Disabling PCI Auditing” on page 68](#).
- The **PCI Compliance Report** offers additional information. Refer to [“Using the PCI Compliance Report” on page 268](#). This report not only contains **Pass** or **Fail** status for each PCI requirement, but cites the action required to resolve a **Fail** status when sufficient information is available.



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

Table 35 *PCI Requirements and Support in OV3600*

| PCI Requirement | Description |
|-----------------|--|
| 1.1 | Monitoring configuration standards for network firewall devices When Enabled: PCI Requirement 1.1 establishes firewall and router configuration standards. A device fails Requirement 1.1 if there are mismatches between the desired configuration and the configuration on the device. When Disabled: When this PCI requirement is disabled in OV3600, firewall router and device configurations are not checked for PCI compliance in firewall configuration, and Pass or Fail status is not reported nor monitored. |
| 1.2.3 | Monitoring firewall installation between any wireless networks and the cardholder data environment When Enabled: A device passes requirement 1.2.3 if it can function as a stateful firewall. When Disabled: When this PCI requirement is disabled in OV3600, firewall router and device installation are not checked for PCI compliance. |
| 2.1 | Monitoring the presence of vendor-supplied default security settings When Enabled: PCI Requirement 2 establishes the standard in which all vendor-supplied default passwords are changed prior to a device’s presence and operation in the network. A device fails requirement 2.1 if the username, passwords or SNMP credentials being used by OV3600 to communicate with the device are on a list of forbidden default credentials. The list includes common manufacturer default passwords, for example. When Disabled: When this PCI requirement is disabled in OV3600, device passwords and other manufacturer default settings are not checked for PCI compliance. |

Table 35 PCI Requirements and Support in OV3600







| PCI Requirement | Description |
|-----------------|---|
| 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 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, then network devices are not checked for forbidden information and PCI Compliance is not established.</p> |
| 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, then OV3600 cannot establish a pass or fail status with regard to PCI encryption requirements on the network.</p> |
| 11.4 | <p>Using intrusion-detection or intrusion-prevention systems to monitor all traffic</p> <p>When Enabled: OV3600 reports pass or fail status when monitoring devices capable of reporting IDS events. Recent IDS events are summarized in the PCI Compliance report or the IDS Report.</p> <p>When Disabled: When this function is disabled, then OV3600 does not monitor the presence of PCI-compliant intrusion detection or prevention systems, nor can it report Pass or Fail status with regard to IDS events.</p> |

Enabling or Disabling PCI Auditing

Perform these steps to verify status and to enable or disable OV3600 support for PCI 1.2 requirements. enabling one or all PCI standards on OV3600 enables real-time information and generated reports that advise on Pass or Fail status. The PCI auditing supported in OV3600 is reported in [Table 35](#).

1. To determine what PCI Compliance standards are enabled or disabled on OV3600, navigate to the **OV3600 Setup > PCI Compliance** page, illustrated in [Figure 26](#).

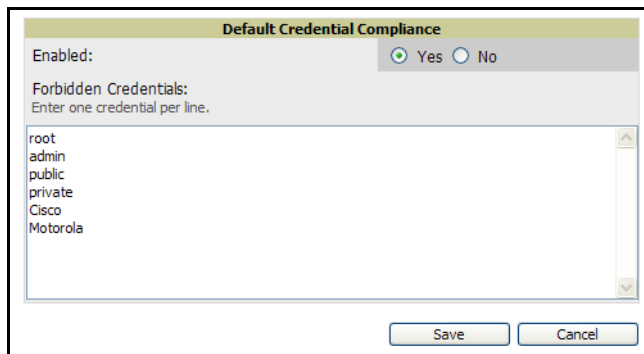
Figure 26 OV3600 Setup > PCI Compliance Page Illustration

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

2. To enable, disable, or edit any category of PCI Compliance monitoring in OV3600, click the **pencil** icon next to the compliance category you wish to change. The **Default Credential Compliance** page displays for the respective PCI standard.

3. Create changes as required. Specific credentials can be cited in the **Forbidden Credentials** section of any **Edit** page to enforce PCI requirements in OV3600. [Figure 27](#) illustrates one example.

Figure 27 Default Credential Compliance for PCI Requirements



4. Click **Save** to retain the settings. The **PCI Compliance** page should reflect changes on the next viewing.
5. To view and monitor PCI auditing on the network, use generated or daily reports. See [Chapter 9, “Creating, Running, and Emailing Reports”](#). In addition, you can view the real-time PCI auditing of any given device online. Perform these steps:
 - a. Navigate to the **APs/Devices > List** page, click a specific device, and the **Monitor** page for that device displays. The **Monitor** page displays a **Compliance** page in the menu bar.
 - b. Click the **Compliance** page to view complete PCI compliance auditing for that specific device.

What Next?

- For additional information about configuring WLAN Gateways or WLAN Controllers such as BlueSocket, ReefEdge, or ProCurve wireless gateways, refer to [“Third-Party Security Integration for OV3600” on page 289](#).
- Navigate to additional tabs in the **OV3600 Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Alcatel-Lucent Support remains available to you for any phase of OV3600 installation. Refer to [“Contacting Alcatel-Lucent” on page 9](#).

Deploying WMS Offload

Overview of WMS Offload in OV3600

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

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

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

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

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

General Configuration Tasks Supporting WMS Offload in OV3600

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

1. Configure WLAN switches for optimal OV3600 monitoring.
 - Disable debugging.
 - Ensure OV3600 server is a trap receiver host.
 - Ensure proper traps are enabled.
2. Configure OV3600 to optimally monitor the Aruba/Alcatel-Lucent infrastructure.
 - Enable WMS offload.
 - Configure SNMP communication.
 - Create a proper policy for monitoring Aruba/Alcatel-Lucent infrastructure.
 - Discover the infrastructure.
3. Configure device classification.
 - Set up rogue classification.
 - Set up rogue classification override.
 - Establish user classification override devices.
4. Deploy Aruba/Alcatel-Lucent-specific monitoring features.
 - Enable remote AP and wired network monitoring.
 - View controller license information.
5. Convert existing floor plans to VisualRF, to include the following elements:
 - MMS
 - AOS
 - RF Plan
6. Use RTLS for increasing location accuracy (optional).
 - Enable RTLS service on the OV3600 server.
 - Enable RTLS on Aruba/Alcatel-Lucent Infrastructure.

Additional Information Supporting WMS Offload

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

- *Alcatel-Lucent and Aruba Best Practices Guide*—primary WMS Offload support information

This chapter describes the deployment of device groups within the Alcatel-Lucent OmniVista Air Manager (OV3600) (OV3600). This chapter describes the **Groups > List** page and all additional **Groups** sub-menus and pages.

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

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

- **List**—This page is the default page in the **Groups** section of OV3600. This page lists all groups currently configured in OV3600 and provides the foundation for all group-level configurations. Refer to [“Viewing All Defined Device Groups” on page 75](#). In the case of WLAN switches and configuration, refer also to the *Alcatel-Lucent Configuration Guide*.
- **Monitor**—This page displays user and bandwidth information, lists devices in a given group, provides an **Alert Summary** table for monitoring alerts for the group, and provides a detailed **Audit Log** for device-level activity in a given group. Several procedures in this chapter cite the **Groups > Monitor** page.



NOTE

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

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

- **Basic**—This sub-menu page appears when you create a new group with the **Add** button on the **Groups > List** page. Once you define a group name, OV3600 displays the **Basic** page from which you configure many group-level settings. This page always remains available for any device group configured in OV3600. Refer to [“Configuring Basic Group Settings” on page 77](#).
- **Templates**—This page manages templates for any device group. Templates allow you to manage the configuration of 3Com, Alcatel-Lucent, Aruba, Cisco Aironet IOS, Enterasys, HP, Hirschmann, LANCOM, Nomadix, Nortel, Symbol and Trapeze devices in a given group using a configuration file. Variables in such templates configure device-specific properties, such as name, IP address and channel. Variables also define group-level properties. For additional information about using the **Templates** page, refer to [Chapter 6, “Creating and Using Templates” on page 163](#).
- **Security**—This page defines general security settings for device groups, to include TACACS+, RADIUS, encryption, and additional security settings on devices. Refer to [“Configuring Group Security Settings” on page 85](#).
- **SSIDs**—This page sets SSIDs, VLANs, and related parameters in device groups. Refer to [“Configuring Group SSIDs and VLANs” on page 87](#).
- **AAA Servers**—This page configures authentication, authorization, and accounting settings in support of TACACS+ and RADIUS servers for device groups. Refer to [“Adding and Configuring Group AAA Servers” on page 92](#).
- **Radio**—This page defines general 802.11 radio settings for device groups. Refer to [“Configuring Radio Settings for Device Groups” on page 93](#).

- **Alcatel-Lucent Configuration**—This page manages Aruba/Alcatel-Lucent Device Groups, AP Overrides, and other profiles specific to Aruba/Alcatel-Lucent devices on the network. Use this page in combination with the **Device Setup > Alcatel-Lucent Configuration** page. For additional information, refer to the *Aruba/Alcatel-Lucent Configuration Guide*.
- **Cisco WLC Config**—This page consolidates controller-level settings from the Group Radio, Security, SSIDs, Cisco WLC Radio and AAA Server pages into one navigation tree that is easier to navigate, and has familiar layout and terminology. Bulk configuration for per-thin AP settings, previously configured on the Group LWAPP APs tab, can now be performed from Modify Devices on the APs/Devices List page. Refer to “[Configuring Cisco Controller Settings](#)” on page 104.
- **PTMP/WiMAX**—This page defines settings specific to Proxim MP devices when present. Refer to “[Configuring Group PTMP/WiMAX Settings](#)” on page 105.
- **Proxim Mesh**—This page defines mesh AP settings specific to Proxim devices when present. Refer to “[Configuring Proxim Mesh Radio Settings](#)” on page 109.
- **MAC ACL**—This page defines MAC-specific settings that apply to Proxim, Cisco Vxworks, Symbol, Intel and Procurve520 devices when present. Refer to “[Configuring Group MAC Access Control Lists](#)” on page 111.
- **Firmware**—This page manages firmware files for many devices. “[Specifying Minimum Firmware Versions for APs in a Group](#)” on page 112.
- **Compare**—This page allows you to compare line item-settings between two device groups. On the **Groups > List** page, click **Compare Two Groups**, select the two groups from the drop-down menus, then click **Compare**. The **Compare** page allows you to edit any line-item configuration for either of the two groups you compare. “[Comparing Device Groups](#)” on page 113.

This chapter concludes by providing the following additional procedures for group-level configurations:

- “[Deleting a Group](#)” on page 114
- “[Changing Multiple Group Configurations](#)” on page 114
- “[Modifying Multiple Devices](#)” on page 115
- “[Using Global Groups for Group Configuration](#)” on page 117

OV3600 Group Overview

Important Group Concepts

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.

Typical group configuration variables include basic settings (SSID, SNMP polling interval, and so forth), security settings (VLANs, WEP, 802.1x, ACLs, and so forth), and some radio settings (data rates, fragmentation threshold, RTS threshold, DTIM, preamble, and so forth). When configuration changes are applied at a *group level*, they are assigned automatically to every device within that group. Such changes must be applied with every device in **Managed** mode. **Monitor** mode is the more common mode.

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

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

Group configuration can be enhanced with the OV3600 *Global Groups* feature; this feature allows you to create global groups with master configurations that are pushed to individual subscriber groups. More information is available in “Using Global Groups for Group Configuration” on page 117 as well as the section on the “Supporting OV3600 Stations with the Master Console” on page 227.

Viewing All Defined Device Groups

To display a list of all groups that have been defined in OV3600, browse to the **Groups > List** page, illustrated in Figure 28. Table 36 describes the contents and functions of this page.

Figure 28 *Groups > List Page Illustration*

| Name | SSID | Total Devices | Down | Mismatched | Ignored | Users | BW (kbps) | Up/Down Status Polling Period | Duplicate |
|---------------|------|---------------|------|------------|---------|-------|-----------|-------------------------------|-----------|
| Access Points | wpa | 38 | 4 | 32 | 0 | 0 | 0 | 5 minutes | |

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

| Column | Description |
|--------------------------------|---|
| Add New Group | Launches a page that enables you to add a new group by name and to define group parameters for devices in that group. For additional information, refer to “Configuring Basic Group Settings” on page 77. |
| Manage (wrench icon) | The wrench icon for any existing group provides a hyperlink to the Groups > Basic configuration page to begin editing Group configuration settings for that group. |
| Name | Displays a user-defined name that uniquely identifies the group by location, 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 | Displays the global group to which the group is subscribed, if any. |
| SSID | Column represents the Service Set Identifier (SSID) assigned to all devices within the group. |
| Total Devices | Column represents the total number of devices contained in the group, including APs, wireless controllers and routers or switches. |

Table 36 Groups > List Page Fields and Default Values (Continued)

| Column | Description |
|--------------------------------------|--|
| Down | Column represents the number of access points within the group that are not reachable via SNMP or are no longer associated to a controller. Note that thin APs are not directly polled with SNMP, but are polled through the controller. That controller may report that the thin AP is down or is no longer on the controller. At this point, OV3600 classifies the device as down. |
| Mismatched | Column represents the number of access points or wireless controllers within the group that are in a mismatched state. |
| Ignored | Column displays the number of ignored devices in that group. |
| Users | Column represents the number of mobile users associated with all access points within the group. To avoid double counting of users, users are only listed in the group of the AP with which they are associated. Note that device groups with only controllers in them report no users. |
| BW (kbps) | Column represents a running average of the sum of bytes in and bytes out for the managed radio page. |
| Up/Down Status Polling Period | Column represents the time between Up/Down SNMP polling periods for each device in the group. Detailed SNMP polling period information is available on the Groups > Basic configuration page. Note that by default, most polling intervals do not match the up/down period. |
| Duplicate | Column represents a hyperlink, and the link creates a new group with the name Copy of <Group Name> with the same group configuration. |



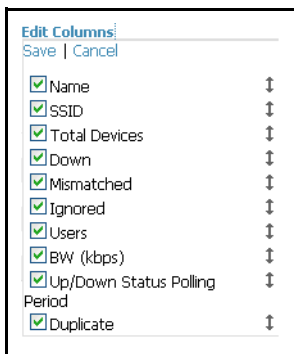
When you first configure OV3600, there is only one default group labeled **Access Points**. If you have no other groups configured, refer to “[Configuring Basic Group Settings](#)” on page 77.

Editing Columns on the Groups > List Page and Additional Pages

Perform the following steps to edit the columns that appear on the **Groups > List** page. All additional list and reports pages in OV3600 Version 6.4 and later allow you to edit the presence and sequence of columns in this manner:

1. Above the list or report, click **Edit Columns**. The supported columns appear in a popup window, as illustrated in [Figure 29](#):

Figure 29 Edit Columns Illustration for the Groups > List Page



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

4. Click **Save** to retain your settings. The **Groups > List** page displays your changes.

The following pages support editable columns for data display:

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

Configuring Basic Group Settings

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

1. Navigate to the **Groups > List** page. Existing device groups appear on this page.
2. To create a new group, click **Add**. Enter a group name and click **Add**. The **Group > Basic** page appears. To edit an existing device group, click the **manage** (wrench) icon next to the group. The **Group > Basic** page appears. If you hover your cursor over an existing group's manage (wrench) icon, a popup menu appears after a moment, and allows you to click **Basic**, **Templates**, **Security**, **SSIDs**, **AAA Servers**, or **Radio** to edit those pages as desired.

Figure 30 illustrates the **Groups > Basic** page. Page content differs according to the devices that a group contains. This page may change over time as you add or remove devices from the group.

Figure 30 **Groups > Basic** Page Illustration

Group: **San Francisco**

| | | | |
|---|--|--|--|
| <p>Basic</p> <p>Name: <input type="text" value="San Francisco"/></p> <p>Missed SNMP Poll Threshold (1-100): <input type="text" value="1"/></p> <p>Regulatory Domain: <input type="text" value="United States"/></p> <p>Timezone: <input type="text" value="OV3600 system time"/></p> <p>Allow One-to-One NAT: <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Audit Configuration on Devices: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> | | <p>Cisco IOS/VxWorks</p> <p>SNMP Version: <input type="text" value="2c"/></p> <p>Cisco IOS CLI Communication: <input checked="" type="radio"/> Telnet <input type="radio"/> SSH</p> <p>Cisco IOS Config File Communication: <input checked="" type="radio"/> TFTP <input type="radio"/> SCP</p> <p>Track Usernames on Cisco Aironet VxWorks APs: <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Configures devices to send SNMP traps to OV3600</p> | |
| <p>Global Groups</p> <p>Is Global Group: <input type="radio"/> Yes <input checked="" type="radio"/> No</p> | | <p>Cisco WLC</p> <p>SNMP Version: <input type="text" value="2c"/></p> <p>CLI Communication: <input type="radio"/> Telnet <input checked="" type="radio"/> SSH</p> | |
| <p>SNMP Polling Periods</p> <p>Up/Down Status Polling Period: <input type="text" value="5 minutes"/></p> <p>Override Polling Period for Other Services: <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>User Data Polling Period: <input type="text" value="10 minutes"/></p> <p>Thin AP Discovery Polling Period: <input type="text" value="15 minutes"/></p> <p>Device-to-Device Link Polling Period: <input type="text" value="5 minutes"/></p> <p>Device Bandwidth Polling Period: <input type="text" value="10 minutes"/></p> <p>802.11 Counters Polling Period: <input type="text" value="15 minutes"/></p> <p>Rogue AP and Device Location Data Polling Period: <input type="text" value="30 minutes"/></p> <p>CDP Neighbor Data Polling Period: <input type="text" value="30 minutes"/></p> | | <p>Proxim/Avaya</p> <p>SNMP Version: <input type="text" value="1"/></p> <p>Enable DNS Client: <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>HTTP Server Port: <input type="text" value="80"/></p> <p>Country Code: <input type="text" value="United States"/></p> | |
| <p>Notes</p> <p>Notes:</p> <div style="border: 1px solid gray; height: 40px;"></div> | | <p>HP ProCurve</p> <p>SNMP Version: <input type="text" value="2c"/></p> | |
| <p>Group Display Options</p> <p>Show device settings for: <input type="text" value="Only devices on this OV3600"/></p> <p>Selected Device Types: 3Com 8750, Alcatel-Lucent, Aruba, Cisco IOS, Cisco VxWorks, Cisco WLC, Enterasys RoamAbout AP3000/AP4102, HP ProCurve 420, HP ProCurve 530, Nomadix, Proxim, Proxim MP.11, Symbol, Symbol Wireless Switch, Trapeze</p> | | <p>Symbol/Intel</p> <p>SNMP Version: <input type="text" value="2c"/></p> <p>Symbol/Intel Client Inactivity Timeout (3-600 min): <input type="text" value="3"/></p> <p>Symbol Controller CLI Communication: <input checked="" type="radio"/> Telnet <input type="radio"/> SSH</p> <p>Web Config Interface: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> | |
| <p>Automatic Static IP Assignment</p> <p>Assign Static IP Addresses to Devices: <input type="radio"/> Yes <input checked="" type="radio"/> No</p> | | <p>Aruba/Alcatel-Lucent</p> <p>SNMP Version: <input type="text" value="2c"/></p> <p>Offload Aruba/Alcatel-Lucent WMS Database: <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Alcatel-Lucent GUI Config: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> | |
| <p>Spanning Tree Protocol</p> <p>Spanning Tree Protocol: Proxim only <input type="radio"/> Yes <input checked="" type="radio"/> No</p> | | <p>3Com/Enterasys/Nortel/Trapeze</p> <p>SNMP Version: <input type="text" value="2c"/></p> | |
| <p>NTP</p> <p>NTP Server #1: <input type="text"/></p> <p>NTP Server #2: <input type="text"/></p> <p>NTP Server #3: <input type="text"/></p> <p>UTC Time Zone: <input type="text" value="0"/></p> <p>Daylight Saving Time: <input type="radio"/> Yes <input checked="" type="radio"/> No</p> | | <p>Routers and Switches</p> <p>Read ARP Table: <input type="text" value="4 hours"/></p> <p>Read CDP Table for Device Discovery: <input type="text" value="4 hours"/></p> <p>Read Bridge Forwarding Table: <input type="text" value="4 hours"/></p> <p>Interface Polling Period: <input type="text" value="5 minutes"/></p> | |
| <p><input type="button" value="Save"/> <input type="button" value="Save and Apply"/> <input type="button" value="Revert"/></p> | | | |

- Define the settings in the **Basic** and **Global Group** sections. [Table 37](#) describes several typical settings and default values of this **Basic** section.

Table 37 Groups > Basic Page > Basic and Global Group Fields and Default Values

| Setting | Default | Description |
|--|-------------------------------------|---|
| Name | Defined when first adding the group | Displays or changes the group name. As desired, use this field to set the user-definable name to uniquely identify the group by location, 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. |
| Timezone | OV3600 System Time | Allows group configuration changes to be scheduled relative to the time zone in which the access points are located. This setting is used for scheduling group-level configuration changes. |
| Allow One-to-One NAT for Groups | No | Allows OV3600 to talk to the devices on a different IP address than the one configured on the device. NOTE: If enabled, the LAN IP Address listed on the AP/Devices > Manage configuration page under the Settings area is different than the IP Address under the Device Communication area. |
| Audit Configuration on Devices | Yes | Auditing and pushing of configuration to devices can be disabled on all the devices in the group. Once disabled, all the devices in the groups will not be counted towards mismatched devices. |
| Global Groups | No | When enabled, this field allows you to define the device group to be a global group. Refer also to "Using Global Groups for Group Configuration" on page 117 . |

- Complete the **SNMP Polling Periods** section. The information in this section overrides default settings. [Table 38](#) describes the SNMP polling settings.

Table 38 Groups > Basic Page > SNMP Polling Period Fields and Default Values

| Setting | Default | Description |
|---|-----------|---|
| Up/Down Status Polling Period | 5 minutes | Sets time between Up/Down SNMP polling for each device in the group. The Group SNMP Polling Interval overrides the global parameter configured on the Device Setup > Communication configuration page. Alcatel-Lucent recommends an initial polling interval of 5 minutes for most networks. |
| Override Polling Period for Other Services | No | Radio button enables or disables overriding the base SNMP Polling Period. If you select Yes for this field, then the other settings in the SNMP Polling Periods section are activated, and you can override default values. |
| User Data Polling Period | 5 minutes | Sets time between SNMP polls for User Data for devices in the group. |
| Thin AP Discovery Polling Period | 5 minutes | Sets time between SNMP polls for Thin AP Device Discovery. Controllers are the only devices affected by this polling interval. |
| Device-to-Device link Polling Period | 5 minutes | Sets time between SNMP polls for Device-to-Device link polling. Mesh APs are the only devices affected by this polling interval. |
| Device Bandwidth Polling Period | 5 minutes | Sets the interval at which OV3600 polls for the bandwidth being used by a device. |
| 802.11 Counters Polling Period | 5 minutes | Sets time between SNMP polls for 802.11 Counter information. |

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

| Setting | Default | Description |
|---|------------|--|
| Rogue AP and Device Location Data Polling Period | 5 minutes | Sets time between SNMP polls for Rogue AP and Device Location Data polling. |
| CDP Neighbor Data Polling Period | 30 minutes | Sets the frequency in which this group polls the network for Cisco Discovery Protocol (CDP) neighbors. |

- Record additional information and comments about the group in the **Notes** section.
- To configure which options and tabs are visible for the group, complete the settings in the **Group Display Options** section. [Table 39](#) describes the settings and default values.

Table 39 Groups > Basic Page > Group Display Options Fields and Default Values

| Setting | Default | Description |
|----------------------------------|-----------------------------|--|
| Show device settings for: | Only Devices on this OV3600 | Drop-down menu determines which Group tabs and options are to be viewable by default in new groups. Settings include the following: <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 in the group. If you use this setting, then to get the group list to display the correct SSIDs for the group, you must perform a Save and Apply action on the group. Only Devices on this OV3600—OV3600 hides all options and tabs that do not apply to the APs and devices currently on OV3600. Use system defaults—Use the default settings defined on the OV3600 configuration page Selected device types—Allows the user to specify the device types for which OV3600 displays Group settings. |
| Selected Device Types | Disabled | If you chose to display selected device types, then this option appears, allowing you to select the device types for which OV3600 displays group settings. Click Select devices in this group for a quick way to display only devices in the current group being configured. |

- To assign dynamically a range of static IP addresses to new devices as they are added into the group, locate the **Automatic Static IP Assignment** section on the **Groups > Basic** configuration page. If you select **Yes** in this section, additional fields appear. Complete these fields as required. [Table 40](#) describes the settings and default values.

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

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

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

| Setting | Default | Description |
|------------------------|---------|--|
| Subnet Gateway | Blank | Sets the gateway to be assigned to the devices in the Group. |
| Next IP Address | Blank | Defines the next IP address queued for assignment. This field is disabled for the initial Access Points group. |

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

Table 41 *Groups > Basic Page, Spanning Tree Protocol Fields and Default Values*

| Setting | Default | Description |
|-------------------------------|---------|--|
| Spanning Tree Protocol | No | Enables or disables Spanning Tree Protocol on WLSE devices and Proxim APs. |
| Bridge Priority | 32768 | Sets the priority for the AP. Values range from 0 to 65535. Lower values have higher priority. The lowest value is the root of the spanning tree. If all devices are at default the device with the lowest MAC address will become the root. |
| Bridge Maximum Age | 20 | Sets the maximum time, in seconds, that the device stores protocol information. The supported range is from 6 to 40. |
| Bridge Hello Time | 2 | Sets the time, in seconds, between Hello message broadcasts. |
| Bridge Forward Delay | 15 | Sets the time, in seconds, that the port spends in listening and learning mode if the spanning tree has changed. |

9. To configure NTP settings locate the **NTP** section and adjust these settings as required. [Table 42](#) describes the settings and default values.

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

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

10. To configure settings specific to Cisco IOS/VxWorks, locate the **Cisco IOS/VxWorks** section and adjust these settings as required. [Table 43](#) describes the settings and default values.

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

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

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

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

11. To configure settings specific to Cisco WLC, locate the **Cisco WLC** section and adjust these settings as required. [Table 44](#) describes the settings and default values.

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

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



When configuring Cisco WLC controllers, refer also to “[Configuring Wireless Parameters for Cisco Controllers](#)” on [page 104](#).

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

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

| Setting | Default | Description |
|-----------------------------|---------|--|
| SNMP Version | 1 | Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the AP. |
| Enable DNS Client | No | Enables the DNS client on the AP. Enabling the DNS client allows you to set some values on the AP by hostname instead of IP address. If you select Yes for this setting, additional DNS fields display. |
| Primary DNS server | Blank | Sets the IP address of the Primary DNS server. |
| Secondary DNS server | Blank | Sets the IP address of the Secondary DNS server. |
| Default DNS domains | Blank | Sets the default DNS domain used by the AP. |
| HTTP Server Port | 80 | OV3600 sets this port as the HTTP server port on all Proxim APs in the group. |

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

| Setting | Default | Description |
|--------------|---------------|---|
| Country Code | United States | Configures OV3600 to derive its time settings based on the country of location, as specified in this field. |

13. To configure HP ProCurve 420 specific settings, locate the **HP ProCurve 420** section and adjust these settings as required. [Table 46](#) describes the settings and default values.

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

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



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

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

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

| Setting | Default | Description |
|--|---------|--|
| SNMP Version | 2c | Drop-down menu specifies the version of SNMP used by OV3600 to communicate to the device. |
| Symbol/Intel Client Inactivity Timeout (3-600 min) | 3 | Sets the minutes of inactivity after which a client associated to an Intel or Symbol AP will be considered "inactive." A lower value typically provides a more accurate representation of current WLAN usage. NOTE: For other APs, OV3600 has more precise methods to determine when inactive clients are no longer associated to an AP. |
| Symbol Controller CLI Communication | Telnet | Select which connection type is to support the command-line interface (CLI) connection. The options are Telnet and secure shell (SSH). This is supported for WS5100 and RFS7000 devices only. |
| Web Config Interface | Yes | Enables or disables the http/https configuration page for the Symbol 4131 and Intel 2011 devices. |

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

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

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

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

| Setting | Default | Description |
|--|---------|---|
| Offload Aruba/Alcatel Lucent WMS database | No | Configures commands previously documented in the <i>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 WLAN switches. Changing the setting to Yes pushes commands via SSH to all WLAN switches in Monitor Only mode without rebooting the controller. The command can be pushed to controllers in manage mode (also without rebooting the controller) if the Allow WMS Offload setting on the OV3600 configuration page is changed to Yes . |
| Aruba/Alcatel-Lucent GUI Config | Yes | Enables or disables OV3600 support for the Aruba/Alcatel-Lucent configuration interface. This setting relates to the Device Setup > Aruba/Alcatel-Lucent Configuration page and all related operations. For additional information, refer to the <i>Aruba/Alcatel-Lucent Configuration Guide</i> . |

16. To configure settings for 3Com, Enterasys, Nortel, or Trapeze devices, locate the **3Com/Enterasys/Nortel/Trapeze** section and adjust these settings as required. [Table 48](#) describes the settings and default values of this section.

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

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

17. To configure support for routers and switches in the Access Points group, locate the **Routers and Switches** section and adjust these settings as required. This section defines the frequency in which all devices in the Access Points group poll for IP routing information. This can be disabled entirely as desired. [Table 48](#) describes the settings and default values of this section.

Table 50 Groups > Basic Page, Routers and Switches Fields and Default Values

| Setting | Default | Description |
|--|-----------|---|
| Read ARP Table | 4 hours | Sets the frequency in which devices poll routers and switches for Address Resolution Protocol (ARP) table information. This setting can be disabled, or set to poll for ARP information in a range from every 15 seconds to 12 hours. |
| Read CDP Table for Device Discovery | 4 hours | Sets the frequency in which devices poll routers and switches for Cisco Discovery Protocol (CDP) information. This setting can be disabled, or set to poll for CDP neighbor information in a range from every 15 seconds to 12 hours. |
| Read Bridge Forwarding Table | 4 hours | Sets the frequency in which devices poll the network for bridge forwarding information. This setting can be disabled, or set to poll bridge forwarding tables from switches in a range from every 15 seconds to 12 hours. |
| Interface Polling Period | 5 minutes | Sets the frequency in which network interfaces are polled. This setting can be disabled, or set to poll bridge forwarding tables from switches in a range from every 15 seconds to 12 hours. |

18. To configure settings for universal devices on the network, including routers and switches that support both wired and wireless networks, locate the Universal Devices, Routers and Switches section of the **Groups > Basic** page and define the version of SNMP to be supported.

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

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

19. Click **Save** when the configurations of the **Groups > Basic** configuration page are complete to retain these settings, but without pushing these settings to all devices in the Access Points group. **Save** is a good option if you intend to make additional device changes in the Access Points group, and wish to wait until all configurations are complete before you push all configurations at one time.

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

What Next?

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

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

Configuring Group Security Settings

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

1. Select the device group for which to define security settings from the **Groups > List** page.
2. Select the **Groups > Security** page. Some controls on this page interact with additional OV3600 pages. [Figure 31](#) illustrates this page and [Table 52](#) explains the fields and default values.

Figure 31 *Groups > Security Page Illustration*

The screenshot shows the configuration page for a device group's security settings. It is organized into several sections:

- VLANs:** Includes options for 'VLAN Tagging and Multiple SSIDs' (Enabled/Disabled), 'Management VLAN ID' (Untagged), 'Permit RADIUS-Assigned Dynamic VLANs' (Yes/No), 'VLAN ID Format' (ASCII/Hex), and 'Ethernet Untagged VLAN ID' (1).
- General:** Includes 'Create Closed Network' (Yes/No) and 'Block All Inter-Client Communication' (Yes/No).
- 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 server selection dropdowns, 'Authentication Profile Name' (AMP-Defined Server #1), and 'Authentication Profile Index' (1).
- RADIUS Accounting Servers:** Includes four server selection dropdowns, 'Accounting Profile Name' (Accounting), and 'Accounting Profile Index' (3).
- MAC Address Authentication:** Includes 'MAC Address Authentication' (Yes/No), 'MAC Address Format' (Single Dash), 'Authorization Lifetime' (1800), and 'Primary RADIUS Server Reattempt Period' (0).

At the bottom of the page, there are three buttons: 'Save', 'Save and Apply', and 'Revert'.

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

| Setting | Default | Description |
|--|---------|---|
| VLANs Section | | |
| VLAN Tagging and Multiple SSIDs | Enabled | This field enables support for VLANs and multiple SSIDs on the wireless network. If this setting is enabled, define additional VLANs and SSIDs on the Groups > SSIDs page. Refer to “ Configuring Group SSIDs and VLANs ” on page 87. |

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

| Setting | Default | Description |
|--|--------------|--|
| Management VLAN ID | Untagged | This setting sets the ID for the management VLAN when VLANs are enabled in OV3600. This setting is supported only for the following devices: <ul style="list-style-type: none"> Proxim AP-600, AP-700, AP-2000, AP-4000 Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8 ProCurve520WL; ProCurve420 Enterasys AP3000 |
| Permit RADIUS-Assigned Dynamic VLANs | No | This setting enables dynamic VLANs to be assigned by the RADIUS server. This setting is supported only for HP ProCurve 420. |
| VLAN ID Format | Hex | This setting defines the naming convention for VLANs to be supported in OV3600. The supported naming formats are ASCII and Hexadecimal. |
| Ethernet Untagged VLAN ID (1-4094) | 1 | This field defines the VLAN that will use untagged Ethernet. The VLAN must be a number between 1 and 4094, and defines the untagged VLAN ID for the RoamAbout AP3000. |
| General Section | | |
| Create Closed Network | No | If enabled, the APs in the Group do not broadcast their SSIDs. NOTE: Alcatel-Lucent recommends creating a closed network to make it more difficult for intruders to detect your wireless network. |
| Block All Inter-client Communication | No | If enabled, this setting blocks client devices associated with an AP from communicating with other client devices on the wireless network. NOTE: This option may also be identified as PSPF (Publicly Secure Packet Forwarding), which can be useful for enhanced security on public wireless networks. |
| EAP Options Section | | |
| WEP Key Rotation Interval | 300 | Sets the frequency at which the Wired Equivalent Privacy (WEP) keys are rotated in the device group being configured. The supported range is from 0 to 10,000,000 seconds. |
| Session Key Refresh Rate | 0 | Sets the frequency at which the general session key is refreshed in the device group being configured. The supported range is from 1 to 40 minutes. This setting is supported only for HP ProCurve 420. |
| Session Timeout | 0 | Sets the time at which the session times out for the device group being configured. The supported range is from 0 to 65,535 seconds. This setting is supported only for HP ProCurve 420. |
| Cisco TKIP | No | Sets the device group to use the Cisco Temporal Key Integrity Protocol (TKIP). If enabled, TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP. NOTE: TKIP can only be enabled when EAP-based security is used. |
| Cisco MIC | Disabled | Sets the device group to use the Cisco Message Integrity Check (MIC). Selecting MMH encryption enables this function. If enabled, Message Integrity Check (MIC) adds several bytes per packet to make it more difficult to tamper with the packets. |
| RADIUS Authentication Servers Section | | |
| RADIUS Authentication Server #1 - #4 | Not selected | Defines one or more RADIUS Authentication servers to be supported in this device group. Select up to four RADIUS authentication servers from the four drop-down menus. |

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

| Setting | Default | Description |
|---|--------------------------|--|
| Authentication Profile Name | OV3600-Defined Server #1 | For Proxim devices only, this field sets the name of the authentication profile to be supported in this device group. |
| Authentication Profile Index | 1 | For Proxim devices only, this field sets the name of the authentication profile index to be supported in this device group. |
| RADIUS Accounting Servers Section | | |
| RADIUS Accounting Server #1 - #4 | Not selected | Defines one or more RADIUS Accounting servers to be supported in this device group. Select up to four RADIUS accounting servers from the four drop-down menus. |
| Authentication Profile Name | Accounting | For Proxim devices only, this field sets the name of the accounting profile to be supported in this device group. |
| Authentication Profile Index | 3 | For Proxim devices only, this field sets the name of the accounting profile index to be supported in this device group. |
| MAC Address Authentication Section | | |
| MAC Address Authentication | No | If enabled, only MAC addresses known to the RADIUS server are permitted to associate to APs in the Group. |
| MAC Address Format | Single Dash | Allows selection of the format for MAC addresses used in RADIUS authentication and accounting requests: <ul style="list-style-type: none"> Ⓐ Dash Delimited: xx-xx-xx-xx-xx-xx (default) Ⓑ Colon Delimited: xx:xx:xx:xx:xx:xx Ⓒ Single-Dash: xxxxxx-xxxxxx Ⓓ No Delimiter: xxxxxxxxxxxx This option is supported only for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8, HP ProCurve 520WL, ProCurve 420 v2.1.0 and higher. |
| Authorization Lifetime | 1800 | Sets the amount of time a user can be connected before reauthorization is required. The supported range is from 900 to 43,200 seconds. |
| Primary RADIUS Server Reattempt Period | 0 | Specifies the time (in minutes) that the AP awaits responses from the primary RADIUS server before communicating with the secondary RADIUS server, and so forth |

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

Configuring Group SSIDs and VLANs

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



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

Figure 32 illustrates an example of the **Groups > SSIDs** page.

Figure 32 *Groups > SSIDs Page Illustration*

WLANs on a Cisco WLC can be configured on the [Cisco WLC Config](#) page.

New SSID/VLAN

| | SSID | VLAN ID | Name | Encryption Mode | First Radio | | Second Radio | | Native VLAN |
|--------------------------|--------------|---------|------|-----------------|-------------------------------------|-----------------------|-------------------------------------|-----------------------|-----------------------|
| | | | | | Enabled | Primary | Enabled | Primary | |
| <input type="checkbox"/> | stores | 11 | - | 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"/> | corp | 51 | - | No Encryption | <input checked="" type="checkbox"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="radio"/> | <input type="radio"/> |

Select All - Unselect All



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



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

1. Navigate to the **Groups > List** page and select the group for which to define SSIDs/VLANs by clicking the group name. Alternatively, click **Add** to create a new group, define a group name. In either case, the **Groups > Monitor** page appears.
2. Select the **Groups > SSIDs** configuration page. [Table 53](#) describes the information that appears for SSIDs and VLANs that are currently configured for the device group.

Table 53 *Groups > SSIDs Fields and Descriptions*

| Setting | Description |
|--------------------------------------|---|
| SSID | Displays the SSID associated with the VLAN. |
| VLAN ID | Identifies the number of the primary VLAN SSID on which encrypted or unencrypted packets can pass between the AP and the switch. |
| Name | Displays the name of the VLAN. |
| Encryption Mode | Displays the encryption on the VLAN. |
| First or Second Radio Enabled | Checkbox enables the VLAN, SSID and Encryption Mode on the radio control. |
| First or Second Radio Primary | Specifies which VLAN to be used as the primary VLAN. A primary VLAN is required. NOTE: If you create an Open network (see Create Closed Network below) in which the APs broadcast an SSID, the Primary SSID is the one that is broadcast. |

Table 53 Groups > SSIDs Fields and Descriptions (Continued)

| Setting | Description |
|--------------------|---|
| Native VLAN | Selects this VLAN to be the native VLAN. Native VLANs are untagged and typically used for management traffic only. OV3600 requires a Native VLAN to be set. Some AP types do not require a native VLAN. For those APs, you need to create a dummy VLAN, disable it on both radio controls and ensure that it has the highest VLAN ID. |

3. Click **Add** to create a new SSID or VLAN, or click the pencil icon next to an existing SSID/VLAN to edit that existing SSID or VLAN. The **Add SSID/VLAN** configuration page appears as illustrated in [Figure 33](#) and explained in [Table 54](#).

Figure 33 Groups > SSIDs > Add SSID/VLAN Page Illustration

4. Locate the **SSID/VLAN** section on the **Groups > SSIDS** configuration page and adjust these settings as required. This section encompasses the basic VLAN configuration. [Table 54](#) describes the settings and default values.

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

| Setting | Default | Description |
|-------------------------------|---------|---|
| Specify Interface Name | Yes | Enables or disables an interface name for the VLAN interface. <ul style="list-style-type: none"> Selecting No for this option displays the Enable VLAN Tagging option. |
| Interface | None | Sets the interface to support the SSID/VLAN combination. |
| SSID | None | Sets the Service Set Identifier (SSID), which is a 32-character user-defined identifier attached to the header of packets sent over a WLAN. It acts as a password when a mobile device tries to connect to the network through the AP, and a device is not permitted to join the network unless it can provide the unique SSID. |
| Name | None | Sets a user-definable name associated with SSID/VLAN combination. |
| VLAN ID | None | Indicates the number of the VLAN designated as the Native VLAN , typically for management purposes |

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

| Setting | Default | Description |
|---|---------|--|
| Service Priority (Cisco VxWorks only) | None | Identifies the delivery priority which packets receive on the VLAN/SSID (VxWorks only). |
| Maximum Allowed Associations (0-2007) | 255 | Indicates the maximum number of mobile users which can associate with the specified VLAN/SSID. NOTE: 0 means unlimited for Cisco and none for Colubris. |
| Broadcast SSID (Proxim only) | No | For specific devices as cited, this setting enables the AP to broadcast the SSID for the specified VLAN/SSID. This setting works in conjunction with the Create Closed Network setting on the Groups> Security configuration page. Proxim devices support a maximum of four SSIDs. NOTE: This option should be enabled to ensure support of legacy users. |
| Partial Closed System (Proxim only) | No | For Proxim only, this setting enables to AP to send its SSID in every beacon, but it does not respond to any probe requests. |
| Unique Beacon (Proxim only) | No | For Proxim only, if more than one SSID is enabled, this option enables them to be sent in separate beacons. |
| Block All Inter-client Communication | Yes | For Colubris only, this setting blocks communication between client devices based on SSID. |

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

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

| Setting | Default | Description |
|------------------------|---------------|---|
| Encryption Mode | No Encryption | Drop-down menu determines the level of encryption required for devices to associate to the APs. The drop-down menu options are as follows. Each option displays additional encryption settings that must be defined. Complete the associated settings for any encryption type chosen: <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 |

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

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

| Setting | Default | Description |
|--|---------|---|
| WEP Key Rotation Interval (seconds) | 120 | Time (in seconds) between WEP key rotation on the AP. |

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

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

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

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

| Setting | Default | Description |
|---|---------|--|
| RADIUS Authentication Server 1-3 (Colubris, ProCurve420, Proxim only) | None | Drop-down menu to select RADIUS Authentication servers previously entered on the Group > RADIUS configuration page. These RADIUS servers dictate how wireless clients authenticate onto the network. |
| Authentication Profile Name (Proxim Only) | None | Sets the Authentication Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs. |
| Authentication Profile Index (Proxim Only) | None | Sets the Authentication Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs. |

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



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

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

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

| Setting | Default | Description |
|---|---------|---|
| RADIUS Accounting Server 1-3 (Proxim Only) | None | Pull-down menu selects RADIUS Accounting servers previously entered on the Group > RADIUS configuration page. These RADIUS servers dictate where the AP sends RADIUS Accounting packets for this SSID/VLAN. |
| Accounting Profile Name (Proxim Only) | None | Sets the Accounting Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs. |
| Accounting Profile Index (Proxim Only) | None | Sets the Accounting Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs. |

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

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

Adding and Configuring Group AAA Servers

Configure RADIUS servers on the **Group > AAA Servers** page. TACACS+ servers are configured as a part of Cisco WLC configuration. In that case, refer to “[Configuring Security Parameters and Functions](#)” on page 104.

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



TACACS+ servers are configurable only for Cisco WLC devices. Refer to “[Configuring Wireless Parameters for Cisco Controllers](#)” on page 104.

- Navigate to the **Groups > List** page and select the group for which to define AAA servers by clicking the group name. Alternatively, click **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
- Select the **AAA Servers** page. The **AAA Servers** page appears, enabling you to add a RADIUS server. [Figure 34](#) and [Figure 35](#) illustrate this page for AAA RADIUS Servers:

Figure 34 *Groups > AAA Servers Page Illustration*

WLANs on a Cisco WLC can be configured on the [Cisco WLC Config](#) page.

New RADIUS Server

| | Hostname/IP Address ▲ | Authentication | Authentication Port | Accounting | Accounting Port | Timeout | Max Retries |
|--------------------------|-----------------------|----------------|---------------------|------------|-----------------|---------|-------------|
| | 10.180.180.180 | Yes | 1812 | No | - | 3 | 0 |
| | 10.181.181.181 | Yes | 1812 | No | - | 4 | 0 |
| <input type="checkbox"/> | 10.183.183.183 | Yes | 1812 | No | - | 2 | 0 |
| <input type="checkbox"/> | 10.182.182.182 | Yes | 1812 | No | - | 2 | 0 |

4 RADIUS Servers

Select All - Unselect All

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

Figure 35 *Adding a RADIUS Server Page Illustration*

RADIUS Server

Hostname/IP Address:
Not all devices support hostnames.

Secret:

Confirm Secret:

Authentication: Yes No

Authentication Port:

Accounting: Yes No

Accounting Port:

Timeout (0-86400):

Max Retries (0-20):

Table 59 Adding a RADIUS Server Fields and Default Values

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

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

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



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

- To make additional RADIUS configurations for device groups, use the **Groups > Security** page, and refer to “[Configuring Group Security Settings](#)” on page 85.

Configuring Radio Settings for Device Groups

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



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

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

1. Navigate to the **Groups > List** page and select the group for which to define radio settings by clicking the group name. Alternatively, click **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Navigate to the **Groups > Radio** page. [Figure 36](#) illustrates this page.

Figure 36 *Groups > Radio Page Illustration*

| Radio Settings | |
|---|---|
| Allow Automatic Channel Selection (2.4 GHz): | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Allow Automatic Channel Selection (5 GHz): | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Allow Automatic Channel Selection (4.9 GHz Public Safety): | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| 802.11b Data Rates (Mbps): | 1.0: Required <input type="button" value="v"/> 2.0: Required <input type="button" value="v"/> 5.5: Optional <input type="button" value="v"/> 11.0: Optional <input type="button" value="v"/> |
| Frag Threshold Enabled: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| RTS/CTS Threshold Enabled: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| RTS/CTS Maximum Retries (1-255): | <input type="text" value="32"/> |
| Maximum Data Retries (1-255): | <input type="text" value="32"/> |
| Beacon Period (19-5000 msec): | <input type="text" value="102"/> |
| DTIM Period (1-255): | <input type="text" value="3"/> |
| Ethernet Encapsulation: | <input type="radio"/> 802.1H <input checked="" type="radio"/> RFC1042 |
| Radio Preamble: | <input checked="" type="radio"/> Long <input type="radio"/> Short |
| HP ProCurve 420 | |
| Slot Time: | <input type="text" value="Auto"/> |
| Multicast Data Rate: | <input type="text" value="5.5 Mbps"/> |
| Rogue Scanning: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Rogue Scanning Interval (15-10080 min): | <input type="text" value="720"/> |
| Rogue Scanning Duration (50-1000 msec): | <input type="text" value="350"/> |
| Rogue Scan Type: | <input type="radio"/> Dedicated <input checked="" type="radio"/> Periodic |
| HP ProCurve 420, Enterasys AP3000 and Enterasys AP4102 | |
| Operational Mode: | <input type="text" value="802.11b + 802.11g"/> |
| Max Station Data Rate: | <input type="text" value="54 Mbps"/> |
| Enterasys AP3000/AP4102 | |
| 802.11a Multicast Data Rate: | <input type="text" value="6 Mbps"/> |
| 802.11b/g Multicast Data Rate: | <input type="text" value="5.5 Mbps"/> |
| Rogue Scanning: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Rogue Scanning Interval (30-10080 min): | <input type="text" value="720"/> |
| Rogue Scanning Duration (200-1000 msec): | <input type="text" value="350"/> |
| Cisco VxWorks | |
| Use Aironet Extensions: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Lost Ethernet Action: | <input type="text" value="Repeater Mode"/> |
| Lost Ethernet Timeout (1-10000 sec): | <input type="text" value="2"/> |
| Upgrade Radio Firmware When AP Firmware Is Upgraded (Require use of radio firmware x.xx): | <input checked="" type="radio"/> Yes <input type="radio"/> 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: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Interference Robustness: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Distance Between APs: | <input type="text" value="Large"/> |
| 802.11g Operational Mode: | <input type="text" value="802.11b + 802.11g"/> |
| 802.11abg Operational Mode: | <input type="text" value="802.11b + 802.11g"/> |
| 802.11b Transmit Rate: | <input type="text" value="Auto Fallback"/> |
| 802.11g Transmit Rate: | <input type="text" value="Auto Fallback"/> |
| 802.11a Transmit Rate: | <input type="text" value="Auto Fallback"/> |
| Rogue Scanning: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Rogue Scanning Interval (15-1440 min): | <input type="text" value="15"/> |
| Proxim 4900M | |
| 4.9GHz Public Safety Channel Bandwidth: | <input type="text" value="20"/> |
| 802.11a/4.9GHz Public Safety Operational Mode: | <input type="text" value="802.11a"/> |
| Colubris | |
| Rogue Scanning: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Rogue Scanning Interval (10-600 sec): | <input type="text" value="600"/> |
| Automatic Channel Interval: | <input type="text" value="12 Hours"/> |
| First Radio: | |
| Operational Mode: | <input type="text" value="802.11b only"/> |
| Multicast Data Rate: | <input type="text" value="1 Mbps"/> |
| Second Radio: CN330 Only | |
| Operational Mode: | <input type="text" value="802.11b only"/> |
| Multicast Data Rate: | <input type="text" value="1 Mbps"/> |
| Symbol | |
| Rogue Scanning: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Rogue Scanning Interval (5-480 min): | <input type="text" value="240"/> |
| Enterasys R2 | |
| Operational Mode: | <input type="text" value="802.11b + 802.11g"/> |
| <input type="button" value="Save"/> <input type="button" value="Save and Apply"/> <input type="button" value="Revert"/> | |

3. Locate the **Radio Settings** area and adjust these settings as required. [Table 60](#) describes the settings and default values.

Table 60 *Groups > Radio Fields and Default Values*

| Setting | Default | Description |
|---|--|--|
| Allow Automatic Channel Select (2.4, 5 GHz and 4.9GHz) | No | If enabled, whenever the AP is rebooted it uses its radio to scan the airspace and automatically select its optimal RF channel based on observed signal strength from other radios. NOTE: If you enable this feature, OV3600 automatically reboots the APs in the group when the change is implemented. |
| 802.11b Data Rates (Mb/sec) | Required: <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. NOTE: This setting does not apply to Cisco LWAPP devices. 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.) |
| Frag Threshold Enabled | No | If enabled, this setting enables packets to be sent as several pieces instead of as one block. In most cases, Alcatel-Lucent recommends leaving this option disabled. |
| Threshold Value | 2337 | If Fragmentation Threshold is enabled, this specifies the size (in bytes) at which packets are fragmented. A lower Fragmentation Threshold setting might be required if there is a great deal of radio interference. |
| RTS/CTS Threshold Enabled | No | If enabled, this setting configures the AP to issue a RTS (Request to Send) before sending a packet. In most cases, Alcatel-Lucent recommends leaving this option disabled. |
| RTS/CTS Threshold Value | 2338 | If RTS/CTS is enabled, this specifies the size of the packet (in bytes) at which the AP sends the RTS before sending the packet. |
| RTS/CTS Maximum Retries | 32 | If RTS/CTS is enabled, this specifies the maximum number of times the AP issues an RTS before stopping the attempt to send the packet through the radio. Acceptable values range from 1 to 128 . |
| Maximum Data Retries | 32 | The maximum number of attempts the AP makes to send a packet before giving up and dropping the packet. |
| Beacon Period (19-5000 Kµsec) | 100 | Time between beacons (in kilo microseconds). |
| DTIM Period (1-255) | 2 | DTIM alerts power-save devices that a packet is waiting for them. This setting configures DTIM packet frequency as a multiple of the number of beacon packets. The DTIM Interval indicates how many beacons equal one cycle. |
| Ethernet Encapsulation | RFC1042 | This setting selects either the RFC1042 or 802.1h Ethernet encapsulation standard for use by the group. |

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

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

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

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



Proprietary settings are only applied to 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 settings exclusively, locate the **HP ProCurve 420** section and adjust these settings as required. [Table 61](#) describes the settings and default values.

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

| Setting | Default | Description |
|--|----------|---|
| Slot Time | Auto | Short-slot-time mechanism, if used on a pure 802.11g deployment, improves WLAN throughput by reducing wait time for transmitter to assure clear channel assessment. |
| Multicast Data Rate | 5.5Mbps | Sets the maximum data rate of the multicast data packets. |
| Rogue Scanning | Enabled | If enabled the 420 APs in the group will scan for rogues. |
| Rogue Scanning Interval (15-10080 min) | 720 | If rogue scanning is enabled, this setting controls the frequency with which scans are conducted (in minutes). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan. NOTE: This setting only applies to Periodic scans. |
| Rogue Scanning Duration (50-1000 msec) | 350 | Specifies the amount of time, in milliseconds, the AP should spend performing the rogue scan. If the duration is set too high users may start to experience connectivity issues. NOTE: This setting only applies to periodic scans. |
| Rogue Scan Type | Periodic | Specifies the Rogue Scanning mode. When set to Dedicated , users are unable to associate to the AP. |

6. To configure the HP ProCurve 240, Enterasys AP 3000 and AP 4102 Operational Mode and Max Station Data Rate, locate the **HP ProCurve 240, Enterasys AP 3000 and AP 4102** section of the **Proprietary Settings** area, and define the settings. [Table 62](#) describes the settings and default values of this page.

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

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

7. To configure settings specific to Enterasys AP3000 and Enterasys AP4102, locate the **Enterasys AP3000 and Enterasys AP4102** section of the **Proprietary Settings** area, and define the settings. [Table 63](#) describes the settings and default values of this page.

Table 63 Enterasys AP3000 and Enterasys AP4102 > Proprietary Settings Fields and Default Values

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

8. To configure radio settings for Cisco VxWorks devices in the group, locate the **Groups > VxWorks** section and adjust these settings as required. [Table 64](#) describes the settings and default values of this page.

Table 64 Groups > VxWorks Proprietary Settings Fields and Default Values

| Setting | Default | Description |
|-------------------------------|---------|---|
| Use Aironet Extensions | Yes | When enabled, this option allows Cisco 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. |

Table 64 Groups > VxWorks Proprietary Settings Fields and Default Values (Continued)

| Setting | Default | Description |
|--|---------------|---|
| Lost Ethernet Action | Repeater Mode | <p>Pull-down menu that specifies the action to take when the Lost Ethernet Timeout threshold is exceeded:</p> <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. |
| Upgrade Radio Firmware When AP Firmware Is Upgraded | Yes | If enabled, this setting mandates that the radio firmware be upgraded to a firmware version compatible with the current version of AP firmware. |

- To configure settings specific to the Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3/4/5/6/7/8, and ProCurve 520WL, locate the appropriate section of **Groups > Radio** page and define the required fields. [Table 65](#) describes the settings and default values.

Table 65 Groups > LWAPP APs, Proprietary Settings Fields and Default Values

| Setting | Default | Description |
|-----------------------------------|------------------|---|
| Load Balancing | No | <p>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.</p> <p>NOTE: This feature is only available when two 802.11b wireless cards are used in an AP-2000.</p> |
| Interference Robustness | No | If enabled, this option will fragment packets greater than 500 bytes in size to reduce the impact of radio frequency interference on wireless data throughput. |
| Distance Between APs | Large | This setting adjusts the receiver sensitivity. Reducing receiver sensitivity from its maximum may help reduce the amount of crosstalk between wireless stations to better support roaming users. Reducing the receiver sensitivity, user stations will be more likely to connect with the nearest access point. |
| 802.11g Operational Mode | 802.11b +802.11g | This setting sets the operational mode of all g radios in the group to either b only, g only or b + g. |
| 802.11abg Operational Mode | 802.11b +802.11g | This setting sets the operational mode of all abg radios in the group to either a only, b only, g only or b + g. |
| 802.11b Transmit Rate | Auto Fallback | This setting specifies the minimum transmit rate required for the AP to permit a user device to associate. |
| 802.11g Transmit Rate | Auto Fallback | This setting specifies the minimum transmit rate required for the AP to permit a user device to associate. |

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

| Setting | Default | Description |
|------------------------------|---------------|---|
| 802.11a Transmit Rate | Auto Fallback | This setting specifies the minimum transmit rate required for the AP to permit a user device to associate. |
| Rogue Scanning | Yes | If enabled, any ORiNOCO, or Avaya access points in the group (with the appropriate firmware) will passively scan for rogue access points at the specified interval. This rogue scan will not break users' association to the network. NOTE: This feature can affect the data performance of the access point. |
| Rogue Scan Interval | 15 minutes | If rogue scanning is enabled, this setting controls the frequency with which scans are conducted (in minutes). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan. |

10. To configure settings specific to Proxim 4900M, locate the **Proxim 4900M** section and define the required fields. [Table 66](#) describes the settings and default values.

Table 66 Proxim 4900, Proprietary Settings Fields and Default Values

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

11. To configure Colubris-only settings in this device group, locate the **Colubris** section and define the required fields. [Table 67](#) describes the settings and default values.

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

| Setting | Default | Description |
|--|------------------------|--|
| Rogue Scanning | Yes | If enabled, Colubris access points in the group will passively scan for rogue access points at the specified interval. This rogue scan will not break a user's association to the network. |
| Rogue Scanning Interval (10-600 secs) | 600 | If rogue scanning is enabled, this setting controls the frequency with which scans are conducted (in minutes). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan. |
| Automatic Channel Interval | 12 Hours | Sets the frequency by which APs monitor radio channels for availability and activity. |
| First Radio | 802.11b only 1 Mbps | Sets the operational mode and multicast data rate for the first Colubris radio. |
| Second Radio (CN330 only) | 802.11b only 1 Mbps | Sets the operational mode and multicast data rate for the second Colubris radio, supported only for the Colubris CN330. |

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

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

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

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

Table 69 *Enterasys Section Fields and Default Values*

| Setting | Default | Description |
|-------------------------|-------------------|---|
| Operational Mode | 802.11b + 802.11g | Drop-down menu defines the 802.11 settings to support with the Enterasys radio devices in this group. Supported options are as follows: <ul style="list-style-type: none"> ● 802.11a only ● 802.11b only ● 802.11g only ● 802.11b + 802.11g |

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

An Overview of Cisco WLC Configuration

The **Groups > Cisco WLC Config** page consolidates the settings from all group pages. In Version 6.4, the **Groups > SSIDs** subtab applies to all device types except for Cisco WLC, which have WLANs configured on the **Cisco WLC Config** page. It is not recommended to have HP Procurve 420s, Symbol 4131 and Proxim APs in the same group as Cisco devices. Also, it is recommended that users set device preferences to “Only devices in this group.” This topic describes how to access and navigate the **Groups > Cisco WLC Config** page.

Accessing Cisco WLC Configuration

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

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

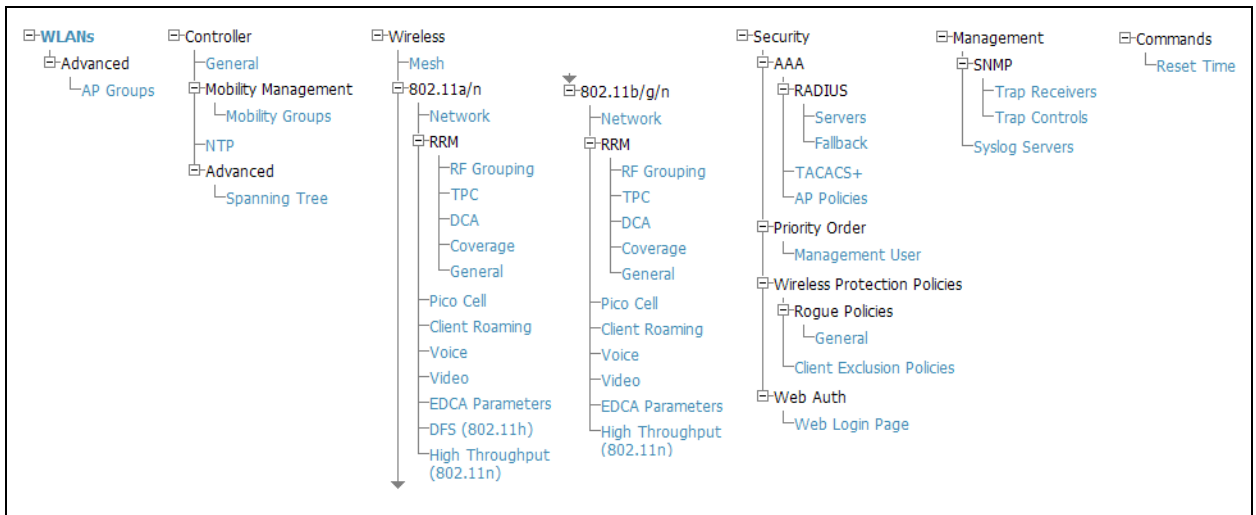
Navigating Cisco WLC Configuration

The navigation pane on the left side of the **Groups > Cisco WLC Config** page is expandable, and displays the Cisco configurations supported and deployed. [Figure 37](#) and [Figure 38](#) illustrate this navigation pane.

Figure 37 *Groups > Cisco WLC Config Page Illustration, Contracted View*



Figure 38 *Groups > Cisco WLC Config Page Illustration, Expanded View*



Configuring WLANs for Cisco WLC Devices

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

1. Navigate to the **Groups > Cisco WLC Config** page, and click **WLANs** in the navigation pane at left. This page displays the SSIDs or VLANs that are available for use with Cisco WLC devices, and enables you to define new SSIDs or VLANs. [Figure 39](#) illustrates this page.
2. To change the ID/position of a WLAN on the controller by dragging and dropping, set the toggle to **yes**. Note that the by setting this flag to **yes**, OV3600 will display a mismatch if the WLANs in the desired and device config differ only on the order.

Figure 39 *Groups > Cisco WLC Config > WLANs Page Illustration*

The screenshot shows the 'WLANs' configuration page for the 'Cisco Gear' group. The 'Enforce WLAN Order on Controllers' toggle is set to 'No'. A table lists 10 WLANs with columns for Profile, SSID, Admin Status, Encryption Mode, and Radio Policy. The table data is as follows:

| | Profile | SSID | Admin Status | Encryption Mode | Radio Policy |
|--------------------------|------------------------|------------------------|--------------|-----------------|--------------|
| <input type="checkbox"/> | 5500 8021x | 5500 8021x | Yes | Require 802.1X | All |
| <input type="checkbox"/> | 5500 CKIP | 5500 CKIP lab la la | Yes | Static CKIP | All |
| <input type="checkbox"/> | 5500 guest | 5500 guest_bundle | Yes | No Encryption | All |
| <input type="checkbox"/> | 5500 wep short ascii 3 | 5500 wep short ascii 3 | Yes | No Encryption | All |
| <input type="checkbox"/> | 5500 WPA PSK | 5500 WPA PSK | Yes | WPA2/PSK | All |
| <input type="checkbox"/> | 5500 WPA2 PSK | 5500 WPA2 PSK | Yes | WPA2/PSK | All |
| <input type="checkbox"/> | 5500 WPA2 WEB | 5500 WPA2 WEB | Yes | No Encryption | All |
| <input type="checkbox"/> | 5500 WPA2C RADIUS | 5500 WPA2C RADIUS | Yes | WPA2 | All |
| <input type="checkbox"/> | 5500-wpa-psk-hex | 5500-wpa-psk-hex | Yes | WPA/PSK | All |
| <input type="checkbox"/> | 5500-wpa2-psk-hex | 5500-wpa2-psk-hex | Yes | WPA2/PSK | All |

3. To add or edit SSIDs or VLANs that are dedicated to Cisco WLC devices, either click the **Add New SSID/VLAN** button, or click the pencil icon for an existing SSID/VLAN. A new page appears comprised of four tabs, as follows:
 - **General**—Defines general administrative parameters for the Cisco WLC WLAN.
 - **Security**—Defines encryption and RADIUS servers.
 - **QoS**—Defines quality of service (QoS) parameters for the Cisco WLC WLAN.
 - **Advanced**—Defines advanced settings that are available only with Cisco WLC devices, for example, AAA override, coverage, DHCP and DTIM period.



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

Figure 40 *Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > General Tab Illustration*

Group: cisco-ios,airespace and switches

General Security QoS Advanced

General

Profile:

SSID:

Admin Status: Yes No

Specify Interface Name: Yes No

Interface: 5500_guest_interface ▾

Radio Policy: All ▾

Broadcast SSID: Yes No

Add Cancel

Figure 41 *Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > Security Tab Illustration*

General Security QoS Advanced

Security

Encryption Mode: No Encryption ▾

Web Policy: Disabled ▾

AAA Servers

RADIUS Authentication Server #1: Select ▾

RADIUS Authentication Server #2: Select ▾

RADIUS Authentication Server #3: Select ▾

RADIUS Accounting Server #1: Select ▾

RADIUS Accounting Server #2: Select ▾

RADIUS Accounting Server #3: Select ▾

Figure 42 *Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > QoS Tab Illustration*

Group: cisco-ios,airespace and switches

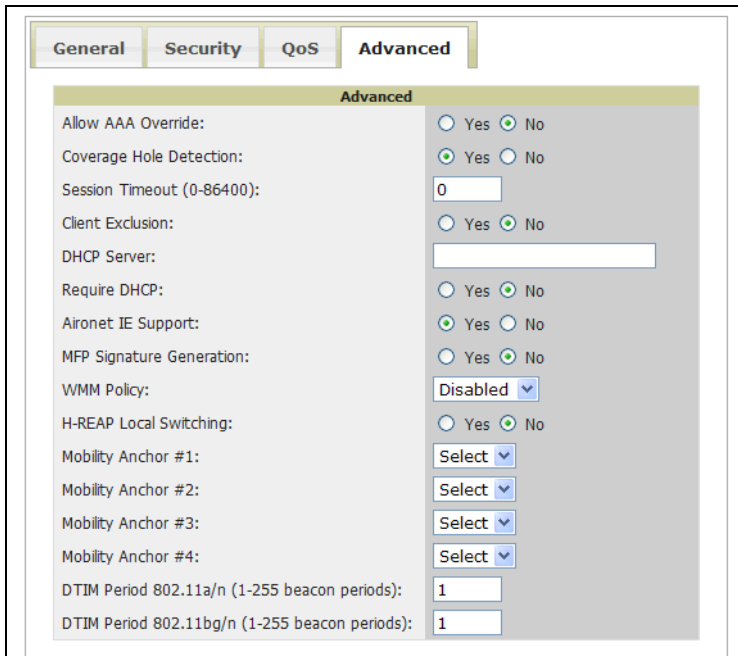
General Security QoS Advanced

QoS

Quality of Service: Silver (best effort) ▾

- Platinum (voice)
- Gold (video)
- Silver (best effort)
- Bronze (background)

Figure 43 *Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > Advanced Tab Illustration*



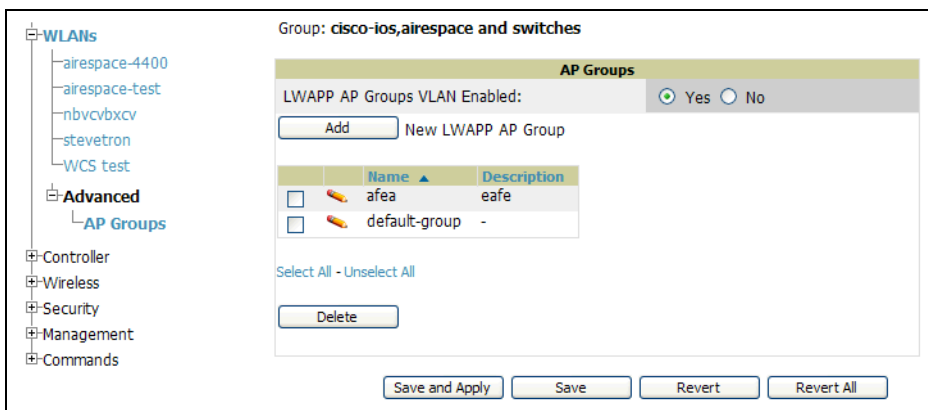
Defining and Configuring LWAPP AP Groups for Cisco Devices

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

Viewing and Creating AP Groups

1. Navigate to the **Groups > Cisco WLC Config** page, and click **WLANs > Advanced > AP Groups** in the navigation pane at left. This page displays the configured LWAPP APs. [Figure 44](#) illustrates this page.

Figure 44 *Groups > Cisco WLC Config > WLANs > Advanced > AP Groups Page Illustration*



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

Configuring Cisco Controller Settings

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

Navigate to the **Groups > Cisco WLC Config > Controller** page. This navigation is illustrated in [Figure 45](#).

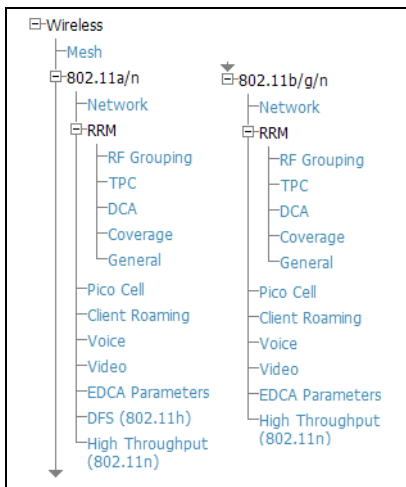
Figure 45 *Groups > Cisco WLC Config > Controller Navigation*



Configuring Wireless Parameters for Cisco Controllers

This section illustrates the configuration of **Wireless** settings in support of Cisco WLC controllers. The navigation for Wireless settings is illustrated in [Figure 46](#).

Figure 46 *Groups > Cisco WLC Config > Wireless Navigation Illustration*



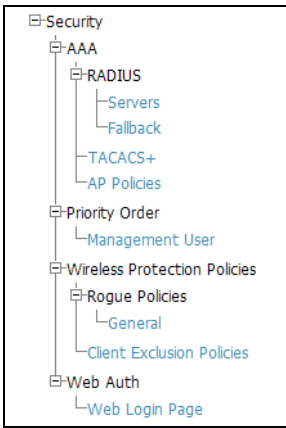
Configuring Security Parameters and Functions

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

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

[Figure 47](#) illustrates these components and this navigation:

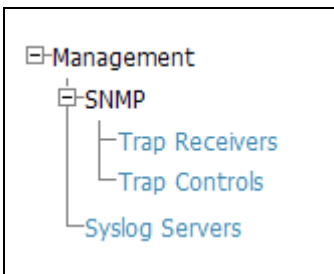
Figure 47 *Groups > Cisco WLC Config > Security Navigation Illustration*



Configuring Management Settings for Cisco Controllers

OV3600 supports the configuration of SNMP and Syslog Server settings for Cisco WLC controllers. Users should be able to configure up to four trap receivers on the Cisco WLC including the OV3600 IP that can be used in global groups. To define SNMP and server settings, navigate to the **Groups > Cisco WLC Config > Management** page, illustrated in [Figure 48](#).

Figure 48 *Groups > Cisco WLC Config > Management Navigation Illustration*



Configuring Group PTMP/WiMAX Settings

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

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

Perform the following steps to configure these functions.

1. Navigate to the **Groups > List** page and select the group for which to define PTMP/WiMAX settings by clicking the group name. Alternatively, click **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Click the PTMP/WiMAX tab in the OV3600 navigation menu. [Figure 49](#) illustrates this page.

Figure 49 *Groups > PTMP/WiMAX Page Illustration*

3. Define the settings on this page. [Table 70](#) describes the settings and default values.

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

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

Table 70 Groups > PTMP/WiMAX Fields and Default Values

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

- 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 50](#) illustrates this page and [Table 71](#) describes the settings and default values.

Figure 50 Groups > PTMP/WiMAX Configuring Packet Identification Rules Page Illustration

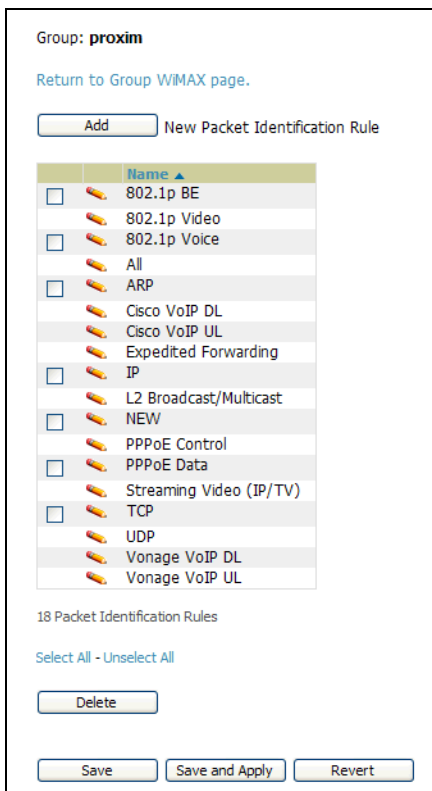


Table 71 Groups > PTMP/WiMAX Configuring Packet Identification Rules Fields and Default Values

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

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

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

- 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 51](#) illustrates this page and [Table 72](#) describes settings and default values.

Figure 51 *Groups > PTMP/WiMAX Configuring Service Flow Classes Page Illustration*

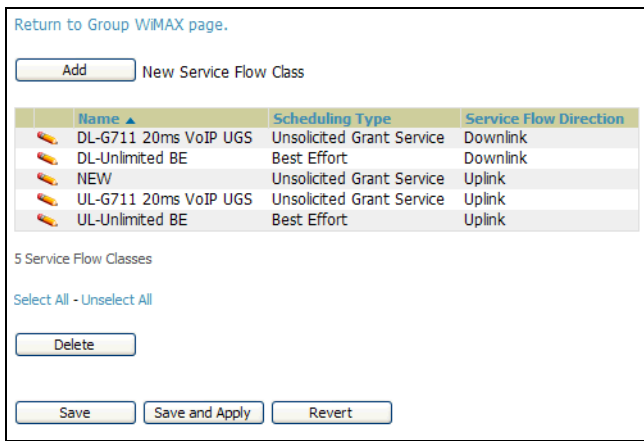


Table 72 *Groups > PTMP/WiMAX Configure Service Flow Classes Fields and Default Values*

| Setting | Default | Description |
|--|-------------|---|
| Name | None | Text field defines the name of the Service Flow Class. The name should be meaningful and descriptive. The name is used to define the subscriber station class. |
| Scheduling Type | Best Effort | Drop-down menu specifies the scheduling priority for the Service Flow Class. There are two options as follows: <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 52](#) illustrates this page and [Table 73](#) describes the settings and default values.

Figure 52 *Groups > PTMP/WiMAX Configuring Subscriber Station Classes Page Illustration*

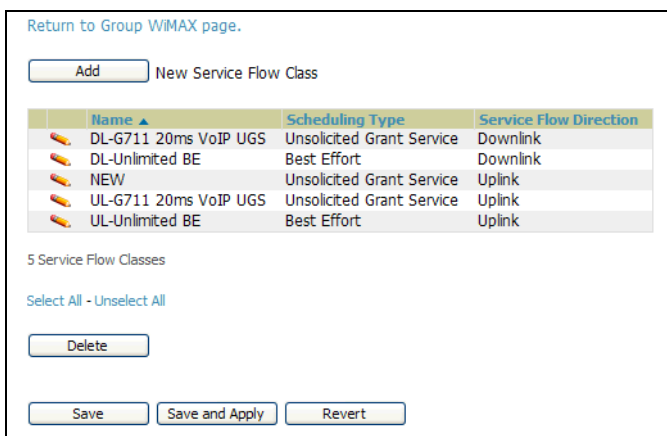


Table 73 Groups > PTMP/WiMAX Configuring Subscriber Station Classes Fields and Default Values

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

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

Configuring Proxim Mesh Radio Settings

1. Navigate to the **Groups > Proxim Mesh** configuration page to configure Mesh-specific radio settings.
2. Define the settings as required for your network. [Figure 53](#) illustrates this page. [Table 73](#) and [Table 75](#) describe the settings and default values.

Figure 53 *Groups > Proxim Mesh Page Illustration*

The screenshot shows the configuration page for Proxim Mesh. It is divided into three main sections: General, Security, and Mesh Cost Matrix. The General section includes fields for Mesh Radio (4.9/5 Ghz), Maximum Mesh Links (6), Neighbor RSSI Smoothing (16), Roaming Threshold (80), and Deauth Client When Uplink is Down (Yes). The Security section includes SSID (Wireless Mesh) and Enable AES (No). The Mesh Cost Matrix section includes fields for Hop Factor (2), Maximum Hops to Portal (4), RSSI Factor (5), RSSI Cut-Off (10), Medium Occupancy Factor (5), and Current Medium Occupancy Weight (7). At the bottom, there are buttons for Save, Save and Apply, and Revert.

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

Table 74 *Groups > Mesh Radio Settings > General Fields and Default Values*

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

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

Table 75 *Groups > Mesh Radio Settings > Security Fields and Default Values*

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

3. The **Mesh Count Matrix** configuration section contains settings for hop factor and maximum hops to portal, RSSI factor and cut-off, medium occupancy factor and current medium occupancy weight. Adjust these settings as required for your network. [Table 76](#) describes these settings and default values.

Table 76 *Groups > Mesh Radio Settings > Mesh Count Matrix Fields and Default Values*

| Setting | Default | Description |
|--|---------|--|
| Hop Factor | 5 | Sets the factor associated with each hop when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink. |
| Maximum Hops to Portal | 4 | Set the maximum number of hops for the AP to reach the Portal AP. |
| RSSI Factor | 5 | Sets the factor associated with the RSSI values used when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink. |
| Minimum RSSI Cutoff | 10 | Specifies the minimum RSSI needed to become a mesh neighbor. |
| Medium Occupancy Factor | 5 | Sets the factor associated with Medium Occupancy when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink. |
| Current Medium Occupancy Weight | 7 | Specifies the importance given to the most recently observed Medium Occupancy against all of the previously viewed medium occupancies. Lower values place more importance on previously observed Medium Occupancies. |

4. Click **Save** when configurations are complete to retain these settings. Click **Save and Apply** to retain these settings and push them to devices in the group. Click **Revert** to cancel out of these changes and return to the most recently saved changes.

Configuring Group MAC Access Control Lists

This configuration is optional. If you use Symbol 4121/4131, Intel 2011/2011b, Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP-3/4/5/6/7/8, or ProCurve 520WL wireless access points, OV3600 enables you to specify the MAC Addresses of devices that are permitted to associate with APs in the Group. Other devices are not able to associate to APs in the Group, even if the users of those devices are authorized users on the network.



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 54](#) illustrates this configuration page.

Figure 54 *Groups > MAC ACL Page Illustration*

The screenshot shows a web-based configuration interface for a group named 'proxim'. At the top, it says 'Group: proxim' and 'These settings apply to Proxim, Cisco Vxworks, Symbol, Intel and Procurve520 devices.' Below this is a section titled 'MAC ACL'. It contains a 'Use MAC ACL:' dropdown menu with options 'Yes', 'No', 'Yes', and 'Use manual setting on each AP'. The 'Yes' option is selected. Below the dropdown is a text area for 'Authorized MAC Addresses:' with a note: 'This list will not be set on Cisco VxWorks APs.' At the bottom of the form are three buttons: 'Save', 'Save and Apply', and 'Revert'.

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

Specifying Minimum Firmware Versions for APs in a Group

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

1. Browse to the **Groups > Firmware** configuration page. [Figure 55](#) illustrates this page.

Figure 55 *Groups > Firmware Page Illustration (Partial View)*

| Device Type | Desired Version |
|---|-----------------|
| 3Com Wx100 | NONE |
| 3Com Wx1200 | NONE |
| 3Com Wx2200 | NONE |
| 3Com Wx4400 | NONE |
| Alcatel-Lucent OAW-4302 | NONE |
| Alcatel-Lucent OAW-4304 | NONE |
| Alcatel-Lucent OAW-4308 | NONE |
| Alcatel-Lucent OAW-4324 | NONE |
| Alcatel-Lucent OAW-4504 | NONE |
| Alcatel-Lucent OAW-4604 | NONE |
| Alcatel-Lucent OAW-4704 | NONE |
| Alcatel-Lucent OAW-5000 | NONE |
| Alcatel-Lucent OAW-6000 | NONE |
| Anuba 200 | NONE |
| Anuba 2400 | NONE |
| Anuba 2400-E | NONE |
| Anuba 3xxx | NONE |
| Anuba 5000/6000 | NONE |
| Anuba 800 | NONE |
| Anuba 800-4 | NONE |
| Anuba 800-E | NONE |
| Avaya AP-3 | NONE |
| Avaya AP-4/5/6 | NONE |
| Avaya AP-7 | NONE |
| Avaya AP-8 | NONE |
| Cisco 2000 WLC | NONE |
| Cisco 2100 WLC | NONE |
| Cisco 4000 WLC | NONE |
| Cisco 4400 WLC | NONE |
| Cisco Aironet 1100 IOS | NONE |
| Cisco Aironet 1130 IOS | NONE |
| Cisco Aironet 1200 IOS | NONE |
| Cisco Aironet 1200 VxWorks | NONE |
| Cisco Aironet 1240 IOS | NONE |
| Cisco Aironet | NONE |
| Cisco Wireless LAN Controller Module | NONE |
| Colubris CN1300 | NONE |
| Colubris CN1350 | NONE |
| Colubris CN1250 | NONE |
| Colubris CN200 | NONE |
| Colubris CN300/CN300R | NONE |
| Colubris CN3000 | NONE |
| Colubris CN320 | NONE |
| Colubris CN3200 | NONE |
| Colubris CN330 | NONE |
| Colubris CN3300 | NONE |
| Colubris CN3400 | NONE |
| Colubris CN3400R | NONE |
| Enterasys RBT800 | NONE |
| Enterasys RBT8200 | NONE |
| Enterasys RBT8400 | NONE |
| Enterasys RoamAbout AP2000 | NONE |
| Enterasys RoamAbout AP3000 | NONE |
| Enterasys RoamAbout AP4102 | NONE |
| Enterasys RoamAbout R2 | NONE |
| Funkwerk Artem W-1000 | NONE |
| HP ProCurve 425 | NONE |
| HP ProCurve 520WL | NONE |
| HP ProCurve 530 | NONE |
| Hirschmann BA754-0ab | NONE |
| Intel 2011 | NONE |
| Intel 2011B | NONE |
| LANCOM 3550 | NONE |
| LANCOM IAP-54 | NONE |
| LANCOM L-54g/sg | NONE |
| LANCOM OAP-54 | NONE |
| Motorola WIAW200 | NONE |
| Motorola WIAW200M | NONE |
| Nortel WSS2350 | NONE |
| Proxim AP-4900MR-LR | 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 Taunani MP.11 2454-R | NONE |
| Proxim Taunani MP.11 4954-R | NONE |
| Proxim Taunani MP.11 5012-SUI | NONE |
| Proxim Taunani MP.11 5054 | NONE |
| Proxim Taunani MP.11 5054-R | NONE |
| Proxim Taunani MP.11 5054-R-LR | NONE |
| Proxim Taunani MP.11 5054e-SUI | NONE |
| Proxim Taunani MP.11 5054e-SUR | NONE |
| Proxim Taunani MP.11 954-R | NONE |
| Proxim Taunani QuickBridge.11 2454-R | NONE |
| Proxim Taunani QuickBridge.11 4954-R | NONE |
| Proxim Taunani QuickBridge.11 5054 | NONE |
| Proxim Taunani QuickBridge.11 5054-R | NONE |
| Proxim Taunani QuickBridge.11 5054-R-LR | NONE |
| Symbol 4121 | NONE |
| Symbol 4131 | NONE |
| Symbol 5131 | NONE |
| Symbol 5181 | NONE |
| Symbol RFS6000 | NONE |
| Symbol RFS7000 | NONE |
| Symbol VSS2000 | NONE |
| Symbol WSS100 | NONE |

2. For each device type in the group, use the pull-down menu to specify the minimum acceptable firmware version. If no firmware versions are listed, you must browse to the **Device Setup > Firmware** configuration page to upload the firmware files to OV3600.
3. Click **Upgrade** to apply firmware preferences to devices in the group. Refer to the firmware upgrade help under **APs/Devices > Manage** configuration page for detailed help on Firmware job options.
4. Click **Save** to save the firmware file as the desired version for the group.
5. If you have opted to assign an external TFTP server on a per-group basis on the **Device Setup > Firmware** configuration page, you can enter the IP address in the **Firmware Upgrade Options** field on the top of this configuration page.
6. Once you have defined your first group, you can configure that group to be the **default** group on your network. When OV3600 discovers new devices that need to be assigned to a management group, the default group appears at the top of all drop-down menus and lists. Newly discovered devices are place automatically in the default group if OV3600 is set to **Automatically Monitor/Manage New Devices** on the OV3600 configuration page.
7. Browse to the **Groups > List** configuration page. See [Figure 29](#) for the **Groups > List** configuration page.

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

Comparing Device Groups

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

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

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

- From the **Groups > List** page, click **Compare two groups**. Two drop-down menus appear.
- Select the two groups to compare to each other in the drop-down menus, and click **Compare**. The **Compare** page appears, displaying some or many configuration categories. [Figure 56](#) illustrates this page.

Figure 56 Comparing Two Devices Groups on the **Groups > List > Compare** Page (Partial View)

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

[Show Similar Fields](#)

| | HQ-RemoteAP (edit) | Basic | Outdoor (edit) |
|---|--------------------------|-------|----------------|
| 802.11 Counters Polling Period: | 30 minutes | ➔ | 15 minutes |
| Allow One-to-One NAT: | No | ➔ | Yes |
| Bridge Forward Delay: | 15 | ➔ | 16 |
| Bridge Hello Time: | 2 | ➔ | 4 |
| Bridge Maximum Age: | 20 | ➔ | 22 |
| Bridge Priority: | 32768 | ➔ | 32760 |
| Cisco IOS CLI Communication: | Telnet | ➔ | SSH |
| Cisco IOS Config File Communication: | TFTP | ➔ | SCP |
| Device Bandwidth Polling Period: | 10 minutes | ➔ | 5 minutes |
| Device-to-Device Link Polling Period: | 15 minutes | ➔ | 30 minutes |
| NTP Polling Interval: | 86400 | ➔ | 3600 |
| NTP Server #1: | (empty string) | ➔ | 10.2.25.162 |
| Override Polling Period for Other Services: | Yes | ➔ | No |
| Read ARP Table: | 4 hours | ➔ | 8 hours |
| Read Bridge Forwarding Table: | 4 hours | ➔ | 8 hours |
| Read CDP Table for Device Discovery: | 4 hours | ➔ | 8 hours |
| SNMP Trap Receiver #1 IP: | (empty string) | ➔ | 10.51.2.37 |
| SNMP Trap Receiver #1 Name: | (empty string) | ➔ | gauss |
| SNMP Trap Receiver #2 IP: | (empty string) | ➔ | 10.51.2.5 |
| SNMP Trap Receiver #2 Name: | (empty string) | ➔ | joule |
| SNMP Trap Receiver #3 IP: | (empty string) | ➔ | 10.51.2.15 |
| SNMP Trap Receiver #3 Name: | (empty string) | ➔ | mole |
| SNMP Version: | 2c | ➔ | 1 |
| SSH Version: | v1 | ➔ | v2 |
| Show device settings for: | Only devices on this AMP | ➔ | All devices |
| Spanning Tree Protocol: | No | ➔ | Yes |
| Thin AP Discovery Polling Period: | 15 minutes | ➔ | 30 minutes |
| User Data Polling Period: | 5 minutes | ➔ | 10 minutes |

- Note the following factors when using the **Compare** page:
 - The **Compare** page can be very long or very abbreviated, depending on how many configurations the device groups share or do not share.
 - When a configuration differs between two groups, the setting is flagged in red text for the group on the right.
 - The default setting of the **Compare** page is to highlight settings that differ between two groups.
 - To display settings that are similar or identical between two device groups, click **Show Similar Fields** at the top left of the page. The result may be a high volume of information.
 - Click **Hide Similar Fields** to return to the default display, emphasizing configuration settings that differ between two groups.

- You can change the configuration for either or both groups by clicking **Edit** in the corresponding column heading. The appropriate configuration page appears.
- If you make and save changes to either or both groups, navigate back to the **Groups > List** page and click **Compare two groups**. Select the same two groups again for updated information.
- Additional topics in this document or in the *Alcatel-Lucent Configuration Guide* describe the many fields that can appear on the **Groups > List > Compare** page.

Deleting a Group

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

1. Browse to the **Groups > List** configuration page.
2. Ensure that the Group you wish to delete is not marked as the **default** group. OV3600 does not permit you to delete the current default Group.
3. Ensure there are no devices in the Group you wish to delete. OV3600 does not permit you to delete a Group that still contains managed devices. You must move all devices to other Groups before deleting a Group.
4. Select the checkbox and click **Delete**.

Changing Multiple Group Configurations

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

1. Browse to the **Groups > List** configuration page.
2. Click the **Manage** link (the pencil icon) for the group you wish to edit. The **Groups > Basic** configuration page appears.
3. Select the fields to be edited on the **Basic** configuration page or navigate to **Radio**, **Security**, **VLANs**, or **MAC ACL** configuration page and edit the fields. Use the **Save** button to store the changes prior to applying them, or click **Save and Apply** to save and push configurations.
4. When all changes for the group are complete click the **Save and Apply** button. [Figure 57](#) illustrates the confirmation message that appears.

Figure 57 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:

5. OV3600 displays a **Configuration Change** screen confirming the changes that will be applied to the group's settings.
6. There are several action possibilities from within this confirmation configuration page.
 - **Apply Changes Now**—This button applies the changes immediately to access points within the group. If you wish to edit multiple groups you must use the Preview button.
 - **Schedule**—This button schedules the changes to be applied to this group in the future. Enter the desired change date in the **Start Date/Time** field. OV3600 takes the time zone into account for the

group if a time zone other than **OV3600 System Time** has been configured on the **Group > Basic** configuration page.

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



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

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

Modifying Multiple Devices

OV3600 provides a very powerful utility that modifies all APs or a subset of access points unrelated to OV3600' 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 one of the following pages:

- **APs/Devices > List**
- **APs/Devices > Up**
- **APs/Devices > Down**
- **APs/Devices > Mismatched**
- **Groups > Monitor** configuration pages

Each of these pages displays a list of devices

2. Click **Modify Devices** to make the checkboxes at the left of all devices appear. In addition, a new section appears in this page location to display various settings that can be configured for multiple devices at one time. [Figure 58](#) illustrates this page.

Figure 58 *Modify Multiple Devices Section Illustration*

| Device | Status | Upstream Device | APs | Users | BW (kbps) | Uptime | Configuration | Group | Controller | SSID | First Radio |
|---------------------|--------|-----------------|-----|-------|-----------|-------------------------|---------------|---------------|------------|------|-------------|
| (id: 9) | Up | - | 0 | 0 | 0 | 131 days 20 hrs 18 mins | Mismatched | Access Points | - | - | - |
| ag-2100 | Up | - | - | 0 | 0 | 1 day 23 hrs 53 mins | Error | Access Points | - | - | 802.11bg |
| Alcatel-Lucent-4308 | Up | - | 0 | 0 | 0 | 10 days 16 hrs 46 mins | Error | Access Points | - | - | - |

3. Select one or more devices that are to share the configurations. Click inside the checkbox for each device to modify.

4. In the Modify Multiple Devices section, click any button or use any drop-down menu for the supported changes. Any action you take applies to all selected devices. Each action you take will direct you to a new configuration page, or prompt you with a confirmation page to confirm your changes.
5. You are taken to a confirmation configuration page that allows you to schedule the change for a time in the future. Enter a start date and time in the scheduling field and select when the change should occur from the drop-down menu (one time is the default, but you may select recurring options for many of the actions). Scheduled jobs can be viewed and edited in the **System > Configuration Change Jobs** tab.
6. Using the neighbor lists, OV3600 is able to optimize channel selection for APs. Select the APs to optimize and OV3600 minimizes the channel interference while giving channel priority to the most heavily used APs. [Table 77](#) describes these action and controls.

Table 77 Modify Multiple Devices Section Fields and Default Values

| Action | Description |
|---|---|
| Set Group | Move the selected APs to a new group. If the AP is in managed mode when it is moved to a new group, it will be reconfigured. |
| Move to Aruba/Alcatel-Lucent AP Group | Moves the selected APs to a new group or folder. If the AP is in managed mode when it is moved to a new group it will be reconfigured. |
| Update Cisco Thin AP Settings | Bulk configuration for per-thin AP settings, previously configured on the Group LWAPP AP tab can be performed from Modify Devices on the APs/Devices List page. Make changes to LWAPP AP groups, including the option that was under Modify Devices, is now available here. |
| 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. |
| Audit selected devices | Fetches the current configuration from the device and compares it to OV3600s desired configuration. The audit action updates the Configuration Status. |
| Import settings of 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. |
| 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. |
| 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. |
| Modify Radio Status | Enables or disables the radios on the selected device. Does <i>not</i> apply Cisco IOS APs. |
| Reboot selected devices | Reboots the selected devices. Use caution when rebooting devices because this can disrupt wireless users. |
| Reprovision selected Aruba/Alcatel-Lucent devices | Configures the controller to send provisioning parameters such as radio, antenna, and IP address settings to the selected APs. Please note that APs will be rebooted as part of reprovisioning. |
| Upgrade firmware for selected devices | Upgrades firmware for the selected devices. Refer to the firmware upgrade help under APs/Devices > Manage configuration page for detailed help on Firmware job options. |
| Cancel firmware upgrade for selected devices | Cancels any firmware upgrades that are scheduled or in progress for the selected APs. |

Table 77 Modify Multiple Devices Section Fields and Default Values (Continued)

| Action | Description |
|--|--|
| Optimize channel assignment to reduce overlap | OV3600 uses the APs neighbor table to determine the optimal channel for the selected APs. |
| Delete selected devices | Removes the selected APs from OV3600. The deletes will be performed in the background and may take a minute to be removed from the list. |

Using Global Groups for Group Configuration

To apply group configurations using 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 59](#) illustrates this configuration page.

Figure 59 Groups > List Page Illustration

| | Name | SSID | Total Devices | Down | Mismatched | Ignored | Users | BW (kbps) | Up/Down Status Polling Period | Duplicate |
|--------------------------|---------------|------|---------------|------|------------|---------|-------|-----------|-------------------------------|-----------|
| <input type="checkbox"/> | Access Points | wpa | 38 | 4 | 32 | 0 | 0 | 0 | 5 minutes | |
| <input type="checkbox"/> | San Francisco | - | 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**, **Cisco WLC Config**, **LWAPP APs**, **PTMP/WiMAX**, **Proxim Mesh** and **MAC ACL** tabs. [Figure 60](#) illustrates this configuration page.

Figure 60 Groups > Basic Page for a Global Group

- When a global group configuration is pushed to subscriber groups, all settings are static except for settings with the checkbox selected; for fields with checkboxes selected, the value or setting can be changed on the corresponding tab for each managed group. In the case of the **Groups > SSIDs** configuration page, override options are available only on the **Add** configuration page (navigate to the **Groups > SSIDs** configuration page and click the **Add** button). Global templates are also configurable as part of global groups; see [“Creating and Using Templates” on page 163](#) 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 61](#) illustrates this page.

Figure 61 *Groups > Basic > Managed Page Illustration*

The screenshot shows a configuration page for a group named 'Access Points'. It is divided into two sections: 'Basic' and 'Global Groups'.
Basic Section:
- Name: Access Points
- Missed SNMP Poll Threshold (1-100): 1
- Regulatory Domain: United States
- Timezone: AMP system time
- Allow One-to-One NAT: No
Global Groups Section:
- Use Global Group: Yes (selected)
- Global Group: globalgroupMC (SSID: -)

- Once the configuration is pushed, the unchecked fields from the global group appears on the subscriber group as static values and settings. Only fields that had the override checkbox selected in the global group appear as fields that can be set at the level of the subscriber group. Any changes to a static field must be made on the global group.
- 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 62 *Groups > Basic > Managed Illustration for a Subscriber Group*

The screenshot shows the configuration page for a subscriber group. The 'Basic' section contains the following fields:
- Name: new group
- Missed SNMP Poll Threshold (1-100): 1
- Regulatory Domain: United States
- Timezone: OV3600 system time
- Allow One-to-One NAT: No
- Audit Configuration on Devices: Yes (selected)

- If a global group has subscriber groups it cannot be changed to a non-global group. A global group without subscriber groups can be changed to a regular group by updating the setting on the **Groups > Basic** configuration interface. The global groups feature can also be used with the **Master Console**. For more information about this feature, refer to [“Supporting OV3600 Stations with the Master Console” on page 227](#).

Introduction

The previous chapter, “Configuring and Using Device Groups in OV3600” on page 73, describes the configuration and implementation of device *groups*. A group sets configuration for all devices in the group. Individual devices can also maximize their vendor-specific attributes and benefits when these are supported. This chapter describes the methods for device-specific configuration and activity. This chapter emphasizes, but is not limited to, the following OV3600 pages:

- **Device Setup**
 - **Device Setup > Discover**
 - **Device Setup > Add**
 - **Device Setup > Communication**
- **APs/Devices**
 - **APs/Devices > List**
 - **APs/Devices > New**
 - **APs/Devices > Audit**
 - **APs/Devices > Manage**
 - **APs/Devices > Monitor**

This chapter contains the following device-oriented topics and procedures:

Discovery of Devices Overview

Defining Networks for SNMP/HTTP Scanning

- Adding Networks for SNMP/HTTP Scanning
- Defining Credentials for SNMP/HTTP Scanning
- Defining a SNMP/HTTP Scan Set
- Executing a Scan by Running a Scan Set

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 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 for AP Communication Settings

Discovery of Devices Overview

Once you have deployed OV3600 on the network and defined at least one device group, the next step is to discover all existing APs connected to your network and to assign them to a group. OV3600 supports multiple methods to discover devices, as follows:

- **SNMP/HTTP scanning**—This is the primary method for OV3600 to discover APs on your network, and this discovery method contains four specific procedures. The interface that configures this discovery method is the **Device Setup > Discovery** page. Refer to this topic for additional information:
 - [Defining Networks for SNMP/HTTP Scanning](#).
- **Manual device entry**—This method of discovery applies when the devices are known to be on the network. The **admin** user adds devices manually with known AP device information. Refer to the following procedures for manual device discovery:
 - [Manually Adding Individual Devices](#)
 - [Adding Access Points, Routers and Switches with a CSV File](#)
 - [Adding Universal Devices](#)
 - [Assigning Newly Discovered Devices to Groups](#)
- **Controller-driven device discovery**—When there are thin APs on the network, you may add controllers to the network, then to OV3600, and the controller then discovers thin AP devices.
- **Automatically assigning new devices to a group**—This configuration enables new devices to be assigned to groups without manual configuration. Refer to the following topic:
 - [Assigning Newly Discovered Devices to Groups](#)
- **Cisco Discovery Protocol (CDP)**—CDP is another common method by which to discover devices on the network. OV3600 enhances support for CDP by discovering a device's CDP neighbors when the IP address for that device is known. Refer to the following procedure:
 - [Adding Access Points, Routers and Switches with a CSV File](#).

This chapter describes each of these device discovery methods.

Defining Networks for SNMP/HTTP Scanning

SNMP/HTTP scanning is the primary method to discover devices on the network, to include discovery of rogue devices. Deploy this scanning method with the **Device Setup > Discover** page. This page contains three sections, as follows:

- **Scan Sets** section—lists the scan sets that have been defined in OV3600, and allows you to add new scan sets. Scan sets combine networks and credentials when scanning for devices.
- **Networks** section—lists the networks that have been defined for scanning, and allows you to define new networks for scanning. A network must be added to OV3600 prior to defining a scan set.
- **Credentials** section—lists the network credentials defined in OV3600, and allows you to define new credentials for network scanning. Credentials must be created prior to using them in scan sets.

Figure 63 illustrates the **Device Setup > Discover** page.

Figure 63 Device Setup > Discover Page Illustration

To scan for manageable devices and rogue APs using SNMP and HTTP, choose one or more networks to scan below. SNMP and HTTP timeouts may be configured on the [Communication](#) page.

Note: Discovered devices will use the default credentials configured on the [Communication](#) page, *not* the credentials defined below for scanning.

1-2 of 2 Scan Sets Page 1 of 1 Choose Columns

| | Network | Credentials | Total Devices Found | New Devices Found | Total Rogues Found | New Rogues Found | Start | Stop | Scheduled |
|--------------------------|-----------|---------------------------------|---------------------|-------------------|--------------------|------------------|--------------------|--------------------|-----------|
| <input type="checkbox"/> | 10.51.1.0 | admin, default, private, public | 8 | 8 | 1 | 0 | 8/26/2009 11:59 AM | 8/26/2009 12:01 PM | - |
| <input type="checkbox"/> | 10.51.3.0 | admin, default, private, public | 30 | 30 | 0 | 0 | 8/26/2009 11:59 AM | 8/26/2009 12:03 PM | - |

1-2 of 2 Scan Sets Page 1 of 1

Select All - Unselect All

Refresh this page for updated results.

Show Scheduling Options

Networks

New Scan Network

1-2 of 2 Scan Networks Page 1 of 1 Choose Columns

| | Name | Network | Subnet Mask |
|--------------------------|-----------|-----------|---------------|
| <input type="checkbox"/> | 10.51.1.0 | 10.51.1.0 | 255.255.255.0 |
| <input type="checkbox"/> | 10.51.3.0 | 10.51.3.0 | 255.255.255.0 |

1-2 of 2 Scan Networks Page 1 of 1

Select All - Unselect All

Credentials

New Scan Credential

| | Name | Type | Username |
|--------------------------|---------|--------|----------|
| <input type="checkbox"/> | admin | HTTP | admin |
| <input type="checkbox"/> | default | HTTP | default |
| <input type="checkbox"/> | private | SNMPv1 | - |
| <input type="checkbox"/> | public | SNMPv1 | - |

4 Scan Credentials

Select All - Unselect All

Adding Networks for SNMP/HTTP Scanning

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

1. Navigate to the **Device Setup > Discover** page, and locate the **Networks** section.
2. In the **Networks** section, click **Add New Scan Network**. The **Scan Network** page appears, as shown in [Figure 64](#). Alternatively, you can edit an existing scan network by clicking the corresponding pencil icon. The **New/Edit Networks** page appears.

Figure 64 Device Setup > Discover > New Network Section Illustration

Networks

Scan Network

Name:

Network:

Subnet Mask:

3. In the **Name** field, provide a name for the network to be scanned (for example, **Accounting Network**).
4. In the **Network** field, define the IP network range, or the first IP address on the network, to be scanned. One example would be 10.52.0.0, as an illustration.
5. Enter the **Subnet Mask** for the network to be scanned (for example, 255.255.252.0). The largest subnet supported by OV3600 is 255.255.0.0.
6. Click **Add**.
7. Repeat these steps to add as many networks for which to support device scanning. All network segments configured in this way appear in the **Network** section of the **Device Setup > Discover** page. These networks comprise one of two elements that comprise scan sets.

8. Complete the configuration of scan credentials, then combine scan networks and scan credentials to create scan sets. The next two procedures in this section describe these tasks.

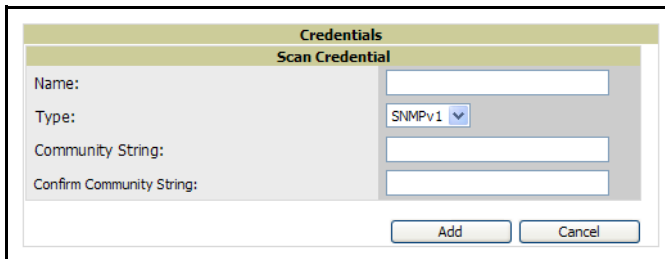
Defining Credentials for SNMP/HTTP Scanning

The next step in SNMP/HTTP device discovery is to define the scan credentials that govern scanning of a given network. New APs inherit scan credentials from the System Credentials that you configure on the **Device Setup > Communications** page.

Perform these steps to define scan credentials for SNMP/HTTP scanning:

1. Locate the **Credentials** section on the **Device Setup > Discover** page. This section displays scan sets, networks, and credentials that have been configured thus far, and enables you to define new elements for device scanning.
2. To create a new scan credential, click **Add New Scan Credential**. [Figure 65](#) illustrates this page.

Figure 65 *Device Setup > Discover > Add/Edit New Scan Credential Section Illustration*



3. Provide a name for the credential in the **Name** field (for example, **Default**). This field supports alphanumeric characters, both upper and lower case, and blank spaces, hyphens, and underscore characters.
4. Choose the type of scan to be completed (**SNMPv1**, **SNMPv2**, or **HTTP**). In most cases, it is advisable to use SNMP scans for device discovery, but the differences are as follows:
 - SNMPv1 and SNMP v2 differ between in their supported traps, supported MIBs, and network query elements used in device scanning.
 - HTTP discovers devices using the HyperText Transfer Protocol in communications between servers and additional network components. HTTP is not as robust in processing network events as is SNMP, but HTTP may be sufficient, simpler, or preferable in certain scenarios.
5. Define and confirm the **Community String** to be used during scanning. In this section, the community string used can be either **read-only** or **read/write**, as OV3600 only uses it for discovering APs. To bring APs under management, OV3600 uses the credentials supplied in the **Device Setup > SNMP** page.



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

6. Click **Add**. The **Device Setup > Discover** page displays the new scan credential or credentials just created or edited.
7. Repeat these steps to add as many credentials as you would like.
8. Once scan networks and scan credentials are defined, combine them by creating scan sets using the next procedure titled [“Defining a SNMP/HTTP Scan Set” on page 124](#).

Defining a SNMP/HTTP Scan Set

Once you have defined at least one network and one scan credential, you can create a scan set that combines the two for device discovery. Perform these steps to create a scan set.

1. Locate the **Scan Set** area at the top of the **Device Setup > Discover** page. [Figure 63](#) illustrates this page.

Figure 66 Device Setup > Discover > Scan Sets Section Illustration

To scan for manageable devices and rogue APs using SNMP and HTTP, choose one or more networks to scan below. SNMP and HTTP timeouts may be configured on the [Communication](#) page.

Note: Discovered devices will use the default credentials configured on the [Communication](#) page, *not* the credentials defined below for scanning.

New Scan Set

1-7 ▼ of 7 Scan Sets Page 1 ▼ of 1

| | Network ▲ | Credentials | Total Devices Found | New Devices Found | Total Rogues Found | New Rogues Found | Start | Stop | Scheduled |
|--------------------------|--------------|--|---------------------|-------------------|--------------------|------------------|-------------------|-------------------|-----------|
| <input type="checkbox"/> | 10.51.1.0 | Default HTTP, private, public | 7 | 0 | 0 | 0 | 5/5/2009 4:29 AM | 5/5/2009 4:30 AM | - |
| <input type="checkbox"/> | 10.51.2.0 | private, public | 0 | 0 | 0 | 0 | 2/25/2009 1:46 PM | 2/25/2009 1:50 PM | - |
| <input type="checkbox"/> | 10.51.3.0 | Aruba AP's, Cisco, Cisco IOS APs, public | 31 | 3 | 0 | 0 | 3/26/2009 2:31 PM | 3/26/2009 2:35 PM | - |
| <input type="checkbox"/> | 10.51.5.0 | private, public | 6 | 0 | 0 | 0 | 1/9/2009 4:22 PM | 1/9/2009 4:24 PM | - |
| <input type="checkbox"/> | Jeremy's Lab | Cisco, public | 0 | 0 | 0 | 0 | 3/27/2009 4:34 PM | 3/27/2009 4:34 PM | - |
| <input type="checkbox"/> | Test Net 1 | private, public | - | - | - | - | - | - | - |
| <input type="checkbox"/> | Test Net 2 | private, public | - | - | - | - | - | - | - |

Select All - Unselect All

[Refresh this page for updated results.](#)

[Show Scheduling Options](#)

2. Click **Add New Scan Set**, and the **Scan Set** section displays. Below the **Scan Set** section, the **Networks** and **Credentials** sections display all scan components configured thus far. If you wish to create a new network, or new scanning credentials, you can click Add in either of these fields to create new components prior to creating a scan set. [Figure 67](#) illustrates the **Add New Scan Set** page.

Figure 67 Device Setup > Discover > Add New Scan Set Page Illustration

To scan for manageable devices and rogue APs using SNMP and HTTP, choose one or more networks to scan below. SNMP and HTTP timeouts may be configured on the [Communication](#) page.

Note: Discovered devices will use the default credentials configured on the [Communication](#) page, *not* the credentials defined below for scanning.

Scan Set

Network:

Credentials: admin (HTTP) default (HTTP) private (SNMPv1) public (SNMPv1)

[Select All - Unselect All](#)

Networks

New Scan Network

1-2 ▼ of 2 Scan Networks Page 1 ▼ of 1 [Choose Columns](#)

| | Name ▲ | Network | Subnet Mask |
|--------------------------|-----------|-----------|---------------|
| <input type="checkbox"/> | 10.51.1.0 | 10.51.1.0 | 255.255.255.0 |
| <input type="checkbox"/> | 10.51.3.0 | 10.51.3.0 | 255.255.255.0 |

1-2 ▼ of 2 Scan Networks Page 1 ▼ of 1

Select All - Unselect All

Credentials

New Scan Credential

| | Name ▲ | Type | Username |
|--------------------------|---------|--------|----------|
| <input type="checkbox"/> | admin | HTTP | admin |
| <input type="checkbox"/> | default | HTTP | default |
| <input type="checkbox"/> | private | SNMPv1 | - |
| <input type="checkbox"/> | public | SNMPv1 | - |

4 Scan Credentials

Select All - Unselect All

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

6. When ready, proceed to the next task, “Executing a Scan by Running a Scan Set” on page 126.



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

Executing a Scan by Running a Scan Set

Once a scan has been defined on the **Device 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. This section lists all scan sets that have been defined thus far. [Figure 68](#) illustrates this page.

Figure 68 *Device Setup > Discover > Executing a Scan Illustration*

To scan for manageable devices and rogue APs using SNMP and HTTP, choose one or more networks to scan below. SNMP and HTTP timeouts may be configured on the [Communication](#) page.

Note: Discovered devices will use the default credentials configured on the [Communication](#) page, *not* the credentials defined below for scanning.

New Scan Set

1-10 ▾ of 10 Scan Sets Page 1 ▾ of 1

| | Network ▲ | Credentials | Total APs Found | New APs Found | Total Rogues Found | New Rogues Found | Start | Stop | Scheduled |
|--------------------------|-------------|-------------------------------|-----------------|---------------|--------------------|------------------|-------------------|-------------------|-----------|
| <input type="checkbox"/> | 10.51.51.51 | Default HTTP, private, public | 1 | 0 | 0 | 0 | 2/27/2009 3:17 AM | 2/27/2009 3:21 AM | - |
| <input type="checkbox"/> | 10.52.52.52 | private, public | 0 | 0 | 0 | 0 | 2/25/2009 1:46 PM | 2/25/2009 1:50 PM | - |
| <input type="checkbox"/> | 10.53.53.53 | private, public | 22 | 0 | 0 | 0 | 2/27/2009 5:04 PM | 2/27/2009 5:08 PM | - |
| <input type="checkbox"/> | 10.51.50.50 | private, public | 6 | 0 | 0 | 0 | 1/9/2009 4:22 PM | 1/9/2009 4:24 PM | - |
| <input type="checkbox"/> | 10.90.90.90 | private, public | 0 | 0 | 0 | 0 | 1/9/2009 3:47 PM | 1/9/2009 3:52 PM | - |

Select All - Unselect All

[Refresh this page for updated results.](#)

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. The **Stop** column displays **In Progress**.
4. For future scans, click **Show Scheduling Options** and enter the desired date and time to schedule a future scan.
5. After several minutes have passed, click the **Refresh** button in your browser to refresh the page and view the results of the scan you have just run. When the **Start** and **Stop** columns display date and time information, and no longer display **In progress**, the scan is available to display the results.
6. Click the **Pencil** icon for the scan you have just run to display the results. [Table 78](#) describes the scan results and related information.

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

| Column | Description |
|------------------------|--|
| Network | Displays the network to be scanned. |
| Credentials | Displays the credentials used in the scan. |
| Total APs Found | Displays the total number of APs detected during the scan that OV3600 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. |
| New APs Found | Displays the number of newly discovered APs that are not yet under OV3600 management but can be managed by OV3600. |

Table 78 Device Setup > Discover > Discovery Execution Fields (Continued)

| Column | Description |
|---------------------------|---|
| Total Rogues Found | Displays 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. |
| New Rogues Found | Displays the number of rogue APs discovered on the most recent scan. |
| Start | Displays the date and time the scan was most recently started. |
| Stop | Displays the date and time the scan most recently completed. |
| Scheduled | Displays the scheduled date and time for scans that are scheduled to be run. |

7. Navigate to the **APs/Devices > New** page to see a full list of the newly discovered devices that the scan detected. [Figure 69](#) illustrates this page.

Figure 69 APs/Devices > New Page Illustration

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

1-35 of 35 APs/Devices Page 1 of 1 Choose Columns

| Device | Controller | Type | IP Address | LAN MAC Address | Discovered |
|--|---------------------|--------------------------|-------------|-------------------|---------------------|
| <input type="checkbox"/> Intel PRO/Wireless LAN | - | Intel 2011B | 10.51.1.60 | 00:03:47:15:EA:53 | 11/2/2009 12:08 PM |
| <input type="checkbox"/> R014-00861 | - | Colubris CN3200 | 10.51.1.105 | 00:03:52:01:63:9C | 11/2/2009 12:07 PM |
| <input type="checkbox"/> RADIO4 | RFS7000 | Symbol AP 100 | - | 00:A0:F8:56:8B:40 | 10/30/2009 1:06 PM |
| <input type="checkbox"/> AP0014.6940.8f22 | Cisco_40:7c:83 | Cisco Aironet 1240 LWAPP | 10.51.1.94 | 00:14:69:40:8F:22 | 10/29/2009 9:20 PM |
| <input type="checkbox"/> 00:24:6c:c0:80:0f | Aruba3600-US | Intel 2011B | 10.51.1.214 | 00:24:6C:C0:80:0F | 10/29/2009 9:07 AM |
| <input type="checkbox"/> AP1 | Cisco_40:7c:83 | Cisco Aironet 1250 LWAPP | 10.51.1.98 | 00:1D:45:91:14:1A | 10/16/2009 4:15 PM |
| <input type="checkbox"/> AP-2 | meru | Meru AP 150 | - | 00:0C:E6:00:DF:86 | 10/13/2009 11:17 AM |
| <input type="checkbox"/> AP-8 | meru | Meru AP 201 | - | 00:12:F2:39:5D:A7 | 10/13/2009 11:17 AM |
| <input type="checkbox"/> AP-3 | meru | Intel 2011B | - | 00:0C:E6:03:33:65 | 10/13/2009 11:17 AM |
| <input type="checkbox"/> AP-7 | meru | Meru AP 201 | - | 00:12:F2:39:57:AF | 10/13/2009 11:17 AM |
| <input type="checkbox"/> AP-4 | meru | Meru AP 100 | - | 00:0C:E6:00:0B:0D | 10/13/2009 11:17 AM |
| <input type="checkbox"/> RADIO8 | RFS7000 | Symbol AP 100 | - | 00:A0:F8:56:8A:CD | 10/12/2009 9:52 AM |
| <input type="checkbox"/> AP-5 | meru | Meru AP 320 | - | 00:0C:E6:05:01:6A | 10/10/2009 12:07 PM |
| <input type="checkbox"/> AP 124 - Trouble with capital T | Aruba2400 | Alcatel-Lucent AP | 10.51.5.17 | 00:1A:1E:C0:2B:34 | 10/9/2009 9:47 AM |
| <input type="checkbox"/> Radio envy | Aruba2400 | Intel 2011B | 10.51.3.250 | 00:08:86:C7:07:EF | 10/9/2009 9:47 AM |
| <input type="checkbox"/> 00:1a:1e:c6:d5:d2 | Aruba800-FIPS | Alcatel-Lucent AP | 10.51.1.232 | 00:1A:1E:C6:D5:D2 | 10/9/2009 9:46 AM |
| <input type="checkbox"/> mesh-portal-c2:2e:4a | Aruba2400 | Aruba AP 65 | 10.51.4.211 | 00:1A:1E:C2:2E:4A | 10/9/2009 9:46 AM |
| <input type="checkbox"/> Alcatel Lucent | - | Aruba Controller | 10.51.5.31 | - | 10/9/2009 9:45 AM |
| <input type="checkbox"/> 00:1a:1e:c0:55:46 | Aruba200 | Intel 2011B | 10.51.5.44 | 00:1A:1E:C0:55:46 | 10/9/2009 9:45 AM |
| <input type="checkbox"/> 00:1a:1e:c0:2b:3e | Alcatel-Lucent-4308 | Alcatel-Lucent AP 124 | 10.51.1.248 | 00:1A:1E:C0:2B:3E | 10/9/2009 9:45 AM |
| <input type="checkbox"/> AP1 | Cisco_40:7c:83 | Cisco Aironet 1250 LWAPP | 10.51.1.247 | 00:1D:45:91:14:42 | 10/9/2009 9:45 AM |
| <input type="checkbox"/> AP0022.bd19.5f2b | Cisco_40:7c:83 | Cisco Aironet 1140 LWAPP | 10.51.1.142 | 00:22:8D:19:5F:2B | 10/9/2009 9:45 AM |
| <input type="checkbox"/> AP0018.19bd.a092 | Cisco_40:7c:83 | Cisco Aironet 1200 LWAPP | 10.51.4.3 | 00:18:19:8D:A0:82 | 10/9/2009 9:45 AM |
| <input type="checkbox"/> Talsker | Aruba200 | Alcatel-Lucent AP | 10.51.9.106 | 00:1A:1E:C6:D5:C2 | 10/9/2009 9:44 AM |
| <input type="checkbox"/> Talsker | Aruba200 | Aruba AP 105 | 10.51.9.105 | 00:24:6C:C0:00:F6 | 10/9/2009 9:44 AM |
| <input type="checkbox"/> ap-Not set | Aruba-800-2X | Alcatel-Lucent AP | 10.51.6.95 | 00:08:86:C7:9D:36 | 10/9/2009 9:43 AM |
| <input type="checkbox"/> ap-Not set | Aruba-800-2X | Aruba AP 70 | 10.51.1.252 | 00:08:86:CE:E1:8C | 10/9/2009 9:43 AM |
| <input type="checkbox"/> ap-Not set | Aruba-800-2X | Alcatel-Lucent AP | 10.51.8.114 | 00:08:86:C0:99:BC | 10/9/2009 9:43 AM |
| <input type="checkbox"/> ap-1.1.1 | Aruba-800-2X | Aruba AP 65 | 10.51.5.2 | 00:1A:1E:C2:2E:F0 | 10/9/2009 9:43 AM |
| <input type="checkbox"/> ap:78 | Aruba3600-Local | Alcatel-Lucent AP | 10.51.5.18 | 00:1A:1E:C0:50:78 | 10/9/2009 9:43 AM |
| <input type="checkbox"/> 3600 AP124 | Aruba3600-Local | Aruba AP 124 | 10.51.5.19 | 00:1A:1E:C0:00:EC | 10/9/2009 9:43 AM |
| <input type="checkbox"/> Alcatel-Lucent AP | - | Aruba Controller | 10.51.5.117 | - | 10/9/2009 9:43 AM |
| <input type="checkbox"/> RADIO 4_4 | WS2000_Controller | Symbol AP 100 | - | 00:A0:F8:56:8A:7D | 10/9/2009 9:43 AM |
| <input type="checkbox"/> brand new shiny name | Aruba-3400 | Alcatel-Lucent AP | 10.51.5.7 | 00:1A:1E:C2:2E:AE | 10/9/2009 9:42 AM |
| <input type="checkbox"/> 00:1a:1e:c0:1a:dc | Aruba-3400 | Aruba AP 125 | 10.51.1.215 | 00:1A:1E:C0:1A:DC | 10/9/2009 9:42 AM |

1-35 of 35 APs/Devices Page 1 of 1

Select All - Unselect All

View Ignored Devices

Group: Access Points (SSID: alcatel-lucent-ap)

Folder: Top

Monitor Only

Manage Read/Write

From this page, you can perform the following tasks with new devices:

- Select one or more devices with the corresponding check box for each, then select a **Group**, **Folder**, and mode (**Monitor** or **Manage**), and click the **Add** button. This action adds the device to the **APs/Devices > List** page for additional processing as desired, and this action adds the device to the group specified.
- Select one or more devices with the corresponding check box for each, and click **Ignore**. This action removes the device or devices from OV3600 processing and pages, and adds such devices to the **APs/Devices > Ignored** page.
- Select one more devices with the corresponding check box for each, and click **Delete** to remove such devices entirely from OV3600. They will not reappear in OV3600 unless they are present during a future scan.

Manually Adding Individual Devices

Some deployment situations may require that you manually add devices to OV3600. You can add APs manually with a CSV file, or by using the **Device Setup > Add** page. This section describes both methods:

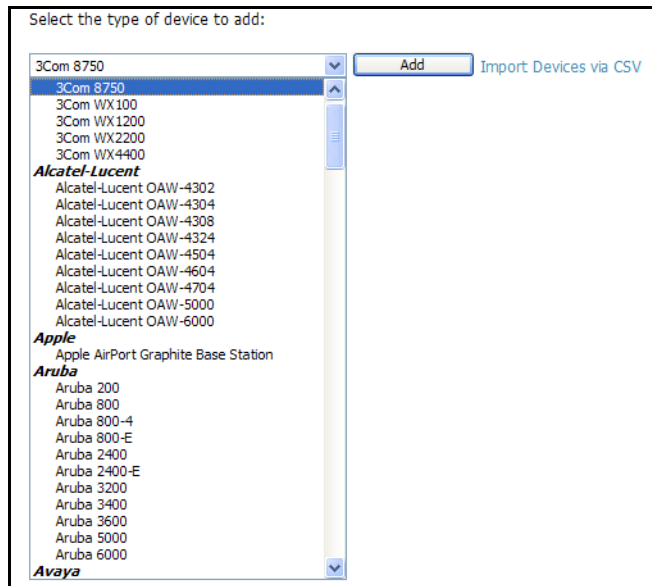
- Adding Devices with the Device Setup > Add Page
- Adding Access Points, Routers and Switches with a CSV File

Adding Devices with the Device Setup > Add Page

Perform these manual steps to add devices to OV3600 with device-specific parameters, depending on the make and model of the device:

1. The first step to add a device manually is to select the manufacturer and model. Browse to the **Device Setup > Add** page and select the manufacturer and model of the device to add. [Figure 70](#) illustrates this page.

Figure 70 *Device Setup > Add Page Illustration*



2. Click **Add**, and the **Device Communications** and **Location** sections appear, illustrated in [Figure 71](#).

Figure 71 *Device Setup > Add > Device Communications and Location Page Illustration*

Configure default credentials on the [Communication](#) page.

Device Communications

Name: Leave name blank to read it from device

IP Address:

SNMP Port:

Community String:

Confirm Community String:

SNMPv3 Username:

Auth Password:

Confirm Auth Password:

SNMPv3 Auth Protocol:

Privacy Password:

Confirm Privacy Password:

SNMPv3 Privacy Protocol:

Telnet/SSH Username:

Telnet/SSH Password:

Confirm Telnet/SSH Password:

"enable" Password:

Confirm "enable" Password:

Location

Group:

Folder:

Monitor Only (no changes will be made to device)

Manage read/write (group settings will be applied to device)

- Complete these **Communications** and **Location** settings for the new device. [Table 79](#) further describes the contents of this page. Note that settings may differ from device to device. In several cases, the default values from any given device derive from the **Device Setup > Communication** page.

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

| Setting | Default | 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. |
| SNMPv3 Username | 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 and password combination to control the Cisco AP. OV3600 creates a user-specified account with which to manage the AP if the User Creation Options are set to Create and user Specified as User. NOTE: New, out-of-the-box Cisco APs typically have SNMP disabled and a blank username and password combination for HTTP and Telnet. Cisco supports multiple community strings per AP. |
| Auth Password (Confirm) | | | |

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

| Setting | Default | AP Type | Description |
|--|--|---|---|
| Privacy Password (Confirm) | Taken from the Device Setup > Communication page | Enterasys R2 | This is the SNMPv3 privacy password. |
| SNMPv3 Auth Protocol | Taken from the Device Setup > Communication page | Cisco VxWorks | Drop-down menu allows you to set the SNMPv3 protocol to be supported by the device being added. |
| Telnet/SSH Username & Password (Confirm) | 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. |

- In the **Location** field, select the appropriate group and folder for the AP. Refer to [Table 80](#).

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

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

- At the bottom of the page, select either the **Monitor Only + Firmware Upgrades** or **Management read/write** radio button. The choice depends on whether or not you wish to overwrite the **Group** settings for the device being added.



NOTE

If you select **Manage read/write**, OV3600 overwrites existing device settings with the **Group** settings. Alcatel-Lucent recommends placing newly discovered devices in **Monitor read/only** mode to enable auditing of actual settings instead of Group Policy settings

- Click **Add** to finish adding the devices to the network.
- The device is now visible on the **APs/Devices > New** page.

Adding Access Points, Routers and Switches with a CSV File

Adding routers and switches to OV3600 as managed devices allows OV3600 to perform the following functions:

- Leverage CDP to discover new access points in a more efficient manner.
- Read the ARP table to correlate MAC addresses of client devices and rogue APs to IP addresses on your network.
- Read the bridge forwarding tables to discover rogue APs.

OV3600 needs **read-only** access to a router or switch for all subnets that contain devices. As each router or switch is added to OV3600, 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 CSV list must contain the following columns:

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

Table 81 illustrates these requirements in a hypothetical configuration.

Table 81 Sample Configuration of Adding Access Points, Routers and Switches with a CSV File

| Item | Example |
|--------------------------|---------------------|
| 1. IP Address | 10.34.64.163 |
| 2. SNMP Community String | private |
| 3. Name | switch1.example.com |
| 4. Type | Router/Switch |
| 5. Auth Password | nonradiance |
| 6. SNMPv3 Auth Protocol | md5 |
| 7. Privacy Password | privacy |
| 8. SNMPv3 Username | sv3user |
| 9. Telnet Username | telnetuser |
| 10. Telnet Password | telnetpwd |
| 11. Enable Password | enable |
| 12. SNMP Port | 161 |

1. To import a CSV file, navigate to the **Device Setup > Add** page.

2. Click **Import Devices via CSV**. The **CSV Upload** page displays, as illustrated in [Figure 72](#).

Figure 72 *Device Setup > Add > Import Devices via CSV Page Illustration*

Upload a list of devices

Location

Group: new group (SSID: -) ▼

Folder: Top ▼

The list must be in comma-separated values (CSV) format, containing the following columns:

1. IP Address
2. SNMP Community String
3. Name
4. Type
5. Auth Password
6. SNMPv3 Auth Protocol
7. Privacy Password
8. SNMPv3 Privacy Protocol
9. SNMPv3 Username
10. Telnet Username
11. Telnet Password
12. Enable Password
13. SNMP Port

IP Address is required, the others are optional.
Type is a case-insensitive string; you can [view a list of device types](#).

[Download a sample file](#) or see the example below:

```
IP Address,SNMP Community String,Name,Type,Auth Password,SNMPv3 Auth Protocol,  
10.34.64.168,private,switch1.example.com,Router/Switch,nonradiance,md5,privacy123,  
10.172.97.172,private,switch2.example.com,router/switch,nonradiance,sha,privacy123,  
10.70.36.172,public,Cisco-WLC-4012-3,Cisco 4000 WLC,  
10.46.111.48,,
```

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

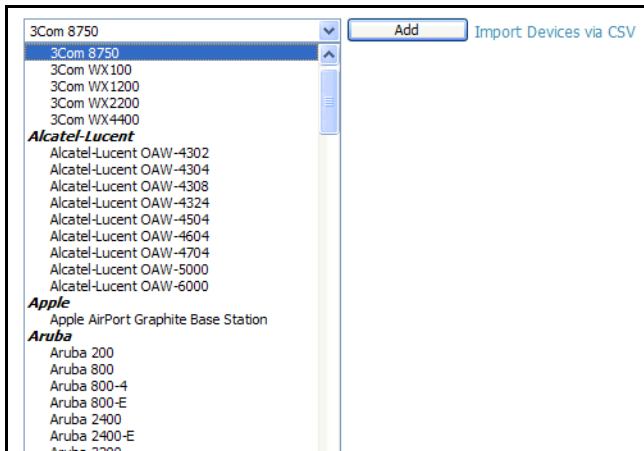
Adding Universal Devices

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.

Figure 73 Device Setup > Add Page Illustration



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

OV3600 collects basic information about universal devices, including name, contact, uptime and location. Once you have added a universal device, you can view a list of the device's interfaces on the **APs/Devices > Manage** page.

By clicking the **pencil** icon next to an interface, you can assign it to be non-monitored or 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 Device Groups in OV3600](#)” on page 73. 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, the related controller, when known, and the device manufacturer, model, MAC Address, IP Address, and the date/time of discovery. [Figure 74](#) illustrates this page.

Figure 74 APs/Devices > New

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

1-35 of 35 APs/Devices Page 1 of 1 Choose Columns

| Device | Controller | Type | IP Address | LAN MAC Address | Discovered |
|--|---------------------|--------------------------|-------------|-------------------|---------------------|
| <input type="checkbox"/> Intel PRO/Wireless LAN | - | Intel 2011B | 10.51.1.60 | 00:03:47:15:EA:53 | 11/2/2009 12:08 PM |
| <input type="checkbox"/> R014-00861 | - | Colubris CN3200 | 10.51.1.105 | 00:03:52:01:63:9C | 11/2/2009 12:07 PM |
| <input type="checkbox"/> RADIO4 | RFS7000 | Symbol AP 100 | - | 00:A0:F8:56:8B:40 | 10/30/2009 1:06 PM |
| <input type="checkbox"/> AP0014.6940.8f22 | Cisco_40:7c:83 | Cisco Aironet 1240 LWAPP | 10.51.1.94 | 00:14:69:40:8F:22 | 10/29/2009 9:20 AM |
| <input type="checkbox"/> 00:24:6c:c0:80:0f | Aruba3600-US | Intel 2011B | 10.51.1.214 | 00:24:6C:C0:80:0F | 10/29/2009 9:07 AM |
| <input type="checkbox"/> AP1 | Cisco_40:7c:83 | Cisco Aironet 1250 LWAPP | 10.51.1.98 | 00:1D:45:91:14:1A | 10/16/2009 4:15 PM |
| <input type="checkbox"/> AP-2 | meru | Meru AP 150 | - | 00:0C:E6:00:DF:B6 | 10/13/2009 11:17 AM |
| <input type="checkbox"/> AP-8 | meru | Meru AP 201 | - | 00:12:F2:39:5D:A7 | 10/13/2009 11:17 AM |
| <input type="checkbox"/> AP-3 | meru | Intel 2011B | - | 00:0C:E6:03:33:65 | 10/13/2009 11:17 AM |
| <input type="checkbox"/> AP-7 | meru | Meru AP 201 | - | 00:12:F2:39:57:AF | 10/13/2009 11:17 AM |
| <input type="checkbox"/> AP-4 | meru | Meru AP 100 | - | 00:0C:E6:00:08:0D | 10/13/2009 11:17 AM |
| <input type="checkbox"/> RADIO8 | RFS7000 | Symbol AP 100 | - | 00:A0:F8:56:8A:CD | 10/12/2009 9:52 AM |
| <input type="checkbox"/> AP-5 | meru | Meru AP 320 | - | 00:0C:E6:05:01:6A | 10/10/2009 12:07 PM |
| <input type="checkbox"/> AP 124 - Trouble with capital T | Aruba2400 | Alcatel-Lucent AP | 10.51.5.17 | 00:1A:1E:C0:2B:34 | 10/9/2009 9:47 AM |
| <input type="checkbox"/> Radio envy | Aruba2400 | Intel 2011B | 10.51.3.250 | 00:08:86:C7:07:EF | 10/9/2009 9:47 AM |
| <input type="checkbox"/> 00:1a:1e:c6:d5:d2 | Aruba800-FIPS | Alcatel-Lucent AP | 10.51.1.232 | 00:1A:1E:C6:D5:D2 | 10/9/2009 9:46 AM |
| <input type="checkbox"/> mesh-portal-c2:2e:4a | Aruba2400 | Aruba AP 65 | 10.51.4.211 | 00:1A:1E:C2:2E:4A | 10/9/2009 9:46 AM |
| <input type="checkbox"/> Alcatel Lucent | - | Aruba Controller | 10.51.5.31 | - | 10/9/2009 9:45 AM |
| <input type="checkbox"/> 00:1a:1e:c0:55:46 | Aruba200 | Intel 2011B | 10.51.5.44 | 00:1A:1E:C0:55:46 | 10/9/2009 9:45 AM |
| <input type="checkbox"/> 00:1a:1e:c0:2b:3e | Alcatel-Lucent-4308 | Alcatel-Lucent AP 124 | 10.51.1.248 | 00:1A:1E:C0:2B:3E | 10/9/2009 9:45 AM |
| <input type="checkbox"/> AP1 | Cisco_40:7c:83 | Cisco Aironet 1250 LWAPP | 10.51.1.247 | 00:1D:45:91:14:42 | 10/9/2009 9:45 AM |
| <input type="checkbox"/> AP0022.bd19.5f2b | Cisco_40:7c:83 | Cisco Aironet 1140 LWAPP | 10.51.1.142 | 00:22:BD:19:5F:2B | 10/9/2009 9:45 AM |
| <input type="checkbox"/> AP0018.19bd.a082 | Cisco_40:7c:83 | Cisco Aironet 1200 LWAPP | 10.51.4.3 | 00:18:19:BD:A0:82 | 10/9/2009 9:45 AM |
| <input type="checkbox"/> Talisker | Aruba200 | Alcatel-Lucent AP | 10.51.9.106 | 00:1A:1E:C6:D5:C2 | 10/9/2009 9:44 AM |
| <input type="checkbox"/> Talisker | Aruba200 | Aruba AP 105 | 10.51.9.105 | 00:24:6C:C0:00:F6 | 10/9/2009 9:44 AM |
| <input type="checkbox"/> ap-Not set | Aruba-800-2X | Alcatel-Lucent AP | 10.51.6.95 | 00:08:86:C7:9D:36 | 10/9/2009 9:43 AM |
| <input type="checkbox"/> ap-Not set | Aruba-800-2X | Aruba AP 70 | 10.51.1.252 | 00:08:86:CE:E1:8C | 10/9/2009 9:43 AM |
| <input type="checkbox"/> ap-Not set | Aruba-800-2X | Alcatel-Lucent AP | 10.51.8.114 | 00:08:86:C0:99:BC | 10/9/2009 9:43 AM |
| <input type="checkbox"/> ap-1.1.1 | Aruba-800-2X | Aruba AP 65 | 10.51.5.2 | 00:1A:1E:C2:2E:F0 | 10/9/2009 9:43 AM |
| <input type="checkbox"/> ap:78 | Aruba3600-Local | Alcatel-Lucent AP | 10.51.5.18 | 00:1A:1E:C0:50:78 | 10/9/2009 9:43 AM |
| <input type="checkbox"/> 3600 AP124 | Aruba3600-Local | Aruba AP 124 | 10.51.5.19 | 00:1A:1E:C0:00:EC | 10/9/2009 9:43 AM |
| <input type="checkbox"/> Alcatel-Lucent AP | - | Aruba Controller | 10.51.5.117 | - | 10/9/2009 9:43 AM |
| <input type="checkbox"/> RADIO 4_4 | WS2000_Controller | Symbol AP 100 | - | 00:A0:F8:56:8A:7D | 10/9/2009 9:43 AM |
| <input type="checkbox"/> brand new shiny name | Aruba-3400 | Alcatel-Lucent AP | 10.51.5.7 | 00:1A:1E:C2:2E:AE | 10/9/2009 9:42 AM |
| <input type="checkbox"/> 00:1a:1e:c0:1a:dc | Aruba-3400 | Aruba AP 125 | 10.51.1.215 | 00:1A:1E:C0:1A:DC | 10/9/2009 9:42 AM |

1-35 of 35 APs/Devices Page 1 of 1

Select All - Unselect All

View Ignored Devices

Group: Access Points (SSID: alcatel-lucent-ap)

Folder: Top

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.

5. 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 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, as verified by that device appearing in the group to which it has been added. Perform the following steps:

1. Browse to the **APs/Devices > List** page, which lists all devices that are managed or monitored by OV3600. Using the drop-down menu at the top of the **Activity Area**, you can determine whether to view all devices or only the devices from a specified Group. [Figure 75](#) illustrates this page.

Figure 75 APs/Devices > List (Partial Split View Accounts for Horizontal Scrolling)

Folder: **Top (38 Devices)** Expand folders to show all APs/Devices Go to folder: **Top (38 Devices)**

Total Devices: 38 Up: 34 Down: 4 Mismatched: 32 Users: 0 Avg/Device: 0 Bandwidth: 0 kbps

Users for folder Top Last 2 hours

Show All Maximum Average
 Max Users 1 user 0.5 users

Bandwidth for folder Top Last 2 hours

Show All Maximum Average
 Avg Bits Per Second In 30 kbps 11 kbps
 Avg Bits Per Second Out 29.9 kbps 11 kbps

1 year ago now

Modify Devices

1-10 of 38 APs/Devices Page 1 of 4 >> | Choose Columns

| Device | Status | Upstream Device | APs | Users | BW (kbps) | Uptime | Configuration | Group | Controller | SSID | First R |
|---------------------|--------|-----------------|-----|-------|-----------|-------------------------|---------------|---------------|------------|------|---------|
| (id: 9) | Up | - | 0 | 0 | 0 | 131 days 23 hrs 22 mins | Good | Access Points | - | - | - |
| 3Com Access Point | Down | - | - | 0 | 0 | - | Unknown | Access Points | - | - | - |
| AaaS Test Customer | Down | - | 0 | 0 | 0 | - | Good | Access Points | - | - | - |
| ag-2100 | Up | - | - | 0 | 0 | 2 days 2 hrs 58 mins | Verifying | Access Points | - | - | 802.11 |
| Alcatel-Lucent-4308 | Up | - | 0 | 0 | 0 | 10 days 19 hrs 51 mins | Good | Access Points | - | - | - |
| ap | Up | - | - | 0 | 0 | 74 days 21 hrs 46 mins | Verifying | Access Points | - | - | 802.11 |
| AP340-425e23 | Down | - | - | 0 | 0 | - | Good | Access Points | - | - | - |
| ap-Cisco3 | Up | - | - | 0 | 0 | 97 days 1 hr 33 mins | Verifying | Access Points | - | - | 802.11 |
| Aruba200 | Up | - | 0 | 0 | 0 | 15 days 4 hrs 10 mins | Good | Access Points | - | - | - |
| Aruba200 | Up | - | 0 | 0 | 0 | 3 days 23 hrs 42 mins | Verifying | Access Points | - | - | - |

1-10 of 38 APs/Devices Page 1 of 4 >> |

Select All - Unselect All

Set Group: - Select Folder - Move

Move to Alcatel-Lucent AP Group: - Alcatel-Lucent AP Group - Move

Update Cisco Thin AP Settings: Update

Update the credentials OV3600 uses to communicate with these devices: Update

Audit selected devices: Audit

Import settings of selected devices: Import Settings

Ignore selected devices: Ignore

Change management level of selected devices: Management Mode

Modify Radio Status: Enable/Disable

Reboot selected devices: Reboot

Reprovision selected Alcatel-Lucent devices: Reprovision

Upgrade firmware for selected devices: Upgrade Firmware

Cancel firmware upgrade for selected devices: Cancel Upgrade

Optimize channel assignment to reduce overlap: Optimize

Delete selected devices: Delete

Alert Summary at 11/2/2009 2:46 PM

| Type | Last 2 Hours | Last Day | Total | Last Event |
|------------------------------|--------------|----------|-------|------------|
| IDS Events | 0 | 0 | 0 | - |
| Incidents | 0 | 0 | 0 | - |
| OV3600 Alerts | 0 | 0 | 0 | - |
| RADIUS Authentication Issues | 0 | 0 | 0 | - |

Add New Folder

2. 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** will change to **Up** when verification is complete.

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

3. Navigate to the **Alert Summary** section of the **APs/Devices > List** page. The **Alert Summary** section cites the number of events that have occurred in the last two hours, the last 24 hours, and total. There are four categories of alerts as follows:
 - OV3600 Alerts
 - IDS Events
 - Incidents
 - RADIUS Authentication Issues



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

Figure 76 *APs/Devices > List > Alert Summary Section Illustration*

| Type ▲ | Last 2 Hours | Last Day | Total | Last Event |
|------------------------------|--------------|----------|-------|--------------------|
| AMP Alerts | 0 | 0 | 0 | - |
| IDS Events | 11 | 387 | 704 | 3/4/2009 10:30 AM |
| Incidents | 0 | 0 | 2 | 2/27/2009 12:18 PM |
| RADIUS Authentication Issues | 10 | 79 | 274 | 3/4/2009 10:28 AM |



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

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

4. You may view details and incidents by clicking the specific **Alert Type**. The alert types and detailed information available for each are as follows:
 - **OV3600 Alerts**—Clicking this link takes you to the **OV3600 Alerts Summary** page, which cites detailed information for the current OV3600 Alerts. [Figure 77](#) illustrates this page.

Figure 77 APs/Devices > List > OV3600 Alerts

Summary
 OV3600 Alerts for devices in folder [Top](#) and subfolders | [Return to APs/Devices list](#)

| Alert Type ▲ | Last 2 Hours | Last 24 Hours | Total |
|---|--------------|---------------|-------|
| Configuration Mismatch All device types | 0 | 0 | 13 |
| Device Down All device types | 5 | 58 | 182 |
| 2 Alert Types | 5 | 58 | 195 |

1-20 ▼ of 195 Alerts Page 1 ▼ of 10 > > |

| <input type="checkbox"/> | Trigger Type | Trigger Summary | Triggering Agent | Severity | Time ▼ |
|--------------------------|--------------|--|------------------|----------|-------------------|
| <input type="checkbox"/> | Device Down | All device types | MXR-2-314644 | Major | 5/15/2009 9:14 AM |
| <input type="checkbox"/> | Device Down | All device types | MXR-2-314644 | Major | 5/15/2009 9:11 AM |
| <input type="checkbox"/> | Device Down | All device types | MXR-2-314644 | Major | 5/15/2009 9:06 AM |
| <input type="checkbox"/> | Device Down | All device types | MXR-2-314644 | Major | 5/15/2009 8:59 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 8:20 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 7:50 AM |
| <input type="checkbox"/> | Device Down | All device types | MXR-2-314644 | Major | 5/15/2009 7:25 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 7:14 AM |
| <input type="checkbox"/> | Device Down | All device types | MXR-2-314644 | Major | 5/15/2009 7:00 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 5:54 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 5:38 AM |
| <input type="checkbox"/> | Device Down | Device uptime indicates that device has rebooted | MXR-2-314644 | Major | 5/15/2009 5:20 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 5:12 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 4:42 AM |
| <input type="checkbox"/> | Device Down | All device types | MXR-2-314644 | Major | 5/15/2009 4:35 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 4:27 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 4:11 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 3:46 AM |
| <input type="checkbox"/> | Device Down | All device types | MXR-2-314644 | Major | 5/15/2009 3:15 AM |
| <input type="checkbox"/> | Device Down | All device types | Unnamed | Major | 5/15/2009 2:44 AM |

Select All - Unselect All

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

Figure 78 APs/Devices > List, Alert Summary, IDS Events Summary Page Illustration

Summary
 IDS Events for devices in folder [Top](#) > [HQ](#) | [Return to APs/Devices list](#)

| Attack ▲ | Last 2 Hours | Last 24 Hours | Total |
|---------------------|--------------|---------------|-------|
| Deauth-Broadcast | 0 | 29 | 29 |
| Netstumbler Generic | 0 | 280 | 530 |
| Null-Probe-Response | 7 | 80 | 147 |
| 3 Attack Types | 7 | 389 | 706 |

1-20 ▼ of 706 IDS Events Page 1 ▼ of 36 > > |

| <input type="checkbox"/> | Attack | Attacker | AP | Radio | Controller | Channel | SNR | Precedence | Time ▼ |
|--------------------------|------------------|-------------------|-----------------|-----------|------------------|---------|-----|------------|------------------|
| <input type="checkbox"/> | Deauth-Broadcast | 00:0C:46:68:3A:2A | Facilities-AL37 | 802.11bgn | ethersphere-lms4 | - | 12 | - | 3/4/2009 8:29 AM |
| <input type="checkbox"/> | Deauth-Broadcast | 00:0C:46:68:3A:2A | AP 1 | 802.11bg | ethersphere-lms4 | - | 37 | - | 3/4/2009 8:29 AM |
| <input type="checkbox"/> | Deauth-Broadcast | 00:0C:46:68:3A:2A | AP 2 | 802.11bg | ethersphere-lms4 | - | 37 | - | 3/4/2009 8:29 AM |
| <input type="checkbox"/> | Deauth-Broadcast | 00:0C:46:68:3A:2A | AP 3 | 802.11bg | ethersphere-lms4 | - | 47 | - | 3/4/2009 8:29 AM |

Select All - Unselect All

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



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

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

Figure 79 APs/Devices > List, Alert Summary, Incidents Summary

| State | Last 2 Hours | Last Day | Total |
|--------|--------------|----------|-------|
| Open | 0 | 0 | 2 |
| Closed | 0 | 0 | 0 |
| Total | 0 | 0 | 2 |

New Incident

1-2 of 2 Incidents Page 1 of 1

| | ID | Summary | State | Opened By | Related | Created | Updated |
|--------------------------|-----|------------------------------|-------|-----------|---------|--------------------|--------------------|
| <input type="checkbox"/> | 156 | Bryan's connection problems | Open | mbruno | 2 | 2/27/2009 12:18 PM | 2/27/2009 12:19 PM |
| <input type="checkbox"/> | 146 | Katie's connectivity problem | Open | mbruno | 3 | 2/12/2009 11:48 AM | 2/12/2009 11:49 AM |

Select All - Unselect All

- **RADIUS Authentication Issues**—Clicking this link takes you to the related **Summary** page, to include groupings of RADIUS Authentication issues by type, and all such issues listed in chronological sequence and by folder. [Figure 80](#) illustrates this page.

Figure 80 RADIUS Authentication Issues Summary

Summary

RADIUS Authentication Issues for devices in folder [Top > HQ](#) | [Return to APs/Devices list](#)

| Event Type | Last 2 Hours | Last 24 Hours | Total |
|--|--------------|---------------|-------|
| Authentication server request timed out for aruba-supersvr | 1 | 3 | 9 |
| Authentication server request timed out for vortex | 2 | 8 | 23 |
| Client authentication failed | 11 | 64 | 249 |
| 3 RADIUS Authentication Issue Event Types | 14 | 75 | 281 |

1-20 of 281 RADIUS Authentication Issues Page 1 of 14 > >|

| Event | Username | User MAC Address | AP | Radio | Controller | RADIUS Server | Time |
|---|----------|-------------------|----|-------|------------------|---------------|-------------------|
| <input type="checkbox"/> Client authentication failed for 00:1F:3B:00:1F:3B | - | 00:1F:3B:00:1F:3B | - | - | ethersphere-lms4 | - | 3/4/2009 12:19 PM |
| <input type="checkbox"/> Client authentication failed for 00:1F:3B:00:1F:3B | - | 00:1F:3B:00:1F:3B | - | - | ethersphere-lms4 | - | 3/4/2009 12:19 PM |
| <input type="checkbox"/> Client authentication failed for 00:1F:3B:00:1F:3B | - | 00:1F:3B:00:1F:3B | - | - | ethersphere-lms4 | - | 3/4/2009 12:17 PM |
| <input type="checkbox"/> Client authentication failed for 00:21:5C:00:21:5C | - | 00:21:5C:00:21:5C | - | - | ethersphere-lms4 | - | 3/4/2009 7:26 AM |

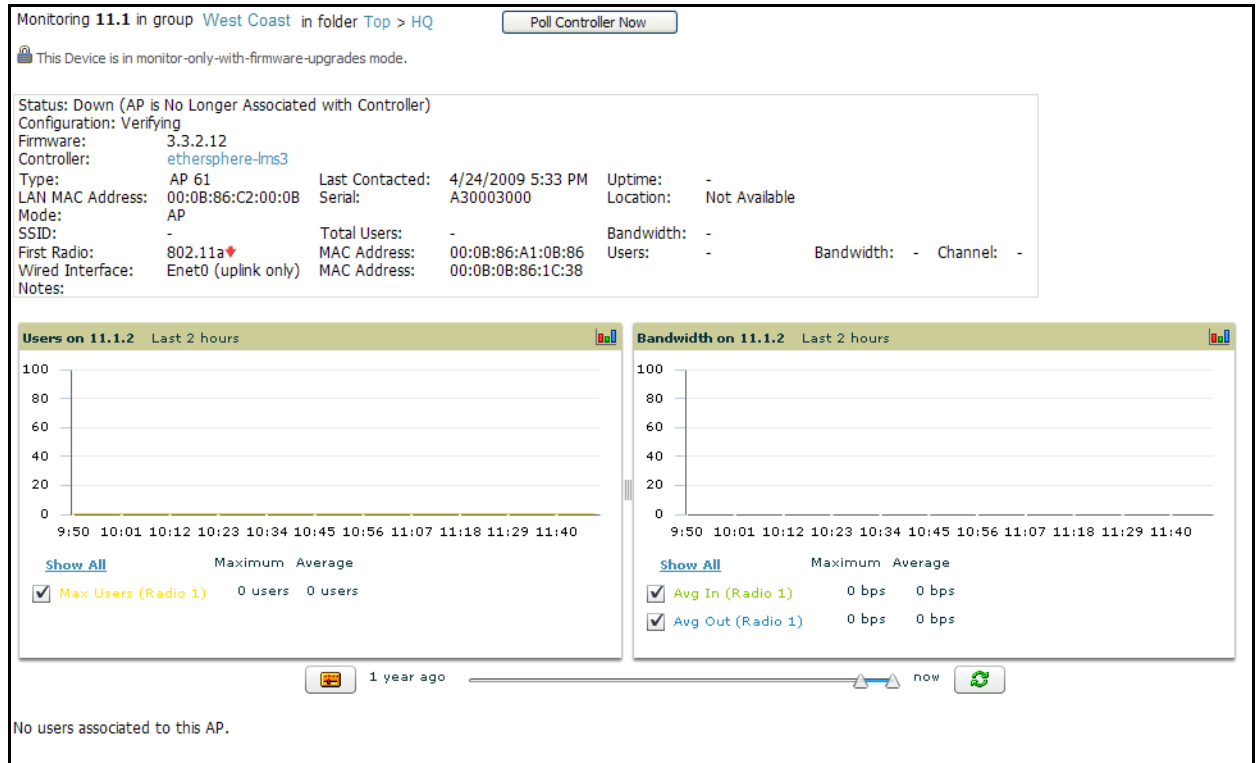
Select All - Unselect All

Troubleshooting a Newly Discovered Device with Down Status

If the device status on the **APs/Devices > List** page remains **Down** after it has been added to a group, the most likely source of the problem is an error in the SNMP community string being used to manage the device. Perform the following steps to troubleshoot this scenario.

1. Click the **Name** of the down device in the list of devices on the **APs/Devices > List** page. This automatically directs you to the **APs/Device > Monitor** page for that device, illustrated in [Figure 81](#):

Figure 81 *APs/Devices > Monitor Page Illustration for a Down Device*



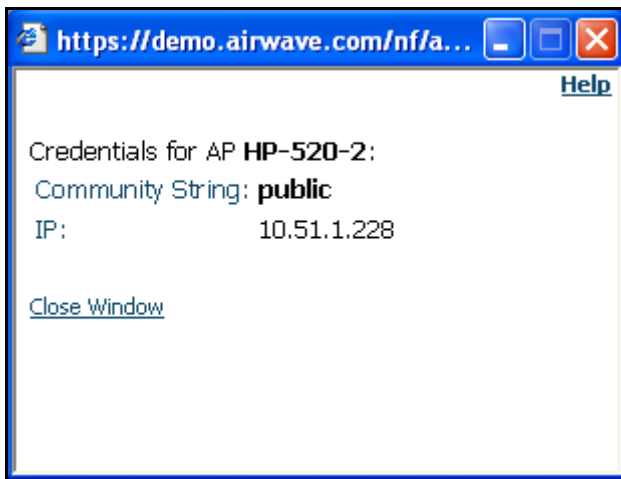
2. Locate the **Status** section. If the Status is **Down**, there is an onscreen error message indicating the cause of the problem. Some of the common system messages are as follows in [Table 82](#):

Table 82 *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. If visible, click the **View device credentials** link in the **Device Communications** area. This displays the credentials OV3600 is using unsuccessfully to communicate with the device. This link can be removed from the OV3600 for security reasons by setting a flag in OV3600. Only users with root access to the OV3600 command line can show or hide this link. If you are interested in disabling this feature, please contact Alcatel-Lucent Support. [Figure 82](#) illustrates this page.

Figure 82 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 83](#) illustrates this page.

Figure 83 APs/Devices > Manage > Device Communication Section Illustration

A screenshot of the "Device Communication" configuration page. The page has a title bar "Device Communication" and a subtitle "If this device is down because its IP address or management ports have changed, update the fields below with the correct information." Below this are input fields for "IP Address:" (10.5.5.5) and "SNMP Port:" (161). Another subtitle reads "If this device is down because the credentials on the device have changed, update the fields below with the correct information." Below this is a dropdown menu for "SNMP version" set to "2c". The form includes several password fields: "Community String:", "Confirm Community String:", "SNMPv3 Username:", "Auth Password:", "Confirm Auth Password:", "Privacy Password:", "Confirm Privacy Password:", "Telnet/SSH Username:" (admin), "Telnet/SSH Password:", "Confirm Telnet/SSH Password:", "'enable' Password:", and "Confirm 'enable' Password:". A dropdown menu for "SNMPv3 Auth Protocol:" is set to "SHA-1".

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



After upgrade to OV3600 version 6.4, the **APs/Devices > Audit** page, and certain additional pages, show only **Mismatched** status by default for non-template devices.

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

Figure 84 illustrates this page.

Figure 84 **APs/Devices > Audit** Page Illustration

Device Configuration of **ServerRoom-AL39** in group **Arba HQ** in folder **Top > HQ**
This Device is in monitor-only-with-firmware-upgrades mode.
Configuration read from device at 5/18/2009 2:26 PM

Configuration: Mismatched

Audit the device's current configuration.

[Show Archived Device Configuration](#)

Choose settings to ignore during configuration audits.

[Show entire config](#)

[Refresh this page](#)

| AP Settings | | |
|-------------------|------------------------------|-----------------------|
| | Current Device Configuration | Desired Configuration |
| Mesh Role | None | Mesh AP |
| Name | AL39 | ServerRoom-AL39 |
| System Properties | | |
| | Current Device Configuration | Desired Configuration |
| Location | (not set) | Not Available |

6. Review the list of changes to be applied to the device to determine whether the changes are appropriate. If not, you need to change the Group settings or reassign the device to another Group.
 - 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. Navigate to the **APs/Devices > List** page and click the **wrench** icon next to the name of the AP to be shifted from **Monitor Only** mode to **Manage Read/Write** mode. This directs you to the **APs/Devices > Manage** page.
2. Locate the **General** area. [Figure 85](#) illustrates this page.

Figure 85 *APs/Devices > Manage > General Section Illustration*

| General | |
|------------------|--|
| Name: | symbol-3021-1 |
| Status: | Up (OK) |
| Configuration: | Good (Ignoring mismatches) |
| Last Contacted: | 5/19/2009 12:21 PM |
| Type: | Symbol 3021 |
| Firmware: | 04.02-19 |
| Group: | HQ |
| Folder: | Top > HQ |
| Management Mode: | <input type="radio"/> Monitor Only + Firmware Upgrades <input checked="" 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 **Save and Apply** to retain these settings and to push configuration to the device.
 - Click **Revert** to cancel out of changes and return to the last saved changes.
 - Click **Delete** to remove this configuration from the device.
 - Click **Ignore** to disregard configuration changes from this page but otherwise retain pre-existing device configurations.
 - Click **Import Settings** to add new configuration settings from another location.
 - Click **Replace Hardware** to replace this device on the network but to retain configuration changes.

5. OV3600 presents a confirmation screen reminding you of all configuration changes that will be applied to the device in **Manage** mode.
6. Click **Confirm Edit** to apply the changes to the device immediately, click **Schedule** to schedule the changes to occur during a specific maintenance window, or click **Cancel** to return to the **APs/Devices > Manage** page.
7. Some device configuration changes may require the device to reboot. Use the **Schedule** function to schedule these changes to occur at a time when WLAN users will not be affected.
8. To move multiple devices into managed mode at once, use the **Modify these devices** link. Refer to [“Modifying Multiple Devices” on page 115](#) for more information.

Configuring Individual Device Settings

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

- [“Overview of Individual Device Configuration” on page 145](#)
- [“Configuring AP Settings” on page 145](#)

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 RF interference between two or more devices.



Any changes made at an individual device level will automatically override Group level settings.

OV3600 automatically saves the last 10 device configurations for reference and compliance purposes. Archived device configurations are linked on the **APs/Devices > Audit** page and identified by name. By default, configuration is tracked by the date and time it was created; devices are also archived by date.

On the **APs/Devices > Audit** page, 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 **APs/Devices > Audit** page. This applies to startup or to running configuration files.

Compare two configurations to highlight the specific lines that are mismatched. The Audit page provides links to the OV3600 pages where any mismatched settings can be configured.

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 for that device.

2. Click the **APs/Devices > Manage** tab and locate the **Settings** area. [Figure 86](#) illustrates this page.

Figure 86 *APs/Devices > Manage Page Illustration*

The screenshot displays the configuration page for an access point (ag-2100). It is divided into several sections:

- General:** Name: ag-2100, Status: Up (OK), Configuration: Error (No matching template could be found for this device. See the templates page.), Last Contacted: 11/2/2009 3:59 PM, Type: Nomadix AG-2100, Firmware: 11.4.138, Group: Access Points, Template: Add a Template, Folder: Top, Management Mode: Monitor Only, Manage Read/Write.
- Settings:** Name: ag-2100, Location: Dev Lab, Sunnyvale, CA, Contact: Dev Team, Latitude: [empty], Longitude: [empty], Altitude (m): [empty], Group: Access Points (SSID: alcatel-lucent-ap), Folder: Top, Auto Detect Upstream Device: Yes, No, Upstream device will automatically be updated when the device is polled. Automatically clear Down Status Message when device comes back up: Yes, No, Down Status Message: [empty].
- Notes:** [empty text area].
- Device Communication:** View Device Credentials, If this device is down because its IP address or management ports have changed, update the fields below with the correct information. IP Address: 10.51.3.93, SNMP Port: 161, Telnet Port: 23. 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: [masked], Confirm Community String: [masked], Telnet/FTP Username: admin, Telnet/FTP Password: [masked], Confirm Telnet/FTP Password: [masked].
- 802.11bg Radio:** Radio Enabled: Yes, No, Transmit Power: Full, Channel: 11.
- Network Settings:** Use DHCP: Yes, No, LAN IP Address: 10.51.3.93, Subnet Mask: 255.255.0.0, Gateway: 10.51.0.1.
- Template Options:** Extra Device Commands #1: This text will replace the %ap_include_1% variable. [empty text area]. ap_include_2: [empty], ap_include_3: [empty], ap_include_4: [empty], ap_include_5: [empty], ap_include_6: [empty], ap_include_7: [empty], ap_include_8: [empty], ap_include_9: [empty], ap_include_10: [empty].

Buttons at the bottom: Save and Apply, Revert, Delete, Ignore, Import Settings, 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 83](#) describes the fields, information, and settings.

Table 83 *APs/Devices > Manage > General Fields and Default Values*

| Message | Meaning |
|------------------------|--|
| Name | Displays the name currently set on the device. |
| Status | Displays the current status of an AP. If an AP is Up , then OV3600 is able to ping it and fetch SNMP information from the AP. If the AP is listed Down then OV3600 is either unable to ping the AP or unable to read the necessary SNMP information from the device. |
| Configuration | Displays the current configuration status of the AP. To update the status, click Audit on the APs/Devices > Audit page. |
| Last Contacted | Displays the last time OV3600 successfully contacted the AP. |
| Type | Displays the type of AP. |
| Firmware | Displays the version of firmware running on the AP. |
| Group | Links to the Group > Monitoring page for the AP. |
| Template | Displays the name of the group template currently configuring the AP. Also displays a link to the Groups > Template page. This is only visible for APs that are being managed 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 to describe device information. |

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 84](#) describes field settings, default values, and information for the **Sections** area of this page.

Table 84 *APs/Devices > Manage > Settings Fields and Default Values*

| Setting | Default | Device Type | Description |
|---------------|---------|-------------|--|
| Name | None | All | User-configurable name for the device (max. 20 characters) |
| Domain | None | IOS | Field is populated upon initial device discovery or rereading settings. Enable this option from OV3600 Setup > Network page to display this field on the APs/Devices > Manage page, with fully-qualified domain names for IOS APs. This field is used in conjunction with Domain variable in IOS templates. |

Table 84 APs/Devices > Manage > Settings Fields and Default Values (Continued)

| Setting | Default | Device Type | Description |
|------------------------------------|----------------------|-------------|--|
| Location | Read from the device | All | The SNMP location set on the device. |
| Latitude | None | All | Text field for entering the latitude of the device. The latitude is used with the Google earth integration. |
| Longitude | None | All | Text field for entering the longitude of the device. The longitude is used with the Google earth integration. |
| Altitude (meters) | None | All | Text field for entering the altitude of the device when known. This setting is used with the Google earth integration. Specify altitude in meters. |
| Group | Default Group | All | Drop-down menu that can be used to assign the device to another Group. |
| Folder | Top | All | Drop-down menu that can be used to assign the device to another Group. |
| Auto Detect Upstream Device | Yes | All | Selecting Yes enables automatic detection of upstream device, which is automatically updated when the device is polled. Selecting No displays a drop-down menu of upstream devices. |
| Down Status Message | None | All | Enter a text message that provides information to be conveyed if the device goes down. |
| Administrative Status | Enable | All | Enables or disables administrative mode for the device. |
| Mode | Local | All | Designates the mode in which the device should operate. Options include the following: <ul style="list-style-type: none"> • Local • H-REAP • Monitor • Rogue Detector • Sniffer |

5. Complete additional settings on the **APs/Devices > Manage** page, to include H-REAP, certificates, radio settings, and network settings. [Table 85](#) describes many of the possible fields.

Table 85 APs/Devices > Manage Page Illustration, Additional Settings

| Setting | Default | Device Type | Description |
|--------------------------|--------------|--------------|--|
| Mesh Role: | Mesh AP | Mesh Devices | Drop-down menu specifies the mesh role for the AP. 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. |

Table 85 APs/Devices > Manage Page Illustration, Additional Settings

| Setting | Default | Device Type | Description |
|---|----------------------|---------------------------|---|
| 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. |
| Downlink Modulation | bpsk-1-2 | WiMAX Subscriber Stations | Drop-down menu that defines the downlink modulation type for the subscriber station. |
| VLAN Mode | Inherit | WiMAX Subscriber Stations | Drop-down menu that defines the VLAN mode of the AP. Inherit - The AP will inherit the VLAN settings from the subscriber class. Transparent - Tagged and untagged traffic is passed along unless blocked by a PIR restriction. |
| Receive Antenna | Diversity | Cisco | Drop-down menu for the receive antenna provides three options: Diversity — Device will use the antenna that receives the best signal. If the device has two fixed (non-removable) antennas, the Diversity setting should be used for both receive and transmit antennas. Right — If your device has removable antennas and you install a high-gain antenna on the device's right connector (the connector on the right side when viewing the back panel of the device), use this setting for both receive and transmit. Left — If your device has removable antennas and you install a high-gain antenna on the device's left connector, use this setting for both receive and transmit. |
| Transmit Antenna | Diversity | Cisco | See description in Receive Antenna above. |
| Antenna Diversity | Primary Only | Intel 2011, Symbol 4131 | Drop-down menu provides the following options: Full Diversity — The AP receives information on the antenna with the best signal strength and quality. The AP transmits on the antenna from which it last received information. Primary Only — The AP transmits and receives on the primary antenna only. Secondary Only : The AP transmits and receives on the secondary antenna only. Rx Diversity — The AP receives information on the antenna with the best signal strength and quality. The AP transmits information on the primary antenna only. |
| Transmit Power Reduction | 0 | Proxim | Transmit Power Reduction determines the APs transmit power. The max transmit power is reduced by the number of decibels specified. |
| 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. |

Table 85 APs/Devices > Manage Page Illustration, Additional Settings

| Setting | Default | Device Type | Description |
|-------------------------------|---|--|--|
| Neighboring APs | Blank | All | Represents top five contiguous access points calculated by summing the number of roams to and from the access point and the access point of focus. Contiguous APs should be set to different channels to minimize "crosstalk," which occurs when the signals from APs overlap and interfere with each other. This RF interference negatively influences WLAN performance. |
| Transmit Power Level | Highest power level supported by the radio in the regulatory domain (country) | Cisco, Colubris, Intel, Symbol, Proxim AP-600, AP-700, AP-2000 (802.11g) | Determines the power level of radio transmission. Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device. You can increase the coverage RADIUS of the access point, by increasing the Transmit Power Level. However, while this increases the zone of coverage, it also makes it more likely that the AP will interfere with neighboring APs. Supported values are: Cisco (100mW, 50mW, 30mW, 20mW, 5mW, 1mW) Intel/Symbol (Full or 50mW, 30mW, 15mW, 5mW, 1mW) Colubris (High or 23 dBm, Med. or 17 dBm, Low or 13 dBm) |
| Distance Between APs | Large | Colubris | Determines how far a user can roam before roaming to another AP. |
| Notes (Optional) | Blank | All | Free form text field for entering fixed asset numbers or other device information. This information is printed on the nightly inventory report. |
| Radio (Enable/Disable) | Enable | All | The Radio option allows you to disable the radio's ability to transmit or receive data while still maintaining Ethernet connectivity to the network. OV3600 will still monitor the Ethernet page and ensure the AP stays online. Customers typically use this option to temporarily disable wireless access in particular locations. This setting can be scheduled at an AP-Level or Group-Level. |
| DHCP | Yes | All (except Colubris) | If enabled, the AP will be assigned a new IP address via DHCP. If disabled, the AP will use a static IP address. For improved security and manageability, Alcatel-Lucent recommends disabling DHCP and using static IP addresses. |
| LAN IP | None | All (except Colubris) | The IP Address of the AP'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). If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area. |
| BSID | 00:00:00:00:00 | WiMAX Base Station | Defines the BSID for the base station. This BSID should match the BSID on the Groups > WiMAX page if you want subscriber stations to associate with the base station. Subscriber stations use the BSID defined on the Groups > WiMAX page to determine which base stations to associate with. |
| Subnet Mask | None | All | Provides the IP subnet mask to identify the sub-network so the IP address can be recognized on the LAN. If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area. |
| Gateway | None | All | The IP address of the default internet gateway. If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area. |

6. Locate the **IOS Template Options** area on the **APs/Devices > Manage** page.



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

Table 86 describes field settings, default values, and additional information for this page.

Table 86 *APs/Devices > Manage > IOS Template Options Fields and Default Values*

| 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. Table 87 describes the settings and default values.

Table 87 *APs/Devices > Manage Fields and Default Values*

| Field | Default | Description |
|---|----------|---|
| Name | None | The name of the interface on the controller. |
| VLAN ID | None | The VLAN ID for the interface on the controller. |
| Port | None | The port on the controller to access the interface. |
| IP Address | None | The IP address of the controller. |
| Subnet Mask | None | The subnet mask for the controller. |
| Gateway | None | The controller's gateway. |
| Primary and Secondary DHCP Servers | None | The DHCP servers for the controller. |
| Guest LAN | Disabled | Indicates a guest LAN. |
| Quarantine | Disabled | Enabled indicates it is a quarantine VLAN; used only for H-REAP-associated clients. |

Configuring Device Interfaces

OV3600 Version 6.4 will introduce the new **APs/Devices > Interface** page.

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 87](#) illustrates this page.

Figure 87 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 of the APs being used.

3. Enter the appropriate **Auth Password** and **Privacy Password**.
4. You can disable the **View AP Credentials** link in OV3600 by the root user. Contact Alcatel-Lucent Support for detailed instructions 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 plan their upgrades using OV3600 accordingly.

[Figure 88](#) illustrates this page and [Table 88](#) describes the settings and default values.

Figure 88 APs/Devices > Manage Firmware Upgrades

Desired Version

Choose the desired firmware version to be applied to **Proxim-AP-4000-partner** (10.51.1.65). Upload firmware files on the Device Setup [Firmware Files](#) page.

Current Version: 3.4.0

Desired version: -- Select firmware ver: ▼

Firmware Upgrade Job Options

Job name: Firmware upgrade for Proxim-

Serve firmware files from this interface: 10.51.2.12 ▼

Failure Notification Options

To be notified when upgrades fail and when a job is stopped, enter email addresses of the form user@domain. Separate multiple addresses by spaces, commas, or semicolons.

Email Recipients:

Sender Address:

Start or Schedule Firmware Upgrade Job: Upgrade Cancel

Table 88 APs/Devices > Manage Firmware Upgrades Fields and Default Values

| 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 for AP Communication Settings

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:

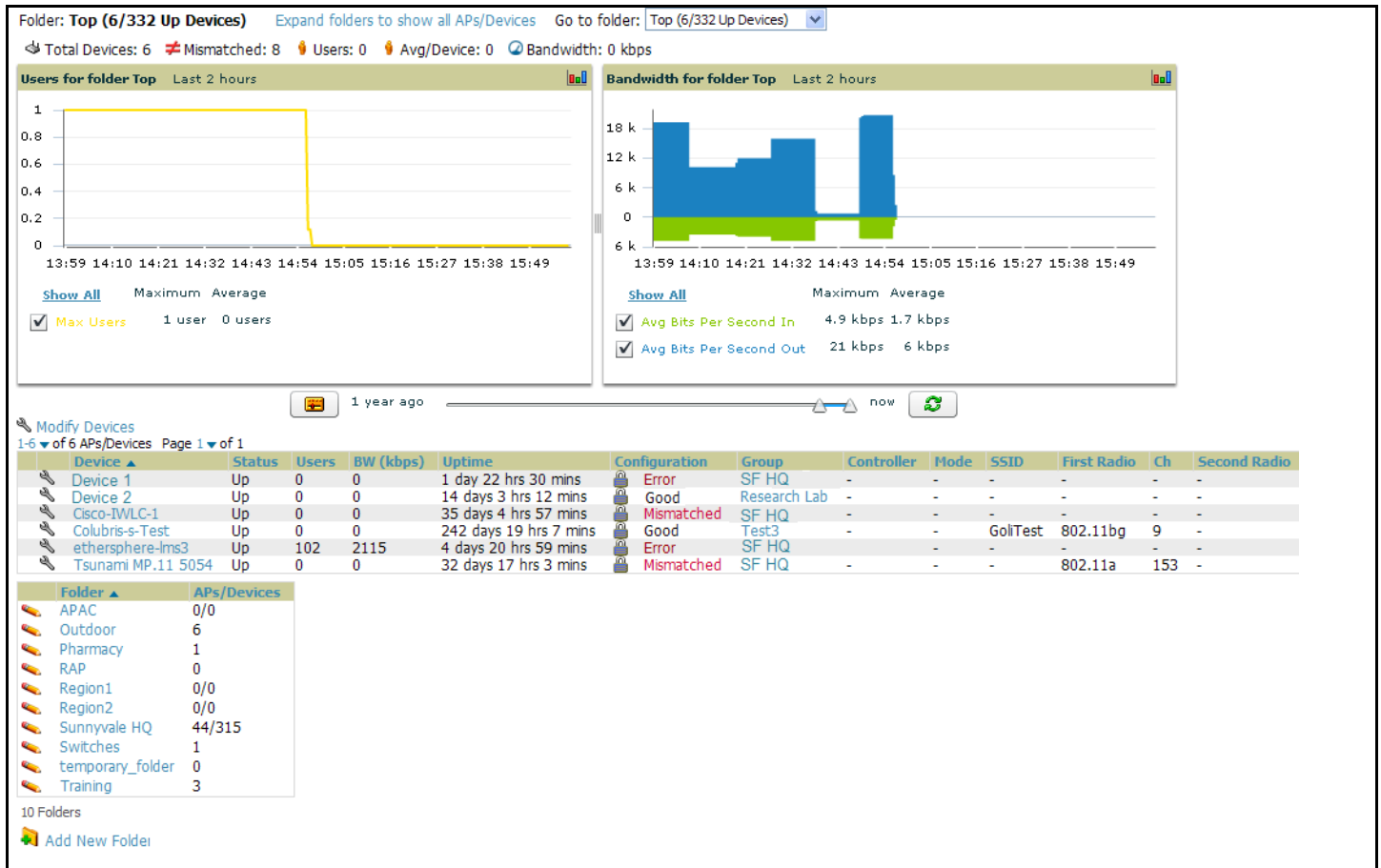
- [Using Device Folders \(Optional\)](#)
- [Monitoring APs with the Monitoring and Controller Pages](#)

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 89](#) and [Figure 90](#) illustrate this component.

Figure 89 APs/Devices > Up Page Example



In [Figure 89](#), 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.

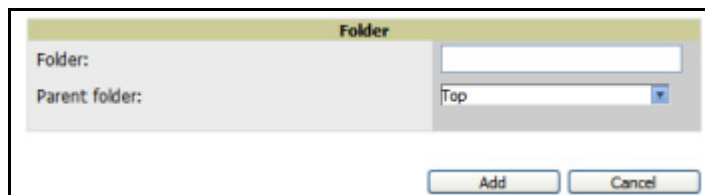
Folder views are persistent in OV3600. If you select the **East Coast** folder and then click the **Down** link at the top of the page, you are taken to all of the down devices in the folder.

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 90](#) illustrates the page that appears.

Figure 90 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 91** illustrates this page.

Figure 91 APs/Devices > List > Monitor Page Illustration (Partial View)

Monitoring AP-AT5 in group **Acme Corporation** in folder **Top** Poll Controller Now

This Device is in monitor-only-with-firmware-upgrades mode.

Status: Up (OK)
 Configuration: Good
 Firmware: 3.3.2.6
 Controller: HQ-3600-CTRL-Primary Switch Port: 1/0
 Type: Acme AP 65 Last Contacted: 12/10/2008 3:22 PM Uptime: 36 days 18 hrs 40 mins
 LAN MAC Address: 00:1A:1E:C2:2E:DC Serial: A90122234 Location: Not Available
 SSID: - Total Users: 7 Bandwidth: 53 kbps
 First Radio: 802.11bg MAC Address: 00:1A:1E:A2:ED:C8 Users: 3 Bandwidth: 34 kbps Channel: 1
 Second Radio: 802.11a MAC Address: 00:1A:1E:A2:ED:C0 Users: 4 Bandwidth: 18 kbps Channel: 48
 Wired Interface: Enet0 (uplink only) MAC Address: 00:1A:1E:C2:2E:DC
 Notes:

AP Client Count by SSID Last 2 hours

AP Bandwidth by SSID Last 2 hours

Location: San Mateo > Borel > AirWave (Floor 5.0)

AP Client Count Summary:

| SSID | Maximum | Average |
|---------------------------|---------|---------|
| Max Users for guest | 4 users | 2 users |
| Max Users for server-wpa2 | 4 users | 3 users |
| Max Users for server-voip | 3 users | 1 user |
| Max Users (Radio 1) | 5 users | 3 users |
| Max Users (Radio 2) | 4 users | 3 users |
| Max Users on Enet0 | 0 users | 0 users |

AP Bandwidth Summary:

| SSID | Maximum | Average |
|-------------------------|------------|-----------|
| Max Out for guest | 864 bps | 47 bps |
| Max In for guest | 955 bps | 228 bps |
| Max Out for server-wpa2 | 171 kbps | 56.4 kbps |
| Max In for server-wpa2 | 62.5 kbps | 24.7 kbps |
| Max Out for server-voip | 455.2 kbps | 52.2 kbps |
| Max In for server-voip | 40 kbps | 8.1 kbps |
| Max Out (Radio 1) | 455.2 kbps | 52.3 kbps |
| Max In (Radio 1) | 41 kbps | 8.3 kbps |
| Max Out (Radio 2) | 171 kbps | 56.4 kbps |
| Max In (Radio 2) | 62.5 kbps | 24.7 kbps |

Associated Users

| Username | Role | MAC Address | SSID | VLAN | AP Radio | Connection Mode | Ch BW | Association Time | Duration | Auth. Type | Cipher | Auth. Time |
|---------------------|---------------|-------------------|-------------|------|----------|-----------------|-------|---------------------|--------------|-------------------|--------|---------------|
| CORPNETWORK\sujatha | employee | 00:19:7E:8A:1A:D5 | server-wpa2 | 29 | 802.11a | 802.11a | - | 12/10/2008 3:00 PM | 6 mins | EAP | - | 6 mins |
| - | visitor-logon | 00:21:E9:59:F8:D6 | guest | 31 | 802.11bg | 802.11g | - | 12/10/2008 2:14 PM | 53 mins | Not Authenticated | - | -53 mins |
| - | visitor-logon | 00:13:02:53:A3:D3 | guest | 31 | 802.11bg | 802.11g | - | 12/10/2008 2:04 PM | 1 hr 3 mins | Not Authenticated | - | -1 hr 3 mins |
| - | visitor-logon | 00:19:7D:14:3A:53 | guest | 31 | 802.11bg | 802.11g | - | 12/10/2008 1:40 PM | 1 hr 26 mins | Not Authenticated | - | -1 hr 26 mins |
| RKS\paul | employee | 00:1C:26:C5:39:CB | server-voip | 30 | 802.11bg | 802.11g | - | 12/10/2008 1:24 PM | 1 hr 43 mins | EAP | - | 1 hr 43 mins |
| CORPNETWORK\peter | employee | 00:1C:8F:31:E2:1D | server-wpa2 | 29 | 802.11a | 802.11a | - | 12/10/2008 12:02 PM | 3 hrs 4 mins | EAP | - | 3 hrs 4 mins |
| William | employee | 00:1E:52:06:EA:99 | server-wpa2 | 29 | 802.11a | 802.11a | - | 12/10/2008 10:05 AM | 5 hrs 1 min | EAP | - | 5 hrs 1 min |
| CORPNETWORK\katie | employee | 00:1F:38:79:EF:E3 | server-wpa2 | 29 | 802.11a | 802.11a | - | 12/10/2008 9:05 AM | 6 hrs 2 mins | EAP | - | 6 hrs 2 mins |

Alert Summary at 12/10/2008 3:22 PM

| Type | Last 2 Hours | Last Day | Total | Last Event |
|------------------------------|--------------|----------|-------|--------------------|
| Server Alerts | 0 | 1 | 2 | 12/9/2008 7:17 PM |
| IDS Events | 22 | 294 | 3538 | 12/10/2008 3:18 PM |
| Incidents | 0 | 0 | 0 | - |
| RADIUS Authentication Issues | 0 | 0 | 0 | - |

Recent Events (view system event log)

| Time | User | Event |
|--------------------------|--------|---|
| Tue Dec 9 19:17:56 2008 | System | Device Bandwidth: Device: Airwave-ATS: Bandwidth >= 20 kbps for 1 min (Warning) |
| Mon Dec 8 18:10:33 2008 | System | Device IDS Events: Device: Airwave-ATS: Count > 0 for 1 minute (Normal) |
| Mon Dec 1 19:21:27 2008 | System | Device Bandwidth: Device: Airwave-ATS: Bandwidth >= 20 kbps for 1 min (Warning) |
| Sun Nov 30 19:33:27 2008 | System | Device IDS Events: Device: Airwave-ATS: Count > 0 for 1 minute (Normal) |
| Wed Nov 26 05:23:39 2008 | System | Configuration verification succeeded; configuration is good |
| Wed Nov 26 05:23:29 2008 | System | Up |

Audit Log

| Time | User | Event |
|--------------------------|---------|--|
| Sun Jul 27 22:32:42 2008 | sujatha | mobility_anchor_id: '0' => '45' |
| Wed Jul 23 08:42:06 2008 | paul | name: 'HW-65-NO-OPEN-2E:DC' => 'HQ-65-NO-OPEN-2E:DC', previous_name: 'HW-NO-OPEN-2E:DC' => 'HW-65-NO-OPEN-2E:DC' |
| Tue Jul 22 13:16:26 2008 | paul | pol_period_up_down: '900' => '90' |
| Tue Jul 22 08:22:55 2008 | dasa | pol_period_client_data: '900' => '120', pol_period_override: '0' => '1' |
| Tue Jul 22 07:50:06 2008 | dasa | pol_period_ap_bw: '600' => '1800', pol_period_client_data: '120' => '900', pol_period_dot11_counters: '600' => '1800', pol_period_mesh_data: '300' => '900', pol_period_override: '0' => '1' |
| Mon Jul 21 18:27:31 2008 | paul | Creating: Template (ap_group_id: '1718', ap_type: '96', atc_version: '3.3.1.3', atc_version_enabled: '0', auth_protocol: 'md5', config_template: 'version 3.3 enable secret '58d7b87301e' |
| Mon Jul 21 13:08:16 2008 | paul | name: 'HW-NO-OPEN-2E:DC' => 'HW-65-NO-OPEN-2E:DC', previous_name: 'Airwave-ATS' => 'HW-NO-OPEN-2E:DC' |
| Mon Jul 21 13:07:54 2008 | paul | name: 'Airwave-ATS' => 'HW-NO-OPEN-2E:DC' |
| Fri Jul 18 17:31:27 2008 | paul | Group: 'Acme Corporation', Folder: 'Top', Device method call: authorize_or_unignore('ap_group_id', '1718', 'monitor_only', '1', 'ap_folder_id', '1') |



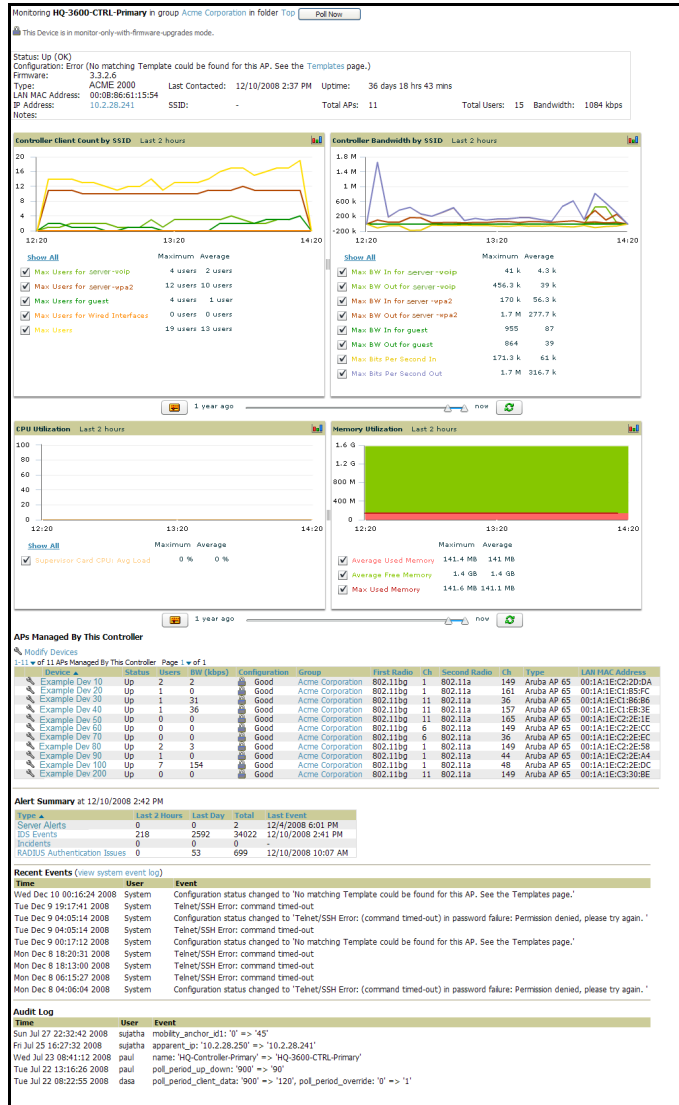
Some data on this page is displayed based on the device type.

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

Figure 92 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 89](#) describes the fields and information displayed.

Table 89 APs/Devices > Monitor > General Fields and Default Values

| Field | Description |
|-------------------------------|---|
| Poll Controller Now | Button immediately polls the individual AP or the controller for a thin AP; this overrides the group's preset polling intervals to force an immediate update of all data except for rogue information. Shows attempt status and last polling times. |
| Status | 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 92 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 89 APs/Devices > Monitor > General Fields and Default Values (Continued)

| 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 90](#) describes graph information displayed in this page.

Table 90 APs/Devices > Monitor > Graphical Data Fields and Default Values

| Graph | Description |
|--|---|
| User | Shows the max and average user count reported by the device radios for a configurable period of time. User count for controllers are the sum of the user count on the associated APs. Checkboxes below the graph can be used to limit the data displayed. |
| Bandwidth | Shows the bandwidth in and out reported by the device for a configurable period of time. Bandwidth for controllers is the sum of the associated APs. Checkboxes below the graph can be used to limit the data displayed. |
| CPU Utilization (controllers only) | Reports overall CPU utilization (not on a per-CPU basis) of the controller. |
| Memory Utilization (controllers only) | Reports average used and free memory and average max memory for the controller. |

4. Locate the **Connected Users** area on the **APs/Devices > Monitor** page. The **Connected Users** area provides details about the users associated to devices. This information also appears on the **Users > All** and **Users > Connected** pages. [Table 91](#) describes the fields and information displayed.

Table 91 APs/Devices > Monitor > Connected Users Fields and Default Values

| Field | Description |
|-------------------------|--|
| User | Provides the name of the User associated to the AP. OV3600 gathers this data in a variety of ways. It can be taken from RADIUS accounting data, traps from Cisco VxWorks APs and tables on Colubris APs. |
| MAC Address | Displays the Radio MAC address of the user associated to the AP. Also provides a link that redirects to the Users > Detail page. |
| Radio | Displays the radio to which the user is associated. |
| 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 | <p>Displays the type of authentication employed by the user. Supported auth types are as follows:</p> <ul style="list-style-type: none"> ● EAP—Extensible Authentication Protocol, only reported by Cisco VxWorks via SNMP traps. ● PPTP—Point-to-Point Protocol, supported by Colubris APs acting as VPNs. ● RADIUS accounting—RADIUS accounting servers integrated with OV3600 provide the RADIUS Accounting Auth type. ● Authenticated—a general category supporting additional authentication types. OV3600 considers all other types as not authenticated. <p>The information OV3600 displays in Auth Type and Cipher columns depends on what information the server receives from the APs and/or controllers it is monitoring. The client devices may all be similar, but if the APs to which they are associated are of different models, or if security is set up differently between them, then different Auth Type or Cipher values may be reported to the OV3600 server.</p> <p>If all APs are the same model and all are set up the same way, then another reason for differing Auth Types might be the use of multiple VLANs or SSIDs. One client device might authenticate on one SSID using one Auth Type and another client device might authenticate on a second SSID using a different Auth Type.</p> |

Table 91 APs/Devices > Monitor > Connected Users Fields and Default Values (Continued)

| Field | Description |
|-----------------------|--|
| Cipher | Displays the encryption or decryption cipher supporting the user, when this information is available. The client devices may all be similar, but if the APs to which they are associated are of different models, or if security is set up differently between them, then different Auth Type or Cipher values may be reported to the OV3600 server. |
| Auth. Time | 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 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 CDP Neighbors area on the **APs/Devices > Monitor** page, if the device supports the Cisco Discovery Protocol (CDP). This section provides detailed CDP information.
6. Locate the **Alerts Summary** area on the **APs/Devices > Monitor** page. The **Pending Alerts** area displays all unacknowledged alerts for the AP.
7. For Aruba/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.
8. 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.
9. 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.
10. 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.
11. **QuickView** runs faster than **VisualRF** because it has fewer features. It is geared toward resolving issues with single clients or single access points.

[Table 92](#) further describes the fields of this **QuickView** page.

Table 92 QuickView Fields

| Field | Description |
|--------------------|---|
| AP Name | Displays the name of the AP that is linked with the currently viewed AP. |
| MAC Address | Displays the radio MAC address of the AP that is linked with the currently viewed AP. |
| Link Time | Displays the day and time when the link was initiated. |

Table 92 QuickView Fields

| Field | Description |
|------------------|--|
| 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. |

12. 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 93](#) describes the fields in this page display.

Table 93 APs/Devices > Monitor > Recent Events Fields and Default Values

| Field | Description |
|--------------|---|
| Time | Displays the day and time the event was recorded. |
| User | Displays the user that triggered the event. Configuration changes are logged as the OV3600 user that submitted them. Automated OV3600 events are logged as the System user. |
| Event | Displays a short text description of the event. |

13. 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 94](#) describes the components of this display.

Table 94 APs/Devices > Monitor > Recent Events Fields and Default Values

| Field | Description |
|--------------|---|
| Time | Displays the day and time the event was recorded. |
| User | Displays the user that triggered the event. Configuration changes 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 Support for detailed explanation of any events logged. |

This chapter provides an overview and several tasks supporting the use of device configuration templates in OV3600. This chapter contains the following topics:

General Template Use

- Group Templates
- Viewing and 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

Templates for Symbol and HP ProCurve WeSM Devices

- Configuring Symbol Controller / HP WESM Templates

Global Templates

- Configuring a Global Template

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

Group Templates

Supported Device Templates

Templates are powerful configuration tools 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 types of devices:

- Alcatel-Lucent
- Aruba



NOTE

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

- Cisco Aironet IOS and 4800 autonomous APs
- HP ProCurve 530 and WeSM controllers
- Hirschmann
- LANCOM
- Nomdix
- Symbol
- Trapeze
 - 3Com
 - Nortel
 - Enterasys

Template Variables

Variables in templates configure device-specific properties, such as name, IP address and channel. Variables can also be used to configure group-level properties, such as SSID and RADIUS server, which may differ from one group to the next. The OV3600 template understands many variables including the following:

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

The variable settings correspond to device-specific values on the **APs/Devices > Manage** configuration page for the specific AP that is getting configured.



NOTE

Changes made on the other **Group** pages (Radio, Security, VLANs, SSIDs, and so forth) are not applied to any APs that are configured by templates.

Viewing and Adding Templates

Perform these steps to display, add, or edit templates.

1. Navigate to the **Groups > List** page, and select a group for which to add or edit templates. This can be a new group, created with the **Add** button, or you can edit an existing group by clicking the corresponding pencil icon. The **Groups > Basic** page for that group appears.

Additional information about adding and editing groups is described in “[Configuring and Using Device Groups in OV3600](#)” on page 73.

2. From the OV3600 navigation pane, click **Templates**. The **Templates** page appears. [Figure 93](#) illustrates the **Groups > Templates** configuration page, and [Table 95](#) describes the information columns.

Figure 93 *Groups > Templates Page Illustration for a Sample Device Group*

Group: **Acme Corporation**

Note: No template is available for Cisco Aironet 1200 IOS devices with firmware version 12.3(8)JA2.
Note: No template is available for Cisco Aironet 1200 IOS devices with firmware version 12.3(8)JEC.
Note: No template is available for Cisco Aironet 1240 IOS devices with firmware version 12.4(10b)JDA.
Note: No template is available for Aruba 5000 devices with firmware version 3.3.2.10.
Note: No template is available for Aruba 5000 devices with firmware version 3.3.2.4.
Note: No template is available for Aruba 2400 devices with firmware version 3.3.2.10.
Note: No template is available for Symbol WS5100 devices with firmware version 3.2.0.0-040R.
Note: No template is available for Aruba 3600 devices with firmware version 3.3.2.7.
Note: No template is available for Cisco Aironet 1250 IOS devices with firmware version 12.4(10b)JA3.
Note: No template is available for Aruba 3400 devices with firmware version 3.3.2.7.
Note: No template is available for Aruba 3200 devices with firmware version 3.3.2.8-rn-3.0.
Note: No template is available for Symbol RFS7000 devices with firmware version 1.1.1.0-003R.
Note: No template is available for Cisco Aironet 871W devices with firmware version 12.4(4)T7.

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 95 *Groups > Templates Fields and Default Values*

| 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. |

Table 95 Groups > Templates Fields and Default Values (Continued)

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

3. To create a new template and add it to the OV3600 template inventory, navigate to the **Groups > List page**, and **select the group to which you will apply the template. Click the group name and the Details page appears. Click Templates**, then click **Add**.
4. Complete the configurations illustrated in [Figure 94](#), and the settings described in [Table 96](#).

Figure 94 Groups > Templates > Add Template Page Illustration

Group: San Francisco

Alcatel-Lucent 4306G

Name:

Device Type:

Restrict to this version: Yes No

Template firmware version:

Template Select

Fetch template from device:

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 %f...% statements must be terminated by %endif% and cannot be nested.

Available Variables:

| | |
|---------------|--------------------|
| ap_include_1 | controller_ip |
| ap_include_10 | gateway |
| ap_include_2 | hostname |
| ap_include_3 | ip_address |
| ap_include_4 | manager_ip_address |
| ap_include_5 | master_ip |
| ap_include_6 | netmask |
| ap_include_7 | syslocation |
| ap_include_8 | |
| ap_include_9 | |
| contact | |

Credentials

Change credentials the OV3600 uses to contact devices after successful config push.

Community String:

Confirm Community String:

Telnet/SSH Username:

Telnet/SSH Password:

Confirm Telnet/SSH Password:

"enable" Password:

Confirm "enable" Password:

SNMPv3 Username:

Auth Password:

Confirm Auth Password:

SNMPv3 Auth Protocol:

Privacy Password:

Confirm Privacy Password:

SNMPv3 Privacy Protocol:

Table 96 *Groups > Templates > Add Template Fields and Default Values*

| Setting | Default | Description |
|---|-----------------------|---|
| Use Global Template | No | Uses a global template that has been previously configured on the Groups > Templates configuration page. Available templates will appear in the drop-down menu. If Yes is selected you can also configure global template variables. For Symbol devices you can select the groups of thin APs to which the template should be applied. For more information about global templates see the Groups > Templates section of the <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 . |

Table 96 *Groups > Templates > Add Template Fields and Default Values (Continued)*

| Setting | Default | Description |
|--------------------------------|---------|---|
| SNMPv3 Privacy Protocol | DES | Specifies the SNMPv3 Privacy protocol, either DES or AES . |

Configuring General Template Files and Variables

This section describes the most general aspects of configuring AP device templates and the most common variables:

- [Configuring General Templates](#)
- [Using Template Syntax](#)
- [Using Directives to Eliminate Reporting of Configuration Mismatches](#)
 - `<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 type of device that will be configured by this template.
5. Select the model AP from the drop-down list, and click **Fetch**.
6. OV3600 automatically attempts to replace some values from the configuration of that AP with *variables* to enable AP-specific options to be set on an AP-by-AP basis. Refer to [“Using Template Syntax” on page 171](#)

These variables are always encapsulated between % signs. On the right side of the configuration page is the **Additional Variables** section. This section lists all available variables for your template. Variables that are in use in a template are green, while variables that are not yet in use are black. Verify these substitutions to ensure that all of the settings that you believe should be managed on an AP-by-AP basis are labeled as variables in this fashion. If you believe that any AP-level settings are not marked correctly, please contact Alcatel-Lucent Technical Support at 866-WIFI-OV3600 before proceeding.

7. Specify the device types for the template. The templates only apply to devices of the specified type.
 - Specify whether OV3600 should reboot the devices after a configuration push. If the **Reboot Devices after Configuration Changes** option is selected, then OV3600 instructs the AP to copy the configuration from OV3600 to the startup configuration file of the AP and reboot the AP.
 - If the **Reboot Devices after Configuration Changes** option is not selected, then OV3600 instructs the AP to copy the configuration to the startup configuration file and then tell the AP to copy the startup configuration file to the running configuration file.
 - Alcatel-Lucent recommends using the **reboot** option when 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.
8. Restrict the template to apply only to the specified version of firmware. If the template should only apply to a specific version of firmware, select Yes and enter the firmware version in the **Template Firmware Version** text field.
9. Click the **Save and Apply** button to push the configuration to all of the devices in the group. If the devices are in monitor-only mode (which is recommended while you are crafting changes to a template or creating a new one), then OV3600 will audit the devices and compare their current configuration to the one defined in the template.



If you set the reboot flag to **No**, then some changes could result in configuration mismatches until the AP is rebooted.

For example, changing the SSID on Cisco IOS APs requires the AP to be rebooted. Two other settings that require the AP to be rebooted for configuration change are Logging and NTP. A configuration mismatch results if the AP is not rebooted.

If logging and NTP service are not required according to the Group configuration, but are enabled on the AP, you would see a configuration file mismatch as follows if the AP is not rebooted:

IOS Configuration File Template:

```
...
(no logging queue-limit)
...
```

Device Configuration File on APs/Devices > Audit Configuration Page

```
...
  line con 0
  line vty 5 15
actual logging 10.51.2.1
actual logging 10.51.2.5
actual logging facility local6
actual logging queue-limit 100
actual logging trap debugging
  no service pad
actual ntp clock-period 2861929
actual ntp server 209.172.117.194
  radius-server attribute 32 include-in-access-req format %h
...
```

10. Once the template is correct and all mismatches are verified on the **AP Audit** configuration page, use the **Modify Devices** link on the **Groups > Monitor** configuration page to place the desired devices into

Management mode. This removes the APs from Monitor mode (read-only) and instructs the AP to pull down its new startup configuration file from OV3600.



Devices can be placed into Management mode individually from the **APs/Devices > Manage** configuration page.

Using Template Syntax

Template syntax is comprised of the following components, described in this section:

- [Using AP-Specific Variables](#)
- [Using Directives to Eliminate Reporting of Configuration Mismatches](#)
- [Using Conditional Variables in Templates](#)
- [Using Substitution Variables in Templates](#)

Using Directives to Eliminate Reporting of Configuration Mismatches

OV3600 is designed to audit AP configurations to ensure that the actual configuration of the access point exactly matches the Group template. When a configuration mismatch is detected, OV3600 generates an automatic alert and flags the AP as having a **Mismatched** configuration status on the user page.

However, when using the templates configuration function, there will be times when the running-config file and the startup-config file do not match under normal circumstances. For example, the `ntp clock-period` setting is almost never identical in the running-config file and the startup-config file. You can use directives such as `<ignore_and_do_not_push>` to customize the template to keep OV3600 from reporting mismatches for this type of variance.

OV3600 provides two types of directives that can be used within a template to control how OV3600 constructs the startup-config file to send to each AP and whether it reports variances between the running-config file and the startup-config file as "configuration mismatches." Lines enclosed in `<push_and_exclude>` are included in the AP'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 97](#):

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

Table 97 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 98](#) 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 98 *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 293](#) 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
%endif%

```

```

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 Symbol Controller / HP WESM Templates

This section describes the configuration of templates for Symbol controllers and HP WESM devices.

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

A sample running-configuration file template is provided in this topic for reference. A template can be fetched from a model device using the Cisco IOS device procedure described in [“Configuring Cisco IOS Templates” on page 175](#).

Certain parameters such as `hostname` and `location` are turned into variables with the % tags so that device-specific values can be read from the individual manage pages and inserted into the template.

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

```
//
// WS2000 Configuration Command Script
// System Firmware Version: 2.1.0.0-035R
//
/
passwd enc-admin b30e1f81296925
passwd enc-manager a11e00942773
/
system
ws2000
// WS2000 menu
set name %hostname%
set loc %location%
set email %contact%
set cc us
set airbeam mode disable
set airbeam enc-passwd a11e00942773
```



```

set applet lan enable
set applet wan enable
set applet slan enable
set applet swan enable
set cli lan enable
set cli wan enable
set snmp lan enable
set snmp wan enable
set workgroup name WORKGROUP
set workgroup mode disable
set ftp lan disable
set ftp wan disable
set ssh lan enable
set ssh wan enable
set timeout 0
/
"templated-running-config-static" 1309L, 28793C
1,1      Top
set port 8 primary 1812

set server 8 secondary 0.0.0.0
set port 8 secondary 1812

/
// Hotspot Whitelist configuration
network
wlan
hotspot
white-list
clear rule all
// Hotspot Whitelist 1 configuration
// Hotspot Whitelist 2 configuration
// Hotspot Whitelist 3 configuration
// Hotspot Whitelist 4 configuration
// Hotspot Whitelist 5 configuration
// Hotspot Whitelist 6 configuration
// Hotspot Whitelist 7 configuration
// Hotspot Whitelist 8 configuration
/
/
network
dhcp
// network->dhcp menu
set firmwareupgrade 1
set configupgrade 1
set interface s2
set dhcpvendorclassid
/
Save

```

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

```

set mac %radio_index% %radio_mac%
set ap_type %radio_index% %ap_type%
set radio_type %radio_index% %radio_type%
set beacon intvl %radio_index% 100
set dtim %radio_index% 10
set ch_mode %radio_index% fixed
%if radio_type=802.11a%
set primary %radio_index% 1

```

```

%endif%
%if radio_type=802.11b%
set short-pre %radio_index% disable
%endif%
%if radio_type=802.11b/g%
set short-pre %radio_index% disable
%endif%
set div %radio_index% full
set reg %radio_index% in/out %channel% %transmit_power%
set rts %radio_index% 2341
set name %radio_index% %description%
set loc %radio_index%
set detectorap %radio_index% %detector%
%if radio_type=802.11a%
set rate %radio_index% 6,12,24 6,9,12,18,24,36,48,54
%endif%
%if radio_type=802.11b%
set rate %radio_index% 1,2 1,2,5.5,11
%endif%
%if radio_type=802.11b/g%
set rate %radio_index% 1,2,5.5,11 1,2,5.5,6,9,11,12,18,24,36,48,54
%endif%

```

Configuring Clustering and Redundancy

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

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

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

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

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

```

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

```

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

Changing Redundancy Configuration

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

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

Adding Clustering Members

This template configuration changes group-level parameters.

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

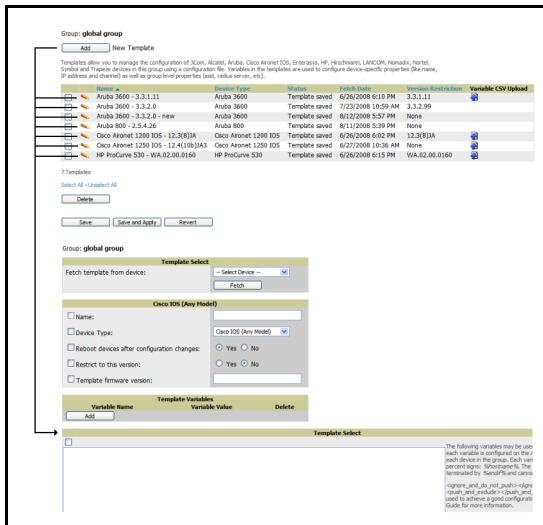
Configuring a Global Template

Global templates allow OV3600 users to define a single template in a global group that can be used to manage access points in subscriber groups. Such a template enables turning settings like group RADIUS servers and encryption keys into variables that can be configured on a per-group basis.

Perform the following steps to create a global template, or to view or edit an existing global template:

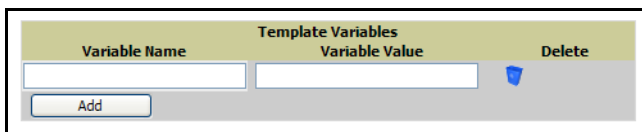
1. Navigate to the **Group > Templates** configuration page for the global group that owns it.
2. Click the **Add** button to add a new template, or click the **pencil** icon next to an existing template to edit that template.
3. Examine the configurations illustrated in [Figure 95](#).

Figure 95 *Group > Templates > Add Page Illustration*



4. Use the drop-down menu to select a device from which to build the global template and click the **Fetch** button. The drop-down menus are populated with all devices that are contained in any group that subscribes to the global group. The fetched configuration populates the template field. Global template variables can be configured with the **Add** button in the **Template Variables** box, illustrated in [Figure 96](#).

Figure 96 *Template Variables Illustration*



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

5. Once you have configured your global template, click **Add** at the bottom of the configuration page. You are taken to a confirmation configuration page where you can review your changes.
6. If you want to add the global template, click the **Apply Changes Now** button. If you do not want to add the template, click the **Cancel and Discard Changes** button. Canceling from the confirmation configuration page causes the template and all of the template variables to be lost.
7. Once you have added a new global template, you can use a CSV upload option to configure global template variables. Navigate to the **Groups > Templates** configuration page and click the **CSV** upload icon for the template. The CSV file must contain columns for **Group Name** and **Variable Name**. All fields must be completed.
 - **Group Name**—the name of the subscriber group that you wish to update.
 - **Variable Name**—the name of the group template variable you wish to update.
 - **Variable Value**—the value to set.

For example, for a global template with a variable called "ssid_1", the CSV file might resemble what follows:

```
Group Name, ssid_1
Subscriber 1, Value 0
```

8. Once you have defined and saved a global template, it is available for use by any local group that subscribes to the global group. Navigate to the **Groups > Template** configuration page for the local group and click the pencil icon next to the name of the global template in the list. [Figure 97](#) illustrates this page.

Figure 97 *Groups > Templates Edit, Topmost Portion*

| | |
|---------------------------------|---|
| Group: SG aruba | |
| Aruba 3600 | |
| Name: | Aruba 3600 - 3.3.1.11 |
| Device Type: | Aruba 3600 |
| Restrict to this version: | Yes |
| Template firmware version: | 3.3.1.11 |
| Group Template Variables | |
| location: | <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.

RAPIDS is used to secure your wireless network. One of the core components of wireless security is rogue device detection. RAPIDS leverages your existing infrastructure to perform wired and wireless scans for rogue devices. Once the rogue devices are discovered, RAPIDS will alert your security team of the threat and provide the key information needed to eliminate the threat.

The RAPIDS module and rogue device classification are detailed in the following sections:

- [“Overview” on page 183](#)
- [“Monitoring Rogue AP Devices” on page 184](#)
- [“Configuring RAPIDS” on page 190](#)
- [“RAPIDS Rules” on page 193](#)
- [“The RAPIDS OUI Score Override” on page 198](#)

Overview

RAPIDS leverages an existing wired and wireless infrastructure without requiring separate rogue-scanning devices to detect and locate devices that pose a security threat to your network and users.

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

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

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

- **Cisco's WLSE** (1100 and 1200 IOS)—OV3600 fetches rogue information from the HTTP interface and gets new AP information from SOAP API. This system provides wireless discovery information rather than rogue detection information.
- **AirMagnet Enterprise**—Fetches a list of managed APs from OV3600.
- **AirDefense**—Uses the OV3600 XML API to keep its list of managed devices up to date.
- **WildPackets OmniPeek**—Fetches a list of managed APs from OV3600.

RAPIDS Tabs

The RAPIDS tabs are:

- **Overview**—This is a starting point for detection and monitoring of rogue devices on the network. This page summarizes IDS events, rogue device data, acknowledged devices, system events, and RAPIDS events. For more information, see [“Viewing a Rogue AP” on page 186](#).
- **Rogue APs**—Provides a summary of rogue data for each unmanaged device discovered by RAPIDS. The information can be sorted and filtered so that you can isolate the devices you need to investigate. For more information, see [“Monitoring Rogue AP Devices” on page 184](#).
- **Setup**—This tab presents the basic RAPIDS configuration, classification options, and filtering option. For more information, see [“Configuring RAPIDS” on page 190](#).

- **Rules**—This tab is where you configure and manage the rules that govern device classification. This tab also defines the default classification of rogue devices that do not match any RAPIDS rules. For more information, see [“RAPIDS Rules” on page 193](#).
- **Score Override**—This tab allows you to change the OUI scores assigned to MAC addresses detected during scans of bridge forwarding tables on switches or routers. For more information, see [“The RAPIDS OUI Score Override” on page 198](#).

Additional Rogue Device Resources

The following OV3600 tools support RAPIDS:

- **System Triggers and Alerts**—Triggers and Alerts that are associated with rogue devices follow the classification-based system described in this chapter. For additional information about triggers that support rogue device detection, see to [“Creating and Using Triggers and Alerts” on page 202](#).
- **Reports**—The **Rogue Devices Report** displays summary and detail information about all rogues first discovered in a given time period. For more information, see [“Defining Reports” on page 275](#).

Additional Security-Related Topics

For additional security-related features and functions, see the following topics in this guide.

- [“Configuring Group Security Settings” on page 85](#)
- [“Configuring Group SSIDs and VLANs” on page 88](#)
- [“Creating and Using Triggers and Alerts” on page 202](#)

Monitoring Rogue AP Devices

This section contains the following topics about the **Rogue APs** page:

- “Monitoring Rogue AP Devices” on page 184
- “Configuring RAPIDS” on page 190
- “Viewing and Configuring RAPIDS Rules” on page 194
- “Using RAPIDS Rules with Additional OV3600 Functions” on page 198

The **Overview** tab displays a page of RAPIDS summary information (see [Figure 98](#)). This page also includes links to the Alcatel-Lucent Management Client, an optional utility that reports wireless discovery information to OV3600. [Table 99](#) defines the summary information that appears on the page.

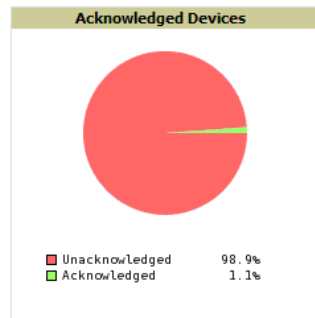
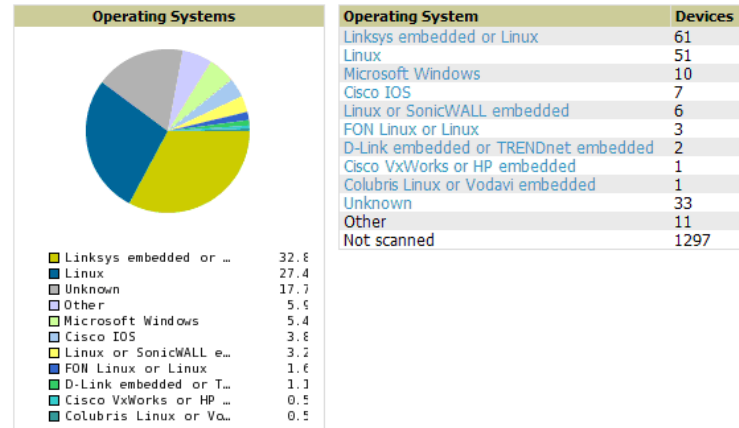
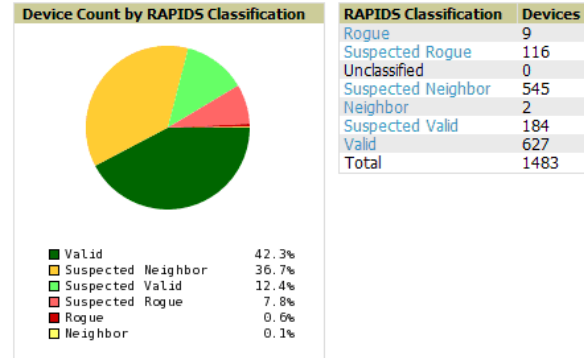
Figure 98 RAPIDS Overview page

Summary

IDS Events for devices in folder [Top](#) and subfolders

| Attack ▲ | Last 2 Hours | Last 24 Hours | Total |
|-------------------------------------|--------------|---------------|-------|
| AP Impersonation | 0 | 42 | 84 |
| Deauth-Broadcast | 0 | 2 | 6 |
| Disconnect Station Attack (AP) | 57 | 661 | 1846 |
| Disconnect Station Attack (Station) | 1 | 41 | 79 |
| Station Associated to Rogue AP | 3 | 106 | 210 |
| Station Unassociated from Rogue AP | 4 | 92 | 169 |
| 6 Attack Types | 65 | 944 | 2394 |

Rogue Data



System Information

- 9 groups have wireless scanning enabled.
- 0 wireline scans are scheduled. [Configure wireline scanning.](#)
- 1 WLSE is being monitored.

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

RAPIDS Changes ([view RAPIDS audit log](#))

| Time | User | Event |
|--------------------------|--------------|--|
| Fri Oct 16 10:13:52 2009 | hstonebraker | rogue_ap (id 147026): 3Com Access Point: 'Identify Operating System' |
| Wed Oct 7 07:44:31 2009 | jason | rogue_ap (id 146864): user_classification: '5' => '6' |
| Thu Oct 1 20:40:51 2009 | patrick | rogue_ap (id 147026): 3Com Access Point: 'Identify Operating System' |

Table 99 Overview Fields

| Summary | Description |
|---|--|
| IDS Events | Displays a list of IDS events for the designated folder (Top is the default) and subfolders. Field displays events from the past two hours, the past 24 hours, and total IDS events. |
| Rogue Data | A summary of rogue device counts by RAPIDS classification in a color coded pie chart format and listed summary. View additional details for rogue devices via the RAPIDS > Rogue APs page. |
| Operating System | Detected operating systems represented in both a color coded pie chart and a summary listing. OS scans can be run manually or enabled to run automatically on the RAPIDS > Setup page. |
| Acknowledge Devices | A color coded pie chart comparing the number of acknowledged devices to the unacknowledged devices. |
| System Information | <p>This section provides links to other pages and downloads:</p> <p>x groups have wireless scanning enabled. The information here is also a link to the detailed Groups > List page.</p> <p>x wireline scans are scheduled. Configure wireline scanning. Displays the number of wireline scans that are scheduled. Select the Configure wireline scanning link to configure and schedule HTTP scans.</p> <p>x WLSE is being monitored Displays the number of WLSE devices that are being monitored by OV3600. WLSE provides RF statistics including Rogue scanning information for 1100 and 1200 IOS access points. Select the x WLSE link to add new devices or view additional details about the monitored devices.</p> |
| Alcatel-Lucent Management Client | <p>Provides links for the AMC module in OV3600:</p> <ul style="list-style-type: none"> Download the Alcatel-Lucent Management Client™ View the Alcatel-Lucent Management Client user guide |
| RAPIDS Changes | RAPIDS change log tracks every change made to the RAPIDS system including changes to rules, manual classification, and anything on the RAPIDS > Setup page. |

Viewing a Rogue AP

To view a rogue AP, select the **RAPIDS > Rogue APs** tab and select a rogue device type from the **Minimum Classification** drop-down menu (see [Figure 99](#)). You can sort the table columns (up/down) by selecting the column head or filter data using the column head drop down menus.

Figure 99 Viewing a Rogue AP by Classification

Minimum Classification: Rogue

[Modify Devices](#)

1-9 of 9 Rogue APs Page 1 of 1 Choose Columns

| Ack | RAPIDS Classification | Threat Level | Name | Classifying Rule | Wired | #APs Hearing | Location | SSID | Signal | RSSI | Network Type |
|-----|-----------------------|--------------|---------------------|--------------------------------|-------|--------------|----------------|-------------------------------|--------|------|--------------|
| No | Rogue | 7 | Linksys-4D:00:8F | Detected Wirelessly and on LAN | Yes | 46 | Sunnyvale > HQ | device-ssid | -20 | 30 | AP |
| No | Rogue | 7 | Ambit Micr-5B:43:7A | Detected Wirelessly and on LAN | Yes | 39 | Sunnyvale > HQ | rmurtest1200 | -20 | 37 | AP |
| No | Rogue | 7 | PROXIM, IN-5A:A4:F0 | Detected Wirelessly and on LAN | Yes | 45 | - | - | -20 | 8 | AP |
| No | Rogue | 7 | PROXIM, IN-5A:64:27 | Detected Wirelessly and on LAN | Yes | 26 | - | - | -20 | 32 | AP |
| No | Rogue | 7 | Aronet WI-4S:DE:C5 | Detected Wirelessly and on LAN | Yes | 26 | Sunnyvale > HQ | vxworks-350-00:40:96:41:89:FD | -20 | 9 | AP |
| Yes | Rogue | 7 | Alpha Netw-17:55:DF | Detected Wirelessly and on LAN | Yes | 32 | Sunnyvale > HQ | default | -22 | 11 | AP |
| No | Rogue | 7 | Jumper Ne-A7:C2:62 | Detected Wirelessly and on LAN | Yes | 50 | Sunnyvale > HQ | dbishop-netscreen | -20 | 6 | AP |
| Yes | Rogue | 7 | Allied Tel-68:3A:2B | Detected Wirelessly and on LAN | Yes | 44 | - | default | -20 | 11 | AP |
| Yes | Rogue | 7 | 3Com Access Point | Detected Wirelessly and on LAN | Yes | 48 | Sunnyvale > HQ | 3com | -20 | 37 | AP |

1-9 of 9 Rogue APs Page 1 of 1

[View Ignored Rogues](#)



The page displayed in [Figure 99](#) may require a moment to load; no rogues displayed for a given classification means that no such rogue device was discovered on your network.

[Table 100](#) details the column information displayed in [Figure 99](#). For additional information about RAPIDS rules, refer to “[RAPIDS Rules](#)” on page 193.

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

Table 100 RAPIDS > Rogue APs Column Definitions

| Column | Description |
|----------------------------------|---|
| Ack | Displays whether or not the rogue device has been acknowledged. Devices can be acknowledged manually or you can configure RAPIDS so that manually classifying rogues will automatically acknowledges them. Rogues should be acknowledged when the OV3600 user has investigated them and determined that they are not a threat (see “Using the Basic Configuration Section” on page 190). |
| RAPIDS Classification | Displays the current RAPIDS classification. This classification is determined by the rules defined on the RAPIDS > Rules page. |
| Threat Level | This field displays the numeric threat level of the device, in a range from 1 to 10. The definition of threat level is configurable, as described in “Rogue Device Threat Level” on page 194 . The threat level is also supported with Triggers (see “Creating and Using Triggers and Alerts” on page 202). |
| Name | Displays the alpha-numeric name of the rogue device, as known. By default, OV3600 assigns each rogue device a name derived from the OUI vendor and the final six digits of the MAC address. |
| Classifying Rule | Displays the RAPIDS Rule that classified the rogue device (see “Viewing and Configuring RAPIDS Rules” on page 194). |
| Controller Classification | Displays the classification of the device based on the controller’s hard-coded rules. NOTE: This column is hidden unless <i>Offload Aruba/Alcatel-Lucent WMS Database</i> is enabled by at least one group on the Groups > Basic page. |
| Wired | Displays whether the rogue device has been discovered on the wire. This column displays Yes or is blank if wired information was not detected. |
| #APs Hearing | Displays the number of AP devices that have wirelessly detected the rogue device. A designation of heard implies the device was heard over the air. |
| Location | As with all List pages in OV3600 Version 6.4, the RAPIDS > Rogue APs page includes the Location column. Click the location associated to the rogue device to view the device in the VisualRF floor plan. RAPIDS and VisualRF must be licensed on the OV3600 for this functionality to be supported. |
| SSID | Displays the most recent SSID that was heard from the rogue device. |
| Signal | Displays the strongest signal strength detected for the rogue device. |
| RSSI | Displays Received Signal Strength Indication (RSSI) designation, a measure of the power present in a received radio signal. |
| Network Type | Displays the type of network in which the rogue is present, for example: <ul style="list-style-type: none"> ● Ad-hoc—This type of network usually indicates that the rogue is a laptop that attempts to create a network with neighboring laptops, and is less likely to be a threat. ● AP—This type of network usually indicates an infrastructure network comprised of ceiling-mounted APs, for example. This may be more of a threat. ● Unknown—The network type is not known. |
| Encryption Type | Displays the encryption that is used by the device as known. Possible contents of this field include the following encryption types: <ul style="list-style-type: none"> ● Open—Definition pending ● WEP—Wired Equivalent Privacy ● WPA—Wi-Fi Protected Access <p>Generally, this field alone does not provide enough information to determine if a device is a rogue, but it is a useful attribute. If a rogue is not running any encryption method, you have a wider security hole than with an AP that is using encryption.</p> |
| Ch | Indicates the RF channel on which the rogue device was detected. |

Table 100 RAPIDS > Rogue APs Column Definitions

| Column | Description |
|----------------------------|---|
| LAN Vendor | Indicates the LAN vendor of the rogue device, when known. |
| Radio Vendor | Indicates the radio vendor of the rogue device, when known. |
| OS | This field displays the OS of the device, as known. OS is the result of a running an OS port scan on a device. An IP addresses is required to run an OS scan. The OS reported here is the best guess. |
| Model | Displays the model of rogue device, if known. This is determined with a fingerprint scan, and this information may not always be available. |
| IP Address | Displays the IP address of the rogue device. The IP address data comes from ARP polling of routers, switches and fingerprint scans. |
| Last Discovering AP | Displays the most recent AP to discover the rogue device. The device name in this column is taken from the device name in the group. |
| Switch/Router | Displays the switch or router where the device's LAN MAC address was last seen. |
| Port | Indicates the physical port of the switch or router to which a rogue was last seen. |
| Last Seen | Indicates the date and time the rogue device was last seen. |

To view the details for any rogue device, select the device name to launch the device's detail page (Figure 100).

Figure 100 Rogue APs Device Detail Page

Name:

Acknowledge: Yes No

Controller Classification:

RAPIDS Classification:

Classification Rule:

RAPIDS Classification Override:

Threat Level:

Threat Level Override:

Radio MAC Address:

Radio Vendor:

LAN MAC Address:

LAN Vendor:

OUI Score:

Operating System:

OS Detail:

Last Scan:

Model: -

IP Address: 10.51.1.64

SSID: device123-ssid

Channel: 6

WEP: No

WPA: No

Network Type: AP

First Discovered: 4/21/2009 3:02 PM

First Discovery Method: -

First Discovery Agent: -

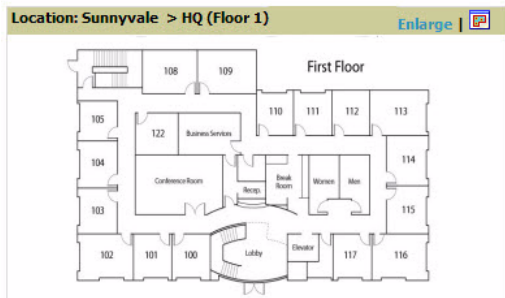
Last Discovered: 10/18/2009 4:02 AM

Last Discovery Method: Wireless AP scan

Last Discovery Agent: AL3

Notes:

[Refresh this page for updated results.](#)



1-20 of 43 Discovery Events Page 1 of 3 >> | [Choose Columns](#)

| RSSI | Signal | Channel | SSID | WEP | WPA | BSSID | Network Type | IP Address | Time | Discovery Method |
|------|--------|---------|----------------|-----|-----|-------------------|--------------|------------|--------------------|------------------|
| 62 | -26 | 6 | device123-ssid | - | - | 00:23:69:4D:00:C0 | AP | - | 10/18/2009 3:56 AM | Wireless AP scan |
| 57 | -30 | 6 | device123-ssid | - | - | 00:23:69:4D:00:C0 | AP | - | 10/18/2009 3:58 AM | Wireless AP scan |
| 34 | -62 | 6 | device123-ssid | - | - | 00:23:69:4D:00:C0 | AP | - | 10/18/2009 4:02 AM | Wireless AP scan |
| 9 | -85 | 6 | device123-ssid | - | - | 00:23:69:4D:00:C0 | AP | - | 10/18/2009 4:02 AM | Wireless AP scan |
| 7 | -88 | 6 | device123-ssid | - | - | 00:23:69:4D:00:C0 | AP | - | 10/17/2009 6:01 PM | Wireless AP scan |



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

Important things to remember regarding the information in the device detail page are:

- Users with the role of **Admin** can see all rogue AP devices.
- Users with roles limited by folder can *see* a rogue AP if there is at least one discovering device that they can see.
- The discovery events displayed are from APs that you can see on the network. There may be additional discovery events that remain hidden.
- Each rogue device typically has multiple discovery methods, all of which are listed.
- As you work through the rogue devices, use the **Name** and **Notes** fields to identify the AP and document its location.
- You can use the global filtering options on the **RAPIDS > Setup** page to filter rogue devices according to signal strength, ad-hoc status, and discovered by remote APs.
- VisualRF uses the heard signal information to calculate the physical location of the device.
- If the device is seen on the wire, RAPIDS reports the switch and port for easy isolation.
- If you find that the rogue belongs to a neighboring business, for example, you can override the classification to a neighbor and acknowledge the device from this page. Otherwise, best practices strongly recommends that you extract the device from your building and delete the rogue device from the system.

To update a rogue device:

1. Select the device name from the list on the **RAPIDS > Rogue APs** page to launch the device detail page (see [Figure 100](#)).
2. Determine if the device has been acknowledged; acknowledge the device manually if required.
3. If an IP address is available for a given device, click the **Identify OS for Suspected Rogues** option to obtain operating system information.
4. Select the **Ignore** button if the rogue device is to be ignored.
5. Select the **Delete** button if the rogue device is to be removed from OV3600 processing.

Viewing Ignored Rogue Devices

The **RAPIDS > Rogue APs** page allows you to view ignored rogues—devices that have been removed from the rogue count displayed by OV3600. Such devices do not trigger alerts and do not display on lists of rogue devices. To display ignored rogue devices, perform the following steps.

1. From the **RAPIDS > Rogue APs** page, click **View Ignored Rogues** (at the bottom left of the page) to launch the **Ignored Rogues** page.
2. From the **Minimum Classification** drop-down menu, select the type of ignored rogue devices to display. [Table 100](#) explains the fields on this page.

Figure 101 Ignored Rogue Devices Page

Minimum Classification:

Ignored Rogues

| Ack | RAPIDS Classification | Threat Level | Name | Classifying Rule | Controller Classification | Wired | # APs hearing | SSID | Signal | RSSI | Network Type | Encryption Type |
|-----|-----------------------|--------------|----------------------|------------------|---------------------------|-------|---------------|----------------|--------|------|--------------|-----------------|
| No | Valid | - | Hewlett- Pa-ASC11-12 | (user set) | Rogue | Yes | 32 | hp-530-testing | -20 | 50 | AP | WPA |
| No | Valid | - | Aruba Netw-8938C20 | (user set) | Rogue | Yes | 36 | guest | -28 | 17 | AP | Open |
| No | Valid | - | Enterasys-36-AE-94 | (user set) | Rogue | Yes | 33 | RambleOnBG-1 | -29 | 60 | AP | Open |
| No | Valid | - | Aruba Netw-115F02 | (user set) | Rogue | - | 6 | guest | -45 | -87 | AP | WPA |
| No | Valid | - | Aruba Netw-97-E5-51 | (user set) | Rogue | - | 17 | RambleOnBG-1 | -56 | -83 | AP | WPA |

| CK | Lab Vendor | Radio Vendor | OS | Platform | IP Address | Last Discovering AP | Switch/Router | Port | Last Seen |
|----|-------------------|--------------|----|----------|------------|---------------------|---------------|-------------------|-----------|
| - | WW PCBA Test | - | - | - | - | switch10.dev.com | Fa0/2 | 4/9/2009 9:18 PM | |
| - | Aruba Networks | - | - | - | - | switch10.dev.com | Fa0/18 | 4/14/2009 9:18 AM | |
| - | Aruba Networks | - | - | - | - | switch10.dev.com | Fa0/9 | 4/14/2009 9:18 AM | |
| - | Cisco Systems | - | - | - | - | switch10.dev.com | Gi0/2 | 4/14/2009 9:18 AM | |
| - | Panix Corporation | - | - | - | 10.54.0.76 | switch10.dev.com | Eth0/46 | 4/14/2009 9:18 AM | |

Once a classification that has rogue devices is chosen from the drop-down menu, a detailed table displays all known information.

Using RAPIDS Workflow to Process Rogue Devices

One suggested workflow for using RAPIDS is as follows:

- Start from the **RAPIDS > Rogue APs** page. Sort the devices on this page based on classification type. Begin with Rogue APs, working your way through the devices listed.
- Click **Modify Devices**, then select all devices that have an IP address and select **Identify OS**. OV3600 performs a port scan on the device and attempts to determine the operating system (see [“Configuring RAPIDS” on page 190](#))

You should investigate devices running an embedded Linux OS installation. The OS scan can help identify false positives and isolate some devices that should receive the most attention.

- Find the port and switch at which the device is located and shut down the port or follow wiring to the device.
- To mitigate the rogue remove it from the network and delete the rogue record. If you want to allow it on the network, classify the device as valid and update with notes that describe it.



Be aware that not all rogue discovery methods will have all information required for resolution. For example, the switch/router information, port, or IP address are found only through switch or router polling. Furthermore, RSSI, signal, channel, SSID, WEP, or network type information only appear through wireless scanning. Such information can vary according to the device type that performs the scan.

Configuring RAPIDS

The **RAPIDS > Setup** page allows for RAPIDS configuration on your wireless network. Complete the settings on this page as desired, and click **Save**.

Using the Basic Configuration Section

On the **RAPIDS > Setup** page, the **Basic Configuration** section allows you to set RAPIDS performance settings. [Figure 102](#) illustrates this page and [Table 101](#) describes default values.

Figure 102 *RAPIDS > Setup Page Illustration*

The screenshot shows the RAPIDS > Setup page with three main sections:

- Basic Configuration:**
 - ARP IP Match Timeout (1-168 hours): 24
 - RAPIDS Export Threshold: Suspected Rogue
 - Wired-to-Wireless MAC Address Correlation (0-8 bits): 8
 - Wireless BSSID Correlation (0-8 bits): 4
 - Delete Rogues not detected for (0-30 days, zero disables): 14
 - Automatically OS Scan Rogue Devices: Yes No
- Filtering Options:**
 - Filter Ad-hoc Rogues: Yes No
 - Filter Rogues by Signal Strength: Yes No
 - Filter Rogues Discovered by Remote APs: Yes No
- Classification Options:**
 - Acknowledge Rogues by Default: Yes No
 - Manually Classifying Rogues Automatically Acknowledges Them: Yes No

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

Table 101 *RAPIDS > Setup Page Fields*

| Field | Default | Description |
|---|------------------------|---|
| Basic Configuration Section | | |
| ARP IP Match Timeout | 24 | Defines the size of the time window in which RAPIDS will correlate MAC addresses and IPs. |
| RAPIDS Export Threshold | Suspected Rogue | Advises VisualRF and the rogue XML APIs of the minimum rogue classification to display on VisualRF sites. Note that this setting does not define the classification that appears on the RAPIDS > Rogue APs page. |
| Wired-to-Wireless MAC Address Correlation (0-8 bits) | 8 | Discovered BSSIDs and LAN MAC addresses which are within this bitmask will be combined into one device. <ul style="list-style-type: none"> 4 requires all but the last digit match (aa:bb:cc:dd:ee:fx). 8 requires all but the last two digits match (aa:bb:cc:dd:ee:XX). |
| Wireless BSSID Correlation (0-8 bits) | 4 | Defines the bitmask used to correlate wireless discovery events. When neighboring devices are broadcasting multiple BSSIDs, this setting is used to determine when those BSSIDs are coming from the same device. Setting this value too high may cause RAPIDS to think 2 physical devices are actually the same device. |
| Automatically OS Scan Rogue Devices | No | Defines if RAPIDS will automatically perform an OS scan on a device when an IP address is discovered. If Yes is selected then RAPIDS will perform an OS port scan of the device to determine the operating system. |

Table 101 *RAPIDS > Setup Page Fields*

| Field | Default | Description |
|--|---------------------|---|
| Delete rogues not detected for... | 0 (disabled) | 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. |
| Automatic OS Scan Rogue Devices | Yes | Defines if RAPIDS will automatically perform an OS scan on a device when an IP address is discovered. If Yes is selected, then RAPIDS will perform an OS port scan of the device to determine the operating system. |
| Classification Options | | |
| Acknowledge Rogues by Default | No | Sets RAPIDS to acknowledge rogue devices upon initial detection, prior to their classification. |
| Manually Classifying Rogues Automatically Acknowledges them | Yes | Defines whether acknowledgement happens automatically whenever a rogue device receives classification. |
| Filtering Options | | |
| Filter ad-hoc rogues | No | Option filters rogues according to ad-hoc status. |
| Filter rogues by signal strength | No | Option filters rogues according to signal strength. It is recommended that signal strength be used as a classification criteria in the rogue rules defined on the RAPIDS > Rules page. If this filter is enabled then no information is recorded about rogues below this level. The only time this filter should be enabled is if you are running into RAPIDS performance problems. |
| Filter rogues discovered by remote APs | No | Option filters rogues according to the remote AP that discovers them. Enabling this option causes OV3600 to drop all rogue discovery information coming from Remote APs. |

Using the Classification Options Section

On the **RAPIDS > Setup** page, the **Classification Options** section allow you to categorize and sort rogue AP devices in one of several categories. The Rogue Devices report supports these rogue classifications.



Changing the controller classification pushes a reclassification message to all WLAN switches that are managed by the OV3600 server, and that are also in Groups with the **Offloading the WMS database** setting set to **Yes**. To reset the classification of a rogue device on OV3600, change the classification on the OV3600 GUI to **unclassified**.

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

Table 102 *Rogue Device Classification Matrix*

| OV3600 | AOS (ARM) |
|------------------------------|-------------------|
| Unclassified (default state) | Unknown |
| Rogue | Rogue |
| Suspected Neighbor | Interfering |
| Neighbor | Known Interfering |
| Valid | Valid |
| Contained | DOS |

Configuring Additional RAPIDS Settings in OV3600

In addition to the many settings you define with RAPIDS pages, you define additional RAPIDS settings on two other OV3600 pages, as follows:

- Use the **OV3600 Setup > Roles > Add/Edit Role Page** to define the ability to use RAPIDS by user role. Refer to “[Creating OV3600 User Roles](#)” on page 42.
- Use the **OV3600 Setup > General > Performance Tuning** page to define the processing priority of RAPIDS in relation to OV3600 as a whole (see [Table 13 on page 37](#)).

RAPIDS Rules

The **RAPIDS > Rules** is one of the core components of RAPIDS. This feature allows you to define rules by which any rogue device on the network is classified.

This section describes how to define, use, and monitor RAPIDS rules, provides examples of such rules, and demonstrates how they are helpful. This section contains the following topics:

- “[Controller Classification with WMS Offload](#)” on page 193
- “[Device OUI Score](#)” on page 193
- “[Rogue Device Threat Level](#)” on page 194
- “[Viewing and Configuring RAPIDS Rules](#)” on page 194
- “[Common RAPIDS Rules Enabled by Default](#)” on page 198
- “[Using RAPIDS Rules with Additional OV3600 Functions](#)” on page 198

Controller Classification with WMS Offload

This classification method is supported only when WMS offload is enabled on WLAN switches. Controller classification of this type remains distinct from RAPIDS classification. WLAN switches feed wireless device information to OV3600, which OV3600 then processes. OV3600 then pushes the WMS classification to all of the ArubaOS controllers that are WMS offload enabled.

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



RAPIDS classification is not pushed to the devices.

For additional information about WMS Offload, refer to the *Aruba and Alcatel-Lucent Best Practices Guide*.

Device OUI Score

The Organizationally Unique Identifier (OUI) score is based on the LAN MAC address of a device. RAPIDS can be configured to poll your routers and switches for the bridge forwarding tables. RAPIDS then takes the MAC addresses from those tables and runs them through a proprietary database to derive the OUI score.

This classification method is viewable from the **Rogue APs** tab and additional OV3600 pages. [Table 103](#) provides list the OUI scores.

Table 103 *Device OUI Scores*

| Score | Description |
|-------------------|--|
| Score of 1 | Indicates any device on the network; this is the lowest threat level on the network. |
| Score of 2 | Indicates any device in which the OUI belongs to a manufacturer that produces wireless (802.11) equipment. |
| Score of 3 | Indicates that the OUI matches a block that contains APs from vendors in the Enterprise and SOHO market. |
| Score of 4 | Indicates that the OUI matches a block that belonged to a manufacturer that produces SOHO access points. |

Rogue Device Threat Level

The threat level classification adds granularity for each general RAPIDS classification, as the two can be combined. Devices of the same classification can have differing threat scores, ranging from 1 to 10, with a default value of 5.

For example, two different devices that are both classified as **Rogue** can have differing threat scores that are based on additional parameters. This combined classification can help identify which of two rogues is likely to be a greater threat. Alerts can be defined and based on threat level; this is helpful for sorting rogue devices.

Threat level and classification are both assigned to a device when a device matches a rule. Once classified, a device's classification and threat level change only if a device is classified by a new rule or is manually changed. The threat scores can be customized via the **RAPIDS > Rules** tabs.

Viewing and Configuring RAPIDS Rules

To view the RAPIDS rules that are currently configured on OV3600, navigate to the **RAPIDS > Rules** page ([Figure 103](#)). [Table 104](#) defines the content of the **RAPIDS > Rules** page.

Figure 103 *RAPIDS > Rules Page Illustration*

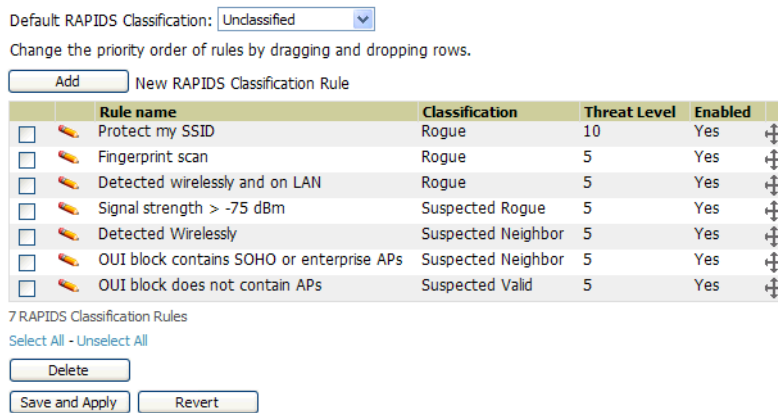



Table 104 *RAPIDS > Rules Page*

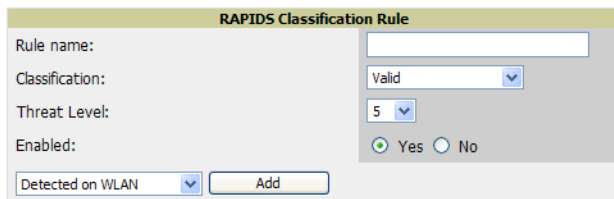
| Field | Description |
|-------------------------------|--|
| Default Classification | Sets the classification that a rogue device receives when it does not match any rules. |

Table 104 RAPIDS > Rules Page

| Field | Description |
|--|---|
| Add New RAPIDS Classification Rule | Click this button to create a RAPIDS classification rule. |
| Rule Name | Displays the name of any rule that has been configured. Rule names should be descriptive and should convey the core purpose for which it was created. |
| Classification | Displays the classification that devices receive if they meeting the rule criteria. |
| Threat Level | Displays the numeric threat level for the rogue device that pertains to the rule. Refer to “Rogue Device Threat Level” on page 194 for additional information. |
| Enabled | Displays the status of the rule, whether enabled or disabled. |
| Reorder Drag and Drop Icon  | Changes the sequence of rules in relation to each other. Click, then drag and drop, the icon for any rule to move it up or down in relation to other rules. A revised sequence of rules must be saved before rogues are classified in the revised sequence. Note: The sequence of rules is very important to proper rogue classification. A device gets classified by the first rule to which it complies, even if it conforms to additional rules later in the sequence. |

To create a new rule, select the **Add** button next to **New RAPIDS Classification Rule** to launch the **RAPIDS Classification Rule** page (see [Figure 104](#)).

Figure 104 Classification Rule Page



Fill in the settings:

- **Rule Name**—Alpha-numeric text field to enter a name for your rule. This name appears on the **RAPIDS > Rules** page, and elsewhere within OV3600 when any device is classified by the rule you create here.
- **Classification**—Sets the classification when any device matches this rule is detected.
- **Threat Level**—Sets the numeric threat level for devices that match this rule. The threat level range is 1 to 10, the default is 5. For additional information, see [“Rogue Device Threat Level” on page 194](#).
- **Enabled**—Enable or disable the rule once it is created.

[Table 106](#), [Table 106](#), and [Table 107](#) define the drop down menu options that are at the bottom left of the RAPIDS Classification Rule dialog box (see [Figure 104](#)). Once all rule settings are defined, click the **Add** button. The new rule automatically appears in the **RAPIDS > Rules** page.

Table 105 Wireless Properties Drop Down Menu


| Option | Description |
|------------------|--|
| Detected on WLAN | Classifies based on how the rogue is detected on the wireless LAN.  |

Table 105 Wireless Properties Drop Down Menu


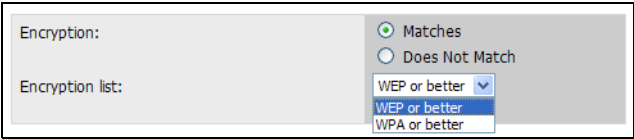
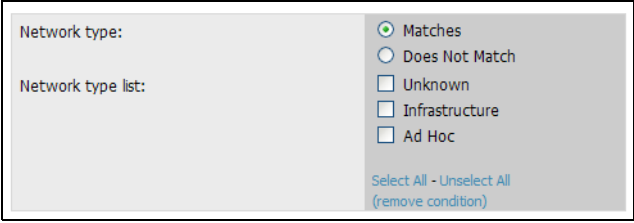
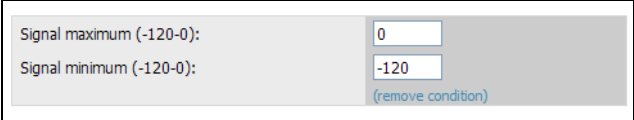
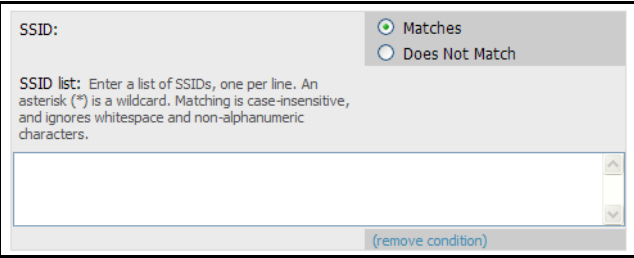
| Option | Description |
|----------------------|--|
| Discovering AP Count | <p>Classifies based on the number of managed devices that can hear the rogue. Enter a numeric value and select At Least or At Most.</p>  |
| Encryption | <p>Classifies based on the rogue matching a specified encryption method.</p>  |
| Network type | <p>Rogue is located on a specified network type, either Ad-hoc or Infrastructure.</p>  |
| Signal Strength | <p>Rogue matches signal strength parameters. Specify a minimum and maximum value in DBm.</p>  |
| SSID | <p>Classifies the rogue when it matches or does not match the specified string for the SSID.</p>  <p>Note: For SSID matching functions, OV3600 processes only alpha-numeric characters and the asterisk wildcard character (*). OV3600 ignores all other non-alpha-numeric characters. For example, the string of ethersphere-* matches the SSID of ethersphere-wpa2 but also the SSID of ethersphere_this_is_an_example (without any dashes).</p> |

Table 106 Wireline Properties Drop Down Menu

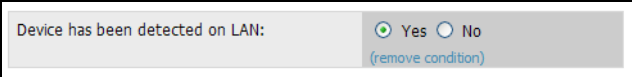
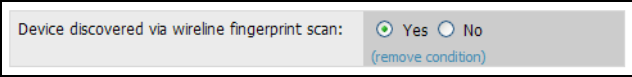
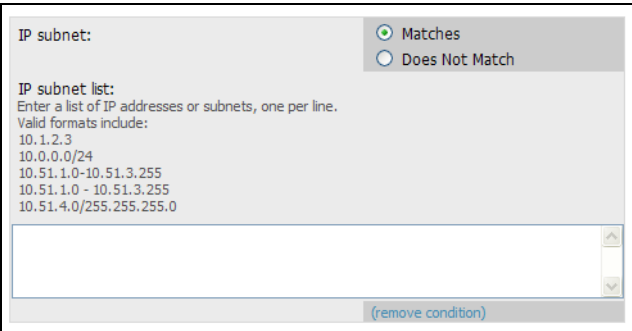
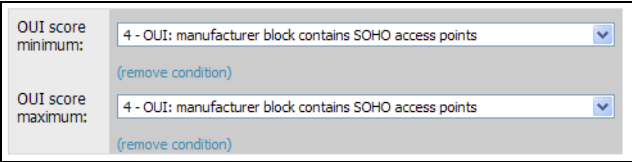
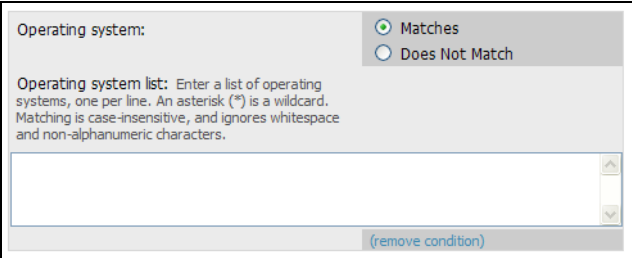
| Option | Description |
|------------------|---|
| Detected on LAN | <p>Rogue is detected on the wired network. Select Yes or No.</p>  |
| Fingerprint Scan | <p>Rogue matches fingerprint parameters.</p>  |
| IP Address | <p>Rogue matches a specified IP address or subnet. Enter IP address or subnet information as explained by the fields.</p>  |
| OUI Score | <p>Rogue matches manufacturer OUI criteria. You can specify minimum and maximum OUI score settings from two drop-down lists. Click remove to remove one or both criteria, as desired.</p>  |
| Operating System | <p>Rogue matches OS criteria. Specify matching or non-matching OS criteria as prompted by the fields.</p>  |

Table 107 Wires/Wireline Properties Drop Down Menu

| Option | Description |
|--------------|---|
| Manufacturer | Rogue matches the manufacturer information of the rogue device. <div data-bbox="734 331 1364 588" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Manufacturer: <input checked="" type="radio"/> Matches <input type="radio"/> Does Not Match</p> <p>Manufacturer list: Enter a list of manufacturers, one per line. An asterisk (*) is a wildcard. Matching is case-insensitive, and ignores whitespace and non-alphanumeric characters.</p> <div style="border: 1px solid gray; height: 20px; width: 100%;"></div> <p style="text-align: right;">(remove condition)</p> </div> |

Deleting or Editing a Rules

To delete a rule, select the check box next to the rule you want to delete, and click the **Delete** button. The rule is automatically deleted from the **RAPIDS > Rules** page.

To edit any existing rule, click the pencil icon next to that rule to launch the **RAPIDS Classification Rule** page (see [Figure 104](#)). Edit or revise the fields (see [Table 106](#)) as necessary then select the Save button.

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

Common RAPIDS Rules Enabled by Default

If Any Device Has Your SSID, Then Classify as Rogue

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

If Any Device Has Your SSID and is Not an Ad-Hoc Network Type, Then Classify as Rogue

This rule classifies a device as a rogue when the SSID for a given device is your SSID and is not an Ad-Hoc device. Windows XP automatically tries to create an Ad-hoc network if it can not find the SSID for which it is searching. This means that user's laptops on your network may appear as Ad-Hoc devices that are broadcasting your SSID. If this happens too frequently, you can restrict the rule to apply to non-ad-hoc devices.

If More Than Four APs Have Discovered a Device, Then Classify as Rogue

By default, OV3600 tries to use Signal Strength to determine if a device is on your premises. Hearing device count is another metric that can be used.

The important concept in this scenario is that legitimate neighboring devices are only heard by a few APs on the edge of your network. Devices that are heard by a large number of your APs are likely to be in the heart of your campus. This rule works best for scenarios in large campuses or that occupy an entire building. For additional rules that may help you in your specific network scenario, contact Alcatel-Lucent Technical Support or refer to the [Alcatel-Lucent Wireless Knowledge Base](#).

Using RAPIDS Rules with Additional OV3600 Functions

Rules that you configure on the **RAPIDS > Rules** page establish an important way of processing rogue devices on your network, and flagging them for attention as required. Such devices appear on the following pages in OV3600, with additional information:

- **RAPIDS > Rogue APs**—Lists rogue devices as classified by rules.
- **RAPIDS > Rules**—Displays the rules that classify rogue devices.
- **RAPIDS > Overview**—Displays general rogue device count and statistical information.
- **System > Triggers**—Displays triggers that are currently configured, including any triggers that have been defined for rogue events.
- **Reports > Definitions**—Allows you to run New Rogue Devices Report with custom settings.
- **VisualRF**—Displays physical location information for rogue devices.

The RAPIDS OUI Score Override

On **RAPIDS > Score Override** page you can change the scores that are given to MAC addresses detected during scans of bridge forwarding tables on routers or switches. [Figure 105](#), [Figure 106](#), and [Table 108](#) illustrate and describe RAPIDS Score Override. Perform these steps to create a score override.

The **RAPIDS > Score Override** page allows you to override the score assigned to a MAC address prefix by Alcatel-Lucent. If you have devices that receive a higher score than they 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 rescoreing 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.

1. Navigate to the **RAPIDS > Score Override** page. This page lists all existing overrides if they have been created.

Figure 105 *RAPIDS > Score Override Page*

The Score Override feature allows you to change the scores that are given to MAC addresses detected during scans of switch bridge forwarding tables.

| | MAC Address Prefix | Vendor | Score |
|--------------------------|--------------------|-------------------------------|--|
| <input type="checkbox"/> | 00:02:2D | Agere Systems | 2 - OUI: manufacturer block contains wireless clients, WiFi tags or scanners |
| <input type="checkbox"/> | 00:02:6F | Senao International Co., Ltd. | 4 - OUI: manufacturer block contains SOHO access points |
| <input type="checkbox"/> | 00:03:03 | JAMA Electronics Co., Ltd. | 3 - OUI: manufacturer block contains enterprise access points |
| <input type="checkbox"/> | 00:0D:54 | 3COM | 4 - OUI: manufacturer block contains SOHO access points |
| <input type="checkbox"/> | 00:10:40 | INTERMEC CORPORATION | 1 - Any device on the network not categorized with a higher score |
| <input type="checkbox"/> | 00:13:72 | Dell | 1 - Any device on the network not categorized with a higher score |
| <input type="checkbox"/> | 00:14:69 | Cisco | 4 - OUI: manufacturer block contains SOHO access points |
| <input type="checkbox"/> | 00:15:2B | Cisco Systems | 4 - OUI: manufacturer block contains SOHO access points |
| <input type="checkbox"/> | 00:30:65 | Apple Computer | 3 - OUI: manufacturer block contains enterprise access points |
| <input type="checkbox"/> | 00:30:89 | Spectrapoint Wireless, LLC | 4 - OUI: manufacturer block contains SOHO access points |
| <input type="checkbox"/> | 00:CO:49 | U.S. ROBOTICS, INC. | 4 - OUI: manufacturer block contains SOHO access points |

2. Click **Add** to create a new override or click the pencil icon next to an existing override to edit that override. The **Score Override** add or edit page appears([Figure 106](#)).

Figure 106 *Add/Edit Score Override Page*

Score Override

MAC Address Prefix:

Score:

- 4 - OUI: manufacturer block contains SOHO access points
- 3 - OUI: manufacturer block contains enterprise access points
- 2 - OUI: manufacturer block contains wireless clients, WiFi tags or scanners
- 1 - Any device on the network not categorized with a higher score

Table 108 *RAPIDS > Add/Edit Score Override Page Fields*

| Field | Description |
|---------------------------|---|
| MAC Address Prefix | Use this field to define the OUI prefix to be re-scored. |
| Score | Use this field to set the score that a device, with the specified MAC address prefix, will receive. |

3. Enter in the six-digit MAC prefix for which to define a score, and select the desired score. Once the new score has been saved, all detected devices with that prefix receive the new score.
4. Click **Add** to create the new override, or click **Save** to retain changes to an existing override. The new or revised override appears on the **RAPIDS > Score Override** page.
5. To remove any override, select that override in the checkbox and click **Delete**.

Introduction

Daily WLAN administration often entails network monitoring, supporting WLAN and OV3600 users, and monitoring OV3600 system operations. This chapter contains the following administration procedures:

Creating and Using Triggers and Alerts

- Overview of Triggers and Alerts
- Viewing Triggers
- Creating New Triggers
- Viewing Alerts
- Responding to Alerts

Monitoring and Supporting WLAN Users

- Overview of the Users Pages
- Monitoring WLAN Users With the Users > Connected and Users > All Pages
- Supporting Users on Thin AP Networks With the Users > Tags Page
- Supporting Guest WLAN Users With the Users > Guest Users Page

Evaluating and Diagnosing User Status and Issues

- Evaluating User Status with the Users > User Detail Page
- Evaluating User Status with the Users > Diagnostics Page

Supporting OV3600 Stations with the Master Console

Monitoring and Supporting OV3600 with the Home Pages

- Monitoring OV3600 with the Home > Overview Page
- Viewing and Updating License Information with the Home > License Page
- Searching OV3600 with the Home > Search Page
- Accessing OV3600 Documentation with the Home > Documentation Page
- Configuring Your Own User Information with the Home > User Info Page

Monitoring and Supporting OV3600 with the 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

Upgrading OV3600

- Upgrade Instructions
- Upgrading Without Internet Access

Backing Up OV3600

- Overview of Backups
- Viewing and Downloading Backups
- Running Backup on Demand
- Restoring from a Backup
- OV3600 Failover

- Adding Watched OV3600 Stations

Creating and Using Triggers and Alerts

This section describes triggers and alerts with the following topics:

- Overview of Triggers and Alerts
- Viewing Triggers
- Creating New Triggers
- Delivering Triggered Alerts
- Viewing Alerts
- Responding to Alerts

Overview of Triggers and Alerts

OV3600 monitors key aspects of wireless LAN performance. When certain parameters or conditions arise that are outside normal bounds, OV3600 generates (or triggers) alerts that enable you to address problems quickly, frequently before users have a chance to report them. OV3600 deploys two types of alerts:

Viewing Triggers

To view defined system triggers, navigate to the **System > Triggers** page. [Figure 107](#) illustrates this page.

Figure 107 System > Triggers Page Illustration (Split View)

Triggers:

New Trigger

| Type | Trigger | Additional Notification Options | NMS Trap Destinations |
|--|---|---------------------------------|-----------------------|
| <input type="checkbox"/> Device Resources | Percent CPU Utilization >= 85 % for 15 | Email | - |
| <input type="checkbox"/> Device Up | Device Type is Access Point | - | - |
| <input type="checkbox"/> Inactive Tag | for >= 2 hrs 0 mins | - | - |
| <input type="checkbox"/> Device IDS Events | Count > 100 for 30 minutes | - | - |
| <input type="checkbox"/> New User | New User Association | NMS | 10.51.1.7 |
| <input type="checkbox"/> Device Down | All device types | NMS | - |
| <input type="checkbox"/> Device RADIUS Authentication Issues | Count >= 20 for 15 secs | NMS | 10.51.1.7 |
| <input type="checkbox"/> 802.11 Frame Counters | WEP Undecryptable Rate >= 100 frames/sec for 1 hour | - | - |
| <input type="checkbox"/> Rogue Device Classified | Classification = Rogue | NMS | 10.51.1.7 |
| <input type="checkbox"/> Radio Down | - | NMS | 10.51.1.7 |

12 Triggers

Select All - Unselect All

| Severity | Folder | Group | Include Subfolders | Logged Alert Visibility | Suppress Until Acknowledged |
|----------|--------|---------|--------------------|-------------------------|-----------------------------|
| Warning | Top | - | Yes | By Role | Yes |
| Warning | Top | - | Yes | By Role | Yes |
| Normal | Top | - | Yes | By Role | - |
| Normal | Top | - | Yes | By Role | Yes |
| Normal | Top | Outdoor | Yes | By Role | - |
| Normal | Top | - | Yes | By Role | Yes |
| Normal | Top | - | Yes | By Role | Yes |
| Normal | Top | - | Yes | By Role | - |
| Minor | Top | - | Yes | By Role | - |
| Major | Top | - | Yes | By Role | Yes |

No Triggers for other roles found.

Creating New Triggers

Perform the following steps to create and configure one or more new triggers. These steps define settings that are required for any type of trigger.

1. To create a new trigger, click the **Add New Trigger** button from the **System > Triggers** page. OV3600 launches the **Trigger Detail** page, illustrated in [Figure 108](#).

Figure 108 System > Trigger Detail Page Illustration

2. Configure the **Trigger Restrictions** and **Alert Notifications**. This configuration is consistent regardless of the trigger type to be defined.
 - a. Configure the **Trigger Restrictions** settings. This establishes how widely or how narrowly the trigger applies. Define the folder, subfolder, and Group covered by this trigger. [Table 109](#) describes the options for trigger restrictions.

Table 109 System > Trigger Details Fields and Default Values

| Notification Option | Description |
|---------------------------|---|
| Folder | Sets the trigger to apply only to APs/Devices in the specified folder or subfolders depending on the Include Subfolders option. NOTE: If the trigger is restricted by folder and group, it only applies to the intersection of the two—it only applies to APs in the group and in the folder. |
| Include Subfolders | Sets the trigger to apply to all devices in the specified folder and all of the devices in folders under the specified folder. |
| Group | Sets the trigger to apply only to APs/Devices in the specified group. NOTE: If the trigger is restricted by folder and group, it only applies to the intersection of the two—it only applies to APs in the group and in the folder. |

- b. Configure the **Alert Notifications** settings. In addition to appearing on the **System > Triggers** page, triggers can be configured to distribute to email or to a network management system (NMS), or to both.
 - If you select **email**, you are prompted to set the sender’s email address and recipient email addresses.
 - If you select **NMS**, you are prompted to provide the IP address of the **NMS Trap Destinations**.
 - Define the **Logged Alert Visibility**, in which you can choose how this trigger is distributed. The trigger can distribute according to how is it generated (triggering agent), or by the role with which it is associated.

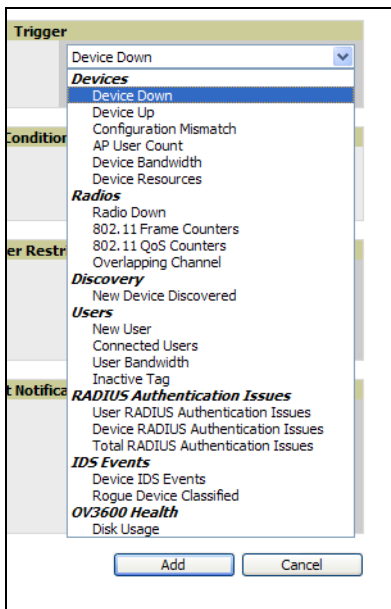
- The **Suppress Until Acknowledged** setting defines whether the trigger requires manual and administrative acknowledgement to gain visibility.

Table 110 System > Trigger Condition Detail Alert Notifications for Defined Alerts

| Notification Option | Description |
|---|--|
| Notification Type | Selects the action OV3600 should take when an alert is triggered. When the NMS checkbox is checked OV3600 sends an SNMP trap to the NMS servers defined for the role. When the Email checkbox is selected, OV3600 sends an email to the specified address. |
| Sender Address | Displays the originator's email address in the From field of alert emails. NOTE: This field is only visible if the Email checkbox is selected. |
| Recipient Email Addresses | Displays the user, users or distribution lists that receive any email alerts. NOTE: This field is only visible if the Email checkbox is selected. |
| Logged Alert Visibility | Defines which users are able to view the alerts. When limited by role only users with the same role as the creator of the alert will be able to view it. When limited by triggering agent, any user who can view the device can view the alert. |
| Suppress new alerts until current alerts are acknowledged/ deleted | Determines how often a trigger will fire. When No is selected a new alert will be created every time the trigger criteria are met. When Yes is selected an alert will only be received the first time the criteria is met. A new alert for the AP/device is not created until the initial one is acknowledged. |

3. In the **Trigger** field, choose the desired trigger **Type** and the desired **Severity**, according to your needs. [Figure 109](#) illustrates the trigger types supported in OV3600. Severity levels are included in the email alerts. The alert summary information at the top of the OV3600 screen can be configured to separately display severe alerts. Please see the **Home > User Info** section for more details.

Figure 109 System > Triggers > Add Trigger Type Drop-down Menu



Once you have selected a trigger type, the **Add Trigger** page changes. In many cases, you must configure at least one **Condition** setting. Conditions, settings, and default values vary according to trigger type.

Complete the creation of your trigger type using one of the following procedures for each trigger:

- “Setting Triggers for Devices” on page 205
- “Setting Triggers for Radios” on page 206
- “Setting Triggers for Discovery” on page 208

- “Setting Triggers for Users” on page 209
- “Setting Triggers for RADIUS Authentication Issues” on page 211
- “Setting Triggers for IDS Events” on page 212
- “Setting Triggers for OV3600 Health” on page 213

Setting Triggers for Devices

After completing steps 1-3 in “Creating New Triggers” on page 202, 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 109](#). [Table 111](#) itemizes and describes device trigger options and condition settings.

Table 111 *Devices Trigger Types*

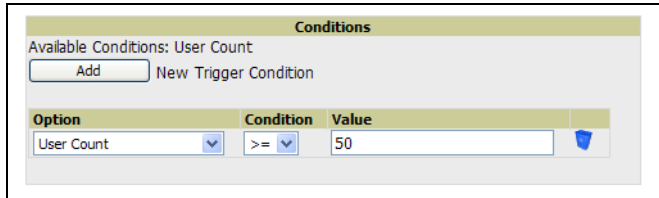
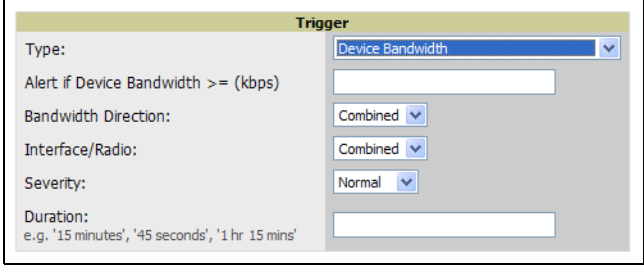
| Devices Trigger Options | Description |
|-------------------------------|--|
| Device Down | <p>This is the default type whenever configuring a new trigger. This type of trigger activates when an authorized, managed AP has failed to respond to SNMP queries from OV3600.</p> <p>To set the conditions 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 device type. Multiple conditions can apply to this type of trigger.</p> |
| Device Up | <p>This trigger type activates when an authorized, previously down AP is now responding to SNMP queries.</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. Multiple conditions can apply to this type of trigger.</p> |
| Configuration Mismatch | <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> |
| AP User Count | <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 110 <i>Sample of Trigger Condition for AP Device User Count</i></p>  |

Table 111 *Devices Trigger Types*

| Devices Trigger Options | Description |
|--------------------------------|---|
| <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 111 Trigger Type Section for Device Bandwidth Type</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 202. ● Duration—The Duration level is likely defined already from an earlier step in this procedure. See “Creating New Triggers” on page 202. |
| <p>Device Resources</p> | <p>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.</p> |

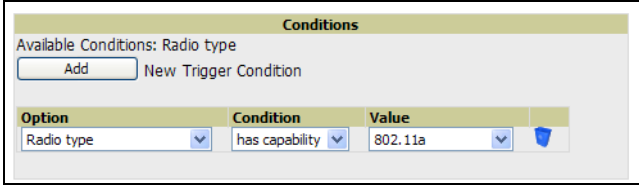
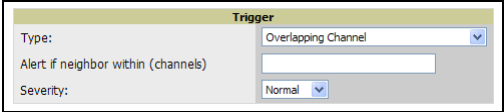
- Delete conditions as desired by clicking the trash can icon to the right of the condition to be removed.
- Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.
- You can edit or delete any trigger as desired from the **System > Triggers** page.
 - 📎 To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in [Table 111](#).
 - 🗑️ To delete a trigger, check the box next to the trigger to remove, and click **Delete**.
- Repeat this procedure for as many triggers and conditions as desired. Refer to the start of [“Creating New Triggers” on page 202](#) to create a new trigger.

Setting Triggers for Radios

After completing steps 1-3 in [“Creating New Triggers” on page 202](#), perform the following steps to complete the configuration of radio-related triggers.

- a. If you have not already done so, choose a trigger type from the **Radios** category, listed in the **Type** drop-down menu. [Table 112](#) itemizes and describes the Radios-related trigger types, and condition settings for each.

Table 112 *Radio-Related Trigger Types*

| Radio Trigger Options | Description |
|-------------------------------------|---|
| <p>Radio Down</p> | <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 112 <i>Sample of Trigger Condition for Radio Type</i></p>  |
| <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.</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>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 113 <i>Trigger Type Section for Overlapping Channel Type</i></p>  <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.

- d. To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in [Table 111](#).
- d. 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 202](#) to create a new trigger.

Setting Triggers for Discovery

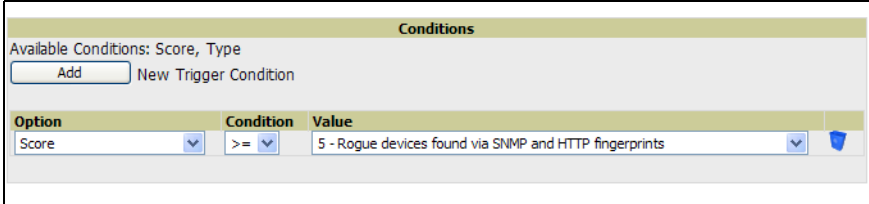
After completing steps 1-3 in [“Creating New Triggers” on page 202](#), perform the following steps to complete the configuration of triggers related to device discovery.



- 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 109](#). [Table 113](#) itemizes and describes the Discovery-related trigger types, and condition settings for each discovery trigger type.

Table 113 *Discovery Trigger Types and Condition Settings*

| Discovery Trigger Options | Description | | | | | | | | |
|-------------------------------|--|---------|----------------------------------|-------|--|------------|----------------|---------|----------------------------------|
| New Devices Discovered | <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. The following example illustrates the Add Condition section for a New Devices Discovered trigger.</p> <p>Figure 114 <i>Sample of Condition for New Device Discovered Trigger Type</i></p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <div style="background-color: #D9E1F2; padding: 2px; text-align: center;">Conditions</div> <p>Available Conditions: Radio type</p> <p style="text-align: right;"><input type="button" value="Add"/> New Trigger Condition</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #D9E1F2;">Option</th> <th style="background-color: #D9E1F2;">Condition</th> <th style="background-color: #D9E1F2;">Value</th> <th style="background-color: #D9E1F2;"></th> </tr> </thead> <tbody> <tr> <td>Radio type</td> <td>has capability</td> <td>802.11a</td> <td style="text-align: center;"><input type="button" value="X"/></td> </tr> </tbody> </table> </div> | Option | Condition | Value | | Radio type | has capability | 802.11a | <input type="button" value="X"/> |
| Option | Condition | Value | | | | | | | |
| Radio type | has capability | 802.11a | <input type="button" value="X"/> | | | | | | |

Table 113 *Discovery Trigger Types and Condition Settings (Continued)*

| Discovery Trigger Options | Description |
|----------------------------------|---|
| New Rogue Device Detected | <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 “Using RAPIDS and Rogue Classification” on page 183 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 115 <i>Sample of Trigger Condition for A Rogue Detected Trigger</i></p>  |

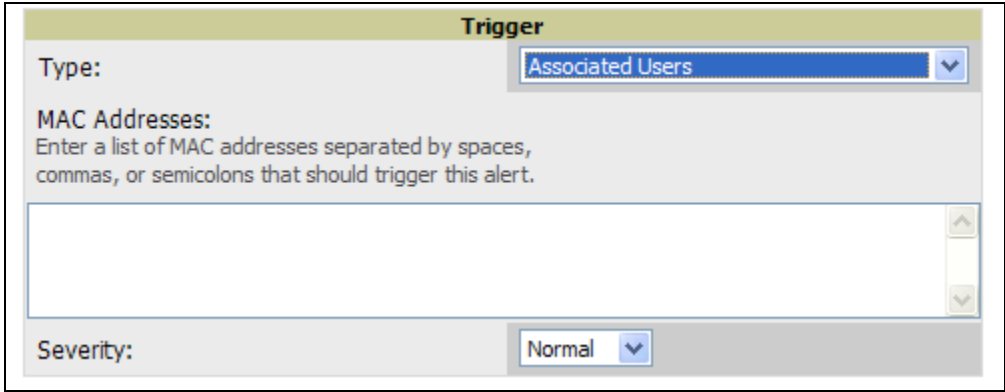
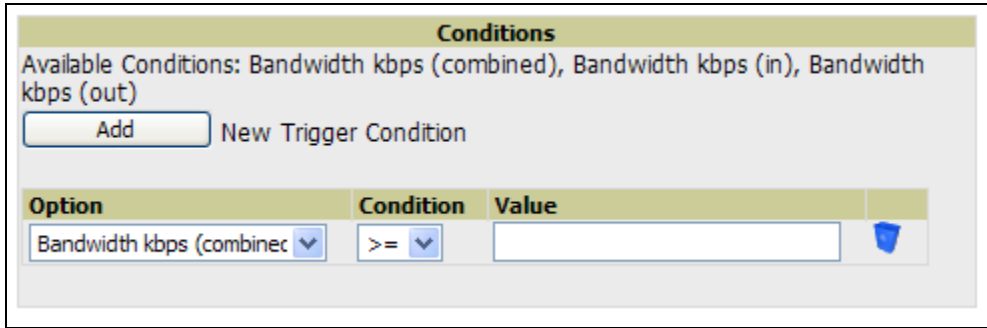
- b. Delete conditions as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.
- d. You can edit or delete any trigger as desired from the **System > 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 111.
 -  To delete a trigger, check the box next to the trigger to remove, and click **Delete**.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of “Creating New Triggers” on page 202 to create a new trigger.

Setting Triggers for Users

After completing steps 1-3 in “Creating New Triggers” on page 202, 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 109. Table 114 itemizes and describes the User-related trigger types, and condition settings for each discovery trigger type.

Table 114 *User Trigger Types and Condition Settings*

| User Trigger Option | Description |
|--------------------------------|--|
| <p>New User</p> | <p>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.</p> |
| <p>Associated Users</p> | <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 116 <i>Example of Associated User Configuration Section</i></p>  |
| <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 117 <i>Sample of User Bandwidth Trigger Condition</i></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 111](#).
 - ☞ To delete a trigger, check the box next to the trigger to remove, and click **Delete**.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of “[Creating New Triggers](#)” on page 202 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 202, 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 109](#). [Table 115](#) itemizes and describes the condition settings for each **RADIUS Authentication** trigger type.

Figure 118 RADIUS Authentication Trigger Condition Settings

Table 115 RADIUS Authentication Trigger Types and Condition Settings

| RADIUS Trigger Options | Description |
|--|---|
| User RADIUS Authentication Issues | This trigger type sets the threshold for the maximum number of failures before an alert is issued for a user. Click Add New Trigger Condition to specify the count characteristics that trigger an alert. The Option , Condition , and Value fields allow you to define the numeric value of user issues. |
| Device RADIUS Authentication Issues | This trigger type sets the threshold for the maximum number of failures before an alert is issued for a device. The Option , Condition , and Value fields allow you to define the numeric value of device issues. |
| Total RADIUS Authentication Issues | This trigger sets the threshold for the maximum number of failures before an alert is issued for both users and devices. The Option , Condition , and Value fields allow you to define the numeric value of device and user issues combined. |

- b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.

- d. You can edit or delete any trigger as desired from the **System > Triggers** page.
 - To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in [Table 111](#).
 - To delete a trigger, check the box next to the trigger to remove, and click **Delete**.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of “[Creating New Triggers](#)” on page 202 to create a new trigger.

Setting Triggers for IDS Events

After completing steps 1-3 in “[Creating New Triggers](#)” on page 202, perform the following steps to complete the configuration of Intrusion Detection System (IDS)-related triggers.

- a. If you have not already done so, choose the **Device IDS Events** trigger type from the drop-down **Type** menu. See [Figure 109](#). [Table 116](#) describes condition settings for this trigger type.

Table 116 Device IDS Events Authentication Trigger Types and Condition Settings

| IDS Trigger Options | Description | | | | | | | | |
|--------------------------|--|--------|-----------|-------|--|-------|----|--|--|
| Device IDS Events | <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 style="text-align: center;">Figure 119 IDS Events Trigger Condition Settings</p> <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #D9E1F2;"> <th>Option</th> <th>Condition</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>Count</td> <td>>=</td> <td></td> <td></td> </tr> </tbody> </table> </div> | Option | Condition | Value | | Count | >= | | |
| Option | Condition | Value | | | | | | | |
| Count | >= | | | | | | | | |

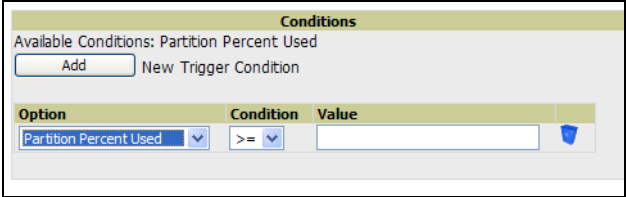
- b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click **Save**. The trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.
- d. You can edit or delete any trigger as desired from the **System > Triggers** page.
 - To edit an existing trigger, click the **Pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in [Table 111](#).
 - To delete a trigger, check the box next to the trigger to remove, and click **Delete**.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of “[Creating New Triggers](#)” on page 202 to create a new trigger.

Setting Triggers for OV3600 Health

After completing steps 1-3 in “Creating New Triggers” on page 202, 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 109](#) for trigger types. [Table 117](#) describes the condition settings for this trigger type.

Table 117 *Disk Usage Trigger and Condition Settings*

| OV3600 Health Trigger | Description |
|-----------------------|---|
| Disk Usage | <p>This trigger type is based on the disk usage of the OV3600 (OV3600) system. This type of trigger indicates that disk usage for the OV3600 server has met or surpassed a defined threshold.</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 120 <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 111](#).
 - To delete a trigger, check the box next to the trigger to remove, and click **Delete**.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of “Creating New Triggers” on page 202 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

OV3600 displays alerts and provides additional alert details in two ways, as follows:

1. The **Alerts Summary** table is one way to monitor and process OV3600 alerts. The **Alert Summary** table is available on the following OV3600 pages, and is illustrated in [Figure 121](#):

- **APs/Devices > List**
- **Groups > Monitor**
- **Home > Overview**
- **Users > Connected**
- **Users > User Detail**

Figure 121 *Alert Summary Table Illustration*

| Alert Summary at 8/13/2009 10:16 AM | | | | |
|-------------------------------------|--------------|----------|-------|--------------------|
| Type ▲ | Last 2 Hours | Last Day | Total | Last Event |
| System Alerts | 6 | 100 | 216 | 8/13/2009 9:23 AM |
| IDS Events | 0 | 14 | 40 | 8/13/2009 4:24 AM |
| Incidents | 0 | 0 | 7 | 7/15/2009 12:32 PM |
| RADIUS Authentication Issues | 45 | 358 | 760 | 8/13/2009 10:08 AM |

This table displays alerts as follows; click the alert **Type** to display alert details:

- **OV3600 Alerts**—Displays details for all device alerts.
- **IDS Events**—Displays details of all Intrusion Detection System (IDS) events and attacks.
- **Incidents**—Displays recent helpdesk incidents in which the incidents are open and associated to an AP. For a complete listing of incidents, navigate to the **Helpdesk > Incidents** page.



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

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

- **RADIUS Authentication Issues**—Displays RADIUS-related alerts for devices in the top viewable folder available to the OV3600 user. The detailed list displays the MAC address, username, AP, radio, controller, RADIUS server, and time of each event. Alerts can be sorted by any column.

2. The second way to display and process alerts is to use the **Alerts** and **Severe Alerts** counters in the **Status** bar at the top of all OV3600 pages, illustrated in [Figure 122](#).

Figure 122 *Alerts in the OV3600 Status Bar*

| | | | | | | | |
|-----------------|---------|-----------|-----------------|------------|------------|-------------|--------------------|
| New Devices: 29 | Up: 349 | Down: 176 | Mismatched: 132 | Rogue: 484 | Users: 213 | Alerts: 217 | Severe Alerts: 217 |
|-----------------|---------|-----------|-----------------|------------|------------|-------------|--------------------|

Click the **Alerts** or the **Severe Alerts** counter or navigate to the **System > Alerts** page. [Figure 123](#) illustrates this page.

Figure 123 *System > Alerts Page Illustration*

| | Trigger Type | Trigger Summary | Triggering Agent | Time ▼ | Severity |
|--------------------------|------------------------|-----------------------------|---------------------|--------------------|----------|
| <input type="checkbox"/> | User Bandwidth | > = 100 kbps for 30 seconds | 00:18:DE:09:89:09 | 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 118](#).

Table 118 *System > Alerts Fields and Default Settings*

| Field | Description |
|-------------------------|---|
| Trigger Type | Displays and sorts triggers by the type of trigger. |
| Trigger Summary | Provides an additional summary information related to the trigger. |
| Triggering Agent | Lists the name of the AP that generated the trigger. Clicking the AP name to display the APs/Devices > Manage page for that AP. |
| Time | Displays the date and time the trigger was generated. |
| Severity | Displays the severity code associated with that trigger. |

Responding to Alerts

Once you have viewed an alert, you may take one of the following courses of action:

- Leave it in active status if it is unresolved. The alert remains on the **New Alerts** list until you acknowledge or delete it. If an alert already exists, the trigger for that AP or user does not create another alert until the existing alert has been acknowledged or deleted. For example, if device AP 7 exceeds a maximum bandwidth trigger, that trigger does not create another alert for AP 7 until the first alert is recognized.
- Move the alert to the Alert Log by selecting the alert and clicking the **Acknowledge** button at the bottom of the page.
- You may see all logged alerts by clicking the **View logged alerts** link at the top of the **System > Alerts** page. Click the **New Alerts** link to return to the list of new alerts.
- Delete the alert by selecting the alert from the list and clicking the **Delete** button at the bottom of the **System > Alerts** page.

Monitoring and Supporting WLAN Users

The OV3600 **Users** pages support WLAN users in OV3600. This section describes the **Users** pages as follows:

- [Overview of the Users Pages](#)
- [Monitoring WLAN Users With the Users > Connected and Users > All Pages](#)
- [Supporting Guest WLAN Users With the Users > Guest Users Page](#)
- [Supporting Users on Thin AP Networks With the Users > Tags Page](#)
- See also [Evaluating and Diagnosing User Status and Issues](#).

For information about creating OV3600 users and OV3600 user roles, refer to the following sections in this guide:

- [Creating OV3600 Users](#)
- [Creating OV3600 User Roles](#)

If you need to create an OV3600 user account for frontline personnel who are to support Guest WLAN users, refer to “[Supporting Guest WLAN Users With the Users > Guest Users Page](#)” on page 218.

Overview of the Users Pages

The **Users** pages display multiple types of user data for existing WLAN users. The data comes from a number of locations, including data tables on the access points, information from RADIUS accounting servers, and OV3600-generated data. OV3600 supports the following **Users** pages:

- **Users > Connected**—Displays active users that are currently connected to the WLAN. For additional information, refer to “[Monitoring WLAN Users With the Users > Connected and Users > All Pages](#)” on page 216.
- **Users > All**—Displays all users of which OV3600 is aware, with related information. Non-active users are listed in gray text. For a description of the information supported on this page, refer to “[Monitoring WLAN Users With the Users > Connected and Users > All Pages](#)” on page 216.
- **Users > Guest Users**—Displays all guest users in OV3600 and allows you to create, edit, or delete guest users. See “[Supporting Guest WLAN Users With the Users > Guest Users Page](#)” on page 218.
- **Users > User Detail**—Displays client device information, alerts, signal quality, bandwidth, and association history. This page appears when you select a user’s MAC address from one of the following pages:
 - **Users > Connected**
 - **Users > All**
 - **Home > Search** page results or **Search** field results that display the user MAC addressSee “[Evaluating and Diagnosing User Status and Issues](#)” on page 222.
- **Users > Diagnostics**—Displays possible client device issues, diagnostic summary data, user counts, AP information, 802.11 counters summary, and additional information. This page appears when you select a user’s MAC address from one of the following pages:
 - **Users > Connected**
 - **Users > All**
 - **Home > Search** page results or **Search** field results that display the user MAC addressSee “[Evaluating and Diagnosing User Status and Issues](#)” on page 222.
- **Users > Tags**—Displays a list of wireless tags, such as Aeroscout, PanGo and Newbury, that are heard by thin APs, and reported back to a controller that is monitored by OV3600. OV3600 displays the information it receives from the controller in a table on this page. “[Supporting Users on Thin AP Networks With the Users > Tags Page](#)” on page 221.

Monitoring WLAN Users With the Users > Connected and Users > All Pages

The **Users > Connected** page displays all users currently connected in OV3600, and is illustrated in [Figure 124](#) and described in [Table 119](#). The information displayed on this page can be adjusted in the following ways:

- You can expand or customize the graphics to show maximum users, maximum average users, and additional custom view options.
- You can expand bandwidth to include custom view options.
- You can display all users, a specific number of users per page, or another custom setting.
- The Alerts section displays custom configured alerts that were defined in the **System > Alerts** page.

OV3600 enhances the **Users > Connection** page to include SSID information for users. This enhancement applies to additional graph-based pages in OV3600. Furthermore, the **Users > Connected** page can display wired users using remote Access Point (RAP) devices in tunnel and split-tunnel mode.



Data that was gathered prior to an upgrade may be reported under an **unknown** SSID.

Figure 124 Users > Connected Page Illustration

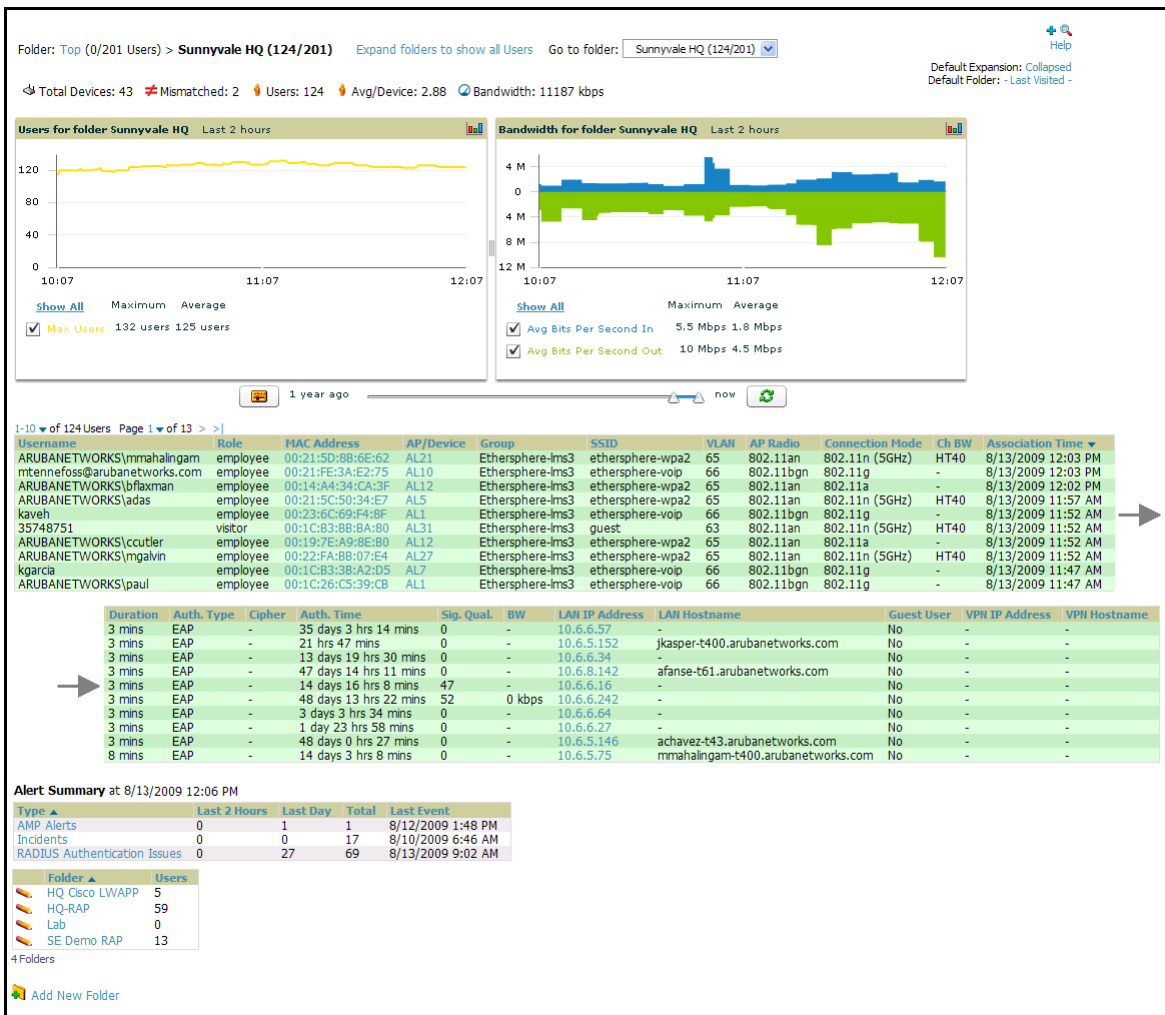


Table 119 Users > Connected Fields and Default Values

| Field | Description |
|--------------------|---|
| Username | Displays the name of the User associated to the AP. OV3600 gathers this data in a variety of ways. It can be taken from RADIUS accounting data, traps from Cisco VxWorks APs and tables on Colubris APs. Usernames appear in italics when a username for that MAC address has been stored in the database from a previous association, but OV3600 is not getting a username for the current association. This may indicate that the user has not yet been authenticated for this session (as indicated if you mouse over the username) or OV3600 may not be getting a username from an external source like a RADIUS server for this association. |
| Role | Specifies the role by which the user is connected. |
| MAC Address | Displays the radio MAC address of the user associated to the AP. Also displays a link that redirects to the Users > Detail page. |
| AP/Device | Displays the name of the AP to which the MAC address is associated Also displays a link that takes you to this AP's Monitoring page. |
| Group | Displays the group containing the AP that the user is associated with. |
| SSID | Displays the SSID with which the user is associated. |
| VLAN | Displays the VLAN assigned to the user. |

Table 119 Users > Connected Fields and Default Values (Continued)

| Field | Description |
|-------------------------|---|
| AP Radio | Displays the radio type of the radio that the user is associated with. |
| Connection Mode | Displays the 802.11 mode by which the user is connected. |
| Ch BW | Displays the channel bandwidth that currently supports 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 | <p>Displays the type of authentication employed by the user: EAP, PPTP, RADIUS accounting, or not authenticated.</p> <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 | <p>Displays WEP with keys. Cipher options are as follows:</p> <ul style="list-style-type: none"> • WEP with 802.11x • WPA PSK (TKIP) • WPA with 802.11x • WPA2 PSK (AES) • WPA2 with 802.11x (AES) <p>This data is also displayed in the User Session report.</p> |
| Auth. Time | Displays the how long ago the user authenticated. |
| Signal Quality | Displays the average signal quality the user enjoyed. |
| BW | Displays the average bandwidth consumed by the MAC address. |
| Location | Displays the QuickView box allows users to view features including heatmap for a device and location history for a user. |
| LAN IP | Displays the IP assigned to the user MAC. This information is not always available. OV3600 can gather it from the association table of Colubris APs or from the ARP cache of switches set up in OV3600. |
| LAN Hostname | Displays the LAN hostname of the user MAC. |
| Guest User | Specifies whether the user is a guest or not. |
| VPN IP | Displays the VPN IP of the user MAC. This information can be obtained from VPN servers that send RADIUS accounting packets to OV3600. |
| VPN Hostname | Displays the VPN hostname of the user MAC. |

Supporting Guest WLAN Users With the Users > Guest Users Page

Overview of the Users > Guest Users Page

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

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

1. Navigate to the **OV3600 Setup > Roles** page and create a new role of the type **Guest Access Sponsor**. Click **Add New Role**, select this role type, and enter a role name. Also, select the top folder for which this role should have access. [Figure 125](#) illustrates this page.

Figure 125 OV3600 Setup > Roles Page Illustration

2. Next, navigate to the **OV3600 Setup > Users** page and create a new user with the role that was just created for **Guest Access Sponsors**. [Figure 126](#) illustrates this page.

Figure 126 OV3600 Setup > Users Page Illustration

3. The newly created login information should be provided to the person or people who will be responsible for creating guest access users. Anyone with an Admin role can also create guest access users.
4. The next step in creating a guest access user is to navigate to the **Users > Guest Users** tab. From this tab, you can add new guest users, you can edit existing users, and you can repair guest user errors.

This page displays a list of guest users and data, to include the expiration date, the SSID (for Cisco WLC) and other information. [Figure 127](#) illustrates this page and [Table 120](#) describes the fields and information displayed.

Figure 127 Users > Guest Users Page Illustration

Guest Users:

New Guest User

1-4 ▼ of 4 Guest Users Page 1 ▼ of 1

| | Username | Enabled | Email | Company Name | Sponsor Name | Expiration | Profile ▼ | Status |
|--------------------------|----------|---------|-------------------|---------------|--------------|--------------------|-----------|-----------------------------|
| <input type="checkbox"/> | rzajnnqw | Yes | vfranc@airess.com | Airess | vfranc | Never | - | Error - Failed to Configure |
| <input type="checkbox"/> | zserkxmm | Yes | - | - | bob | Never | - | Error - Failed to Configure |
| <input type="checkbox"/> | bobo | No | bobo@nowhere.com | arus networks | arus | 5/27/2009 12:00 AM | - | User Expired |
| <input type="checkbox"/> | jestwrqg | Yes | - | - | Oriol | 6/5/2009 12:00 PM | - | User Expired |

Select All - Unselect All

Table 120 Users > Guest Users Fields

| Field | Description |
|--|---|
| Repair Guest User Errors button | Sets OV3600 to attempt to push the guest user again in an attempt to repair any errors in the Status column. |
| Add New Guest Users button | Adds a new guest user to a controller via OV3600. |
| Username | Randomly generates a user name for privacy protection. This name appears on the Guest User detail page. |
| Enabled | Enables or disables the user status. Set the status of the guest user as active (enabled) or expired (disabled). Configure the user on the Guest User edit page by clicking the pencil icon. |
| Email | Displays the optional email address of the user. Set the email address with the Guest User edit page by clicking the pencil icon. |
| Company Name | Displays the optional company name for the user. Set the company name with the Guest User edit page by clicking the pencil icon. |
| Sponsor Name | Displays the name of the sponsor for the guest user. This setting is optional. Set the sponsor with the Guest User edit page by clicking the pencil icon. |
| Expiration | Displays the date the guest user's access is to expire. Set the expiration with the Guest User edit page by clicking the pencil icon. |
| Profile/SSID | Sets the SSID that the guest user can access. This setting applies to Cisco WLC only. Set the SSID with the Guest User edit page by clicking the pencil icon. |
| Status | Reports current status by the controller. If error messages appear in this column, select the user with the checkbox at left, and click the Repair guest user errors button. |
| Print button (for checked users) | Sends the selected guest user's information to an external printer. |
| Delete button (for checked users) | Removes the selected guest user from OV3600 and from the controller. |

Guest users associated to the wireless network appear on the same list as other wireless users, but are identified as guest users in the **SSID** column, when this column is present for Cisco WLC. The **User Detail** page for a guest user also contains a box with the same guest information that appears for each user on the **Users > Guest Users** list.

- To add a new guest user, click **Add**, and complete the required and optional fields in the **User Detail** page, illustrated in [Figure 128](#). [Table 120](#) describes most fields. The first three fields are required, and the remaining fields are optional.

Figure 128 Users > Guest Users > Add New Guest User Page Illustration

Guest User

Username:

Password:

Enabled: Yes No

Email:

Company Name:

Sponsor Name:

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.

Expiration: Blank means no expiration

Description:

To make the **Username** or **Password** anonymous and to increase security, complete these fields then click **Generate**. The anonymous and secure **Username** and **Password** appear in the respective fields.

- Click **Add** to complete the new guest user, or click **Cancel** to back out of new user creation. The **Users > Guest Users** page appears and displays results, as applicable.

Supporting Users on Thin AP Networks With the Users > Tags Page

Radio Frequency Identification (RFID) is an industry-standard method that supports identifying and tracking wireless devices with radio waves. RFID uses radio wave tags for these and additional functions. Active tags have a battery and transmit signals autonomously, and passive tags have no battery. RFID tags often support additional and proprietary innovations that improve network integration, battery life, and other functions.

The **Users > Tags** page displays a list of wireless tags, such as Aeroscout, PanGo and Newbury, that are heard by thin APs, and reported back to a controller that OV3600 monitors. OV3600 displays the information it receives from the controller in a table on this page. [Figure 129](#) illustrates this page, and [Table 121](#) describes fields and information displayed.

Figure 129 Users > Tags Page Illustration

Tags

1-5 of 5 Tags Page 1 of 1

| 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 121 Users > Tags Fields

| Field | Description |
|----------------------|--|
| Name | Displays the user-editable name associated with the tag. |
| MAC Address | Displays the MAC address of the AP that reported the tag. |
| Vendor | Displays the vendor of the tag (Aeroscout, PanGo and Newbury)—display all or filter by type. |
| Battery Level | Displays battery information—filterable in drop-down menu at the top of the column; is not displayed for Aeroscout tags. |

Table 121 Users > Tags Fields

| Field | Description |
|-----------------------|---|
| Chirp Interval | Displays the tag chirp frequency or interval, filterable from the drop-down menu at the top of the column. Note that the chirp interval from the RFID tag influences the battery life of active tags as well as search times. If a tag chirps with very long chirp interval, it may take longer time for the location engine to accurately measure x and y coordinates. |
| Last Seen | Date and time the tag was last reported to OV3600. |
| Closest AP | The AP that last reported the tag to the controller (linked to the AP'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 [“Creating and Using Triggers and Alerts”](#) on page 202.

Evaluating and Diagnosing User Status and Issues

If a WLAN user reports difficulty with the wireless network, the administration or Helpdesk personnel can view and process related user information from the **User Detail** and **Diagnostic** pages. This section describes these two pages as follows:

- [Evaluating User Status with the Users > User Detail Page](#)
- [Evaluating User Status with the Users > Diagnostics Page](#)

Evaluating User Status with the Users > User Detail Page

The **Users > User Detail** page is a focused sub-menu that becomes visible when you select a specific user. Access the **Users > User Detail** page in one of the following ways:

- Click the MAC Address for a specific user from one of the following pages:
 - **Users > Connected**
 - **Users > All**
- Search for a user and click the associated MAC address in the search results, then select the **User Detail** page from the navigation pane.

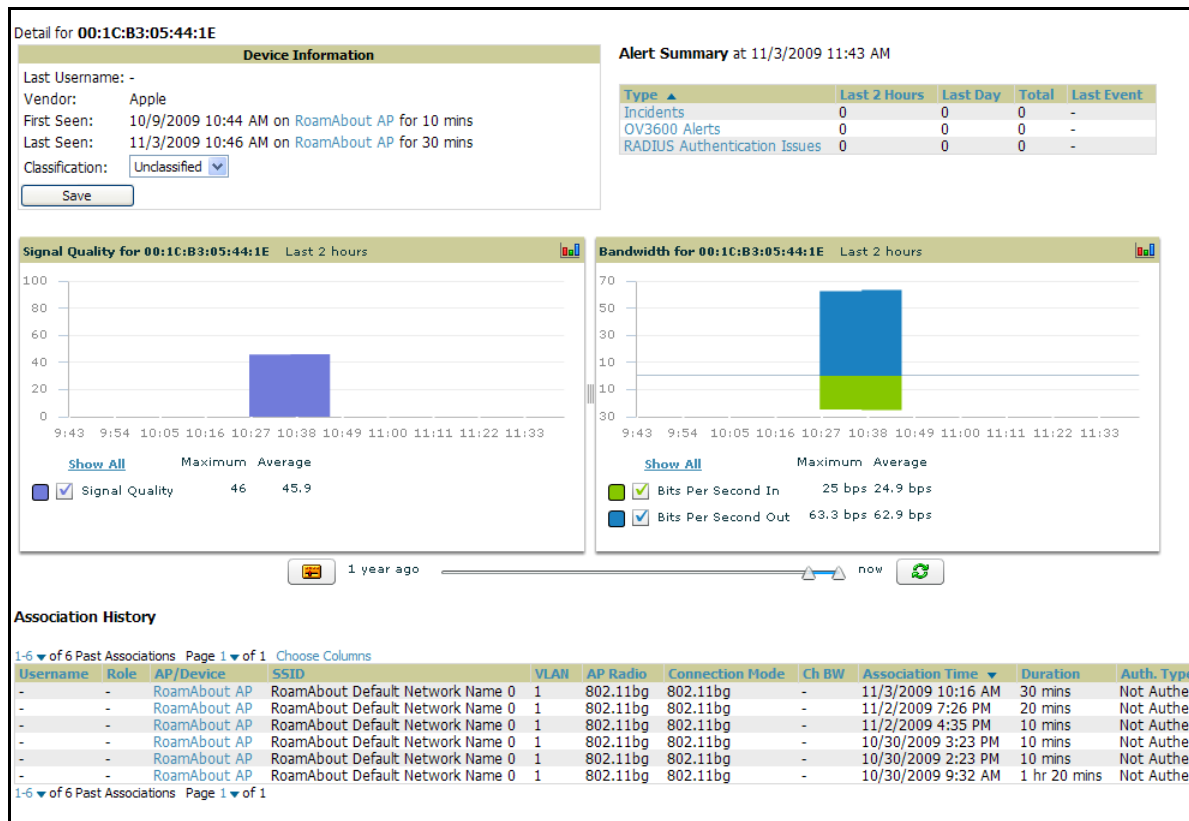
[Figure 130](#) illustrates the contents of **Users > User Details** page.

This page provides information for the wireless device, signal quality, and bandwidth consumption. This page also provides an AP association history and current association status. Finally, when VisualRF is licensed and enabled, this page provides a graphical map of the user location and facility information.

If you have deployed WLAN switches and have WMS offload enabled on the network, the **Users > User Detail** page allows you to classify the device in the **Device Information** section, and to push this configuration to the WLAN switches that govern the devices. The classifications are as follows:

- **Unclassified**—Devices are unclassified by default.
- **Valid**—Designates the device as a legitimate network device. Once this **Valid** setting is pushed to the WLAN switch, and if the **Protect Valid Stations** option is also enabled on the switch, then this setting prevents valid stations from connecting to a non-valid AP.
- **Contained**—Controls the user on the device, as defined with containment configurations set with WMS Offload in AOS.

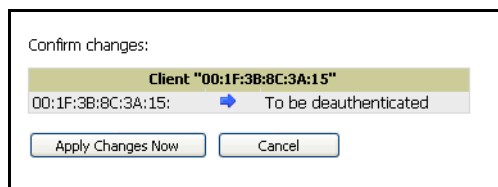
Figure 130 *Users > User Detail Page Illustration*



Using the Deauthenticate User Feature

Some displays of the **User > User Detail** page includes the **Deauthenticate User** feature in the **Current Association** field. Click the **Deauthenticate User** button to use this feature. Refer to [Figure 131](#) as an illustration:

Figure 131 *Users > User Detail > Deauthenticate User Page:*



Evaluating User Status with the Users > Diagnostics Page

Introduction and Overview of the Diagnostics Page

The **Users > Diagnostics** page is a focused sub-menu that becomes visible when you select user-specific information. Access the **Users > Diagnostics** page in one of the following ways:

- Click the MAC Address for a specific user from one of the following pages:
 - **Users > Connected**
 - **Users > All**
- You can search for a user and click the associated MAC address from the search results.

This page provides an overview of a user's general status and connectivity on the network.

Each section of the **Users > Diagnostics** page displays information by which to evaluate possible user issues. Refer to [Table 122](#) for explanation and illustration of page components.

Table 122 Users > Diagnostics Page Sections

| Section | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|-------------------|--|--|-------|-------|--------|---------------------|-------|----------|--------------------------------------|-------------|---|----------------------|--------------------------|----------------|-----------------------|---------------|-----|-----------------------------|-------|-----------|--------------------------|--------------------------|-------------------|--|------|---|---|------|----------|----------------------|--------|---|
| Possible Issues | <p>This section summarizes the most likely items to create issues for a user on the network. Figure 132 illustrates this section.</p> <p>Figure 132 Groups > Diagnostics > Possible Issues Illustration</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #D9EAD3;"> <th colspan="3">Possible Issues</th> </tr> <tr> <th style="text-align: left;">Issue</th> <th style="text-align: left;">Ideal</th> <th style="text-align: left;">Actual</th> </tr> </thead> <tbody> <tr> <td>Low signal quality:</td> <td>>= 20</td> <td>0</td> </tr> <tr> <td>Excessive roaming in last two hours:</td> <td><= 10 roams</td> <td>0</td> </tr> <tr> <td>High user bandwidth:</td> <td><= 50% of radio capacity</td> <td>0 kbps (0.00%)</td> </tr> <tr> <td>Unauthenticated user:</td> <td>Authenticated</td> <td>EAP</td> </tr> <tr> <td>High user load on AP/radio:</td> <td><= 15</td> <td>26</td> </tr> <tr> <td>High AP/radio bandwidth:</td> <td><= 75% of radio capacity</td> <td>1910 kbps (0.77%)</td> </tr> <tr> <td>802.11b users associated to 802.11g radio:</td> <td>None</td> <td>0</td> </tr> <tr> <td>802.11g or 802.11a users associated to 802.11n radio:</td> <td>None</td> <td>5</td> </tr> <tr> <td>High FCS error rate:</td> <td><= 100</td> <td>0</td> </tr> </tbody> </table> <ul style="list-style-type: none"> ● Low signal quality—If signal quality falls outside of ideal range, then possible resolution might be installation of more or better antennas on the APs, adding APs, increasing the transmit power of the APs, investigating intermittent RF interference, such as the startup schedule of a nearby air conditioning unit, or evaluating the client settings. ● Excessive roaming in last 2 hours—Roaming means that a user’s connection moves from one AP to another. Excessive roaming is generally classified as 10 or more roaming instances in the past two hours. If there is excessive roaming, but the user has been stationary, then the user might be located where there is weak coverage from two overlapping APs. In this case, adjusting the signal strength for one of those APs may resolve the issue. ● High User Bandwidth—If a user reports issues with network performance, the issue could derive from excessive bandwidth consumption. Additionally, another user on the same AP might be consuming excessive bandwidth. In that latter case, investigate user bandwidth consumption for all users on a given AP, not strictly the user who reports an issue. ● Unauthenticated User—This section conveys the user’s current authentication status and the actual authentication type. If a network deploys RADIUS authentication, then the RADIUS server could be experiencing issues even if a user attempts to log in with valid authentication credentials but shows as Unauthenticated on this page. ● High user load on AP/radio—This field indicates if the number of users on a given AP has exceeded that AP’s functional capacity. Excessive users on an AP could degrade performance for all users on that AP. Some users will start to experience performance issues, may start to drop off, You may need to add an additional AP in that area, or take other steps to distribute the user load more evenly across multiple APs. Refer to the Current User Counts section on this page for additional details. ● High AP radio bandwidth—This figure derives from how groups of users share radio bandwidth on a shared AP. You may get a high figure in this category if nearby APs have gone down. You may not need to add an additional AP to resolve this issue, but you would need to determine why neighboring APs are not functioning properly. ● 802.11 radio parameters—These two sections indicate the likelihood that a user’s issues are derived from mismatched 802.11 deployment. That is, an 802.11ab or g user who is connected through an 802.11n radio might not benefit from full 802.11n functionality. These two fields indicate the likelihood of such an issue impacting a user’s experience on the network. | Possible Issues | | | Issue | Ideal | Actual | Low signal quality: | >= 20 | 0 | Excessive roaming in last two hours: | <= 10 roams | 0 | High user bandwidth: | <= 50% of radio capacity | 0 kbps (0.00%) | Unauthenticated user: | Authenticated | EAP | High user load on AP/radio: | <= 15 | 26 | High AP/radio bandwidth: | <= 75% of radio capacity | 1910 kbps (0.77%) | 802.11b users associated to 802.11g radio: | None | 0 | 802.11g or 802.11a users associated to 802.11n radio: | None | 5 | High FCS error rate: | <= 100 | 0 |
| Possible Issues | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Issue | Ideal | Actual | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Low signal quality: | >= 20 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Excessive roaming in last two hours: | <= 10 roams | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| High user bandwidth: | <= 50% of radio capacity | 0 kbps (0.00%) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Unauthenticated user: | Authenticated | EAP | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| High user load on AP/radio: | <= 15 | 26 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| High AP/radio bandwidth: | <= 75% of radio capacity | 1910 kbps (0.77%) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 802.11b users associated to 802.11g radio: | None | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 802.11g or 802.11a users associated to 802.11n radio: | None | 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| High FCS error rate: | <= 100 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Table 122 Users > Diagnostics Page Sections

| Section | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--------------------|-------------------|---------------------|---------------------|--|--|--|---------|-----------|--------------|--------------|--------------|----------------|----------------|-----------------|------------------|------------------|------------------|-----------------|-------------------|-------------------|-------------------|---------------------|---------------------|--------------|-------------------|-------------------|-------------------|--------------------|--------------------|------------------|----|----|----|----|----|---------------|----|----|----|----|----|----------------|---|----|----|----|----|
| <p>Possible Issues (Cont'd)</p> | <ul style="list-style-type: none"> <p>High FCS error rates—Frame Check Sequence (FCS) errors indicate that frames of data that transmit across the network are experiencing corruption. A high FCS error rate indicates wireless link interference in the area.</p> <p>Frames that are transmitted by APs managed in OV3600 are susceptible to interference from other devices with radios operating in the same frequencies range (same channel), or electromagnetic interference from electronic devices such as power cables in the office.</p> <p>The 802.11 MAC layer uses the Frame Check Sequence (FCS) field to determine if errors have occurred during the transmission. Each MAC layer frame has a FCS field that is used to store a checksum. The checksum is added at the source AP, and verified at the destination.</p> <p>If the FCS checksum included in the frame does not match the recalculated number, then an error has occurred during the transmission, the frame is discarded, and the destination host requests it to be resent. This can effectively reduce the bandwidth and throughput in the network.</p> <p>A high FCS error rate in this field could indicate that the APs are experiencing a high level of link interference and the clients are getting less bandwidth and throughput due to MAC layer frame retransmissions.</p> <p>One response is to assign a different channel to the AP to improve the performance from your OV3600 server. Use the Optimize feature to assign the best available channel to the AP.</p> <ol style="list-style-type: none"> Log in to your OV3600. From the AP/Devices > List page, click the Modify Devices link. Select the APs that are running into channel interference problems by checking the corresponding box for each. Several new settings appear below the device list by which to configure these devices. Toward the bottom of this section, click Optimize for the Optimize channel assignment to reduce overlap setting. A confirm changes page appears by which to apply and schedule this change, or to cancel out of this setting. <p>NOTE: This explanation derived from the following location:</p> <ul style="list-style-type: none"> <i>Airheads Online Forum</i>, explanation by bjacobs: http://airheads.arubanetworks.com/vBulletin/showthread.php?p=1266#post1266 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>Diagnostics Summary</p> | <p>This section summarizes bandwidth, user count, and signal quality parameters for specific windows of time. This section is useful when diagnosis or troubleshooting follows issues that had been observed a few or several hours prior. Figure 133 illustrates this section.</p> <p>Figure 133 Users > Diagnostics > Diagnostics Summary Illustration (Partial Display)</p> <table border="1" data-bbox="500 1381 1455 1598"> <thead> <tr> <th colspan="6">Diagnostic Summary</th> </tr> <tr> <th></th> <th>Current</th> <th>Last Hour</th> <th>Last 2 Hours</th> <th>Last 4 Hours</th> <th>Last 8 Hours</th> </tr> </thead> <tbody> <tr> <td>User Bandwidth</td> <td>0 kbps (0.00%)</td> <td>69 kbps (0.03%)</td> <td>121 kbps (0.05%)</td> <td>198 kbps (0.08%)</td> <td>198 kbps (0.08%)</td> </tr> <tr> <td>Radio Bandwidth</td> <td>1910 kbps (0.77%)</td> <td>4377 kbps (1.76%)</td> <td>4377 kbps (1.76%)</td> <td>33963 kbps (13.69%)</td> <td>33963 kbps (13.69%)</td> </tr> <tr> <td>AP Bandwidth</td> <td>1911 kbps (0.39%)</td> <td>4377 kbps (0.88%)</td> <td>4377 kbps (0.88%)</td> <td>33963 kbps (6.85%)</td> <td>33963 kbps (6.85%)</td> </tr> <tr> <td>Radio User Count</td> <td>19</td> <td>20</td> <td>20</td> <td>20</td> <td>20</td> </tr> <tr> <td>AP User Count</td> <td>26</td> <td>27</td> <td>27</td> <td>27</td> <td>27</td> </tr> <tr> <td>Signal Quality</td> <td>0</td> <td>50</td> <td>50</td> <td>49</td> <td>49</td> </tr> </tbody> </table> <p>The following categories link to additional details pages:</p> <ul style="list-style-type: none"> User Bandwidth—click this link to display flash graphs for user bandwidth metrics. Radio Bandwidth—click this link to display flash graphs for radio bandwidth consumption. AP Bandwidth—click this link to display flash graphs for AP bandwidth consumption. Radio User Count—click this link to display flash graphs for user count metrics. AP User Count—click this link to display flash graphs for user count metrics. Signal Quality—click this link to display flash graphs for signal quality. | Diagnostic Summary | | | | | | | Current | Last Hour | Last 2 Hours | Last 4 Hours | Last 8 Hours | User Bandwidth | 0 kbps (0.00%) | 69 kbps (0.03%) | 121 kbps (0.05%) | 198 kbps (0.08%) | 198 kbps (0.08%) | Radio Bandwidth | 1910 kbps (0.77%) | 4377 kbps (1.76%) | 4377 kbps (1.76%) | 33963 kbps (13.69%) | 33963 kbps (13.69%) | AP Bandwidth | 1911 kbps (0.39%) | 4377 kbps (0.88%) | 4377 kbps (0.88%) | 33963 kbps (6.85%) | 33963 kbps (6.85%) | Radio User Count | 19 | 20 | 20 | 20 | 20 | AP User Count | 26 | 27 | 27 | 27 | 27 | Signal Quality | 0 | 50 | 50 | 49 | 49 |
| Diagnostic Summary | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Current | Last Hour | Last 2 Hours | Last 4 Hours | Last 8 Hours | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| User Bandwidth | 0 kbps (0.00%) | 69 kbps (0.03%) | 121 kbps (0.05%) | 198 kbps (0.08%) | 198 kbps (0.08%) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Radio Bandwidth | 1910 kbps (0.77%) | 4377 kbps (1.76%) | 4377 kbps (1.76%) | 33963 kbps (13.69%) | 33963 kbps (13.69%) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AP Bandwidth | 1911 kbps (0.39%) | 4377 kbps (0.88%) | 4377 kbps (0.88%) | 33963 kbps (6.85%) | 33963 kbps (6.85%) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Radio User Count | 19 | 20 | 20 | 20 | 20 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AP User Count | 26 | 27 | 27 | 27 | 27 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Signal Quality | 0 | 50 | 50 | 49 | 49 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Table 122 *Users > Diagnostics Page Sections*

| Section | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--------------------------------|------------|------------------|-----------------------|---------------------|---------------------|---------|-----------|----------|----------------|------------|------------------|---------|---------------------|------|----------|----|----|------------------|-----------------------|----------|-------------------|----------|----------------------|-----------|------------|-----------------------|--------------|------------------------|----------------|------------|---|---|-----------------------|----|
| <p>Current User Counts</p> | <p>The Current User Counts section displays user counts for APs and radios, and includes additional summary information for APs. Figure 134 illustrates this section:</p> <p>Figure 134 <i>Users > Diagnostics > Current User Counts Illustration</i></p> <div data-bbox="500 348 984 653" data-label="Table"> <table border="1"> <thead> <tr> <th colspan="3">Current User Counts</th> </tr> <tr> <th></th> <th>User Count on AP</th> <th>User Count on Radio</th> </tr> </thead> <tbody> <tr> <td>802.11a</td> <td>4</td> <td>0</td> </tr> <tr> <td>802.11n (5GHz)</td> <td>6</td> <td>0</td> </tr> <tr> <td>802.11g</td> <td>10</td> <td>10</td> </tr> <tr> <td>Total</td> <td>20</td> <td>10</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="2">AP Information</th> </tr> </thead> <tbody> <tr> <td>Name:</td> <td>AL1</td> </tr> <tr> <td>Uptime:</td> <td>1 day 15 hrs 44 mins</td> </tr> <tr> <td>Location:</td> <td>-</td> </tr> <tr> <td>Type:</td> <td>Aruba AP 125</td> </tr> <tr> <td>Controller IP Address:</td> <td>10.252.252.252</td> </tr> </tbody> </table> </div> <p>Use this section in combination with the Possible Issues section.</p> | Current User Counts | | | | User Count on AP | User Count on Radio | 802.11a | 4 | 0 | 802.11n (5GHz) | 6 | 0 | 802.11g | 10 | 10 | Total | 20 | 10 | AP Information | | Name: | AL1 | Uptime: | 1 day 15 hrs 44 mins | Location: | - | Type: | Aruba AP 125 | Controller IP Address: | 10.252.252.252 | | | | | |
| Current User Counts | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | User Count on AP | User Count on Radio | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 802.11a | 4 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 802.11n (5GHz) | 6 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 802.11g | 10 | 10 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Total | 20 | 10 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AP Information | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Name: | AL1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Uptime: | 1 day 15 hrs 44 mins | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Location: | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Type: | Aruba AP 125 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Controller IP Address: | 10.252.252.252 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>802.11 Counters Summary</p> | <p>The 802.11 Counters Summary section conveys the same information that is available from the Radio Statistics link from the APs/Devices > Monitor page. Figure 135 illustrates this section.</p> <p>Figure 135 <i>Users > Diagnostics > 802.1 Counters Summary Illustration</i></p> <div data-bbox="500 877 984 1073" data-label="Table"> <table border="1"> <thead> <tr> <th colspan="5">802.11 Counters Summary</th> </tr> <tr> <th></th> <th>Current</th> <th>Last Hour</th> <th>Last Day</th> <th>Last Week</th> </tr> </thead> <tbody> <tr> <td>Unacked</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Retries</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Failures</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Dup Frames</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>FCS Errors</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table> </div> <p>NOTE: This section is supported for Cisco devices. OV3600 does not gather device counter information from certain other device vendors.</p> <p>For additional information, click a Cisco device from the APs/Devices > List page, and on the Monitor page for that device, click Statistics. The ensuing page displays the 802.11 Counters Summary table, which summarizes counters on the AP level. Scroll down on this page to convey additional information from which the counters summary on the Diagnostics page is derived. Some of the sections on the Statistics page only populate when there is a user when an associated user is generating traffic on the network. Other sections convey information if there is no user associated and the device is strictly listening for traffic.</p> | 802.11 Counters Summary | | | | | | Current | Last Hour | Last Day | Last Week | Unacked | 0 | 0 | 0 | 0 | Retries | 0 | 0 | 0 | 0 | Failures | 0 | 0 | 0 | 0 | Dup Frames | 0 | 0 | 0 | 0 | FCS Errors | 0 | 0 | 0 | 0 |
| 802.11 Counters Summary | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Current | Last Hour | Last Day | Last Week | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Unacked | 0 | 0 | 0 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Retries | 0 | 0 | 0 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Failures | 0 | 0 | 0 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Dup Frames | 0 | 0 | 0 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FCS Errors | 0 | 0 | 0 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>Radios That Can Hear This User</p> | <p>The Radios That Can Hear This User section summarizes the AP correspondence to Radios, with SNR values, user count metrics, bandwidth consumption and additional information that collectively describe the user's device-level activity on the network. Figure 136 illustrates this section.</p> <p>Figure 136 <i>Users > Diagnostics > Radios That Can Hear This User Illustration</i></p> <div data-bbox="500 1549 1406 1696" data-label="Table"> <table border="1"> <thead> <tr> <th colspan="7">Radios That Can Hear This User</th> </tr> <tr> <th>AP</th> <th>Radio</th> <th>SNR</th> <th>User Count</th> <th>Bandwidth (kbps)</th> <th>Uptime</th> <th>Recently Associated</th> </tr> </thead> <tbody> <tr> <td>AL39</td> <td>802.11an</td> <td>25</td> <td>2</td> <td>0.93712090369561</td> <td>8 days 16 hrs 12 mins</td> <td>No</td> </tr> <tr> <td>00:1a:1e:c0:55:46</td> <td>802.11an</td> <td>26</td> <td>0</td> <td>0</td> <td>32 days 12 hrs 5 mins</td> <td>No</td> </tr> <tr> <td>AL30</td> <td>802.11an</td> <td>24</td> <td>0</td> <td>0</td> <td>8 days 14 hrs 56 mins</td> <td>No</td> </tr> </tbody> </table> </div> | Radios That Can Hear This User | | | | | | | AP | Radio | SNR | User Count | Bandwidth (kbps) | Uptime | Recently Associated | AL39 | 802.11an | 25 | 2 | 0.93712090369561 | 8 days 16 hrs 12 mins | No | 00:1a:1e:c0:55:46 | 802.11an | 26 | 0 | 0 | 32 days 12 hrs 5 mins | No | AL30 | 802.11an | 24 | 0 | 0 | 8 days 14 hrs 56 mins | No |
| Radios That Can Hear This User | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AP | Radio | SNR | User Count | Bandwidth (kbps) | Uptime | Recently Associated | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AL39 | 802.11an | 25 | 2 | 0.93712090369561 | 8 days 16 hrs 12 mins | No | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 00:1a:1e:c0:55:46 | 802.11an | 26 | 0 | 0 | 32 days 12 hrs 5 mins | No | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AL30 | 802.11an | 24 | 0 | 0 | 8 days 14 hrs 56 mins | No | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Supporting OV3600 Stations with the Master Console

The **Master Console** (MC) is used to monitor multiple OV3600 stations from one central location. The **Master Console** is designed for customers running multiple OV3600 servers. Once an OV3600 station has been added to the MC, it will be polled for basic OV3600 information.

- Reports can be run from the **Master Console** to display information from multiple OV3600 stations; because such reports can be extremely large, reports can also be run as **summary only** so that they generate more quickly and finish as a manageable file size.
- The **Master Console** can also be used to populate group-level configuration on managed OV3600 installations using the **Global Groups** feature.
- The **Master Console** supports:
 - The **Master Console** offers a display of devices that are in a **down** or **error** state, anywhere on the network. This information is supported on **Master Console** pages that display device lists, to include **Home > Overview**, **APs Devices > List**, **RAPIDS > Rogue APs**, and additional such pages.
 - The **Public Portal** of the **Master Console** supports configuration of the iPhone interface. This can be configured using the **Master Console OV3600** page. See “[Defining General OV3600 Server Settings](#)” on [page 32](#).
 - The **Master Console** and **Failover** servers can be configured with a **Device Down** trigger that generates an alert if communication is lost to a managed or watched OV3600 station. In addition to generating an alert, the **Master Console** or **Failover** server can also send email or NMS notifications about the event. See “[Creating and Using Triggers and Alerts](#)” on [page 202](#).



The license key determines if the server will behave as a **Master Console** or as a standard OV3600 server.

The **Master Console** also contains an optional Public Portal, which allows any user to view basic group-level data for each managed OV3600. This feature is disabled by default for security reasons, no OV3600 or **Master Console** login is required to view the public portal. It can be enabled by navigating to the **OV3600 Setup > General** and then to the **Master Console** section. Once enabled, a new Portal tab will appear to the right of the **Groups** tab. The URL of the public portal will be <https://your.OV3600.name/public>. Upon upgrading to OV3600 6.4, the public portal is disabled by default, regardless of the type of license.

Much like the normal **Home > Overview** page, the **Master Console Home > Overview** page provides summary statistics for the entire network at a glance.

Adding a Managed OV3600 with the Master Console

Perform the following steps to add a managed OV3600 console.

1. Navigate to the **Home > Managed OV3600s** page.
2. Click the **Pencil Icon** to edit or reconfigure an existing OV3600 console.
3. Click the **Add New Managed OV3600** button to create a new OV3600 console. The **Managed OV3600** page appears. Complete the settings on this page as described in [Table 123](#).

Table 123 *Master Console > Manage OV3600s > IP/Hostname Fields and Default Values*

| Field | Default | Description |
|-----------------------|-----------|---|
| Hostname / IP Address | N/A | Enter the IP address or Hostname of the OV3600 server that will be managed. |
| Polling Enabled | Yes | Enables or disables the Master Console polling of managed OV3600 server. |
| Polling Period | 5 minutes | Determines how frequently the Master Console polls the managed OV3600 server. |

Table 123 Master Console > Manage OV3600s > IP/Hostname Fields and Default Values (Continued)

| Field | Default | Description |
|------------------------------------|---------|---|
| Username | N/A | The username used by the Master Console to login to the managed OV3600 server. The user needs to be an AP/Device Manager or OV3600 Administrator. |
| Password (Confirm Password) | N/A | The password used by the Master Console OV3600 to login to the managed OV3600. |
| HTTP Timeout (5-1000 sec) | 60 | Defines the timeout period used when polling the managed OV3600 server. |
| Manage Group Configuration | No | Defines whether the Master Console can manage device groups on the managed OV3600 server. |

- To push configurations to managed groups using OV3600' global groups feature, first navigate to the Master Console's **Groups > List** 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. 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).
- Clicking the name of an existing group on the **Master Console** loads the subtabs for **Basic, Security, SSIDs, AAA Servers, Radio, WLC Radio, LWAPP APs, PTMP/WIMAX, Proxim Mesh** and **MAC ACL** pages, if such pages and configurations are active for the devices in that group.

These subtabs contain the same fields as the group subtabs on a monitored OV3600, but each field also has a checkbox. The Master Console can also configure global templates that can be used in subscriber groups. The process is the same as described in the [Chapter 6, "Creating and Using Templates"](#), except that there is no process by which templates can be fetched from devices in the subscriber group on managed OV3600s. Instead, the template must be copied and pasted into the Master Console global group.

When a global group is pushed from the **Master Console** to subscriber groups on managed OV3600s, all settings will be static except for settings with the checkbox selected; for fields with checkboxes selected, the value or setting can be changed on the corresponding tab for each managed group. In the case of the **Groups > SSIDs** page, override options are available only on the **Add** page (navigate to the **Groups > SSIDs** page and click the **Add** button).

Once global groups have been configured on the **Master Console**, groups must be created or configured on the managed OV3600s to subscribe to a particular Global Group. It will take several minutes for changes to global groups on the **Master Console** to be pushed to the managed OV3600s; make sure that the Manage Group Configuration option is enabled for each managed OV3600.

To configure subscriber groups, navigate to the **Group > Basic** page of a group on a managed OV3600 and locate the **Use Global Groups** section. Select the **Yes** radio button and select the name of the global group from the drop-down menu. Then click **Save** and **Apply** for the configuration from the global group to be pushed to the subscriber group on the managed OV3600.

Once the configuration is pushed, the non-overridden fields from the global group will appear on the subscriber group as static values and settings. Only fields that had the override checkbox selected in the global group will appear as fields that can be set at the level of the subscriber group. Any changes to a static field must be made on the global group.

In the example below, the field **Name** was overridden with the checkbox in the global group on the Master Console, so it can be configured for each subscriber group on the managed OV3600. The other four fields in

the Basic section were not overridden, so they are static fields that will be the same for each subscriber group. These fields can only be altered on the global group on the Master Console.

The global groups feature can also be used without the Master Console. For more information about how this feature works, refer to the chapter “[Configuring and Using Device Groups in OV3600](#)” on page 73.

Monitoring and Supporting OV3600 with the Home Pages

Overview of the Home Pages

The **Home** section of OV3600 provides the most frequent starting point for monitoring network status and establishing primary OV3600 functions, once OV3600 configuration is complete. Access the following pages in the **Home** section of the OV3600 graphical user interface (GUI):

- The **Home > Overview** and the **Home > License** pages condense a large amount of information about your OV3600. From these two pages you can view the health and usage of your network as well as click common links and shortcuts to view system information. Refer to “[Monitoring OV3600 with the Home > Overview Page](#)” on page 229.
- The **Home > Search** page provides a simple way to find users and managed devices. OV3600 enhances searching by adding an ability to search for rogue devices by multiple criteria. Refer to “[Searching OV3600 with the Home > Search Page](#)” on page 232.
- The **Home > Documentation** page provides easy access to all relevant OV3600 documentation. Refer to “[Accessing OV3600 Documentation with the Home > Documentation Page](#)” on page 234.
- 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 “[Configuring Your Own User Information with the Home > User Info Page](#)” on page 235.

Monitoring OV3600 with the Home > Overview Page

Navigate to **Home > Overview** page with the standard OV3600 menus. [Figure 137](#) illustrates this page, and [Table 124](#) describes the contents.

Figure 137 Home > Overview Page Illustration

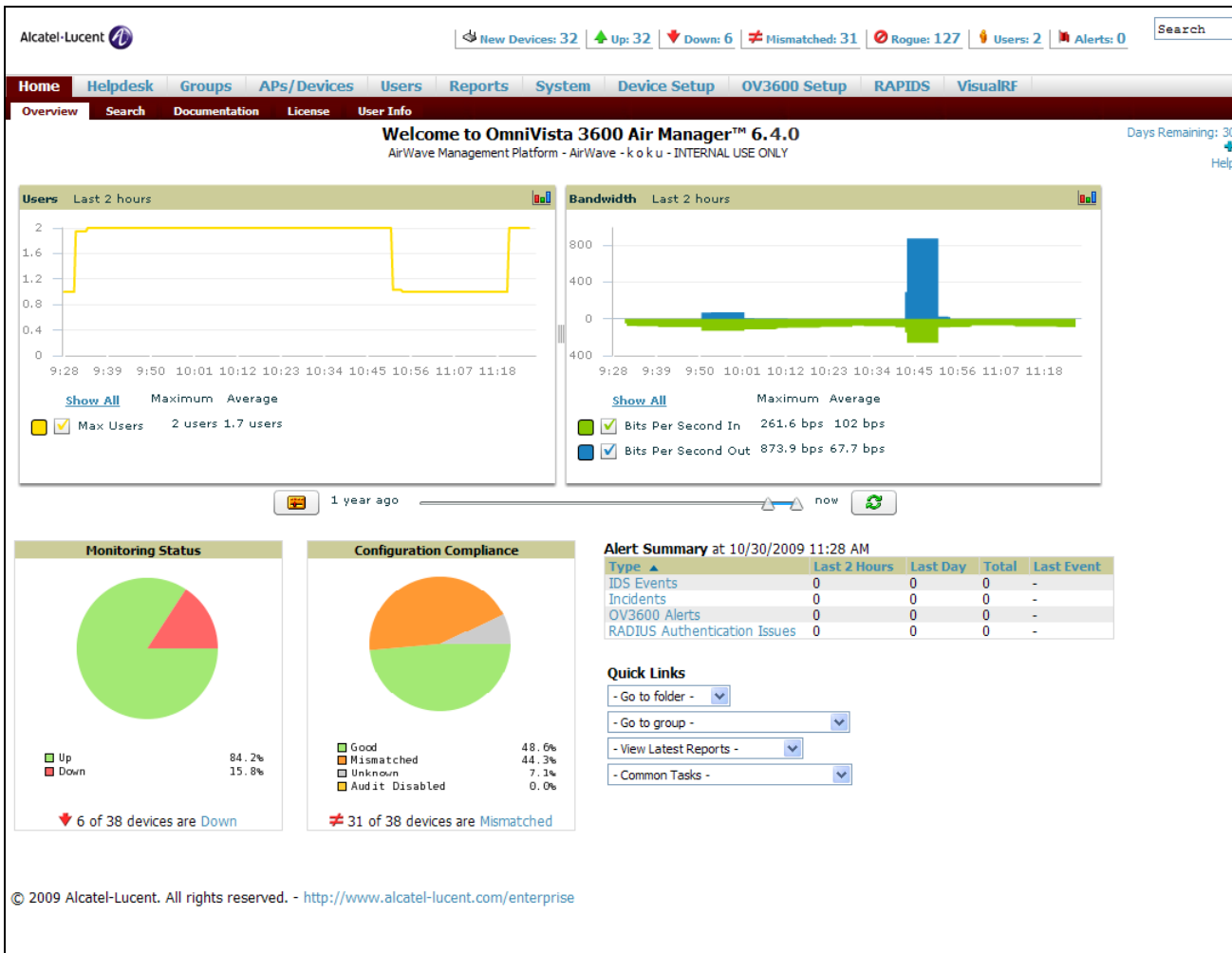


Table 124 Home > Overview Sections and Descriptions

| Section | Description |
|---------------------------------|--|
| Users | The Users section displays a graphical summary of the number of users on the network during a period of time. The time can be adjusted. Click Show All to display a complete list of users. Remove the check in the Max Users option to change the display of the graph. The graph displays the maximum number of users by default. |
| Bandwidth | The Bandwidth section displays bandwidth data, and this display can be adjusted. To remove bandwidth in or out from the graphical display, clear the check box for In or Out . To display details for specific devices, click Show All and select the devices to be included in the graphical bandwidth summary chart. |
| Monitoring Status | This Monitoring Status chart displays the percentage of devices that are up and down on the network. This chart covers 100% of the known devices on the network. To review devices that are down, click Down , and the APs/Devices > Down page displays. |
| Configuration Compliance | The Configuration Compliance chart displays all known device configuration status on the network. Devices are classified as Good, Unknown, or Mismatched. Click the Mismatched link to obtain additional information, and the APs/Devices > Mismatched page displays. |

Table 124 *Home > Overview Sections and Descriptions*

| Section | Description |
|-----------------------------|--|
| <p>Alert Summary</p> | <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). The Alert Summary field displays four types of alerts, as follows:</p> <ul style="list-style-type: none"> ● OV3600 Alerts ● IDS Events ● Incidents ● RADIUS Authentication Issues <p>Click any alert type, and the Alert Summary page appears for that alert type, enabling further analysis and investigation.</p> <p>NOTE: The Incidents portion of this summary table only increments the counter for incidents that are open and associated to an AP. This is also the case if you click Incidents and view incident details. To view all incidents, including those not associated to an AP, navigate to the Helpdesk > Incidents page.</p> |
| <p>Quick Links</p> | <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, as follows:</p> <ul style="list-style-type: none"> ● Go to folder—This menu lists all folders defined in OV3600 from the APs/Devices List page, and enables you to display information for any or all of them. See “Using Device Folders (Optional)” on page 153. ● Go to group—This menu lists all groups defined in OV3600, and enables you to display information for any or all of them. Use the Groups pages to edit, add, or delete groups that appear in this section. See “Configuring and Using Device Groups in OV3600” on page 73. ● View latest reports—OV3600 supports 13 reports, enabling you to generate custom reports, or to display the latest daily version of any report. Click any report type to display the daily version. See “Creating, Running, and Emailing Reports” on page 247. ● Common tasks—This menu provides an inventory of and quick links to the most heavily used task-oriented pages in OV3600, to include the following: <ul style="list-style-type: none"> ■ Configure Alert Thresholds—This link takes you to the System > Triggers page. See “Creating and Using Triggers and Alerts” on page 202. ■ Configure Default Credentials—This link takes you to the Device Setup > Communication page. See “Configuring Communication Settings for Discovered Devices” on page 46. ■ Discover New Devices on Your Network—This link takes you to the Device Setup > Discover page. See “Discovering, Adding, and Managing Devices” on page 121. ■ Supported Devices and Features—This link launches and displays a PDF file that summarizes all supported devices and features in chart format for OV3600. Adobe Reader is required. ■ Upload Device Firmware—This link launches and displays the Device Setup > Upload Files page. See “Overview of the Device Setup > Upload Files Page” on page 49. ■ View Event Log—This link launches and displays the System > Event Log page. See “Using the System > Event Logs Page” on page 238. |

Viewing and Updating License Information with the Home > License Page

Navigate to the **Home > License** page using the standard OV3600 menu. [Figure 138](#) illustrates this page, and [Table 125](#) describes the contents.

Figure 138 *Home > License Page Illustration*

| System Overview | | | |
|-----------------|---------------|----------|----------------------|
| System Name: | aire.com | Time: | 9/23/2009 7:25 PM |
| Organization: | Aire Networks | Uptime: | 1 day 12 hrs 50 mins |
| Hostname: | aire.com | Version: | 6.4 |
| IP Address: | 10.19.19.19 | OS: | CentOS release 5 |

This is a licensed version of AirWave Wireless Management Suite.

Refer to your license agreement for complete information about the terms of this license.
Contact AirWave Technical Support at support@airwave.com or 1-866-943-4267 (866-WIFI-AMP) for more information.

Enter New License:

```

--- Begin AMP License Key ---
Product:  AWMMS Professional
Organization:  Aruba Networks
Hardware_ID:  00:21:9B:8B:B2:C4
APs:  1000
RAPIDS:  Yes
VisualRF:  Yes
Generated:  Wed Mar 4 22:48:19 2009 UTC by VPKasf4K/eXQisetIOc+Aw
--- Signature ---
iD8DBQFJrwUzvN8PdJTKS2ERaUzmAJ9EwYfhciAI7C3oPCOYjoAipUZXgCfaw9q
UmDiGqRmGOH7s3S2F37HZd0=
=6V+1
--- End AMP License Key ---

```

Table 125 *Home > License Fields*

| Field | Description |
|-------------------------|--|
| System Name | Displays a user-definable name for OV3600 (maximum 20 characters). The System Name can be configured from the OV3600 Setup > General page. |
| Organization | Displays the organization listed on your license key. |
| Hostname | Displays the DNS name assigned to OV3600. |
| IP Address | Displays the static IP address assigned to OV3600. The IP Address can be configured from the OV3600 Setup > Networking page. |
| Current Time | Displays the current date and time set on OV3600. |
| Uptime | Displays the amount of time since the operating system was last booted. OV3600 processes get restarted daily as part of the nightly maintenance. |
| Software Version | Displays the version number of OV3600 code currently running. |
| Operating system | Displays the version of Linux installed on the server. |

Searching OV3600 with the Home > Search Page

The **Home > Search** page provides a simple way to find users, managed devices, rogue devices, groups, folders, and more. Search performs partial string searches on a large number of fields including the notes, version, secondary version, radio serial number, device serial number, LAN MAC, radio MAC and apparent IP address of all the APs, as well as the client MAC, VPN user, User, LAN IP and VPN IP fields.

Figure 139 illustrates this page.

Figure 139 Home > Search Page Illustration with Sample Hits on “00:”

Search for managed devices and wireless users. A single substring match is used. To search by MAC address, include colons (e.g. 00:40:96).

00:

APs/Devices:
Modify Devices
1-45 of 45 APs/Devices Page 1 of 1

| Device | Status | Users | BW (kbps) | Uptime | Configuration | Group | Folder | Controller | Master Controller |
|-------------------|--------|-------|-----------|------------------------|---------------|---------------|------------|------------------|-------------------|
| 00:0b:86:66:03:4e | Down | 0 | 0 | - | Unknown | Access Points | .airespace | - | - |
| 00:0b:86:c1:a0:52 | Up | 0 | 0 | 16 hrs 59 mins | Mismatched | Access Points | .airespace | - | - |
| 1250-91:14:1a | Up | 0 | 0 | 8 days 19 hrs 3 mins | Mismatched | iwlc thin aps | .airespace | airespace-4400-1 | - |
| 1250-91:14:42 | Up | 0 | 0 | 12 days 20 hrs 18 mins | Mismatched | iwlc thin aps | .airespace | airespace-4400-1 | - |
| Airespace-4012-2 | Up | 0 | 0 | 54 days 22 hrs 46 mins | Mismatched | Access Points | .airespace | - | - |
| airespace-4400-1 | Up | 0 | 0 | 12 days 21 hrs 28 mins | Mismatched | 4400 | .airespace | - | - |

Users:
1-50 of 325 Users Page 1 of 7 > > |

| Username | Role | MAC Address | AP/Device | SSID | VLAN | AP Radio | Connection Mode | Ch BW | Association Time | Duration |
|--------------------|------|-------------------|-------------------|----------------|------|----------|-----------------|-------|--------------------|----------|
| lagon | - | 00:00:48:39:96:08 | 00:0b:86:c1:a0:52 | alpaca-alpaca | 51 | 802.11bg | 802.11g | 0 | 2/13/2009 12:50 PM | - |
| - | - | 00:04:23:4C:C1:33 | AP2 | ws5100_102 | 1 | 802.11b | 802.11b | - | 3/10/2009 5:22 PM | - |
| - | - | 00:05:4E:48:14:2E | - | - | - | - | - | - | - | - |
| - | - | 00:05:4E:4D:9D:6A | - | - | - | - | - | - | - | - |
| - | - | 00:05:4E:4F:86:81 | - | - | - | - | - | - | - | - |
| ArubaGuestLogon | - | 00:06:25:2C:A5:AD | 00:0b:86:c1:a0:52 | guest | 51 | 802.11bg | 802.11b | 0 | 1/23/2009 9:07 AM | - |
| - | - | 00:09:EF:05:1E:B2 | - | - | - | - | - | - | - | - |
| - | - | 00:09:EF:05:20:CF | - | - | - | - | - | - | - | - |
| lagon | - | 00:0A:88:7F:08:01 | 00:0b:86:c1:a0:52 | aruba-ap | 51 | 802.11bg | 802.11b | 0 | 1/29/2009 2:25 PM | - |
| ArubaNotGuestLogon | - | 00:0A:88:7F:0B:11 | ap-Not set | dpb_test_guest | 51 | 802.11bg | 802.11b | 0 | 1/29/2009 2:19 PM | - |
| - | - | 00:0A:88:7F:0B:1E | - | - | - | - | - | - | - | - |
| - | - | 00:0C:F1:38:0F:A6 | - | - | - | - | - | - | - | - |
| - | - | 00:0E:38:49:08:31 | RADIO1 | 101 | 1 | 802.11b | 802.11b | 0 | 3/5/2009 3:18 PM | - |
| - | - | 00:0E:38:49:08:3E | ap-Not set | guest | 51 | 802.11a | 802.11a | 0 | 2/24/2009 1:08 PM | - |
| - | - | 00:0E:98:CC:CE:F3 | - | - | - | - | - | - | - | - |
| - | - | 00:0E:98:D7:35:BA | ap | open-ops | 0 | 802.11a | 802.11a | - | 1/29/2009 8:59 AM | - |
| - | - | 00:0F:86:81:D5:3F | - | - | - | - | - | - | - | - |
| - | - | 00:0F:CB:82:33:A4 | - | - | - | - | - | - | - | - |
| - | - | 00:11:24:C6:2B:52 | - | - | - | - | - | - | - | - |
| - | - | 00:11:F5:53:AE:0F | - | - | - | - | - | - | - | - |
| - | - | 00:13:02:1E:67:15 | RADIO1 | 101 | 1 | 802.11b | 802.11b | - | 2/5/2009 5:30 PM | - |
| - | - | 00:13:02:84:39:8D | ap | open-ops | 0 | 802.11bg | 802.11bg | - | 1/28/2009 7:41 PM | - |
| - | - | 00:13:02:AD:7C:3E | - | - | - | - | - | - | - | - |
| - | - | 00:13:02:C2:39:28 | - | - | - | - | - | - | - | - |
| - | - | 00:13:02:CD:F3:D5 | 00:0b:86:c1:a0:52 | guest | 51 | 802.11a | 802.11a | 0 | 2/20/2009 7:59 AM | - |
| - | - | 00:13:CE:45:91:A0 | ap-Not set | guest | 51 | 802.11bg | 802.11g | 0 | 1/29/2009 4:00 PM | - |

No Folders found.
No Groups found.

Rogues:
Modify Devices
1-50 of 187 Rogue Devices Page 1 of 4 > > |

| Ack | RAPIDS Classification | Threat Level | Name | Classifying Rule | Device Classification | Wired | #APs hearing | SSID |
|---------|-----------------------|--------------|---------------------|--|-----------------------|-------|--------------|--------------------------------|
| - All - | - All - | - | - | - | - All - | - | - | - |
| No | Valid | - | Enterasys-68:FA:C3 | <user set> | Unclassified | - | 6 | test012 |
| No | Suspected Neighbor | 5 | Tropos Net-04:0F:BB | Suspected Neighbor - detected wirelessly | Unclassified | - | 5 | TroposNetworks |
| No | Suspected Neighbor | 5 | Cisco Syst-A7:B9:ED | Suspected Neighbor - detected wirelessly | Valid | - | 3 | dbishop-airespace-open |
| No | Valid | - | Aruba Netw-88:89:32 | <user set> | Unclassified | - | 5 | ethersphere-voip |
| No | Valid | - | Enterasys-27:F6:48 | <user set> | Unclassified | - | 6 | RoomAbout Default Network Name |
| No | Suspected Neighbor | 5 | SYMBOL TEC-D7:64:A6 | Suspected Neighbor - detected wirelessly | Valid | - | 6 | ws5100_102 |
| No | Valid | - | NOMADIX IN-05:02:D0 | <user set> | Unclassified | - | 6 | Nomadix |
| No | Valid | - | Meru Netwo-B9:CC:05 | <user set> | Unclassified | - | 6 | BetsyFromPike |

Tags:
1-5 of 5 Tags Page 1 of 1

| Name | MAC Address | Vendor | Battery Level | Chirp Interval | Last Seen | Closest AP |
|------|-------------------|----------------|---------------|----------------|--------------------|---------------------|
| - | 00:0C:CC:5E:7F:9E | Aeroscout Ltd. | - | 45 secs | 3/12/2009 10:25 AM | 1250-91:14:42 |
| - | 00:14:7E:00:4C:DC | InnerWireless | Normal | 1 min | 3/12/2009 10:24 AM | 1250-91:14:42 |
| - | 00:0C:CC:7A:3B:8A | Aeroscout Ltd. | - | 50 secs | 3/12/2009 10:24 AM | lwapp-1250-13:21:1e |
| - | 00:14:7E:00:4C:B9 | InnerWireless | Normal | 2 mins | 3/12/2009 10:23 AM | lwapp-1250-13:21:1e |
| - | 00:14:7E:00:4C:F2 | InnerWireless | Normal | 0 mins | 3/10/2009 10:00 AM | - |

1. Enter the keyword or text with which to search. If searching for a MAC address, enter it in colon-delimited format.



The OV3600 Search utility is case-insensitive.

2. Click **Search**, and the results display after a short moment. Results support several hypertext links to additional pages, and drop-down menus allow for additional filtering of search returns.

Search results are categorized in the following sequence. Not all categories below may offer returns for a given search:

- **APs/Devices**
- **Users**

- Rogues
- Tags
- Folder
- Group

Accessing OV3600 Documentation with the Home > Documentation Page

The **Home > Documentation** page provides easy access to all relevant OV3600 documentation. All of the documents on the **Home > Documentation** page are hosted locally by OV3600 and can be viewed by any PDF viewer. [Figure 140](#) illustrates this page.

Figure 140 *Home > Documentation Page Illustration*



If you have any questions that are not answered by the documentation please contact Alcatel-Lucent support at Esd.support@alcatel-lucent.com.

Configuring Your Own User Information with the Home > User Info Page

The **Home > User Info** page displays information about the user that is logged into OV3600. This page includes the authentication type (local user or TACACS+) and access level. This page also provides the user with the ability to customize some of the information displayed in OV3600 and change their password.

To create new users, navigate to the **OV3600 Setup > Users** page, and refer to “[Creating OV3600 Users](#)” on [page 40](#). Users can customize the information displayed in the OV3600 header.

Figure 141 *Home > User Info Page Illustration*

admin is logged in as a local user with role *OV3600 Administration* and Read/Write access to RAPIDS .

User Information

Name:

Email Address:

Phone:

Notes:

Top Header Stats

Filter Level For Rogue Count:

Customize Header Columns: Yes No

Display Preferences

Default Number of Records per List:

Reset List Preferences:

Customize Columns for Other Roles: Yes No

Console Refresh Rate:

Change Password

New Password:

Confirm New Password:

Table 126 *Home > User Info Fields*

| Field | Description |
|---|--|
| Customize Header columns | Enables/Disables the ability to customize the data displayed at the top of every OV3600 screen. |
| Stats | Select the specific data you would like to see in the header. |
| Severe Alert Threshold | Configures the minimum severity of an alert to be included in the Severe Alerts count. Note: The severe alerts count header info will only be displayed if ‘Severe Alerts’ is selected in the Stats section above. |
| Include Device Types | Configures the types of devices that should be included in the header stats. If a device type is not selected then it will not be included in the header stats. |
| Default Number of Records per list | Defines the number of rows to appear in any list that has not had a row count manually set. If a row count is manually set it will override the default setting. |
| Reset List PReferences | Reset all list preferences including number of records per list, column order and hidden column information. |
| Customize Columns for Other Roles | Allows admin users to determine the columns that should be displayed and the order they should be displayed for specific user roles. To customize lists for other users, navigate to that list and click the Choose Columns for roles link above the list. Make the desired column changes; select the roles to update and click save. |
| Filter Level For Rouge Count | Specifies the minimum classification that will cause a device to be included in the Rogue count header information. |

Perform the following steps to configure your own user account with the **Home > User Info** page:

1. In the **User Information** section, enter the following information:
 - **Name**—Enter the ID by which a you logs into and operate in OV3600.
 - **Email Address**—Enter the email address to be used for alerts, triggers, and additional OV3600 functions that support an email address.
 - **Phone**—Enter the area code and phone number, if desired.
 - **Notes**—Enter any additional text-based information that helps other OV3600 users or administrators to understand the functions, roles, or other rights of the user being created.

Monitoring and Supporting OV3600 with the System Pages

The **System** pages provide a centralized location for system-wide OV3600 data and settings. Apart from **Triggers**, **Alerts**, and **Backups** pages that are described elsewhere in this chapter, the remaining pages of the **System** section are as follows:

- **System > Status**—Displays status of all OV3600 services. Refer to [“Using the System > Status Page” on page 236](#).
- **System > Event Log**—This useful debugging tool keeps a list of recent OV3600 events, including APs coming up and down, services restarting, and most OV3600-related errors as well as the user that initiated the action. Refer to [“Using the System > Event Logs Page” on page 238](#).
- **System > Configuration Change Jobs**—Manages configuration changes in OV3600. Refer to [“Using the System > Configuration Change Jobs Page” on page 239](#).
- **System > Performance**—Displays basic OV3600 hardware information as well as resource usage over time. Refer to [“Using the System > Performance Page” on page 239](#).
- **System > Firmware Upgrade Jobs**—Displays information about current and scheduled firmware upgrades.

Using the System > Status Page

The **System > Status** page displays the status of all of OV3600 services. Services will either be **OK**, **Disabled**, or **Down**. **OK** and **Disabled**, displayed in green, are the expected states of the services. If any service is **Down**, displayed in red, please contact Alcatel-Lucent support. The **Reboot** button provides a graceful way to power cycle your OV3600 remotely when it is needed. The **Restart OV3600** button will restart the OV3600 services without power cycling the server or reloading the OS. [Figure 142](#) illustrates this page.

Figure 142 *System > Status Page Illustration*



Refresh

D diagnostic report file for sending to customer support: diagnostics.tar.gz
VisualRF diagnostics report file: VisualRFdiag.tar.gz

| Service ▲ | Status | Log |
|------------------------------------|----------|------------------------------------|
| Airbus Message Server | OK | /var/log/airbus.log |
| Alert Cache Builder | OK | /var/log/alerts_stats_cacher |
| Alert Monitor | OK | /var/log/alertd |
| Asynchronous Work Scheduler | OK | /var/log/tuple_scheduler |
| At | OK | /var/log/at |
| AWMS News Fetcher | OK | /var/log/awms_news_fetcher |
| Cisco ACS | OK | /var/log/acs |
| Cisco WLSE Poller | OK | /var/log/wlse |
| Client Monitor Worker | OK | /var/log/async_logger_client |
| Configuration Monitor | OK | /var/log/config_verifier |
| Configuration Server | OK | /var/log/config_pusher |
| Cron | OK | /var/log/amp_cron |
| Database | OK | /var/log/pgsql |
| Device List Cacher | OK | /var/log/ap_list_cacher |
| Device Monitor | OK | /var/log/ap_watcher |
| Device Monitor (Poll Now) | OK | /var/log/ap_watcher_poll_now |
| Discovery Event Existing-AP Cacher | OK | /var/log/discovery_event_cacher |
| DNS Fetcher | OK | /var/log/dns_fetcher |
| DNS Refresh | OK | /var/log/dns_refresh |
| Fallover Monitor | Disabled | /var/log/amp_watcher |
| Firmware Server | OK | /var/log/firmware_enforcer |
| FTP Server | Disabled | /var/log/xferlog |
| Guest User Credential Enabler | OK | /var/log/guest_user_pusher |
| HTTP/SNMP Scanner | OK | /var/log/ap_scanner |
| LWAPP Managed Certificate Builder | OK | /var/log/lwapp_rebuild |
| Master Console | Disabled | /var/log/mc_stat_collector |
| MC Report Runner | OK | /var/log/mc_report_runner |
| Mobile Device Management Engine | Disabled | /var/log/mdm.log |
| NTP Client | OK | |
| PAPI Message Processor | OK | /var/log/papi |
| PAPI Message Router | OK | /var/log/msgHandler.log |
| Parallel HTTP Fetcher | Disabled | /var/log/http_fetcher |
| Performance Monitor | OK | /var/log/perf_collector |
| Persistent TupleSpaces Server | OK | /var/log/persistent_tuple_spaces |
| Postfix Mail Server | OK | /var/log/maillog |
| RADIUS Accounting Server | OK | /var/log/radius/radius.log |
| Report Runner | OK | /var/log/amp_report_runner |
| Rogue Filter | OK | /var/log/rogue_filter |
| RTLS Collector | OK | /var/log/rtls |
| SNMP Enabler | OK | /var/log/snmp_enabler |
| SNMP Fetcher | OK | /var/log/snmp_fetcher |
| SNMP V2 Fetcher | OK | /var/log/snmp_v2_fetcher |
| SNMP Trap Handler | OK | /var/log/snmp_trap_handler |
| Synchronous Event Handler | OK | /var/log/syncd |
| Tag Expiration | OK | /var/log/expire_wifi_tags |
| TupleSpaces Server | OK | /var/log/tuple_spaces |
| VisualRF Engine | OK | /var/log/visualrf.log |
| Web Server | OK | /var/log/httpd/ssl_error_log |
| WEP Key Setter | OK | /var/log/wep_key_setter |
| Whitelist Collector | Disabled | /var/log/whitelist_collector |
| Work Queue Collision Logger | OK | /var/log/work_queue_clobber_logger |

Additional Log Files

| Description ▲ | Log |
|----------------------|--------------------------------|
| Nightly Maintenance | /var/log/nightly_maintenance |
| System Audit Log | /var/log/system_audit_log |
| Telnet Commands | /var/log/telnet_cmds |
| Upgrade to 6.4_beta6 | /tmp/AMP-6.4_beta6-upgrade.log |

4 Additional Log Files

Restart AWMS Reboot System

- The link **diagnostics.tar.gz** downloads a tar file that contains reports and logs that are helpful to Alcatel-Lucent Support in troubleshooting and solving problems. Alcatel-Lucent support may request that you submit this file along with other logs that are linked on this page. Logs that are contained in **diagnostics.tar.gz** include **cron_stopped_maintenance**, **OV3600_events**, **OV3600_watcher**, **async_logger**, **ssl_error** and **pgsql**.
- Similarly, the **VisualRFdiag.tar.gz** link downloads a diagnostic file containing VisualRF information that might be requested by Alcatel-Lucent support

- A summary table lists logs that appear on the **System > Status** page. These are used to diagnose OV3600 problems. Additional logs are available via SSH access in the /var/log and /tmp directories; Alcatel-Lucent Technical Support Engineers may request these logs for help in troubleshooting problems and will provide detailed instructions on how to retrieve them. [Table 127](#) describes the log information.

Table 127 System > Status Log

| Log | Description |
|------------------------|---|
| pgsql | Logs database activity. |
| ssl_error_log | Reports problems with the web server. This report is also linked from the internal server error page that displays on the web page; please send this log to Alcatel-Lucent support whenever reporting an internal server error. |
| maillog | Applies in cases where emailed reports or alerts do not arrive at the intended recipient's address. |
| radius | Displays error messages associated with RADIUS accounting. |
| async_logger | Tracks many device processes, including user-AP association. |
| config_verifier | Logs device configuration checks. |
| config_pusher | Logs errors in pushing configuration to devices. |
| visualrf.log | Details errors and messages associated with the VisualRF application. |

Using the System > Event Logs Page

The **System > Event Logs** page is a very useful debugging tool. The event log keeps a list of recent OV3600 events, including APs coming up and down, services restarting, and most OV3600-related errors as well as the user that initiated the action. [Figure 143](#) illustrates this page, and [Table 128](#) describes the page components.

Figure 143 System > Event Logs Page Illustration

| Time | User | Type | Event |
|--------------------------|--------|---------------|---|
| Mon Feb 12 15:31:33 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good |
| Mon Feb 12 15:31:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Up |
| Mon Feb 12 15:31:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Down |
| Mon Feb 12 15:31:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Device uptime indicates that device has rebooted |
| Mon Feb 12 15:29:38 2007 | System | System | Wireless station 00:13:02:9D:04:C2 deauthenticated via EAP |
| Mon Feb 12 15:29:38 2007 | System | System | Wireless station 00:13:CE:14:5E:9B deauthenticated via EAP |
| Mon Feb 12 15:21:33 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good |
| Mon Feb 12 15:21:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Up |
| Mon Feb 12 15:21:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Down |
| Mon Feb 12 15:21:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Device uptime indicates that device has rebooted |
| Mon Feb 12 15:19:38 2007 | System | System | Wireless station 00:13:02:9D:04:C2 deauthenticated via EAP |
| Mon Feb 12 15:19:37 2007 | System | System | Wireless station 00:90:96:F0:A9:EC deauthenticated via EAP |
| Mon Feb 12 15:09:37 2007 | System | System | Wireless station 00:11:24:2D:78:12 deauthenticated via EAP |
| Mon Feb 12 15:09:01 2007 | System | Router/Switch | corp1 (switch1.corp.airwave.com): can't reach device for CDP data collection |
| Mon Feb 12 15:08:32 2007 | System | Router/Switch | corp2 (switch2.corp.airwave.com): can't reach device for CDP data collection |
| Mon Feb 12 15:08:03 2007 | System | Router/Switch | Corporate Gateway (10.200.0.1): can't reach device for CDP data collection |
| Mon Feb 12 15:06:33 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good |
| Mon Feb 12 15:06:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Up |
| Mon Feb 12 15:06:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Down |
| Mon Feb 12 15:06:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Device uptime indicates that device has rebooted |
| Mon Feb 12 15:04:37 2007 | System | System | Wireless station 00:13:02:9D:04:C2 deauthenticated via EAP |
| Mon Feb 12 15:01:33 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good |
| Mon Feb 12 15:01:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Up |
| Mon Feb 12 15:01:32 2007 | System | Device | Aruba AP 65 Aruba-AP65-ap.2.2.3 Down |

Table 128 System > Event Logs Fields

| Field | Description |
|-------------|---|
| Time | Date and time of the event. |
| User | The OV3600 user that triggered the event. When OV3600 itself is responsible for the event, System is displayed as the user. |

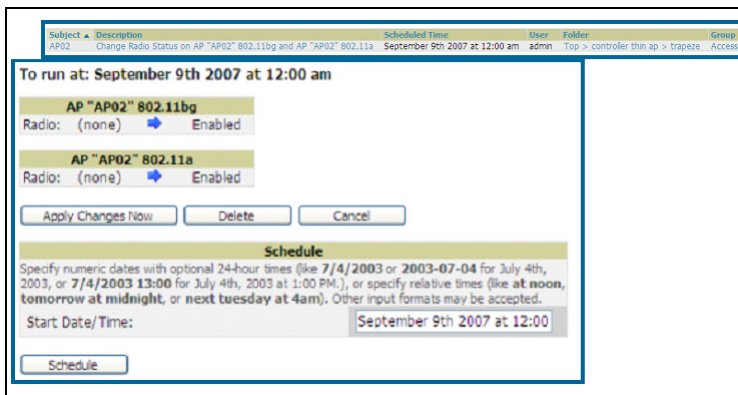
Table 128 System > Event Logs Fields

| Field | Description |
|--------------|--|
| Type | Displays the Type of event recorded, which is one of four types, as follows: <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 > 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 144](#).

Figure 144 System > Configuration Change Jobs Page Illustration



1. To edit an existing configuration change job click on the linked description name. On the subsequent edit page you can choose to run the job immediately by clicking the **Apply Changes Now** button, reschedule the job using the **Schedule** box, delete the job using the **Delete** button, or cancel the job edit by clicking the **Cancel** button.
2. Click the linked AP or group name under the **Subject** column to go to the monitoring page of the AP or group.
3. Click the linked group and folder names under **Folder** or **Group** to go to the AP's folder or group page.
4. Scheduled configuration change jobs will also appear on the **Manage** page for an AP or the **Monitoring** page for a group.

Using the System > Performance Page

The **System > Performance** page displays basic OV3600 hardware information as well as resource usage over time. OV3600 logs performance statistics such as load average, memory and swap data every minute. The historical logging can be used to help determine the best usable polling period and track the health of OV3600 over time. [Figure 145](#) illustrates this page and [Table 129](#) describes fields and information displayed.

Figure 145 System > Performance Page Illustration (Partial Screen Shown)

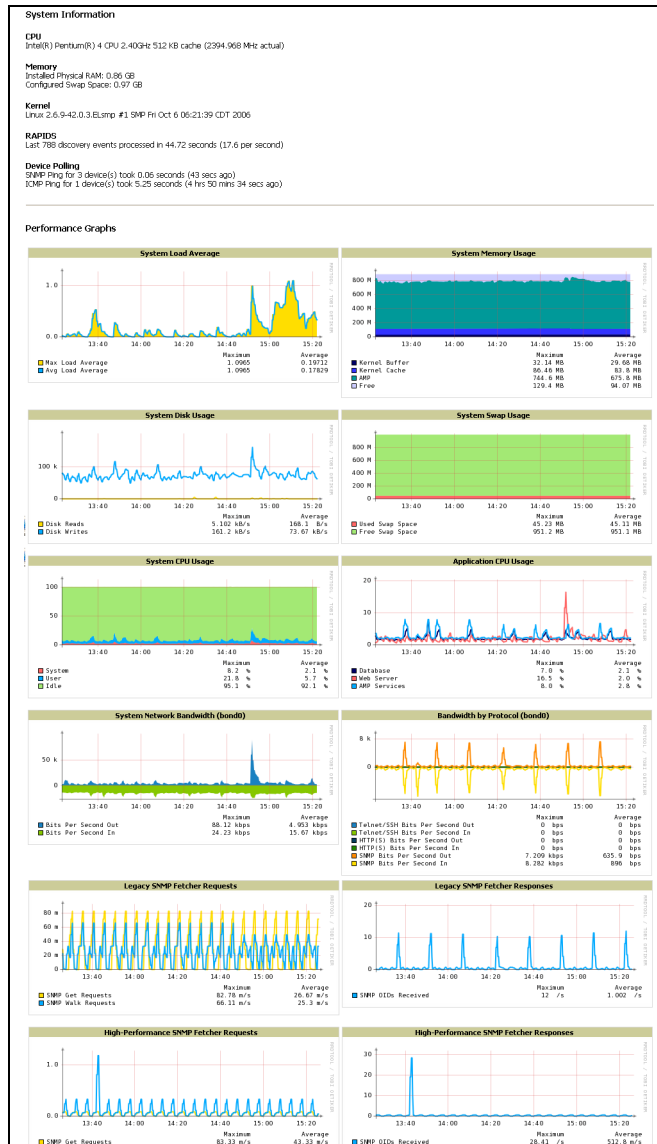


Table 129 System > Performance Page Fields

| Field | Description |
|-----------------------|---|
| CPU(s) | Basic CPU information as reported by Linux. |
| Memory | The amount of physical RAM and Swap space seen by the operating system. OV3600 requires a minimum of 1 gigabyte of physical RAM |
| Kernel | The version of Linux kernel running on the box. |
| RAPIDS | Displays how long it took to process the last payload of MAC address. |
| Device Polling | Displays some AP/Device polling statistics. |

Table 129 System > Performance Page Fields (Continued)

| Field | Description |
|---|--|
| System Load Average | The System Load average is the number of jobs currently waiting to be processed. Load is a rough metric that will tell you how busy a server is. A typical OV3600 load is around 3. A constant load of 5 to 7 is cause for concern. A load above 10 is a serious issue and will probably result in 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 milliseconds or 1/1000ths of 1. |
| System Memory Usage | The amount of RAM that is currently used broken down by usage. It is normal for OV3600 to have very little free RAM. Linux automatically allocates all free ram as cache and buffer. If the kernel needs additional RAM for process it will dynamically take it from the cache and buffer. |
| System Disk Utilization | The amount of data read from the disk and written to the disk. |
| Swap Usage | The amount of Swap memory used by OV3600. Swap is used when there is no more free physical RAM. A large performance penalty is paid when swap is used. If an OV3600 consistently uses swap you should consider installing additional RAM for the box. |
| System CPU Usage | The percentage of CPU that has been used by the user and the system as well as the amount that was idle. |
| Application CPU Usage | CPU usage broken down by application. OV3600 services includes all OV3600 processes except the database and the webserver. |
| System Network Bandwidth (Eth0) | All traffic in and out of Eth0 measured in bits per second. |
| Bandwidth by Protocol (Eth0) | Displays the amount of traffic used by Telnet, HTTPS and SNMP on Eth0. |
| Legacy SNMP Fetcher (SNMP Get/walk Requests) | The number of SNMP get and walk requests per second performed by the legacy (v1 and v3) SNMP fetcher. |
| Legacy SNMP Fetcher (SNMP OIDs Received) | The number of SNMP OIDs received per second performed by the legacy (v1 and v3) SNMP fetcher. |
| High Performance SNMP Fetcher (SNMP Get/walk Requests) | The number of SNMP get and walk requests per second performed by the high performance SNMP (v2c) fetcher. |
| High Performance SNMP Fetcher (SNMP OIDs Received) | The number of SNMP OIDs received per second performed by the high performance SNMP (v2c) fetcher. |
| Top 5 Tables (by row count) | The five largest tables in OV3600. Degraded performance has been noticed for in some cases for tables over 200,000 rows. Alcatel-Lucent recommends decreasing the length of time client data is stored on the OV3600 page if a user/client table exceeds 250,000 rows. |
| Database Table Scans | The number of Database table scans performed by the database. |
| Database Row Activity | The number of insertions, deletions and updates performed to the database. |

Table 129 System > Performance Page Fields (Continued)

| Field | Description |
|--------------------------------------|---|
| 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 support at 1-408-419-4098 or support@ind.alcatel.com for the latest recommendations.

Upgrading OV3600

The OV3600 upgrade process may change. Please consult support of the latest OV3600 release announcement for detailed instructions. The following is sample instructions from the 6.4 announcement email:

Upgrade Instructions

To upgrade your OV3600:

1. Login to the OV3600 server as the root user.
2. Run the following command

```
# start_ov3600_upgrade -v 6.4.0
```

Upgrading Without Internet Access

If your OV3600 cannot get to the Internet:

1. Download OV3600 6.4.0 from our download page: <http://service.esd.alcatel-lucent.com>
2. Copy the file to OV3600's /root directory using WinSCP.
3. On the OV3600, run the following command:

```
# start_ov3600_upgrade -v 6.4.0
```

The `start_ov3600_upgrade` script will check the /root directory for the latest update. If the update is not found, the script will attempt to download it from the Alcatel-Lucent support page. The script will then extract the version specific upgrade script. The version specific script will deploy all needed files, update the database, perform any data migrations and restart the OV3600 services.

Backing Up OV3600

Overview of Backups

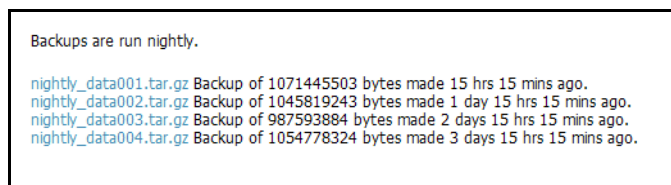
OV3600 creates nightly archives of all relational data, statistical data, and log files. This occurs by default at 4:15 AM, but is configurable on the **OV3600 Setup > General** page under the **Nightly Maintenance Time** setting.

Although OV3600 only keeps the last four sets of archives, the archives can be downloaded manually or automatically off-site for more extensive backup strategies. OV3600 creates one data backup file each night. The data backup file contains all of the device and group information as well as historical data and system files, including IP address, NTP information, mail relay hosts, and other OV3600 settings.

Viewing and Downloading Backups

To view current OV3600 backup files, go to the **System > Backups** page. [Figure 146](#) illustrates this page.

Figure 146 *System > Backups Page Illustration*



To download a backup file, click the filename URL and the **File Download** popup page appears. Proceed as prompted.

Alcatel-Lucent recommends regularly saving the data backup file to another machine or media. This process can be automated easily with a nightly script.



Nightly maintenance and `ov3600_backup` scripts back up the full OV3600 data and save the file as `nightly_data001.tar.gz`. In previous OV3600 versions, the scripts created both config backup and data backup files. In order to restore the OV3600 data, it is only necessary to have most recent data backup file, and OV3600 no longer uses or supports the config backup file, effective with OV3600 6.3.2 and later OV3600 versions.

Running Backup on Demand

To create an immediate backup, use the following procedure:

1. Log into the OV3600 system as root.
2. Run the backup script by typing `ov3600_backup`

This creates a backup of the system located in `/alternative/databackup.tar.gz`.

Restoring from a Backup

To restore a backup file on a new machine use the following procedure:

1. Use your OV3600 Installation CD to build a new machine. The new machine must be running the same version as the OV3600 that created the backup file.
2. Copy the `nightly_data00[1-4].tar.gz` file to the new OV3600. The `/tmp` directory is an appropriate destination.

A good open source Windows file transfer client that supports SFTP and SCP for is WinSCP which is available from <http://winscp.sourceforge.net/eng/>.

WINSCP allows you to transfer the `nightly00[1-4].tar.gz` file from your local PC to the new OV3600 using the secure copy protocol (SCP).

3. Log onto the new server as **root**.
4. Run the restore script by typing **ov3600_restore -d /tmp/nightly_data00[1-4].tar.gz**.

OV3600 Failover

The failover version of OV3600 provides a many to one hot backup server. The Failover OV3600 polls the watched OV3600s to verify that 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 130](#) describes the contents of this page.

Table 130 Contents of the **Navigation Section of Failover**

| Main Tab | Description | Sub-Menus |
|---------------------|---|--|
| Home | The Home page provides basic OV3600 Failover information, including system name, hostname, IP address, current time, running time, software version, and watched OV3600 information. | <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 [“Backing Up OV3600” on page 242](#).

Table 131 *Home > Watched Page Fields and Default Values*

| Setting | Default | Description |
|----------------------------------|-----------|---|
| IP/Hostname | None | The IP address or Hostname of the watched OV3600. The Failover OV3600 needs HTTPS access to the watched OV3600s. |
| Username | None | A username with management rights on the watched OV3600. |
| Password | None | The password for the username with management rights specified above. |
| HTTP Timeout (5-1000 Sec) | 60 | The amount of time before OV3600 considers a polling attempt failed. |
| Polling Enabled | Yes | Enables or disables polling of the Watched OV3600. NOTE: You do not need to disable polling of the watched OV3600 system if it is set to be down during nightly maintenance or is being upgraded. |
| Polling Period | 5 minutes | The amount of time between polls of the Watched OV3600. |
| Missed Poll Threshold | None | The number of polls that can be missed before the failover OV3600 will begin actively monitoring the Watched OV3600s APs. |

Introduction

This chapter describes OV3600 reports, including report access, creation, scheduling, and distribution via email and XML processing. This chapter contains the following sections:

Overview of OV3600 Reports

- Supported Report Types in OV3600
- Reports > Definitions Page Overview
- Reports > Generated Page Overview

Using Daily Reports

- Viewing Generated Reports
- Using the Capacity Planning Report
- Using the Configuration Audit Report
- Using the Device Summary Report
- Using the Device Uptime Report
- Using the IDS Events Report
- Using the Inventory Report
- Using the Memory and CPU Utilization Report
- Using the Network Usage Report
- Using the New Rogue Devices Report
- Using the New Users Report
- Using the PCI Compliance Report
- Using the RADIUS Authentication Issues Report
- Using the User Session Report

Defining Reports

Emailing and Exporting Reports

- Emailing Reports in General Email Applications
- Emailing Reports to Smarthost
- Exporting Reports to XML



OV3600 ships with several reports as enabled by default. Default reports may run each night or weekly, depending on the OV3600 release. Alcatel-Lucent recommends that you review the list of defined and scheduled reports with the **Reports > Generated** and **Reports > Definition** pages to determine if default reports are desired. If not, you can delete, disable, or reschedule any report.



OV3600 supports additional and more specialized reports as follows:

- **System > Status** page supports the diagnostic report file for sending to customer support: diagnostics.tar.gz.
- **System > Status** page supports the VisualRF diagnostics report file: VisualRFdiag.tar.gz.
- **VisualRF > Network View** supports the Bill of Materials (BOM) report. Refer to the *VisualRF User Guide*.

Overview of OV3600 Reports

OV3600 supports a wide variety of reports. These reports are powerful tools in network analysis, user configuration, device optimization, and network monitoring on multiple levels. These reports provide an interface for multiple configurations, allowing you to act upon information in the reports.

Supported Report Types in OV3600

Table 132 summarizes the report types supported in OV3600, and provides links to additional topics that describe each. Most of these reports can be custom-configured.

Table 132 Report Types in OV3600

| Report Type | Description | Additional Information |
|--|---|---|
| Custom | Allows for creating custom reports using information from all other report types. | Using Custom Reports |
| Capacity Planning Report | Tracks bandwidth capacity and consumption according to thresholds for data throughput. This is a device-oriented report. | Using the Capacity Planning Report |
| 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, one device group at a time, or complete device inventory. | Using the Configuration Audit Report |
| Device Summary Report | Identifies the most heavily used devices and the most under-used devices on the network. | Using the Device Summary Report |
| 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 | Using the Device Uptime Report |
| IDS Events Report | Lists and tracks IDS events on the network according to Access Point (AP) or controller device. | Using the IDS Events Report |
| Inventory Report | Itemizes all devices and firmware versions on the network, to include manufacturer information and graphical summary. | Using the Inventory Report |
| 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. | Using the Memory and CPU Utilization Report |
| Network Usage Report | Contains network-wide information of 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) | Using the Network Usage Report |
| New Rogue Devices Report | Summarizes rogue device information in a number of ways, to include time, associated AP, enhanced classification supported in OV3600, and additional parameters. | Using the New Rogue Devices Report |
| New Users Report | Lists all new users that have appeared on the network during the time duration specified for the report. | Using the New Users Report |
| PCI Compliance Report | Displays current PCI configurations and compliance status when OV3600 enables such monitoring on the network. | Using the PCI Compliance Report |
| RADIUS Authentication Issues Report | Contains RADIUS-related issues that may appear with AP controllers, RADIUS Servers, and users. | Using the RADIUS Authentication Issues Report |

Table 132 Report Types in OV3600

| Report Type | Description | Additional Information |
|----------------------------|---|---|
| User Session Report | Tracks user-level activity by session. Session information can be established and tracked by multiple parameters. | Using the User Session Report |

OV3600 reports have the following general parameters:

- OV3600 runs daily versions of all reports during predefined windows of time. All reports can be scheduled so that they run in the background.
- The daily version of any report is available instantly using the **Reports > Generated** page and scrolling to the report links at the bottom of the page.
- The **Inventory** and the **Configuration Audit** reports are the only reports that do not span a period of time. Instead, these two reports provide a detailed snapshot of the current state of the network.
- Users can create all other reports over a custom time period on the **Reports > Definitions** page. All reports can be emailed or exported to XML format for easy data manipulation using a spreadsheet.

Reports > Definitions Page Overview

The **Reports > Definitions** page allows you to define new reports and to take inventory of reports already defined. The **Definitions** page has these sections:

- **Report Definitions**—This section lists all reports that are currently defined in OV3600.
- **Add**—This button launches a report definition page to create and schedule a new report of any type.
- **Run**—This button allows you to run any report that has been defined.
- **Delete**—This button enables you to delete the definition of any report.
- **Reports Definitions for Other Roles**—This section, supported for **admin** users, displays additional reports that have been scheduled for other roles. This section of the page adds the **Role** column, and other columns are the same.

Once custom reports have been created with the **Definition** page, these appear on the **Generated** page. OV3600 Version enhances this page by displaying reports for other user roles.

Figure 147 illustrates the Report > Definition page, and Table 133 describes the fields.

Figure 147 Report > Definitions Page Illustration (Split View)

Report definitions:

New Report Definition

Reports are available on the [Generated Reports](#) page after they have been run.

1-20 of 45 Report Definitions Page 1 of 3 > |

| <input type="checkbox"/> | | Title | Type | Subject |
|--------------------------|--|------------------------------|-------------------|-------------------------------|
| <input type="checkbox"/> | | VoWLAN Devices | Device Summary | SSID intranet-voip |
| <input type="checkbox"/> | | VoWLAN Usage | Network Usage | SSID intranet-voip |
| <input type="checkbox"/> | | VoWLAN User Sessions | User Session | SSID intranet-voip |
| <input type="checkbox"/> | | Avir-upptime | Device Uptime | Group HQ |
| <input type="checkbox"/> | | Capacity Planning Max Values | Capacity Planning | All Groups, Folders and SSIDs |
| <input type="checkbox"/> | | Custom Device Summary Report | Device Summary | Group HQ |
| <input type="checkbox"/> | | Custom IDS Events Report | IDS Events | All Groups and Folders |

| Latest Report | Report Start | Report End | Last Run Time | Scheduled |
|------------------------------|---------------|------------------|--------------------|-----------------------------|
| VoWLAN Devices | 2 weeks ago | now | 5/15/2009 3:00 PM | Every Friday at 3:00 pm PDT |
| VoWLAN Usage | 1 week ago | now | 5/15/2009 3:00 PM | Every Friday at 3:00 pm PDT |
| VoWLAN User Sessions | 2 weeks ago | now | 5/15/2009 3:00 PM | Every Friday at 3:00 pm PDT |
| Avir-upptime | last week | today | 5/19/2009 12:19 AM | - |
| Capacity Planning Max Values | 3/1/2009 | 12:00 a.m. today | 5/21/2009 12:15 AM | Daily at 12:15 am PDT |
| Custom Device Summary Report | 2 weeks ago | now | 5/14/2009 6:36 AM | - |
| Custom IDS Events Report | 5/14/09 22:00 | 5/14/09 23:00 | 5/15/2009 7:13 AM | - |

Select All - Unselect All

Report definitions for other roles:

1-4 of 4 Report Definitions Page 1 of 1

| <input type="checkbox"/> | | Role | Title | Type | Subject |
|--------------------------|--|-----------------------|----------------------------------|------------------------------|---|
| <input type="checkbox"/> | | corp-users-via-radius | Radius Auth Problems | RADIUS Authentication Issues | All Groups, Folders and SSIDs |
| <input type="checkbox"/> | | Partner | Device Summary Report | Device Summary | All Groups, Folders and SSIDs |
| <input type="checkbox"/> | | Partner | RADIUSReport | RADIUS Authentication Issues | Group Research Lab and Folder Top > Sunnyvale HQ > HQ Cisco LWAPP and SSID wpa2 |
| <input type="checkbox"/> | | Partner | PCICompliance-Detailed-3wks-Acme | PCI Compliance | Group HQ |

| Latest Report | Report Start | Report End | Last Run Time | Scheduled |
|----------------------------------|--------------|------------|-------------------|-----------|
| - | yesterday | now | 4/27/2009 2:21 PM | - |
| Device Summary Report | 5/5/2009 | 5/8/2009 | 5/8/2009 10:58 AM | - |
| - | 1/1/2009 | 3/31/2009 | 3/31/2009 6:08 AM | - |
| PCICompliance-Detailed-3wks-Acme | 3 weeks ago | now | 4/28/2009 7:12 AM | - |

Select All - Unselect All

Table 133 Report > Definition Page Fields and Descriptions

| Field | Description |
|----------------------|--|
| Title | Displays title of the report. This is a user-configured field when creating the report. |
| Type | Displays the type of the report. This can be one of 13 report types in OV3600. |
| Subject | Displays the scope of the report, to include groups, folders, SSIDs, or any combination of these that are included in the report. |
| 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. |
| Roles | Added to the Reports definitions for other roles section, this column cites the roles for which additional reports are defined. |

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 four primary sections, as follows:

- Generated reports configured for the current role and for additional roles
- Generated reports for other roles
- The option to view the latest daily reports with a single click for immediate online viewing

Figure 148 Reports > Generated Page Example

Generated reports:
 Visit the Report Definitions page to run new reports.
 1-20 of 959 Reports Page 1 of 48 > >|

| Generation Time | Title | Type | Subject | Report Start | Report End |
|--|---|------------------------------|-------------------------------|--------------------|-------------------|
| <input type="checkbox"/> 5/21/2009 3:24 AM | test | Network Usage | All Groups, Folders and SSIDs | 11/21/2008 2:51 AM | 5/21/2009 2:51 AM |
| <input type="checkbox"/> 5/21/2009 3:05 AM | yourdomain.user session | User Session | All Groups, Folders and SSIDs | 5/20/2009 2:00 AM | 5/21/2009 2:00 AM |
| <input type="checkbox"/> 5/21/2009 3:05 AM | yourdomain.radius authentication issues | RADIUS Authentication Issues | All Groups, Folders and SSIDs | 5/20/2009 2:00 AM | 5/21/2009 2:00 AM |
| <input type="checkbox"/> 5/21/2009 2:48 AM | yourdomain.new users | New Users | All Groups, Folders and SSIDs | 5/20/2009 2:00 AM | 5/21/2009 2:00 AM |
| <input type="checkbox"/> 5/21/2009 2:48 AM | yourdomain.new rogue devices | New Rogue Devices | All Groups and Folders | 5/20/2009 2:00 AM | 5/21/2009 2:00 AM |
| <input type="checkbox"/> 5/21/2009 2:48 AM | yourdomain.network usage | Network Usage | All Groups, Folders and SSIDs | 5/20/2009 2:00 AM | 5/21/2009 2:00 AM |
| <input type="checkbox"/> 5/21/2009 2:24 AM | yourdomain.memory and cpu utilization | Memory and CPU Utilization | All Groups and Folders | 5/20/2009 2:00 AM | 5/21/2009 2:00 AM |
| <input type="checkbox"/> 5/21/2009 2:23 AM | yourdomain.inventory | Inventory | All Groups and Folders | - | - |
| <input type="checkbox"/> 5/21/2009 2:23 AM | yourdomain.ids-event | IDS Events | All Groups and Folders | 5/20/2009 2:00 AM | 5/21/2009 2:00 AM |

Select All - Unselect All

Generated reports for other roles:
 1-5 of 5 Reports Page 1 of 1

| Role | Generation Time | Title | Type | Subject | Report Start | Report End |
|-------------------------------------|-------------------|----------------------------------|-------------------|-------------------------------|--------------------|--------------------|
| <input type="checkbox"/> Admin Team | 4/24/2009 9:19 AM | Capacity Report From Cron | Capacity Planning | All Groups, Folders and SSIDs | 4/23/2009 12:00 AM | 4/24/2009 12:00 AM |
| <input type="checkbox"/> Admin Team | Failed | Capacity Report From Cron | Capacity Planning | All Groups, Folders and SSIDs | 4/23/2009 12:00 AM | 4/24/2009 12:00 AM |
| <input type="checkbox"/> Partner | 4/28/2009 7:15 AM | PCICompliance-Detailed-3wks-Acme | PCI Compliance | Group Acme HQ | 4/7/2009 7:12 AM | 4/28/2009 7:12 AM |

Select All - Unselect All

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

Figure 149 Reports > Generated Page with 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 149 displays the **Detail** page for the most recent version of that report.

Using Daily Reports

This section describes the reports supported in OV3600. These reports can be accessed from the bottom of the **Reports > Generated** page, and are presented in alphabetical order as follows in [Table 134](#):

Viewing Generated Reports

To display all generated reports that are currently scheduled on OV3600, navigate to the **Reports > Generated** page. [Figure 148](#) and [Figure 149](#) illustrate this page. This page supports the following general viewing options:

- By default, the reports on the **Reports > Generated** page are sorted by **Generation Time**. You can sort reports by any other category (column header) in sequential or reverse sequential order.
- Click a report title to view details for each scheduled report. Click **Add** to create new generated reports. Generated reports are scheduled and custom configurable.
- Scroll to the bottom of the **Reports > Generated** page, and click any of the 13 report types to view the most recent version of any report. This function is independent of scheduled reports.
- The **Reports > Details** page launches when you click any report title from this page. The content of the **Reports > Details** page varies significantly according to the report type.

The **Generated Reports** page contains less columns and information than the **Definitions** page. [Table 134](#) describes each column for the **Reports > Generated** page.

Table 134 Report > Definition Page Fields and Descriptions

| Field | Description |
|-----------------------|---|
| Generated Time | Displays the date and time of the last time the report was run, or when the latest report is available. Clicking the link in this field displays the latest version of a given report. When the latest version of a given report is not available, this field is blank. In this case, a report can be run by selecting the report title and clicking Run . |
| Title | Displays title of the report. This is a user-configured field when creating the report. |
| Type | Displays the type of the report. This can be one of 13 report types in OV3600. |
| Subject | Displays the scope of the report, to include groups, folders, SSIDs, or any combination of these that are included in the report. |
| Report Start | Displays the beginning of the time period covered in the report. |
| Report End | Displays the end of the time period covered in the report. |
| Role | Added to the Reports definitions for other roles section, this column cites the roles for which additional reports are defined. |

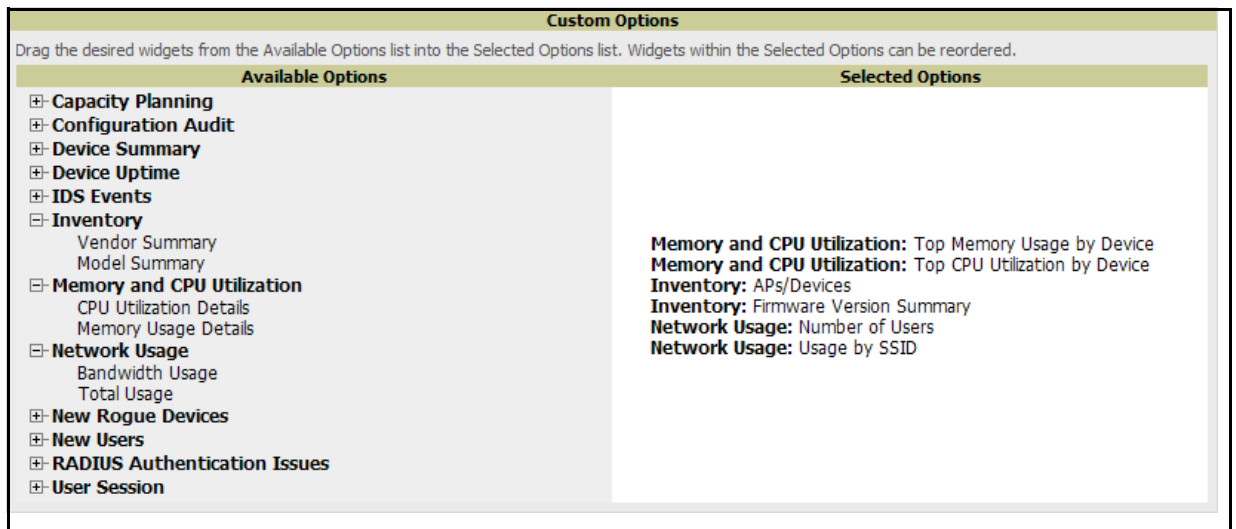
Using Custom Reports

Custom reports allow users to specify the data that should be included in a report and how it should be displayed.

Perform these steps to create a **Custom Report**.

1. Navigate to the **Reports > Definitions** page.
2. Click the **Add** button.
3. Select **Custom** in the type drop down. The **Custom Options** section will open up as shown in [Figure 150](#).

Figure 150 OV3600 Custom Options Illustration



The left pane of the **Custom Options** window lists all available data that can be included in the report. The data is broken down by report. If for example, the data you want to include is in the Inventory report, click **Inventory** to view a list of all available inventory information. Then, simply drag the desired data from the **Available Options** list on the left to the **Selected Options** pane on the right. The order of the data in the **Selected Options** section is the order that it will appear in the report. The data can be reordered by dragging an item up or down the list.

Using the Capacity Planning Report

The **Capacity Planning Report** tracks device bandwidth capacity and throughput in device groups, folders, and SSIDs. This report assists in analyzing device capacity and performance on the network, and such analysis can help to achieve network efficiency and improved experience for users.

This report is based on interface-level activity. The information in this report can be sorted by any column header in sequential or reverse-sequential order by clicking the column heading.

Refer also to the “[Using the Network Usage Report](#)” on page 264 for additional bandwidth information.

Perform these steps to view the most recent **Capacity Planning Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Latest Capacity Planning Report** to display **Detail** device capacity information for all devices. The report provides multiple links to additional device configuration, folders, and additional OV3600 pages.

The following figures and [Table 135](#) illustrate and describe the contents of the **Capacity Planning Report**.

Figure 151 *OV3600 Capacity Planning Report Illustration (Split View)*

Daily Capacity Planning Report for All Groups, Folders and SSIDs

Restricted to hours 08:00-18:00
 1% of Capacity for 0-100% of the time, weekdays only
 5/13/2009 9:00 PM to 5/20/2009 9:00 PM
 Generated on 5/20/2009 9:01 PM

XML (XHTML) export
 Email this report
 Print report

Interfaces

1-3 of 3 Interfaces Page 1 of 1

| Device | Interface | Group | Folder | Controller | Time Above 1% of Capacity | Capacity Combined (b/s) |
|---------|-----------|-----------------|------------------------------|--------------|---------------------------|-------------------------|
| Unnamed | 802.11a | airespacegroup | Top | MXR-2-314644 | 14 hrs 30 mins (8.63%) | 24000000 |
| Unnamed | 802.11b | airespacegroup | Top | MXR-2-314644 | 14 hrs 30 mins (8.63%) | 24000000 |
| ap:78 | 802.11an | ControllerGroup | Top > Controllers > ArubaAps | Aruba3600-US | 3 hrs 0 mins (1.79%) | 15000000 |

| Usage While > Threshold (Combined) | Overall Usage (Combined) | Usage While > Threshold (In) | Overall Usage (In) | Usage While > Threshold (Out) | Overall Usage (Out) |
|------------------------------------|--------------------------|------------------------------|--------------------|-------------------------------|---------------------|
| 270.98% | 74.85% | 124.18% | 34.30% | 146.79% | 40.55% |
| 278.47% | 76.92% | 131.67% | 36.37% | 146.80% | 40.55% |
| 48.03% | 2.79% | 3.46% | 0.21% | 44.57% | 2.58% |

Table 135 *Capacity Planning Report Fields and Contents, Top Portion*

| Field | Description |
|--|--|
| Device | Displays the device type or name. |
| Interface | Displays the type of 802.11 wireless service supported by the device. |
| Group | Displays the device group with which the device is associated. |
| Folder | Displays the folder with which the device is associated. |
| Controller | Displays the controller with which a device operates. |
| Time Above 1% of Capacity | Displays the time duration in which the device has functioned above 0% of capacity. A low percentage of use in this field may indicate that a device is under-used or poorly configured in relation to its capacity, or in relation to user needs. |
| Capacity Combined (b/s) | Displays the combined capacity in and out of the device, in bits-per-second. |
| Usage While > Threshold (Combined) | Displays the time in which a device has functioned above defined threshold capacity, both in and out. |
| Overall Usage (Combined) | Displays the overall usage of the device, both combined in and out traffic. |

Table 135 Capacity Planning Report Fields and Contents, Top Portion (Continued)

| Field | Description |
|---|---|
| Usage While > Threshold (in) | Displays device usage that exceeds the defined and incoming threshold capacity. |
| Overall Usage (In) | Displays overall device usage for incoming data. |
| Usage While > Threshold (Out) | Displays device usage for outgoing data that exceeds defined thresholds. |
| Overall Usage (Out) | Displays device usage for outgoing data. |

Using the Configuration Audit Report

The **Configuration Audit Report** provides an inventory of device configurations on the network, enabling you to display information one device at a time, one folder at a time, or one device group at a time. This report links to additional configuration pages.

Perform these steps to view the most recent version of the report, then to configure a given device using this report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Latest Configuration Audit Report** to display **Detail** device configuration information for all devices. The ensuing **Detail** report can be very large in size, and provides multiple links to additional device configuration or information display pages.
3. You can display device-specific configuration to reduce report size and to focus on a specific device. When viewing configured devices on the **Detail** page, click a device in the **Name** column. The device-specific configuration appears.
4. You can create or assign a template for a given device from the **Detail** page. Click **Add a Template** when viewing device-specific configuration information.
5. You can audit the current device configuration from the **Detail** page. Click **Audit** when viewing device-specific information.
6. You can display archived configuration about a given device from the **Detail** page. Click **Show Archived Device Configuration**.

Figure 152 and Table 136 illustrate and describe the general **Configuration Audit** report and related contents.

Figure 152 Reports > Generated > Daily Configuration Audit Report Illustration, Abbreviated Example

Daily Configuration Audit Report for All Groups, Folders and SSIDs

Generated on 5/21/2009 2:21 AM

[XML \(XHTML\) export](#)
[Email this report](#)
[Print report](#)

1-20 of 360 Items Page 1 of 18 > > |

| Name ▲ | Folder | Group | Mismatches | | | | | | |
|------------------------------|--|----------|---|------------------------------|------------------------------|----------|--|-----------|---|
| 11.1.3 | Top > Sunnyvale HQ | Aruba HQ | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e0e0e0;"> <th style="text-align: left;">Current Device Configuration</th> <th style="text-align: left;">Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Location</td> <td>(failed to fetch) Not Available</td> </tr> <tr> <td>Mesh Role</td> <td>None Mesh AP</td> </tr> </tbody> </table> | Current Device Configuration | Desired Device Configuration | Location | (failed to fetch) Not Available | Mesh Role | None Mesh AP |
| Current Device Configuration | Desired Device Configuration | | | | | | | | |
| Location | (failed to fetch) Not Available | | | | | | | | |
| Mesh Role | None Mesh AP | | | | | | | | |
| 11.1.4 | Top > Sunnyvale HQ | Aruba HQ | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e0e0e0;"> <th style="text-align: left;">Current Device Configuration</th> <th style="text-align: left;">Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Location</td> <td>(failed to fetch) Not Available</td> </tr> <tr> <td>Mesh Role</td> <td>None Mesh AP</td> </tr> </tbody> </table> | Current Device Configuration | Desired Device Configuration | Location | (failed to fetch) Not Available | Mesh Role | None Mesh AP |
| Current Device Configuration | Desired Device Configuration | | | | | | | | |
| Location | (failed to fetch) Not Available | | | | | | | | |
| Mesh Role | None Mesh AP | | | | | | | | |
| 11.1.5 | Top > Sunnyvale HQ | Aruba HQ | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e0e0e0;"> <th style="text-align: left;">Current Device Configuration</th> <th style="text-align: left;">Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Location</td> <td>(failed to fetch) Not Available</td> </tr> <tr> <td>Mesh Role</td> <td>None Mesh AP</td> </tr> </tbody> </table> | Current Device Configuration | Desired Device Configuration | Location | (failed to fetch) Not Available | Mesh Role | None Mesh AP |
| Current Device Configuration | Desired Device Configuration | | | | | | | | |
| Location | (failed to fetch) Not Available | | | | | | | | |
| Mesh Role | None Mesh AP | | | | | | | | |
| 11.1.6 | Top > Sunnyvale HQ | Aruba HQ | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e0e0e0;"> <th style="text-align: left;">Current Device Configuration</th> <th style="text-align: left;">Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Location</td> <td>(failed to fetch) Not Available</td> </tr> <tr> <td>Mesh Role</td> <td>None Mesh AP</td> </tr> </tbody> </table> | Current Device Configuration | Desired Device Configuration | Location | (failed to fetch) Not Available | Mesh Role | None Mesh AP |
| Current Device Configuration | Desired Device Configuration | | | | | | | | |
| Location | (failed to fetch) Not Available | | | | | | | | |
| Mesh Role | None Mesh AP | | | | | | | | |
| 1210-5 | Top > Sunnyvale HQ > Lab | Aruba HQ | <pre> Template: Actual aaa accounting network acct_methods start-stop group rad_acct Actual aaa authentication login eap_methods group rad_eap Actual aaa authentication login eap_methods4 group rad_eap4 Actual aaa authentication login mac_methods local Actual aaa authorization exec default local Actual aaa cache profile admin_cache Actual all Actual aaa group server radius dummy Actual aaa group server radius rad_acct Actual aaa group server radius rad_admin Actual cache authentication profile admin_cache Actual cache authorization profile admin_cache Actual cache expiry 1 Actual aaa group server radius rad_eap Actual aaa group server radius rad_eap4 Actual server 10.2.25.180 auth-port 1645 acct-port 1646 Actual server 10.2.25.180 auth-port 1812 acct-port 1813 </pre> | | | | | | |

Airwave_Cisco_LWAPP Top > Sunnyvale HQ > HQ Cisco LWAPP Research Lab

| | Current Device Configuration | Desired Device Configuration |
|-----------------------------------|--|--|
| 802.11a Channel Assignment Method | Automatic | Static |
| 802.11a Coverage Measurement | 180 | 300 |
| 802.11a DCA Channel 165 | Disabled | Enabled |
| 802.11a DCA Channel 190 | Disabled | Enabled |
| 802.11a DCA Channel 196 | Disabled | Enabled |

Table 136 Information Categories in Reports > Generated > Daily Configuration Audit Report

| Field | Description |
|-------------------|--|
| Name | Displays the device name for every device on the network. Clicking a given device name in this column allows you to display device-specific configuration. |
| Folder | Displays the folder in which the device is configured in OV3600. Clicking the folder name in this report displays the APs/Devices > List page for additional device, folder and configuration options. |
| Group | Displays the group with which any given device associates. Clicking the group for a given device takes you to the Groups > Monitor page for that specific group, to display graphical group information, modification options, alerts, and an audit log for the related group. |
| Mismatches | This field displays configuration mismatch information. When a device configuration does not match ideal configuration, this field displays the ideal device settings compared to current settings. |

Using the Device Summary Report

The **Device Summary Report** identifies devices that are the most or least used devices, and a comprehensive list of all devices. One potential use of this report is to establish more equal bandwidth distribution across multiple devices. This report contains the following five lists of devices.

- **Most Utilized by Maximum Number of Users**—By default, this list displays the 10 devices that support the highest numbers of users. This list provides links to additional information or configuration pages for each device to make adjustments, as desired.
- **Most Utilized by Bandwidth**—By default, this list displays the 10 devices that consistently have the highest bandwidth consumption during the time period defined for the report. This list provides links to additional information or configuration pages for each device.
- **Least Utilized by Maximum Number of Simultaneous Users**—By default, this list displays the 10 devices that are the least used, according to the number of users.
- **Least Utilized by Bandwidth**—By default, this list displays the 10 devices that are the least used, according to the bandwidth throughput.



You can specify the number of devices that appear in each of the first four categories in the Reports > Definitions > Add page.

- **Devices**—This list displays all devices in OV3600. By default is sorted alphabetically by device name.

Any section of this report can be sorted by any of the columns:

- **Rank**
- **AP/Device**
- **Number of Users**
- **Max Simultaneous Users**
- **Total Bandwidth (MB)**
- **Average Bandwidth (kbps)**
- **Location**
- **Controller**
- **Folder**
- **Group**

For example, you can specify a location and then sort the **Devices** list by the **Location** column to see details by location, or you can see all of the APs associated with a particular controller by sorting on the controller column. If the AP name contains information about the location of the AP, you can sort by AP name.

If sorting the **Devices** list does not provide you with sufficient detail, you can specify a **Group** or **Folder** in the report **Definition** of a custom report. If you create a separate Group or Folder for each set of master and local controllers, you can generate a separate report for each Group or Folder. With this method, the summary sections of each report contain only devices from that Group or Folder.

Perform these steps to view the most recent version of this report, and to adjust configurations for over-used or under-used devices.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Device Summary Report** to display **Detail** device information. You can use this report as the central starting point to reconfigure over-used or under-used devices.
3. To generate more reports that cover a greater span of time, refer to [“Viewing Generated Reports” on page 252](#).

Figure 153 Reports > Generated > Daily Device Summary Report Illustration

| Daily Device Summary Report for All Groups, Folders and SSIDs | | | | | | | | | |
|---|---------------------|------------------------|------------------------|--------------------------|--------------------------|---------------------|-------------------------------------|-------------------------------------|-------------|
| 5/20/2009 2:00 AM to 5/21/2009 2:00 AM Generated on 5/21/2009 2:22 AM | | | | | | | | | |
| XML (XHTML) export 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 | AL16 | 210 | 165 | 34028.71 | 3150.81 | Aruba Networks | - | Top | HQ |
| 2 | RAP-Local | 210 | 94 | 24047.37 | 2226.61 | 1344 Server Room | - | Top > Sunnyvale HQ > HQ-RAP | HQ-RemoteAP |
| 3 | Finance-AL27 | 42 | 27 | 3132.23 | 290.02 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 4 | AL12 | 32 | 20 | 1262.57 | 116.90 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 5 | Operations-AL25 | 38 | 19 | 3705.61 | 343.11 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 6 | Sales-AL7 | 33 | 19 | 2011.28 | 186.23 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 7 | AL16 | 25 | 18 | 1133.07 | 104.91 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 8 | TrainingCenter-AL31 | 26 | 17 | 1946.03 | 180.19 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 9 | DevPit-AL1 | 31 | 17 | 9556.34 | 884.85 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 10 | Legal-AL21 | 36 | 15 | 2851.14 | 263.99 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| Most Utilized by Bandwidth | | | | | | | | | |
| Rank | AP/Device | Number of Users | Max Simultaneous Users | Total Bandwidth (MB) | Average Bandwidth (kbps) | Location | Controller | Folder | Group |
| 1 | jluther-ap7 | 210 | 165 | 34028.71 | 3150.81 | Aruba Networks | - | Top | HQ |
| 2 | RAP-Local | 210 | 94 | 24047.37 | 2226.61 | 1344 Server Room | - | Top > Sunnyvale HQ > HQ-RAP | HQ-RemoteAP |
| 3 | DevPit-AL1 | 31 | 17 | 9556.34 | 884.85 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 4 | Operations-AL25 | 38 | 19 | 3705.61 | 343.11 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 5 | Finance-AL27 | 42 | 27 | 3132.23 | 290.02 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 6 | Legal-AL21 | 36 | 15 | 2851.14 | 263.99 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 7 | MainLobby-AL15 | 13 | 6 | 2582.02 | 239.08 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| 8 | mnadella-ap65 | 1 | 2 | 2524.86 | 233.78 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 9 | jluther-ap70 | 1 | 1 | 2393.47 | 221.62 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 10 | Sales-AL7 | 33 | 19 | 2011.28 | 186.23 | Not Available | ethersphere-lms3 | Top > Sunnyvale HQ | HQ |
| Least Utilized by Maximum Number of Simultaneous Users | | | | | | | | | |
| Rank | AP/Device | Number of Users | Max Simultaneous Users | Total Bandwidth (MB) | Average Bandwidth (kbps) | Location | Controller | Folder | Group |
| 1 | dfskn-ap70 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 2 | LWAPP_A082 | 0 | 0 | 0.00 | 0.00 | default location | Airwave_Cisco_LWAPP | Top > Sunnyvale HQ > HQ Cisco LWAPP | HQ-RemoteAP |
| 3 | mkirby-ap70 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 4 | 1210-5 | 0 | 0 | 0.00 | 0.00 | - | - | Top > Sunnyvale HQ > Lab | HQ |
| 5 | jtse-ap65 | 0 | 0 | 0.00 | 0.00 | - | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 6 | wldng-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 7 | jhoward-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 8 | AP4 | 0 | 0 | 0.00 | 0.00 | - | WS2000 | Top > Pharmacy | HQ |
| 9 | hkurmala-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 10 | SW-3 | 0 | 0 | 0.00 | 0.00 | Not Available | alpha-master-1 | Top > Outdoor | HQ |
| Least Utilized by Bandwidth | | | | | | | | | |
| Rank | AP/Device | Number of Users | Max Simultaneous Users | Total Bandwidth (MB) | Average Bandwidth (kbps) | Location | Controller | Folder | Group |
| 1 | dfskn-ap70 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 2 | LWAPP_A082 | 0 | 0 | 0.00 | 0.00 | default location | Airwave_Cisco_LWAPP | Top > Sunnyvale HQ > HQ Cisco LWAPP | HQ-RemoteAP |
| 3 | mkirby-ap70 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 4 | 1210-5 | 0 | 0 | 0.00 | 0.00 | - | - | Top > Sunnyvale HQ > Lab | HQ |
| 5 | jtse-ap65 | 0 | 0 | 0.00 | 0.00 | - | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 6 | wldng-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 7 | jhoward-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 8 | AP4 | 0 | 0 | 0.00 | 0.00 | - | WS2000 | Top > Pharmacy | HQ |
| 9 | hkurmala-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ |
| 10 | SW-3 | 0 | 0 | 0.00 | 0.00 | Not Available | alpha-master-1 | Top > Outdoor | HQ |
| Devices | | | | | | | | | |
| 1-20 of 487 Devices Page 1 of 25 > > | | | | | | | | | |
| AP/Device | Number of Users | Max Simultaneous Users | Total Bandwidth (MB) | Average Bandwidth (kbps) | Location | Controller | Folder | Group | |
| bmoyle-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ | |
| Test Devices | 0 | 0 | 0.00 | 0.00 | - | - | Top | HQ-RemoteAP | |
| psanford-ap65 | 0 | 0 | 0.00 | 0.00 | - | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ | |
| (id: 13653) | 0 | 0 | 0.00 | 0.00 | - | - | Top | HQ | |
| SV-1252-SHIP-22:60 | 0 | 0 | 0.00 | 0.00 | - | - | Top > Sunnyvale HQ > Lab | HQ | |
| dmontgomery-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ | |
| jhoward-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ | |
| mkirby-ap70 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ | |
| lwapp-1250-13:21:1e | 0 | 0 | 0.00 | 0.00 | somewhere | CiscoController | Top > Sunnyvale HQ > Lab | HQ | |
| Cisco-IWL-1 | 0 | 0 | 0.00 | 0.00 | Indoor Laborador | - | Top | HQ | |
| jtse-ap65 | 0 | 0 | 0.00 | 0.00 | - | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ | |
| LWAPP_A082 | 0 | 0 | 0.00 | 0.00 | default location | Airwave_Cisco_LWAPP | Top > Sunnyvale HQ > HQ Cisco LWAPP | HQ | |
| 1210-5 | 0 | 0 | 0.00 | 0.00 | - | - | Top > Sunnyvale HQ > Lab | HQ | |
| wldng-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ | |
| dfskn-ap70 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ | |
| SW-3 | 0 | 0 | 0.00 | 0.00 | Not Available | alpha-master-1 | Top > Outdoor | HQ | |
| AP4 | 0 | 0 | 0.00 | 0.00 | - | WS2000 | Top > Pharmacy | HQ | |
| Aruba800 | 0 | 0 | 0.00 | 0.00 | - | - | Top | HQ | |
| hkurmala-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ | |
| svtamanti-ap65 | 0 | 0 | 0.00 | 0.00 | Not Available | RAP-Local | Top > Sunnyvale HQ > HQ-RAP | HQ | |

Table 137 Reports > Generated > Daily Device Summary Report Fields and Descriptions

| Field | Description |
|-------------------------------|---|
| Rank | The rank column for any section of this report establishes the top 10 devices for any category, and these are listed in sequential or reverse-sequential order. |
| AP/Device | Displays the name of the device, which can be a MAC address or other identifier. |
| Number of Users | Displays the number of users associated with each device. |
| Max Simultaneous Users | Displays the maximum number of users that were active on the associated device during the period of time that the report covers. |

Table 137 Reports > Generated > Daily Device Summary Report Fields and Descriptions

| Field | Description |
|---------------------------------|--|
| Total Bandwidth (MB) | Displays the bandwidth in megabytes that the device supported during the period of time covered by the report. |
| Average Bandwidth (kbps) | Displays the average bandwidth throughput for the device during the period of time covered by the report. |
| Location | Displays the location of the device that is included in any category of the report. |
| Controller | Displays the controller to which any included device is associated. |
| Folder | Displays the folder with which a device is associated. |
| Group | Displays the device group with which a device is associated. |

Using the Device Uptime Report

The **Device Uptime Report** monitors device performance and availability on the network, tracking uptime by multiple criteria to include the following:

- Total average uptime by SNMP and ICMP
- Average uptime by device group
- Average uptime by device folder

You can use this report as the central starting point to improve uptime by multiple criteria. This report covers protocol-oriented, device-oriented, or SSID-oriented information. This report can help to monitor and optimize the network in multiple ways. This report can demonstrate service parameters, can establish locations that have superior or problematic uptime availability, and can help with additional analysis in multiple ways. Locations, device groups, or other groupings within a network can be identified as needing attention or can be proven to have superior performance when using this report.

Perform these steps to view the most recent version of the **Device Uptime** report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Device Uptime Report** to display report **Detail** information.
3. To generate more reports of this type that cover a greater span of time, refer to [“Reports > Definitions Page Overview” on page 249](#).

Figure 154 and Table 137 illustrate and describe the **Reports > Generated > Device Uptime Detail** report.

Figure 154 Reports > Generated > Device Uptime Report Illustration

Daily Device Uptime Report for All Groups, Folders and SSIDs

5/20/2009 2:00 AM to 5/21/2009 2:00 AM
Generated on 5/21/2009 2:23 AM

[XML \(XHTML\) export](#)
[Email this report](#)
[Print report](#)

Total Average Uptime

| SNMP Uptime | ICMP Uptime |
|-------------|-------------|
| 66.82% | 68.10% |

Average Uptime by Group

1-10 of 10 Groups Page 1 of 1

| Group | SNMP Uptime | ICMP Uptime |
|-----------------------|-------------|-------------|
| HQ | 54.55% | 58.28% |
| HQ-RemoteAP | 72.88% | 72.88% |
| Korea Regional Office | 0.00% | 0.00% |
| Outdoor | 100.00% | 100.00% |
| Research Lab | 57.55% | 65.11% |
| Routers/Switches | 49.45% | 69.45% |
| Test3 | 42.38% | 44.45% |
| testlab | 60.42% | 60.42% |
| Training | 39.52% | 45.56% |
| Wireless | 15.11% | 15.11% |

Average Uptime by Folder

1-10 of 10 Folders Page 1 of 1

| Folder | SNMP Uptime | ICMP Uptime | SNMP Uptime (incl. subfolders) | ICMP Uptime (incl. subfolders) |
|-------------------------------------|-------------|-------------|--------------------------------|--------------------------------|
| Top | 27.39% | 42.25% | 66.82% | 68.10% |
| Top > APAC > Korea | 0.00% | 0.00% | 0.00% | 0.00% |
| Top > Outdoor | 54.55% | 54.55% | 54.55% | 54.55% |
| Top > Pharmacy | 7.04% | 7.30% | 7.04% | 7.30% |
| Top > Sunnyvale HQ | 94.19% | 94.19% | 69.77% | 70.54% |
| Top > Sunnyvale HQ > HQ Cisco LWAPP | 66.67% | 66.67% | 66.67% | 66.67% |
| Top > Sunnyvale HQ > HQ-RAP | 72.88% | 72.88% | 72.88% | 72.88% |
| Top > Sunnyvale HQ > Lab | 20.78% | 28.35% | 20.78% | 28.35% |
| Top > Switches | 61.81% | 61.81% | 61.81% | 61.81% |
| Top > Training | 43.91% | 50.63% | 43.91% | 50.63% |

Uptime by Device

1-20 of 217 Devices Page 1 of 11 >>

| Device | Group | Folder | SNMP Uptime | ICMP Uptime | Time Since Last Boot |
|------------------|-------------|-----------------------------|-------------|-------------|------------------------|
| 00:0b:86: | HQ | Top > Sunnyvale HQ > Lab | 0.00% | 0.00% | 0 mins |
| 00:0b:86: | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 0.00% | 0.00% | 0 mins |
| 00:0b:86: | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 0.00% | 0.00% | 0 mins |
| 00:0b:86: | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 0.00% | 0.00% | 0 mins |
| 00:1a:1e: | Acme HQ | Top > Sunnyvale HQ > Lab | 0.00% | 0.00% | 0 mins |
| 00:1a:1e: | Acme HQ | Top > Sunnyvale HQ > Lab | 0.00% | 0.00% | 0 mins |
| 00:1a:1e: | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 99.31% | 99.31% | 13 days 17 hrs 34 mins |
| 00:1a:1e: | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 0.00% | 0.00% | 0 mins |
| 00:1a:1e: | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 0.00% | 0.00% | 0 mins |
| 11.1.2 | Acme HQ | Top > Sunnyvale HQ | 0.00% | 0.00% | 0 mins |
| 1210-5 | Acme HQ | Top > Sunnyvale HQ > Lab | 33.00% | 33.00% | 0 mins |
| 4400 | Acme HQ | Top > Sunnyvale HQ > Lab | 60.42% | 60.42% | 0 mins |
| aayami-ap65 | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 99.66% | 99.66% | 1 day 14 hrs 29 mins |
| acctontw-ap125 | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 23.26% | 23.26% | 0 mins |
| aemory-ap65 | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 99.32% | 99.32% | 22 hrs 48 mins |
| aferm2-ap65 | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 0.00% | 0.00% | 0 mins |
| aharding-ap65 | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 0.00% | 0.00% | 0 mins |
| Airespace-4012-2 | Acme HQ | Top > Sunnyvale HQ > Lab | 0.00% | 60.42% | 0 mins |
| alevy-ap65 | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 98.97% | 98.97% | 0 mins |
| alogan-ap65 | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | 0.00% | 0.00% | 0 mins |

Table 138 Reports > Generated > Device Uptime Report Fields and Descriptions

| Field | Description |
|-----------------------------|--|
| Device | Displays the name of the device. |
| Group | Displays the name of the device's group. |
| Folder | Displays the folder to which the device belongs. |
| SSID | Displays the Service Set Identifier (SSID) set on the device. |
| SNMP Uptime | Displays the percentage of time the device was reachable via ICMP. OV3600 polls the device via SNMP at the rate specified on the Groups > Basic page. |
| ICMP Uptime | Displays the percentage of time the device was reachable via ICMP. If the device is reachable via SNMP it is assumed to be reachable via ICMP. OV3600 only pings the device if SNMP fails and then it pings at the SNMP polling interval rate. |
| Time Since Last Boot | The uptime as reported by the device at the end of the time period covered by the report. |

Using the IDS Events Report

The **IDS Events Report** lists and tracks IDS events on the network involving Access Points (APs) or controller devices. This report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours, and provides links to support additional analysis or configuration in response.

The **Home > License** page also cites IDS events, and triggers can be configured for IDS events. Refer to “[Setting Triggers for IDS Events](#)” on page 212 for additional information.

Perform these steps to view the most recent version of the **IDS Events** report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **IDS Events Report** to display report **Detail** information.
3. Clicking the AP device or controller name takes you to the **APs/Devices > List** page.

[Figure 155](#) and [Table 139](#) illustrate and describe the **Reports > Generated > IDS Events Detail** page.

Figure 155 Reports > Generated > IDS Events Report Illustration

The screenshot shows the 'IDS event yesterday for All Groups and Folders' report. It includes a header with the date range '5/20/2009 2:00 AM to 5/21/2009 2:00 AM' and 'Generated on 5/21/2009 2:23 AM'. There are links for 'XML (XHTML) export', 'Email this report', and 'Print report'. The report is divided into sections: 'Top IDS Events by AP' and 'Top IDS Events by Controller'. Below these are two summary tables. The first table shows 'idhasoft-ap70-2' with 2 total events, first and most recent events on 5/20/2009 at 11:06 PM. The second table shows 'RAP-Local' with 2 total events, also first and most recent on 5/20/2009 at 11:06 PM. At the bottom, a detailed table shows two 'Null-Probe-Response' events with attacker MAC '00:1A:70:77:9C:CF', AP 'idhasoft-ap70-2', Controller 'RAP-Local', Radio '802.11bg', Channel '-', SNR '4', and Precedence '-'. The time for both is '5/20/2009 11:06 PM'.

| AP | Total Events ▲ | First Event | Most Recent Event |
|-----------------|----------------|--------------------|--------------------|
| idhasoft-ap70-2 | 2 | 5/20/2009 11:06 PM | 5/20/2009 11:06 PM |

| Controller | Total Events ▲ | First Event | Most Recent Event |
|------------|----------------|--------------------|--------------------|
| RAP-Local | 2 | 5/20/2009 11:06 PM | 5/20/2009 11:06 PM |

| Attack | Attacker | AP | Controller | Radio | Channel | SNR | Precedence | Time ▼ |
|---------------------|-------------------|-----------------|------------|----------|---------|-----|------------|--------------------|
| Null-Probe-Response | 00:1A:70:77:9C:CF | idhasoft-ap70-2 | RAP-Local | 802.11bg | - | 4 | - | 5/20/2009 11:06 PM |
| Null-Probe-Response | 00:1A:70:77:9C:CF | idhasoft-ap70-2 | RAP-Local | 802.11bg | - | 4 | - | 5/20/2009 11:06 PM |

Table 139 Reports > Generated > IDS Events Detail Fields

| Field | Description |
|--------------------------|---|
| AP | This column lists the AP devices for which IDS events have occurred in the prior 24 hours, and provides a link to the APs/Devices > Monitor page for each. |
| Total Events | This column cites the total number of IDS events for each device that has experienced them during the prior 24-hour period. |
| First Event | This column cites the first IDS event in the prior 24-hour period. |
| Most Recent Event | This column cites the most recent or latest IDS event in the prior 24-hour period. |
| Attack | Displays the name or label for the IDS event. |
| Controller | This column lists the controllers for which IDS events have occurred in the prior 24 hours, and provides a link to the APs/Devices > Monitor page for each. |
| Attacker | Displays the MAC address of the device that generated the IDS event. |
| Radio | Displays the 802.11 radio type associated with the IDS event. |
| Channel | Displays the 802.11 radio channel associated with the IDS event, when known. |
| SNR | Displays the signal-to-noise (SNR) radio associated with the IDS event. |
| Precedence | Displays precedence information associated with the IDS event, when known. |
| Time | Displays the time of the IDS event. |

Using the Inventory Report

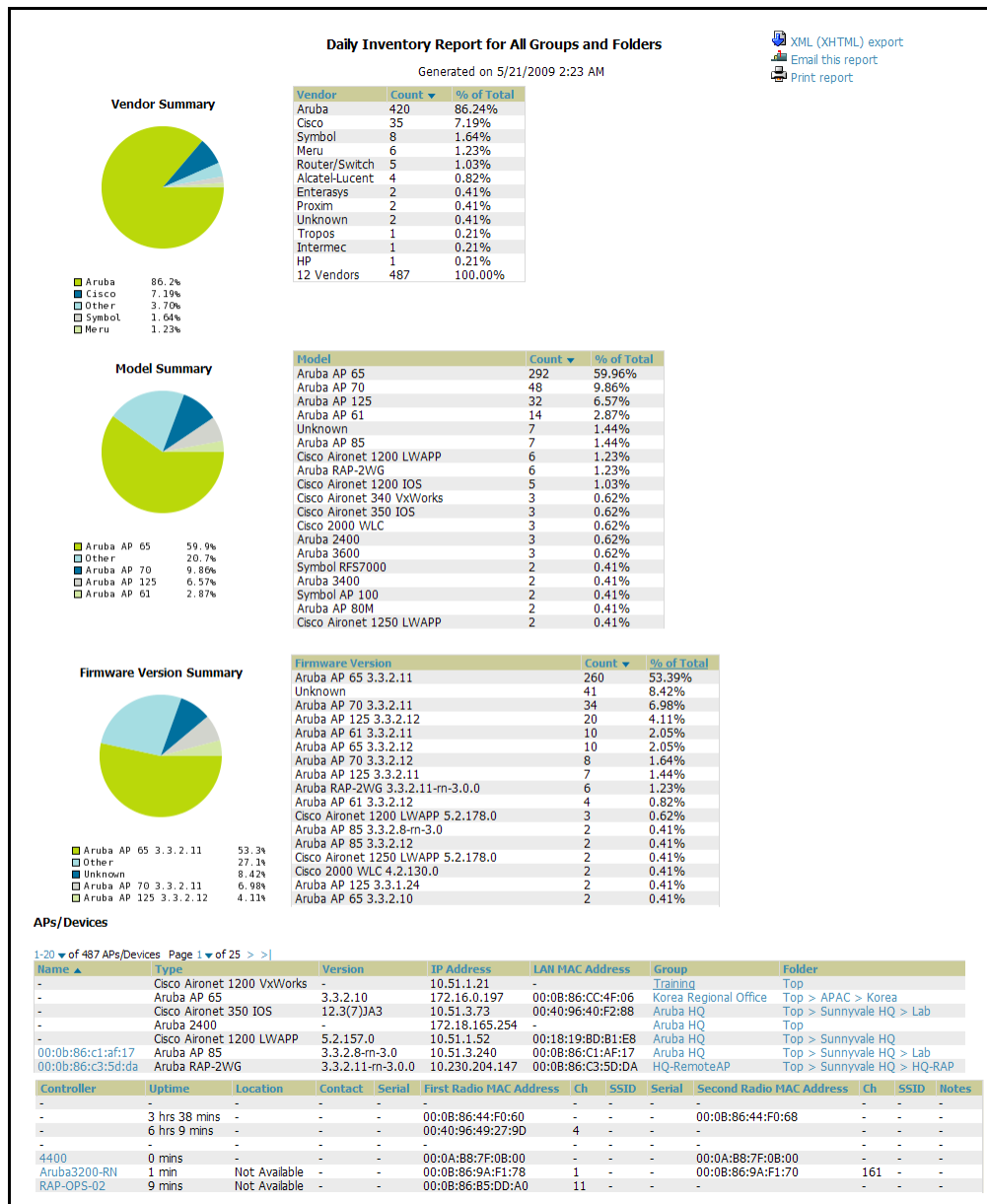
The **Inventory Report** itemizes all devices and firmware versions on the network, to include manufacturer information and graphical pie-chart summaries. The primary sections of this report are as follows:

- **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.

Perform these steps to view the most recent version of the **Inventory report**, illustrated in **Figure 156**

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.

Figure 156 Reports > Generated > Inventory Report Illustration (Split View)



Using the 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 create a scheduled and generated report of this type, refer to “Using Daily Reports” on page 252.

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 157 illustrates the **Reports > Generated > Daily Memory and CPU Utilization Detail** page.

Figure 157 Reports > Generated > Daily Memory and CPU Utilization Report Illustration
(Contents Rearranged for Space)

memory and cpu utilization for All Groups and Folders

5/20/2009 2:00 AM to 5/21/2009 2:00 AM
Generated on 5/21/2009 2:24 AM

XML (XHTML) export

Email this report

Print report

Top CPU Utilization by Device

| Device | Utilization |
|------------------|-------------|
| Aruba-800-116 | 24.76% |
| Aruba2400 | 17.43% |
| Aruba800 | 14.64% |
| Aruba200 | 13.22% |
| alpha-master-1 | 10.43% |
| ethersphere-lms4 | 9.67% |
| ethersphere-lms3 | 7.17% |
| (id: 13260) | 5.45% |
| corp1344-mesh-01 | 4.90% |
| Cisco4-ap | 4.20% |

Top Memory Usage by Device

| Device | Usage |
|------------------|--------|
| Aruba3200-RN | 71.15% |
| alpha-master-1 | 70.86% |
| ethersphere-lms3 | 70.47% |
| Aruba2400 | 70.09% |
| corp1344-mesh-01 | 69.28% |
| Aruba800 | 68.94% |
| ethersphere-lms4 | 68.81% |
| ap | 65.79% |
| Aruba200 | 64.09% |
| Cisco2000 | 63.33% |

CPU Utilization Details

1-20 of 27714 CPU Utilization Details Page 1 of 1386 > >|

| Device | CPU | Start Time | End Time | Utilization |
|--------|-------------|-------------------|-------------------|-------------|
| 1210-5 | Overall CPU | 5/20/2009 2:05 AM | 5/20/2009 2:10 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 2:10 AM | 5/20/2009 2:15 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 2:15 AM | 5/20/2009 2:20 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 2:20 AM | 5/20/2009 2:25 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 2:25 AM | 5/20/2009 2:30 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 2:30 AM | 5/20/2009 2:35 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 2:35 AM | 5/20/2009 2:40 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 2:40 AM | 5/20/2009 2:45 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 2:45 AM | 5/20/2009 2:50 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 2:50 AM | 5/20/2009 2:55 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 2:55 AM | 5/20/2009 3:00 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 3:00 AM | 5/20/2009 3:05 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 3:05 AM | 5/20/2009 3:10 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 3:10 AM | 5/20/2009 3:15 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 3:15 AM | 5/20/2009 3:20 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 3:20 AM | 5/20/2009 3:25 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 3:25 AM | 5/20/2009 3:30 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 3:30 AM | 5/20/2009 3:35 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 3:35 AM | 5/20/2009 3:40 AM | 1.00% |
| 1210-5 | Overall CPU | 5/20/2009 3:40 AM | 5/20/2009 3:45 AM | 1.00% |

Memory Usage Details

1-20 of 4362 Memory Usage Details Page 1 of 218 > >|

| Device | Start Time | End Time | Free | Used | Usage |
|--------|-------------------|-------------------|----------|----------|--------|
| 1210-5 | 5/20/2009 2:05 AM | 5/20/2009 2:10 AM | 2.25 MIB | 3.50 MIB | 60.86% |
| 1210-5 | 5/20/2009 2:10 AM | 5/20/2009 2:15 AM | 2.26 MIB | 3.49 MIB | 60.70% |
| 1210-5 | 5/20/2009 2:15 AM | 5/20/2009 2:20 AM | 2.26 MIB | 3.49 MIB | 60.66% |
| 1210-5 | 5/20/2009 2:20 AM | 5/20/2009 2:25 AM | 2.26 MIB | 3.49 MIB | 60.66% |
| 1210-5 | 5/20/2009 2:25 AM | 5/20/2009 2:30 AM | 2.26 MIB | 3.49 MIB | 60.66% |
| 1210-5 | 5/20/2009 2:30 AM | 5/20/2009 2:35 AM | 2.26 MIB | 3.49 MIB | 60.66% |
| 1210-5 | 5/20/2009 2:35 AM | 5/20/2009 2:40 AM | 2.26 MIB | 3.49 MIB | 60.66% |
| 1210-5 | 5/20/2009 2:40 AM | 5/20/2009 2:45 AM | 2.26 MIB | 3.49 MIB | 60.66% |
| 1210-5 | 5/20/2009 2:45 AM | 5/20/2009 2:50 AM | 2.26 MIB | 3.49 MIB | 60.66% |
| 1210-5 | 5/20/2009 2:50 AM | 5/20/2009 2:55 AM | 2.24 MIB | 3.51 MIB | 60.98% |
| 1210-5 | 5/20/2009 2:55 AM | 5/20/2009 3:00 AM | 2.24 MIB | 3.51 MIB | 61.10% |
| 1210-5 | 5/20/2009 3:00 AM | 5/20/2009 3:05 AM | 2.24 MIB | 3.51 MIB | 61.11% |
| 1210-5 | 5/20/2009 3:05 AM | 5/20/2009 3:10 AM | 2.24 MIB | 3.51 MIB | 61.11% |
| 1210-5 | 5/20/2009 3:10 AM | 5/20/2009 3:15 AM | 2.24 MIB | 3.51 MIB | 61.11% |
| 1210-5 | 5/20/2009 3:15 AM | 5/20/2009 3:20 AM | 2.24 MIB | 3.51 MIB | 61.11% |
| 1210-5 | 5/20/2009 3:20 AM | 5/20/2009 3:25 AM | 2.24 MIB | 3.51 MIB | 61.11% |
| 1210-5 | 5/20/2009 3:25 AM | 5/20/2009 3:30 AM | 2.24 MIB | 3.51 MIB | 61.11% |
| 1210-5 | 5/20/2009 3:30 AM | 5/20/2009 3:35 AM | 2.25 MIB | 3.50 MIB | 60.86% |
| 1210-5 | 5/20/2009 3:35 AM | 5/20/2009 3:40 AM | 2.24 MIB | 3.51 MIB | 61.01% |
| 1210-5 | 5/20/2009 3:40 AM | 5/20/2009 3:45 AM | 2.24 MIB | 3.51 MIB | 61.06% |

Using the Network Usage Report

The **Network Usage Report** contains network-wide information in three categories:

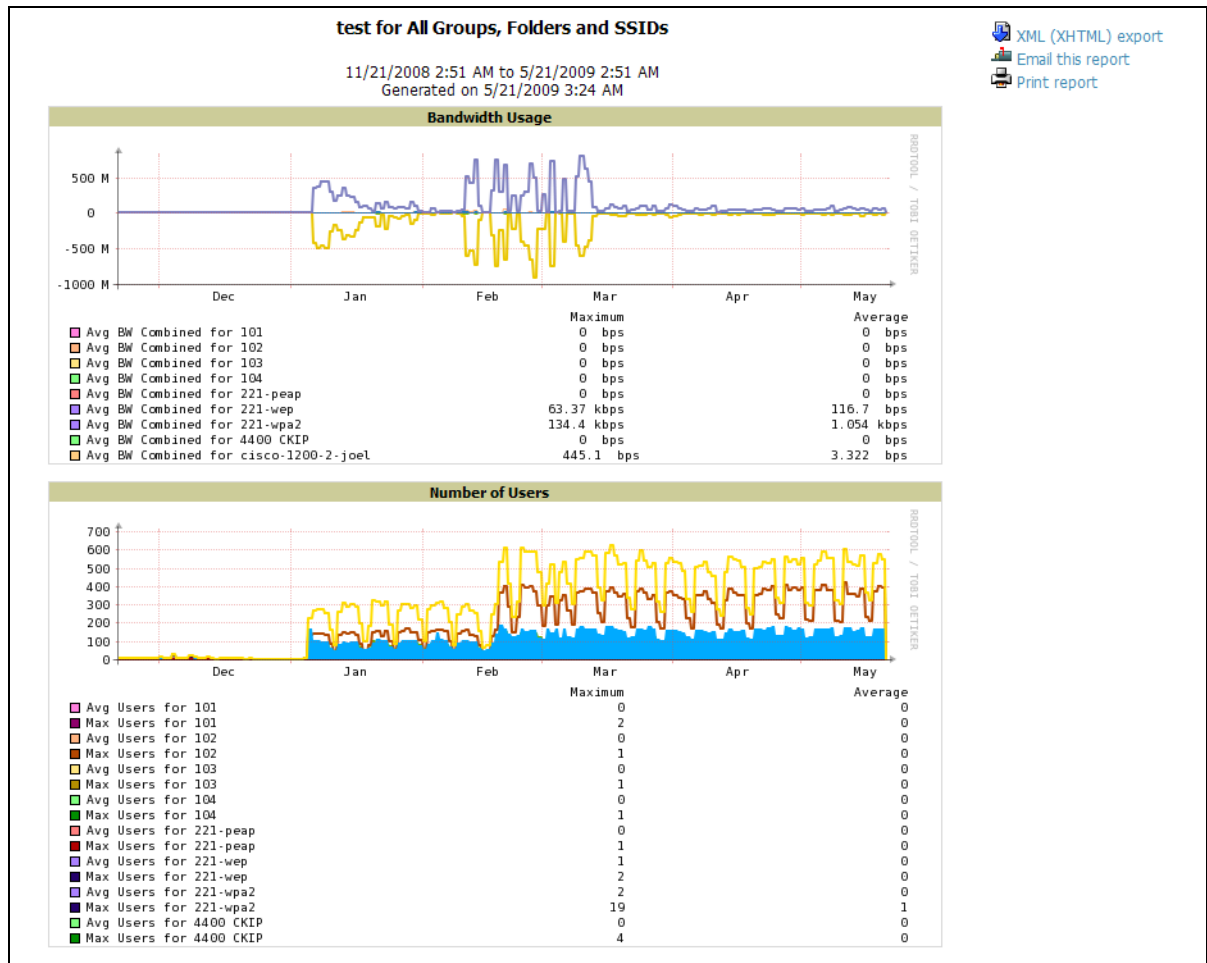
- **Bandwidth usage by device**—maximum and average bandwidth in kbps
- **Number of users by device**—maximum and average by connection instances
- **Number of users by time period**—average bandwidth in and out

Perform these steps to view the most recent version of the **Network Usage Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Network Usage** to display report **Detail** information.
3. The **Details** page allows you to view bandwidth and device usage in three sections, illustrated below.

Figure 158 illustrates the **Reports > Generated > Daily Memory and CPU Utilization Detail** page.

Figure 158 Reports > Generated > Network Usage Report Illustration (Partial Example)



Using the New Rogue Devices Report

The **New Rogue Devices Report** summarizes rogue device information in a number of ways, to include the following categories of information:

- Rogue devices by RAPIDS classification—described in “Using RAPIDS and Rogue Classification” on page 183
- Top rogue devices by number of discovering APs
- Top rogue devices by signal strength
- Graphical summary of rogue devices by LAN MAC address vendor
- Graphical summary of rogue devices by radio MAC address vendor
- Text-based table summary of rogue device counts
- Detailed and text-based table of rogue devices discovered only wirelessly with extensive device parameters and hyperlink interoperability to additional OV3600 pages
- Detailed and text-based table of all rogue devices supporting all discovery methods with extensive device parameters and hyperlink interoperability to additional OV3600 pages
- Detailed and text-based table of discovery events pertaining to the discovery of rogue devices with extensive parameters and hyperlink interoperability to additional OV3600 pages

Perform these steps to view the most recent version of the **New Rogue Devices Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **New Rogue Devices** to display report **Detail** information.
3. The **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 159 Reports > Generated > New Rogue Devices Report Illustration, Top Half of Report

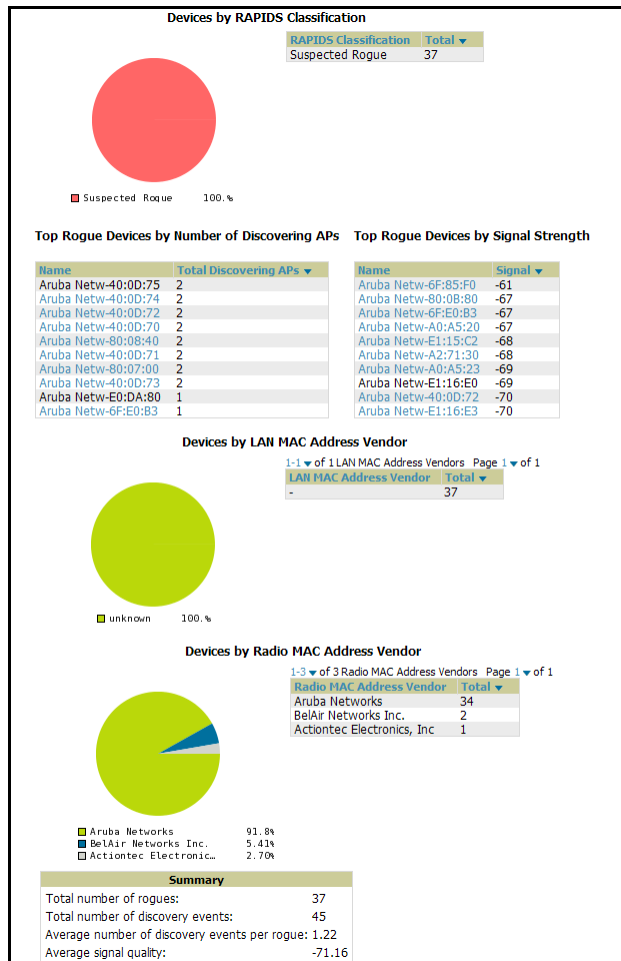


Figure 160 Reports > Generated > New Rogue Devices Report Illustration, Bottom Half of Report (Partial View)

| Devices Discovered Only Wirelessly | | | | | | | | | |
|--|-----------------------|--------------|-----|--------------------|---|-----------------------|---------------------|------|---|
| 1-20 of 37 Rogue Devices Page 1 of 2 > > | | | | | | | | | |
| Name | RAPIDS Classification | Threat Level | Ack | First Discovered | First Discovery Method | First Discovery Agent | Last Discovering AP | Type | |
| Aruba Netw-6F85:F0 | Suspected Rogue | 5 | No | 5/20/2009 4:38 PM | Wireless AP scan | SW-2 | SW-2 | - | - |
| Aruba Netw-A0:A5:20 | Suspected Rogue | 5 | No | 5/20/2009 12:41 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Actontec-F1:CD:02 | Suspected Rogue | 5 | No | 5/20/2009 4:35 AM | Wireless AirWave Management Client scan | - | - | - | - |
| Aruba Netw-80:0B:80 | Suspected Rogue | 5 | No | 5/20/2009 8:12 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-9F:E0:B3 | Suspected Rogue | 5 | No | 5/20/2009 7:07 AM | Wireless AP scan | SW-3 | SW-3 | - | - |
| Aruba Netw-E1:15:C2 | Suspected Rogue | 5 | No | 5/20/2009 9:10 AM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-A2:71:30 | Suspected Rogue | 5 | No | 5/20/2009 4:41 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-A0:A5:23 | Suspected Rogue | 5 | No | 5/20/2009 9:10 AM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-E1:16:E0 | Suspected Rogue | 5 | No | 5/20/2009 12:10 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-8B:74:43 | Suspected Rogue | 5 | No | 5/20/2009 5:12 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-E1:16:E3 | Suspected Rogue | 5 | No | 5/20/2009 12:10 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-40:0D:72 | Suspected Rogue | 5 | No | 5/20/2009 12:41 PM | Wireless AP scan | Corp1344-SW-AP85 | Facilities-AL37 | - | - |
| Aruba Netw-C8:3D:60 | Suspected Rogue | 5 | No | 5/20/2009 6:12 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-40:0D:71 | Suspected Rogue | 5 | No | 5/20/2009 5:12 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| BeAir Net-0F:C8:05 | Suspected Rogue | 5 | No | 5/20/2009 4:35 AM | Wireless AirWave Management Client scan | - | - | - | - |
| BeAir Net-0F:C8:04 | Suspected Rogue | 5 | No | 5/20/2009 4:35 AM | Wireless AirWave Management Client scan | - | - | - | - |
| Aruba Netw-E0:DA:80 | Suspected Rogue | 5 | No | 5/20/2009 7:12 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-E1:B3:C2 | Suspected Rogue | 5 | No | 5/21/2009 1:52 AM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-40:0D:73 | Suspected Rogue | 5 | No | 5/20/2009 8:42 PM | Wireless AP scan | Corp1344-SW-AP85 | Facilities-AL37 | - | - |
| Aruba Netw-40:10:80 | Suspected Rogue | 5 | No | 5/20/2009 8:40 AM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |

| Rogue Devices | | | | | | | | | |
|--|-----------------------|--------------|-----|--------------------|---|-----------------------|---------------------|------|---|
| 1-20 of 37 Rogue Devices Page 1 of 2 > > | | | | | | | | | |
| Name | RAPIDS Classification | Threat Level | Ack | First Discovered | First Discovery Method | First Discovery Agent | Last Discovering AP | Type | |
| Aruba Netw-80:07:00 | Suspected Rogue | 5 | No | 5/20/2009 4:41 PM | Wireless AP scan | Corp1344-SW-AP85 | Facilities-AL37 | - | - |
| Aruba Netw-40:09:03 | Suspected Rogue | 5 | No | 5/20/2009 9:22 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-E1:B3:C1 | Suspected Rogue | 5 | No | 5/20/2009 4:11 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-E1:15:C2 | Suspected Rogue | 5 | No | 5/20/2009 9:10 AM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Actontec-F1:CD:02 | Suspected Rogue | 5 | No | 5/20/2009 4:35 AM | Wireless AirWave Management Client scan | - | - | - | - |
| Aruba Netw-6F:85:F0 | Suspected Rogue | 5 | No | 5/20/2009 7:07 AM | Wireless AP scan | SW-2 | SW-2 | - | - |
| Aruba Netw-6F:E0:B3 | Suspected Rogue | 5 | No | 5/20/2009 7:07 AM | Wireless AP scan | SW-3 | SW-3 | - | - |
| Aruba Netw-E0:DA:80 | Suspected Rogue | 5 | No | 5/20/2009 7:12 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| BeAir Net-0F:C8:04 | Suspected Rogue | 5 | No | 5/20/2009 4:35 AM | Wireless AirWave Management Client scan | - | - | - | - |
| BeAir Net-0F:C8:05 | Suspected Rogue | 5 | No | 5/20/2009 4:35 AM | Wireless AirWave Management Client scan | - | - | - | - |
| Aruba Netw-9F:85:F0 | Suspected Rogue | 5 | No | 5/20/2009 4:38 PM | Wireless AP scan | SW-2 | SW-2 | - | - |
| Aruba Netw-40:10:80 | Suspected Rogue | 5 | No | 5/20/2009 8:40 AM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-8B:74:41 | Suspected Rogue | 5 | No | 5/20/2009 4:11 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-E1:16:E3 | Suspected Rogue | 5 | No | 5/20/2009 12:10 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-96:C8:11 | Suspected Rogue | 5 | No | 5/20/2009 4:11 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-40:0D:73 | Suspected Rogue | 5 | No | 5/20/2009 8:42 PM | Wireless AP scan | Corp1344-SW-AP85 | Facilities-AL37 | - | - |
| Aruba Netw-40:0D:72 | Suspected Rogue | 5 | No | 5/20/2009 12:41 PM | Wireless AP scan | Corp1344-SW-AP85 | Facilities-AL37 | - | - |
| Aruba Netw-A0:A5:20 | Suspected Rogue | 5 | No | 5/20/2009 12:41 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |
| Aruba Netw-80:08:40 | Suspected Rogue | 5 | No | 5/20/2009 7:42 PM | Wireless AP scan | Corp1344-SW-AP85 | Facilities-AL37 | - | - |
| Aruba Netw-80:0A:20 | Suspected Rogue | 5 | No | 5/20/2009 10:52 PM | Wireless AP scan | Corp1344-SW-AP85 | Corp1344-SW-AP85 | - | - |

| Discovery Events | | | | | | | | | | |
|---|------|---------|---------------------------------|-----|--------------|---------------|------|------------|-------------------|------------------|
| 1-20 of 45 Discovery Events Page 1 of 3 > > | | | | | | | | | | |
| Rogue | RSSI | Channel | SSID | WEP | Network Type | Switch/Router | Port | IP Address | Time | Discovery Method |
| Aruba Netw-E4:50:21 | 21 | 11 | aruba-ap | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-E1:B3:C3 | 12 | 11 | sus_4 | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-E1:B3:C1 | 12 | 11 | aruba-ap | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-E1:16:E3 | 23 | 11 | sus_4 | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-E1:16:E0 | 20 | 11 | gre2 | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-E1:15:C2 | 18 | 11 | sus_3 | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-C8:3D:60 | 13 | 11 | gre2 | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-96:C8:11 | 25 | 52 | ethersphere-wpa2 | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-96:C8:10 | 24 | 52 | guest | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-80:0B:80 | 14 | 11 | aruba-ap | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-80:0A:20 | 17 | 11 | aruba-ap | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-80:08:40 | 10 | 11 | aruba-ap | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-49:10:80 | 19 | 11 | qa-hk-soak-chuck-bridge | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-40:0D:73 | 13 | 11 | qa-hk-soak-chuck-bridge-persist | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-40:0D:71 | 10 | 11 | qa-hk-soak-chuck-bridge-always | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-40:0D:71 | 22 | 11 | qa-hk-soak-chuck-bridge-always | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-40:0D:70 | 13 | 11 | qa-hk-soak-chuck-bridge | - | AP | - | - | - | 5/21/2009 2:22 AM | Wireless AP scan |
| Aruba Netw-E1:B3:C2 | 22 | 11 | sus_3 | - | AP | - | - | - | 5/21/2009 1:52 AM | Wireless AP scan |
| Aruba Netw-E0:DA:80 | 22 | 11 | gre2 | - | AP | - | - | - | 5/21/2009 1:52 AM | Wireless AP scan |
| Aruba Netw-A0:A5:20 | 22 | 11 | gre2 | - | AP | - | - | - | 5/21/2009 1:52 AM | Wireless AP scan |

The rogue device inventories that comprise this report contain many fields, described in [Table 140](#).

Table 140 New Rogue Devices Report Fields

| Field | Description |
|-------------------------------|--|
| Name | Displays the device name, as able to be determined. |
| RAPIDS Classification | Displays the RAPIDS classification for the rogue device, as classified by rules defined on the RAPIDS > Rules page. Refer to “Using RAPIDS and Rogue Classification” on page 183 for additional information. |
| Threat Level | Displays the numeric threat level by which the device has been classified, according to rules defined on the RAPIDS > Rules page. Refer to “Using RAPIDS and Rogue Classification” on page 183 for additional information. |
| Ack | Displays whether the device has been acknowledged with the network. |
| First Discovered | Displays the date and time that the rogue device was first discovered on the network. |
| First Discovery Method | Displays the method by which the rogue device was discovered. |
| First Discovery Agent | Displays the network device that first discovered the rogue device. |

Table 140 New Rogue Devices Report Fields (Continued)

| Field | Description |
|-------------------------------|--|
| Last Discovering AP | Displays the network device that most recently discovered the rogue device. |
| Type | Displays the rogue device type when known. |
| Operating System | Displays the operating system for the device type, when known. |
| IP Address | Displays the IP address of the rogue device when known. |
| SSID | Displays the SSID for the rogue device when known. |
| Network Type | Displays the network type on which the rogue was detected, when known. |
| Channel | Displays the wireless RF channel on which the rogue device was detected. |
| WEP | Displays Wired Equivalent Privacy (WEP) encryption usage when known. |
| RSSI | Displays Received Signal Strength (RSSI) information for radio signal strength when known. |
| Signal | Displays signal strength when known. |
| LAN MAC Address | Displays the MAC address for the associated LAN when known. |
| LAN Vendor | Displays LAN vendor information associated with the rogue device, when known. |
| Radio MAC Address | Displays the MAC address for the radio device, when known. |
| Radio Vendor | Displays the manufacturer information for the radio device when known. |
| Port | Displays the router or switch port associated with the rogue device when known. |
| Last Seen | Displays the last time in which the rogue device was seen on the network. |
| Total Discovering APs | Displays the total number of APs that detected the rogue device. |
| Total Discovery Events | Displays the total number of instances in which the rogue device was discovered. |

Using the New Users Report

The **New Users Report** lists all new users that have appeared on the network during the time duration defined for the report. This report covers the user identifier, the associated role when known, device information and more.

Perform these steps to view the most recent version of the **New Users Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **New Users** to display report **Detail** information.
3. The **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 161 illustrates the fields and information in the **New Users Report**.

Figure 161 Reports > Generated > New Users Report Illustration

| 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 | | | | | | |
| <div style="text-align: right;"> XML (XHTML) export Email this report Print report </div> | | | | | | |
| 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 141 Reports > Generated > New Users Report Fields

| Field | Description |
|-------------------------|--|
| Username | Displays the username when known. |
| Role | Displays the role with which the user is associated. |
| MAC Address | Displays the MAC address of the AP device by which the user connected. |
| Vendor | Displays vendor information for the AP device by which the user connected. |
| AP/Device | Displays the device type by which the user connected. |
| Association Time | Displays the time in which the AP device associated with the controller. |
| Duration | Displays the duration of the user's connection. |

Using the PCI Compliance Report

OV3600 supports PCI requirements in accordance with the Payment Card Industry (PCI) Data Security Standard (DSS). The **PCI Compliance Report** displays current PCI configurations and status as enabled on the network.

In addition to citing simple pass or fail status with regard to each PCI requirement, OV3600 introduces very detailed diagnostic information to recommend the specific action or actions required to achieve Pass status, when sufficient information is available.

Refer to the “[Deploying PCI Auditing](#)” on page 211 for information about enabling PCI on the network. The configurations in that section enable or disable the contents of the PCI Compliance Report that is viewable on the **Reports > Generated** page.

Perform these steps to view the most recent version of the **PCI Compliance Report**.




1. Verify that OV3600 is enabled to monitor compliance with PCI requirements, as described in the “[Deploying PCI Auditing](#)” on page 211.
2. Navigate to the **Reports > Generated** page.
3. Scroll to the bottom, and click **PCI Compliance** to display **Detail** information.

Figure 162 illustrates the fields and information in the most recent **PCI Compliance Report**.

Figure 162 Reports > Generated > PCI Compliance Report Illustration, Pass or Fail Example

Daily PCI Compliance Report for All Groups, Folders and PCI Requirements

1/20/2009 12:00 AM to 1/21/2009 12:00 AM
Generated on 1/21/2009 12:23 AM

 XML (XHTML) export
 Email this report
 Print report

This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.2 requirements that are relevant to security in your network. PCI DSS standard requirements are available at <https://www.pcisecuritystandards.org>.

Disclaimer: The PCI Compliance Report must be completed by an authorized QSA. The sole purpose of this report is to provide IT administrators with an on-demand internal audit of components which are visible to AirWave Wireless Management Suite.

Summary

| PCI Requirement ▲ | Description | Status |
|-------------------|---|--------|
| 1.1 | Configuration standards for router. A device fails if it is in read-write management mode and there are mismatches between the desired configuration and the configuration on the device. | Pass |
| 1.2.3 | Install firewalls between any wireless networks and the cardholder data environment. A device passes if it can function as a stateful firewall. | Pass |
| 2.1 | Always change vendor-supplied defaults. A device fails if the usernames, passwords or SNMP credentials being used by AWMS to communicate with the device are on a list of forbidden credentials. The list includes common manufacturer defaults. | Pass |
| 2.1.1 | Change vendor-supplied defaults for wireless environments. A device fails if the passphrases, SSIDs or other security-related settings are on a list of forbidden values. The list includes common manufacturer defaults. | Pass |
| 4.1.1 | Use strong encryption in wireless networks. A device fails if the desired or actual configuration reflect that WEP is enabled or if associated users can connect with WEP. | Pass |
| 11.1 | Identify unauthorized wireless devices. A report will indicate a failure if there are unacknowledged rogue APs present in RAPIDS or there are no wireless rogues discovered in the last three months. | Pass |
| 11.4 | Use intrusion-detection systems and/or intrusion-prevention systems to monitor all traffic. A report will indicate a "pass" for the requirement if AWMS is monitoring devices capable of reporting IDS events. Recent IDS events will be summarized in the report. | Pass |

Figure 163 Reports > Generated > PCI Compliance Report Illustration, Diagnostics Example

Issues for requirement 1.1: Configuration standards for routers. (Fail)

1-20 ▼ of 466 PCI Compliance Issues Page 1 ▼ of 24 >> |

| AP/Device ▲ | Status | Detail | | | | | | | | | |
|-------------------|------------------------------|---|--|------------------------------|------------------------------|----------|--------------------|-------------------|------|-------------|-------------------|
| 00:0b:86:c1:af:17 | Unable to Determine | Device is currently down or was never contacted. | | | | | | | | | |
| 00:0b:86:c3:5d:da | Unable to Determine | Device is currently down or was never contacted. | | | | | | | | | |
| 00:0b:86:c7:71:bc | Unable to Determine | Device is currently down or was never contacted. | | | | | | | | | |
| 00:0b:86:cd:d9:42 | Fail | <table border="1" style="width: 100%;"> <thead> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Location</td> <td>(failed to fetch)</td> <td>Not Available</td> </tr> <tr> <td>Name</td> <td>ahouk-ap65</td> <td>00:0b:86:cd:d9:42</td> </tr> </tbody> </table> | | Current Device Configuration | Desired Device Configuration | Location | (failed to fetch) | Not Available | Name | ahouk-ap65 | 00:0b:86:cd:d9:42 |
| | Current Device Configuration | Desired Device Configuration | | | | | | | | | |
| Location | (failed to fetch) | Not Available | | | | | | | | | |
| Name | ahouk-ap65 | 00:0b:86:cd:d9:42 | | | | | | | | | |
| 00:1a:1e:c0:1a:dc | Unable to Determine | Device is currently down or was never contacted. | | | | | | | | | |
| 00:1a:1e:c0:2b:32 | Fail | <table border="1" style="width: 100%;"> <thead> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>aruba-124-c0:2b:32</td> <td>00:1a:1e:c0:2b:32</td> </tr> </tbody> </table> | | Current Device Configuration | Desired Device Configuration | Name | aruba-124-c0:2b:32 | 00:1a:1e:c0:2b:32 | | | |
| | Current Device Configuration | Desired Device Configuration | | | | | | | | | |
| Name | aruba-124-c0:2b:32 | 00:1a:1e:c0:2b:32 | | | | | | | | | |
| 00:1a:1e:c5:a9:30 | Fail | <table border="1" style="width: 100%;"> <thead> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Location</td> <td>(failed to fetch)</td> <td>Not Available</td> </tr> <tr> <td>Name</td> <td>marcus-ap65</td> <td>00:1a:1e:c5:a9:30</td> </tr> </tbody> </table> | | Current Device Configuration | Desired Device Configuration | Location | (failed to fetch) | Not Available | Name | marcus-ap65 | 00:1a:1e:c5:a9:30 |
| | Current Device Configuration | Desired Device Configuration | | | | | | | | | |
| Location | (failed to fetch) | Not Available | | | | | | | | | |
| Name | marcus-ap65 | 00:1a:1e:c5:a9:30 | | | | | | | | | |

Defining and Generating PCI Compliance Reports

Perform these steps to define and generate PCI Compliance generated reports in OV3600. These steps are a modification to general report creation procedures, with an emphasis on PCI requirements.

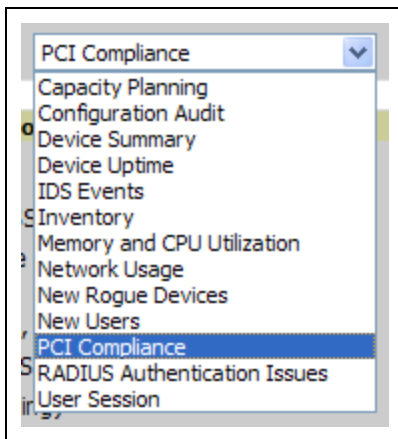


Only **admin** users have complete access to complete PCI Compliance information. The OV3600 reports and online displays of information can vary with configuration, User Roles, and Folders.

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 164 *Report Type Drop-down Menu in Reports > Definitions > Add Illustration*



3. Use the **Group** and **Folder** sections to define the scope of the PCI Compliance report. These report parameters apply to any OV3600 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 [“Auditing PCI Compliance on the Network” 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 153](#) for additional information.
4. Use the **PCI Requirements** section to define the PCI Compliance standards to include in tracking and reports generation. [Table 135](#) 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.

Using the RADIUS Authentication Issues Report

The **RADIUS Authentication Issues Report** contains issues that may appear with AP controllers, RADIUS Servers, and users.

Perform these steps to view the most recent version of the **RADIUS Authentication Issues Report**.




1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **RADIUS Authentication Issues Report** to display report **Detail** information.
3. The **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 165 illustrates the fields and information in the **RADIUS Authentication Issues Report**.

Figure 165 Reports > Generated > RADIUS Authentication Issues Details Illustration

Daily RADIUS Authentication Issues Report for All Groups, Folders and SSIDs

1/20/2009 12:00 AM to 1/21/2009 12:00 AM
Generated on 1/21/2009 12:21 AM

 XML (XHTML) export
 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 11:54 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 | - | - |

Using the User Session Report

The **User Session Report** itemizes user-level activity by session. A session is any instance in which a user connects to the network. 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

Perform these steps to view the most recent version of the **User Session Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **User Session Report** to display report **Detail** information.
3. The **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 166 Reports > Generated > User Session Detail, Connection Mode Information

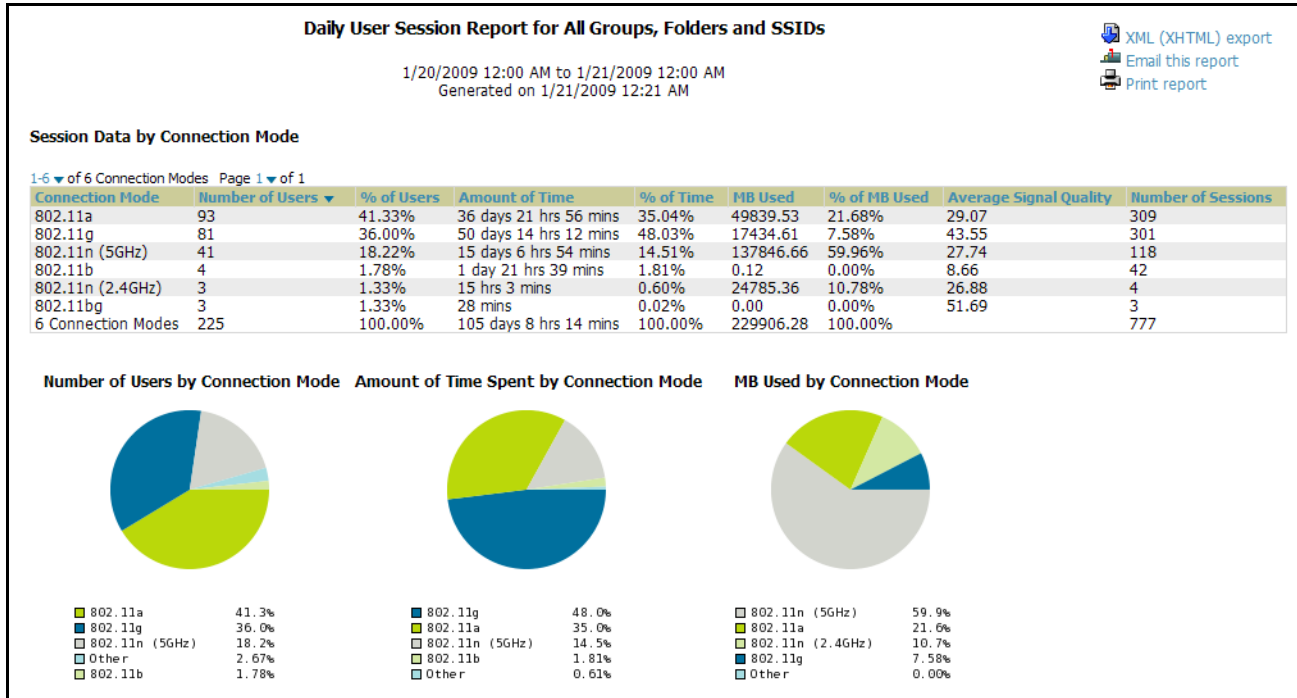


Figure 167 Reports > Generated > User Session Detail > SSID Information

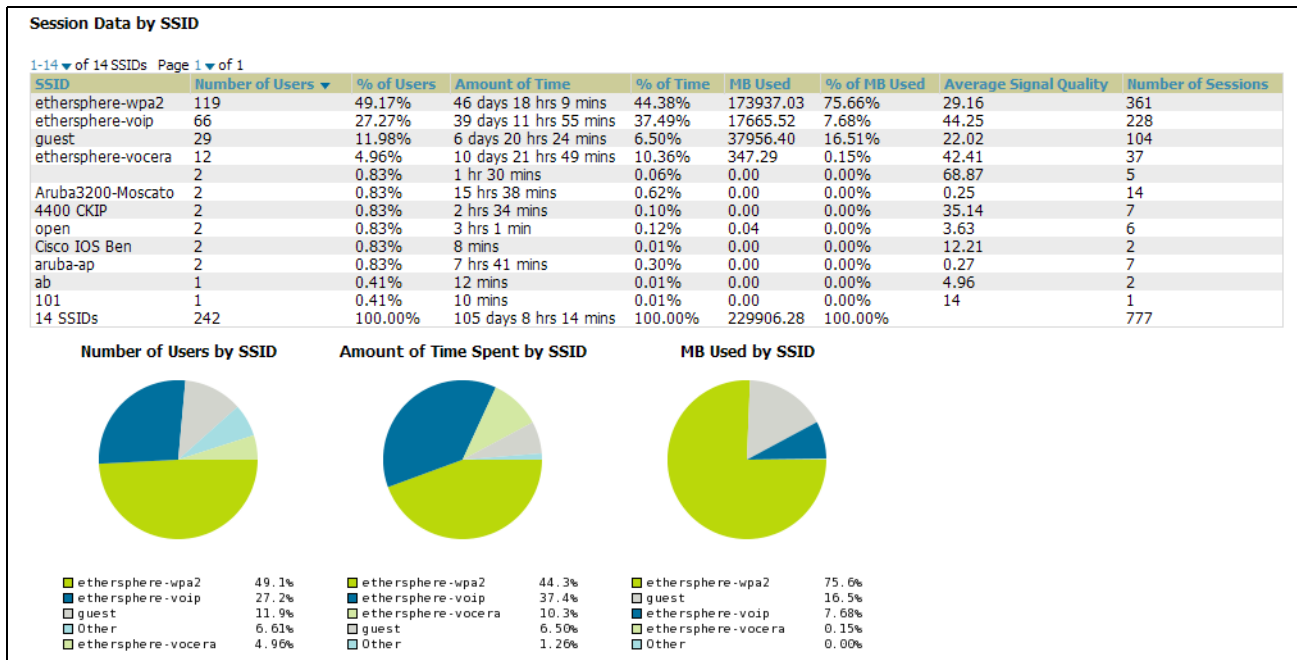


Figure 168 Reports > Generated > User Session Detail > VLAN Information

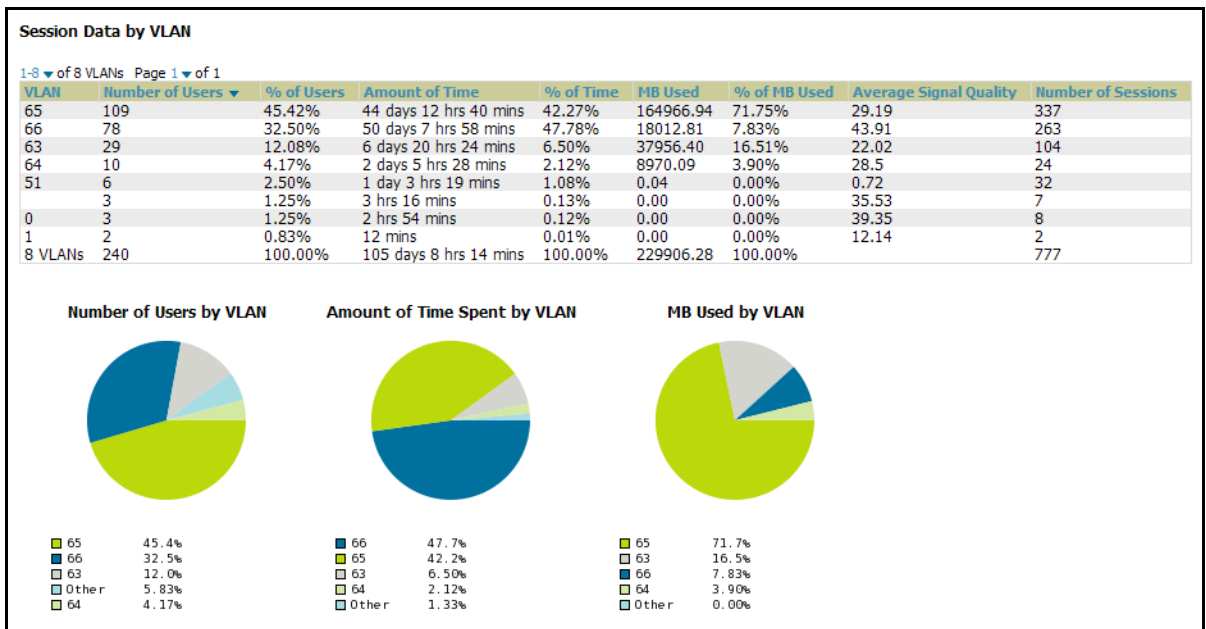


Figure 169 Reports > Generated > User Session Detail > Cipher Information

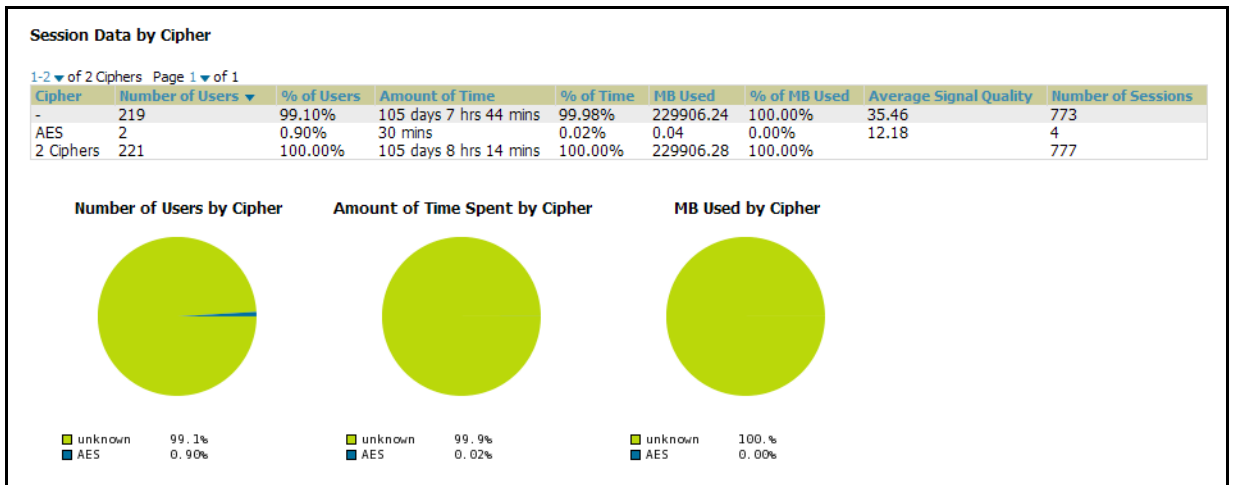


Figure 170 Reports > Generated > User Session Detail > Summary and User Information (Partial View)

| Summary | | | | | | | | | |
|-----------------------------------|---------------|--|--|--|--|--|--|--|--|
| Number of sessions | 777 | | | | | | | | |
| Number of unique users | 220 | | | | | | | | |
| Number of guest users | 0 | | | | | | | | |
| Number of unique APs | 36 | | | | | | | | |
| Average session duration | 3 hrs 15 mins | | | | | | | | |
| Total traffic (MB) | 229906.28 | | | | | | | | |
| Average traffic per session (MB) | 295.89 | | | | | | | | |
| Average traffic per user (MB) | 1045.03 | | | | | | | | |
| Average bandwidth per user (kbps) | 289.39 | | | | | | | | |
| Average signal quality | 35.45 | | | | | | | | |

| Sessions | | | | | | | | | |
|---------------------------------------|-------------------------|-----------|----------------|------------------|-------------|-----------------------------|---------------|--------------------|--|
| 1-20 of 1397 Sessions Page 1 of 70 >> | | | | | | | | | |
| MAC Address | Username | Role | Device Name | Controller | Group | Folder | AP Location | Connect Time | |
| 00:21:5C:6B:54:15 | ARUBANETWORKS\laankumah | employee | aankumah-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 1:56 AM | |
| 00:1F:38:3F:43:3F | ARUBANETWORKS\osucadi | employee | osucadi-RAP2WG | RAP-OPS-02 | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 1:51 AM | |
| 00:19:7D:78:DE:C8 | ARUBANETWORKS\khamilton | employee | khamilton-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 1:50 AM | |
| 00:24:36:54:02:18 | khamilton | employee | khamilton-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 1:36 AM | |
| 00:21:5C:6B:54:15 | ARUBANETWORKS\laankumah | employee | aankumah-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 1:36 AM | |
| 00:1D:09:05:05:BF | ARUBANETWORKS\mdevine | employee | mdevine-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 1:34 AM | |
| 00:03:2A:02:6B:34 | wifiphone | employee | AL19 | ethersphere-lms3 | Aruba HQ | Top > Sunnyvale HQ | Not Available | 5/21/2009 1:23 AM | |
| 00:19:79:0F:6E:72 | dharaks | performer | dharaks-ap70 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 1:21 AM | |
| 00:1E:3B:7D:A6:21 | ARUBANETWORKS\phauff | employee | phauff-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 1:11 AM | |
| 00:0E:9B:CA:64:FF | ARUBANETWORKS\kstan | employee | kstan-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 1:01 AM | |
| 00:16:CF:BC:0F:C2 | ARUBANETWORKS\thoida | employee | thoida-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 12:53 AM | |
| 00:03:2A:02:6B:52 | wifiphone | employee | Finance-AL27 | ethersphere-lms3 | Aruba HQ | Top > Sunnyvale HQ | Not Available | 5/21/2009 12:48 AM | |
| 00:19:7E:76:90:AD | ARUBANETWORKS\jburg | employee | jburg-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 12:47 AM | |
| 00:1E:4C:68:C3:C5 | ARUBANETWORKS\thargin | employee | thargin1-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | - | 5/21/2009 12:38 AM | |
| 00:1C:26:C5:39:D8 | ARUBANETWORKS\ggopalan | employee | ggopalan-ap | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 12:36 AM | |
| 00:05:4E:4E:85:25 | ARUBANETWORKS\vravula | employee | vravula-ap65-2 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 12:34 AM | |
| 00:16:CF:23:7B:7A | ARUBANETWORKS\fviseel | employee | fviseel-ap65 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 12:30 AM | |
| 00:05:4E:4E:85:25 | ARUBANETWORKS\vravula | employee | vravula-ap65-2 | RAP-Local | HQ-RemoteAP | Top > Sunnyvale HQ > HQ-RAP | Not Available | 5/21/2009 12:30 AM | |
| 00:03:2A:02:6B:49 | wifiphone | employee | AL12 | ethersphere-lms3 | Aruba HQ | Top > Sunnyvale HQ | Not Available | 5/21/2009 12:27 AM | |
| 00:03:2A:02:6B:36 | wifiphone | employee | Haystack-AL29 | ethersphere-lms3 | Aruba HQ | Top > Sunnyvale HQ | Not Available | 5/21/2009 12:27 AM | |

| 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 | |
| 00:03:2A:02:4F:95 | wifiphone | employee | 23 hrs 59 mins | 0.43 | 0.04 | 49.24 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:50:E3 | wifiphone | employee | 1 day 0 hrs 0 mins | 8.12 | 0.77 | 52.91 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:52:8C | wifiphone | employee | 23 hrs 59 mins | 7.35 | 0.7 | 50.65 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:5F:84 | - | VoFi | 5 hrs 34 mins | 0.12 | 0.05 | 44.74 | UniData Communication Systems, Inc. | 802.11b | |
| 00:03:2A:02:67:FD | wifiphone | employee | 14 hrs 58 mins | 0.15 | 0.02 | 46.99 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:69:7A | azndel | employee | 23 hrs 59 mins | 5.65 | 0.54 | 40.53 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:69:88 | wifiphone | employee | 23 hrs 59 mins | 8382.05 | 794.75 | 44.87 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:69:C8 | wifiphone | employee | 23 hrs 59 mins | 16.70 | 1.58 | 41.3 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:69:D4 | wifiphone | employee | 1 day 0 hrs 0 mins | 12.53 | 1.19 | 55.55 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:69:F4 | wifiphone | employee | 1 day 0 hrs 0 mins | 16.04 | 1.52 | 53.05 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:6A:05 | wifiphone | employee | 23 hrs 59 mins | 0.45 | 0.04 | 47.31 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:6A:08 | wifiphone | employee | 23 hrs 59 mins | 3.68 | 0.35 | 50.34 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:6A:0C | wifiphone | employee | 23 hrs 59 mins | 0.46 | 0.04 | 42.12 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:6A:13 | wifiphone | employee | 1 day 0 hrs 0 mins | 0.37 | 0.04 | 47.81 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:6A:16 | wifiphone | employee | 23 hrs 59 mins | 0.39 | 0.04 | 46.13 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:6A:1E | wifiphone | employee | 23 hrs 59 mins | 0.43 | 0.04 | 42.36 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:6A:23 | wifiphone | employee | 23 hrs 59 mins | 1.17 | 0.11 | 46.36 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:6A:25 | wifiphone | employee | 23 hrs 59 mins | 0.39 | 0.04 | 51.69 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:6A:C8 | wifiphone | employee | 1 day 0 hrs 0 mins | 0.66 | 0.06 | 43.29 | UniData Communication Systems, Inc. | 802.11g | |
| 00:03:2A:02:6A:D3 | wifiphone | employee | 23 hrs 59 mins | 0.37 | 0.04 | 42.15 | UniData Communication Systems, Inc. | 802.11g | |

Defining Reports

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 report, browse to the **Reports > Definition** page and click the **Add** button, or click the pencil icon to edit an existing report definition. [Figure 171](#) illustrates the **Report Definition** page.

Figure 171 Defining a Report with **Reports > Definitions > Add Button**

2. Complete the fields described in [Table 142](#) 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](#)” on page 252.

Table 142 **Report > Definitions > Add Page Fields**

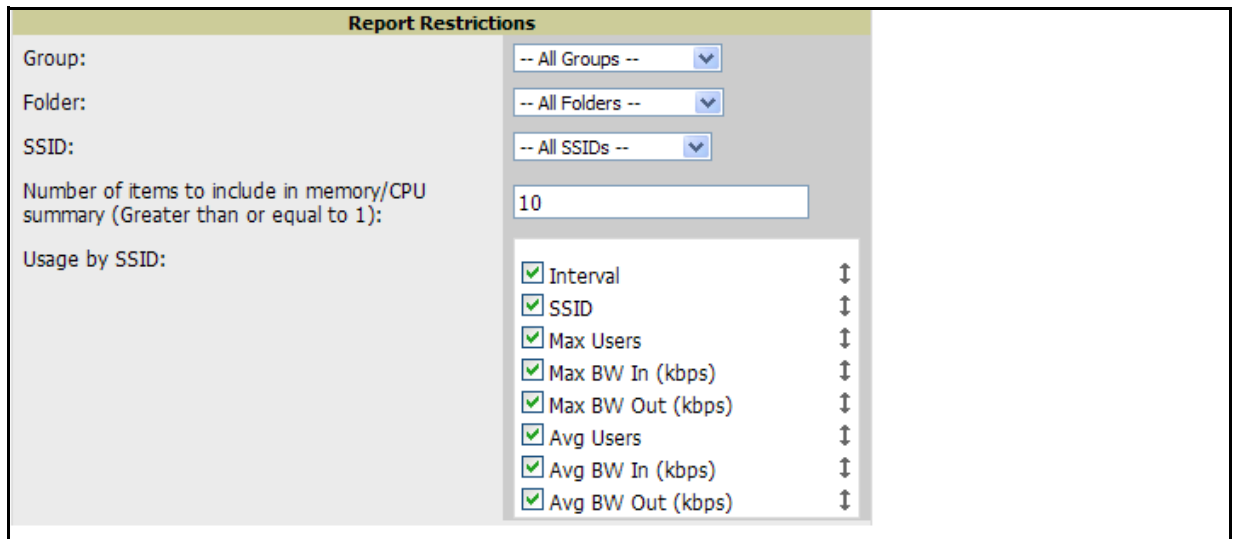
| Field | Default | Description |
|---------------|-------------|---|
| Title | Empty | Enter a Report Title . Alcatel-Lucent recommends using a title that is a meaningful and descriptive, so it may be found easily on the lists of reports that appear on either Generated or Definitions pages. |
| Type | Capacity | Choose the type of report you wish to create in the Report Type drop-down menu. |
| Group | All Groups | Specify the groups and folders to be covered in the report by choosing All Groups (or All Folders) or specifying Use selected groups (or Use selected folders) in the drop-down menu. If Use selected groups is chosen, a menu with checkboxes appears, allowing you to choose the groups to include in the report. |
| Folder | All Folders | |
| 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. |

Table 142 Report > Definitions > Add Page Fields (Continued)

| Field | Default | Description |
|--|---------|--|
| 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 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. |

In the report restrictions section you can customize any detailed information contained in a chosen report. [Figure 172](#) shows a sample **Report Restrictions** page.

Figure 172 Report Restrictions Illustration



By default all data will be included. Deselect the checkbox to hide specific information. The list can also be reordered by dragging and dropping the separate lines. The order displayed here will match the column order in the report.

3. 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.

Table 143 describes the configurable settings for the custom report to be created.

Table 143 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 (ifSpeed 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. |

Emailing and Exporting Reports

This section describes three ways in which distribute reports from OV3600:

- [Emailing Reports in General Email Applications](#)
- [Emailing Reports to Smarthost](#)
- [Exporting Reports to XML](#)

Emailing Reports in General Email Applications

Perform these steps to set up email distribution of reports in OV3600:

- All reports contain a link to export the report to an XML file and a text box where you may specify email addresses, separated by commas, to which reports are sent.
- Click **Email This Report** to email the report to the address specified in the text box above the button.

Additional information about email-based report generation is described in [“Defining Reports” on page 274](#), and in [“Emailing Reports to Smarthost” on page 278](#).

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 the **Reports > Generated** page and click the name of the report you wish to export. You can also click on the link at the bottom of the page for the latest version of a report. The corresponding **Detail** page displays.
2. On the top right of the page, click **XML (XHTML) export**. After a moment the XML page appears in your browser.
3. In your browser, click **File > Save As....** Define the filename and location, select **Web Page Complete** as the file type, then click **Save**. A brief **Save Webpage** status box appears to display the saving process. Allow the process sufficient time, particularly for reports that contain many links or large graphics.
4. Open the resulting file in MS Excel. You may need to display files of all type to access the file.
5. From Excel you can save the report as a single file using the **Save As > Excel Workbook** option (Excel 2007). You can also save it as a .xls file for compatibility with older versions of Excel though some formatting in the report might not be supported.



This method of exporting files supports graphics and links, and prevents **Missing File C:\filename.css** error messages.

Introduction

This chapter presents the functions, configuration, and use of the OV3600 **Helpdesk**. This chapter contains the following sections:

[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 Air Manager (OV3600) allows front-line technical support staff to take full advantage of the data available in the OmniVista Air Manager (OV3600). The OV3600 Helpdesk includes the following features and functions, with additional 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.
- **Admin** users can make the Helpdesk available to users of any role by selecting the **enabled** radio button on the **role detail** page. To edit existing roles, click the **pencil icon** next to a role on the **OV3600 Setup > Roles** page.
- The OV3600 Helpdesk allows you to document incidents associated with users on the network.
- 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 283 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 173 illustrates the components of the OV3600 **Helpdesk Incidents** page.

Figure 173 Helpdesk > Incidents Page Illustration

| State | Last 2 Hours | Last Day | Total |
|--------|--------------|----------|-------|
| Open | 0 | 0 | 126 |
| Closed | 0 | 0 | 0 |
| Total | 0 | 0 | 126 |

Add New Incident

1-20 of 126 Incidents Page 1 of 7 > >|

| | ID | Summary | State | Opened By | Related | Created | Updated |
|--------------------------|-----|-----------------------------|-------|-------------|---------|--------------------|--------------------|
| <input type="checkbox"/> | 202 | Paul's connection issue | Open | mbruno | 0 | 5/19/2009 9:37 AM | 5/19/2009 9:37 AM |
| <input type="checkbox"/> | 201 | lotte's wlan issue | Open | aruba-se | 0 | 5/13/2009 9:31 PM | 5/13/2009 9:31 PM |
| <input type="checkbox"/> | 199 | testing - ps | Open | patrick | 0 | 5/13/2009 7:42 PM | 5/13/2009 7:42 PM |
| <input type="checkbox"/> | 198 | Damien - more typing issues | Open | patrick | 0 | 5/13/2009 7:34 PM | 5/13/2009 7:34 PM |
| <input type="checkbox"/> | 197 | thomas' wireless issue | Open | patrick | 0 | 5/11/2009 11:01 PM | 5/11/2009 11:01 PM |
| <input type="checkbox"/> | 196 | Martin Has a Problem | Open | ARUBATM | 0 | 5/5/2009 6:25 AM | 5/5/2009 6:25 AM |
| <input type="checkbox"/> | 195 | Katie's Problem | Open | aruba-se | 0 | 4/27/2009 2:24 PM | 4/27/2009 2:24 PM |
| <input type="checkbox"/> | 194 | test | Open | aruba-se | 0 | 4/27/2009 2:00 PM | 4/27/2009 2:00 PM |
| <input type="checkbox"/> | 193 | demo for X | Open | aruba-se | 0 | 4/27/2009 8:33 AM | 4/27/2009 8:33 AM |
| <input type="checkbox"/> | 192 | ym's wlan issue | Open | aruba-se | 0 | 4/26/2009 9:49 PM | 4/26/2009 9:49 PM |
| <input type="checkbox"/> | 191 | Nishith can't connect | Open | danccomfort | 0 | 4/23/2009 2:12 PM | 4/23/2009 2:23 PM |
| <input type="checkbox"/> | 190 | AHK | Open | aruba-se | 0 | 4/21/2009 2:39 AM | 4/21/2009 2:39 AM |
| <input type="checkbox"/> | 189 | Bryan's network problem | Open | mbruno | 1 | 4/20/2009 11:25 AM | 4/20/2009 11:26 AM |
| <input type="checkbox"/> | 185 | Peter's connection problems | Open | mbruno | 1 | 4/9/2009 7:44 AM | 4/9/2009 7:45 AM |
| <input type="checkbox"/> | 184 | dcomfort's wlan issue | Open | aruba-se | 0 | 4/7/2009 1:02 AM | 4/7/2009 1:02 AM |
| <input type="checkbox"/> | 183 | Joe's Incident | Open | aruba-se | 0 | 4/6/2009 4:51 PM | 4/6/2009 4:51 PM |
| <input type="checkbox"/> | 182 | Test | Open | ARUBATM | 0 | 4/6/2009 7:58 AM | 4/6/2009 7:58 AM |
| <input type="checkbox"/> | 181 | euf's wlan issue | Open | aruba-se | 0 | 4/5/2009 10:19 PM | 4/5/2009 10:19 PM |
| <input type="checkbox"/> | 177 | Axians connectie probleem | Open | aruba-se | 0 | 3/31/2009 6:49 AM | 3/31/2009 6:49 AM |
| <input type="checkbox"/> | 175 | gary-test | Open | aruba-se | 0 | 3/25/2009 3:36 PM | 3/25/2009 3:36 PM |

Select All - Unselect All

Delete

The table in **Helpdesk > Incidents** displays the count of incidents by state and by time. You can sort incidents from within any category of information, whether in sequential or reverse-sequential order. You can display all incidents, or strictly open or closed incidents, and you can display incidents according to the person who created them. Finally, the **Helpdesk > Incidents** page allows you to add or delete incidents.

Table 144 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 and Total | Shows the count of incidents in the last two hours, the last day, and the total count. |

The table at the bottom of the page, as described in [Table 145](#) below, summarizes the incidents that have been reported thus far, and which OV3600 has not yet purged.

Use the **OV3600 Setup > General** page and the **Historical Data Retention** page. Using the **Closed Helpdesk Incidents** field, set the number of days that OV3600 is to retain records of closed Helpdesk incidents. Settings this value to 0 disables this function.

Clicking the **pencil** icon next to any incident opens an edit page where you can modify and update the incident. An incident can be deleted by selecting the checkbox next to it and clicking the **Delete** button at the bottom of the table.

Table 145 *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. |
| Created | Displays the time and date the incident was created. |
| Updated | Displays the time and date the incident was last modified by an OV3600 user. |

Creating a New Incident with Helpdesk

To create a new Helpdesk incident, click the **Add New Incident** button underneath the top table. This launches and displays an incident edit page, as illustrated in [Figure 174](#). The contents of this page are described in [Table 146](#).

Figure 174 *Add Incident Page Illustration*

Table 146 *Helpdesk Incident Edit Page Fields*

| Field | Description |
|--------------------|--|
| Summary | Displays user-entered text that describes a short summary of the incident |
| State | Provides a drop-down menu with the options "Open" or "Closed" |
| Description | Provides a longer user-entered text area for a thorough description of the incident. |

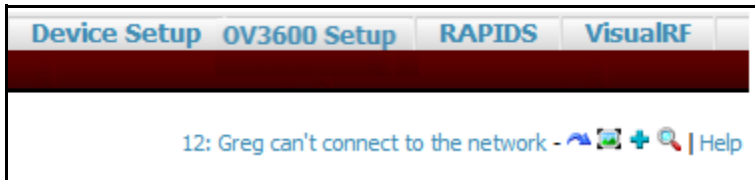


The **Incidents** portion of the **Alert Summary** table on other OV3600 pages only increments the counter for incidents that are open and associated to an AP. This field displays incidents based on folder, which is the Top folder on this page and on the **Home > Overview** page. Incidents that are not related to devices in that folder are not counted in the **Alert Summary** table on other pages.

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

Helpdesk icons appear at the top of other OV3600 pages, allowing graphical snapshots and other records to be associated to existing incidents. These appear in the upper right-hand corner next to the **Help** link. Refer to [Figure 175](#).

Figure 175 Helpdesk Icons on Additional Pages



[Table 147](#) describes the Helpdesk icon components.

Table 147 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 147](#)) 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 176](#) illustrates these GUI tools.

Figure 176 Relationships and Snapshots on the Incident Edit Page

The screenshot shows the 'Incident Edit Page' with the following details:

- Incident Summary:**
 - Summary: Patricks Wireless Issue
 - State: Open
 - Description: notes
- Snapshots:**
 - 1-2 of 2 Incident Snapshots Page 1 of 1
 - Table with columns: Description, Created
 - Snapshot 261, 12/23/2008 5:31 PM
 - Snapshot 262, 12/23/2008 5:31 PM
 - Select All - Unselect All
 - 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 177](#) illustrates this appearance, and [Table 148](#) describes the components.

Figure 177 Helpdesk > Setup with Remedy Enabled

The screenshot shows the 'BMC Remedy Setup' page with the following fields:

- Remedy Enabled: Yes No
- Middle Tier Host:
- Port:
- SOAP URL:
- Server:
- Timeout: 60
- Username:
- Password:
- Confirm Password:
- Save and Revert buttons

Table 148 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. |

Table 148 Components of **Helpdesk > Setup** with Remedy Enabled

| Field | Description |
|--------------------------------------|---|
| 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 178](#) illustrates the appearance and [Table 149](#) describes the components of this page.

Figure 178 **Helpdesk > Incidents** with Remedy Enabled

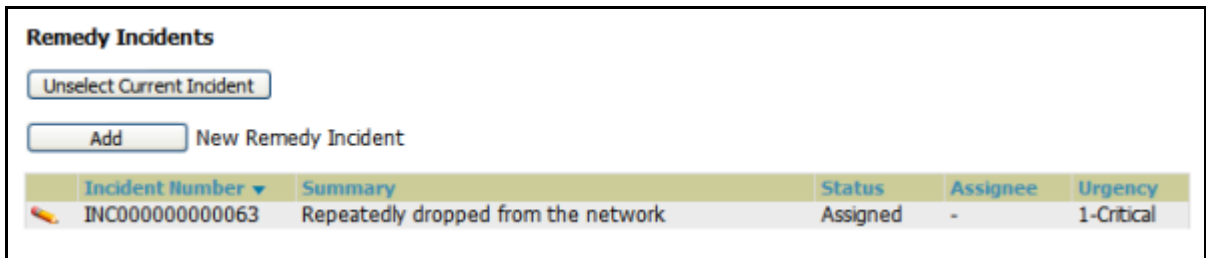


Table 149 Components of **Helpdesk > Incidents** with Remedy Enabled

| 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 |
| Assignee | Assigned by Remedy installation; cannot be changed in OV3600. |

Table 149 Components of **Helpdesk > Incidents** with Remedy Enabled

| Field | Description |
|----------------|--|
| 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 179](#) and [Table 150](#) for additional illustration and explanation.

Figure 179 **Helpdesk > Incidents > Add a New Remedy Incident** Page Illustration

Table 150 Components of **Helpdesk > Incidents > Add a New Remedy Incident** Fields

| Field | Description |
|-------------------------------------|---|
| Customer First and Last Name | These must match exactly a customer that already exists on the Remedy server. There is no way to create a new customer from OV3600 or to search Remedy customers remotely. |
| Impact | <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 appendix describes the Yum packaging management system, and provides advisories on alternative methods that may cause issues with OV3600.

Yum for OV3600

Alcatel-Lucent recommends running Yum to ensure your packages are up to date, and so that your OV3600 is as secure as possible if you are running RHEL 4/5 or CentOS 4/5.

Yum is an automated package management system that verifies OV3600 is running the most recently released RPMs and upgrades any out-of-date packages. Yum accesses the Internet, and downloads and installs new versions of any installed RPMs. It is important to keep OV3600' RPMs as current as possible to close any known security holes in the OS as quickly as possible.

Check the **Operating System** field on the **Home > Overview** page to determine if OV3600 can safely run Yum. Perform the following steps to run Yum with OV3600.

To run Yum on a CentOS 4 machine, use the steps below; for a CentOS 5 machine, yum-cron is also required.

1. Before running Yum for the first time, you need to install the GPG key. The GPG key is used to validate the authenticity of all packages downloaded by Yum.
2. To install the GPG key, type `rpm --import /usr/share/doc/fedora-release-3/RPM-GPG-KEY-fedora`.
3. To run Yum manually, log in to the OV3600 console and type `yum update` and press **Enter**. If the packages seem to be downloading slowly, press **ctrl-c** to connect to a new mirror.
4. To configure Yum to run nightly, type `chkconfig yum on` and press **Enter**. The `chkconfig` command instructs yum to run nightly at 4:02 AM when the yum service is running, but `chkconfig` does not start yum.
5. Type `service yum start` and press **Enter** to start Yum, or restart the server and Yum automatically starts.
6. In some instances, running Yum may cause a problem with OV3600. If that happens, a good first step is to use SSH to go into the OV3600 server as root, and issue the following command:

```
# root; make
```

If that does not resolve the issue, please contact Alcatel-Lucent Support at support@ind.alcatel.com for further assistance.

Package Management System Advisories for OV3600



NOTE

Alcatel-Lucent does not support Yum or Up2date on Red Hat 8 or 9. Running Yum on RH8 or RH9 will cause serious problems.

Introduction

This appendix describes the optional integration of third party security products for OV3600, as follows:

- [Bluesocket Integration](#)
- [ReefEdge Integration](#)
- [HP ProCurve 700wl Series Secure Access Controllers Integration](#)

Bluesocket Integration

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. Log in into the Bluesocket Server via HTTP with proper user credentials.
2. Navigate to the **Users > External Accounting Servers** page.
3. Select **External RADIUS Accounting** from the **Create** drop-down list.
4. Click **Enable server** onscreen.
5. Enter the user-definable **Name** for the OV3600 server.
6. Enter the **Server IP Address** or **DNS entry** for OV3600.
7. Accept the default Port setting of 1813.
8. Enter the **Shared Secret** (matching OV3600's shared secret).
9. Enter Notes (optional).
10. Click the **Save** button.
11. If you are you using an External LDAP Server, ensure that the accounting records are forwarding to OV3600 upon authentication.
12. Navigate to **Users > External Authentication Servers**.
13. Modify the LDAP server.
14. Ensure under the Accounting server matches the server entered in step 5.
15. Click the **Save** button.
16. To verify and view the log files on the Bluesocket server, proceed to **Status > Log**.
17. To verify and view the log files on OV3600, proceed to **SYSTEM > Event Log**.

ReefEdge Integration

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 a RADIUS Accounting Server” on page 57.](#)

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

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 a RADIUS Accounting Server” on page 57.](#)

Example Network Configuration

In this example, the APs are connected to the Access Controller. The Access Controller routes wireless user traffic to the Employee Network, while bridging AP management traffic. Each AP is presumed to have a static IP address.

Perform these steps for HP ProCurve 700wl Series Configuration, allowing OV3600 to manage APs through **Control** pages.

1. Log in to the Access Control Server via HTTP with proper credentials.
2. Navigate to **Rights > Identity Profiles**.
3. Select **Network Equipment**.
4. Enter the **Name**, **LAN MAC** and ensure the device is identified as an **Access Points in the Identity Profile** section for all access points in the network.

The Access Points Identity Profile is the default profile for network equipment. Enabling this option instructs the Access Controller to pass management traffic between the Access Points and the Customer's wired network.

HP ProCurve 700wl Series Configuration

This procedure enables the sending of client authentication information to OV3600. Perform the following steps to enable this configuration.

1. Login to the Access Control Server via HTTP with proper credentials.
2. Navigate to the **Rights > Authentication Policies** configuration page.
3. Select **Authentication Services**.
4. Select **New Services**.
5. Select **RADIUS**.
6. Enter **Name - Logical Name**.
7. Enter **Server - OV3600'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 `:resetall` and press **Enter**.

4. Type **yes**, and press **Enter** to confirm the command.



The :resetall command is valid for only two minutes after the AP reboots. If you do not enter and confirm the:resetall command during that two minutes, reboot the AP again.

5. After the AP reboots and the **Express Setup** screen appears, reconfigure the AP by using the terminal emulator or an Internet browser.

IOS Dual Radio Template

A dual-radio Cisco IOS AP template is included as reference.

```
! Template created from Cisco Aironet 1240 IOS 12.3(11)JA1 'newName'
! at 2/12/2007 10:14 AM by user 'admin'
<ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push>

version 12.3
no service pad
service timestAMPs debug datetime msec
service timestAMPs log datetime msec
service password-encryption
hostname %hostname%
enable secret 5 $1$ceH2$/1BN2DQpOoBAz/KI2opH7/
ip subnet-zero
ip domain name Alcatel-Lucent.com
ip name-server 10.2.24.13
no aaa new-model
dot11 ssid OpenSSID
    authentication open
power inline negotiation prestandard source
username newpassword password 7 05050318314D5D1A0E0A0516
username Cisco password 7 01300F175804
bridge irb
interface Dot11Radio0
    %enabled%
    no ip address
    no ip route-cache
    ssid OpenSSID
    speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
    channel %channel%
    station-role root
    bridge-group 1
    bridge-group 1 subscriber-loop-control
    bridge-group 1 block-unknown-source
    no bridge-group 1 source-learning
    no bridge-group 1 unicast-flooding
    bridge-group 1 spanning-disabled
%if interface=Dot11Radio1%
interface Dot11Radio1
    no ip address
    no ip route-cache
    %enabled%
    ssid OpenSSID
    dfs band 3 block
    speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
    channel %channel%
```

```

station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
%endif%
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
interface BVI1
%if ip=dhcp%
ip address dhcp client-id FastEthernet0
%endif%
%if ip=static%
ip address %ip_address% %netmask%
%endif%
no ip route-cache
%if ip=static%
ip default-gateway %gateway%
%endif%
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
access-list 111 permit tcp any any neq telnet
snmp-server view iso iso included
snmp-server community public view iso RW
control-plane
bridge 1 route ip
line con 0
line vty 0 4
login local
end

```

Speed Issues Related to 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.

The Support Connection Manager establishes a secure point-to-point connection between the customer OV3600 and Alcatel-Lucent's support organization. Using this secure connection, Alcatel-Lucent support engineers can remotely diagnose problems or upgrade software without breaching security and exposing OV3600 to the Internet.

Network Requirements

OV3600's Support Connection initiates a TCP connection on port 23 to Alcatel-Lucent's support server. Please ensure your firewall allows this. The connection can be configured to run on 22,80,443 and a few other ports if necessary. Please contact Alcatel-Lucent support if you need to make any changes.



Initiating the support connection will create a point to point tunnel between OV3600 and a support server at Alcatel-Lucent.

Procedure

Perform these steps to initiate a support connection for OV3600:

1. Sign into the serial or regular console with your root login.
2. Type `service support_connection start` at the command line interface.
3. Type `service support_connection status` to verify that the connection is running properly.
4. To end the connection to Alcatel-Lucent Support, type `service support_connection stop` at the command line interface.

If you have any questions, please contact Alcatel-Lucent Technical Support at support@ind.alcatel.com.

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:

```
hpasm-7.8.0-88.rhel4.i386.rpm <- This is the actual HP agents
hpsmh-2.1.9-178.linux.i386.rpm <- This is the HP web portal to the agents
```

2. Type `rpm -i hpasm-7.8.0-88.rhel4.i386.rpm` at the command line interface.
3. Type `hpasm activate` at the command line interface.

Take the default values. You will need the SNMP RW and RO strings at this point.

4. Type `rpm -i --nopre hpsmh-2.1.9-178.linux.i386.rpm` at the command line interface. The `nopre` syntax component is required to keep the rpm from producing errors on CentOS, as opposed to RedHat. This rpm *must* be run after the hpasm rpm, because the pre-install scripts in the hpsmh rpm are not being run.
5. Type `perl /usr/local/hp/hpSMHSetup.pl` at the command line interface.

This configures the web server.

Configure the **Add Group > Administrator** page with a name '0'.

Enable IP Binding—type `1` at the command line interface.

At the next interface enter the IP address and mask of the server.

6. Type `/etc/init.d/hpasm reconfigure` at the command line interface.
When going through this menu this time, select 'y' to use the existing snmpd.conf.
7. Type `vi /etc/snmp/snmpd.conf` at the command line interface.

Change the following two lines:

```
rwcommunity xxxstringxxx 127.0.0.1
rocommunity xxxstringxxx 127.0.0.1
```

Change these lines to read as follows:

```
rwcommunity xxxstringxxx
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.

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 *OmniVista Air Manager (OV3600) 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.

Alcatel-Lucent Management Platform contains some software provided by third parties (both commercial and open-source licenses).

Source code to third-party open-source packages are available on Alcatel-Lucent's website and by request:

<http://service.esd.alcatel-lucent.com>

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 acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SWFObject v. 1.5:

Flash Player detection and embed - <http://blog.deconcept.com/swfobject/>

SWFObject is (c) 2007 Geoff Stearns and is released under the MIT License

mod_auth_tacacs - TACACS+ authentication module:

Copyright (c) 1998-1999 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>)."

4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the Apache Group
for use in the Apache HTTP server project (<http://www.apache.org>)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSS

| | |
|---|-------------|
| A | |
| AAA servers | 92 |
| access control lists..... | 111 |
| access points | |
| adding with CSV file..... | 131 |
| ACLs..... | 111 |
| ACS | |
| integrating with OV3600 | 64 |
| servers | 64 |
| Alcatel..... | 164 |
| Alcatel-Lucent | |
| Support | 15 |
| alerts | |
| viewing | 214 |
| Aruba..... | 164 |
| B | |
| backups..... | 242 |
| C | |
| Cisco | |
| configuring IOS templates | 170, 175 |
| Cisco IOS | 164 |
| Cisco WLC | 82 |
| Cisco WLSE | |
| configuring | 58 |
| Colubris | 48 |
| CSV File..... | 131 |
| D | |
| date and time | |
| configuring | 16 |
| devices | 121 |
| adding discovered devices to groups..... | 134 |
| adding manually..... | 129 |
| communication settings..... | 46 |
| discovering, managing, and troubleshooting ... | 121 |
| modifying | 115 |
| replacing | 143 |
| troubleshooting a newly discovered device | 141 |
| verifying..... | 136, 143 |
| F | |
| failover..... | 12 |
| firewall | |
| configuring..... | 20 |
| firmware | |
| loading device firmware | 49 |
| specifying minimum firmware..... | 112 |
| G | |
| global templates | 180 |
| groups | |
| assigning newly discovered devices to groups | 134 |
| changing multiple group configurations..... | 114 |
| configuring and using | 73 |
| configuring basic group settings..... | 77 |
| configuring group AAA servers..... | 92 |
| configuring group SSIDs and VLANs..... | 87 |
| configuring group templates | 164 |
| configuring PTMP/WiMAX settings | 105 |
| configuring radio settings..... | 93 |
| configuring security settings | 85 |
| deleting a group | 114 |
| global groups..... | 117 |
| MAC access control lists..... | 111 |
| overview | 74 |
| viewing..... | 75 |
| H | |
| Helpdesk..... | 279 |
| creating a new incident | 281 |
| creating snapshots and incident relationships | 282 |
| monitoring incidents..... | 280 |
| using with remedy server | 283 |
| Hirschmann..... | 164 |
| host name | |
| assigning host name | 19 |
| HP ProCurve..... | 83, 96, 164 |
| I | |
| incidents | |
| creating..... | 281 |
| installation | |
| checking | 18 |
| IP address | |

| | | | |
|---|--------|--|-------------------------|
| adding to the OV3600 system | 18 | APs/Devices > List | 137 |
| iPhone | 227 | APs/Devices > Manage | 142 |
| L | | APs/Devices > New | 135 |
| Lancom..... | 164 | Authentication Dialog Box..... | 29 |
| Linux CentOS 5 | | Buttons and Icons | 27 |
| installing | 16 | Configuration Change Confirmation..... | 114 |
| M | | Device Setup > Add | 133 |
| MAC access control lists..... | 111 | Device Setup > Communication..... | 46, 47, 48, 49 |
| Master Console | 227 | Device Setup > Discover..... | 124, 126 |
| Master Console and Failover..... | 12 | Device Setup > Firmware Files..... | 50 |
| N | | flash graphs..... | 23 |
| network settings | | Group SNMP Polling Period..... | 79 |
| defining | 38 | Groups..... | 24 |
| NMS | 65, 66 | Groups > Basic..... | 78, 80, 81, 82, 83, 118 |
| integrating with OV3600 | 65 | Groups > Firmware..... | 112 |
| Nomdix..... | 164 | Groups > List..... | 75 |
| NTP..... | 81 | Groups > MAC ACL..... | 111 |
| O | | Groups > PTMP/WiMAX..... | 106, 107, 108, 109 |
| OV3600 | | Groups > Radio | 94 |
| additional interfaces and tools..... | 201 | Groups > Templates..... | 165, 167, 180, 181 |
| assigning IP address..... | 18 | GRUB screen..... | 16 |
| changing default root password | 19 | Help | 25 |
| checking installation | 18 | Helpdesk > Incident | 283 |
| configuring date and time | 16 | Helpdesk > Incidents..... | 280, 284 |
| configuring mesh radio settings | 109 | Helpdesk > Setup..... | 283 |
| core components..... | 11 | Home..... | 23, 229 |
| defining a scan..... | 124 | Home > Documentation | 15, 234 |
| executing a scan..... | 126 | Home > License | 232 |
| getting started with..... | 29 | Home > Overview | 230 |
| hardware requirements..... | 15 | Home > Search..... | 233 |
| initial login | 29 | Home > User Info | 235 |
| installing..... | 15, 19 | Home Overview | 23 |
| integrating into network | 12 | Master Console | 227 |
| naming the network administration system..... | 19 | Master Console > Groups > Basic | 228, 229 |
| Package Management..... | 287 | Master Console > Groups > Basic, Managed .. | 228 |
| unified wireless network command center | 11 | Master Console > Manage OV3600s, IP/Hostname | 227 |
| OV3600 interface | | RAPIDS..... | 25 |
| OV3600 Setup..... | 25 | RAPIDS > Rogue APs (Detail), Score Override | 199 |
| OV3600 Setup > General..... | 32 | RAPIDS > Score Override | 199 |
| OV3600 Setup > Network..... | 38 | Reports..... | 24 |
| OV3600 Setup > NMS | 65, 66 | Reports > Definitions..... | 252, 275 |
| OV3600 Setup > RADIUS Accounting..... | 57 | sections | 21 |
| OV3600 Setup > Roles | 219 | Activity section..... | 25 |
| OV3600 Setup > Users | 40 | Navigation section | 23 |
| OV3600 Setup > WLSE..... | 62 | Status section | 22 |
| APs/Devices..... | 24 | System..... | 24, 236 |
| APs/Devices > Audit | 143 | System > Alerts | 214 |
| | | System > Backups | 243 |
| | | System > Configuration Change Jobs | 239 |
| | | System > Event Logs | 238 |
| | | System > Performance..... | 239 |
| | | System > Status | 236 |
| | | System > Status Log | 238 |
| | | System > Trigger Detail | 203 |
| | | System > Triggers | 202 |
| | | Triggers and Alerts | 202 |
| | | Users | 24, 216 |
| | | Users > Connected | 216 |

| | |
|---------------------------|-----|
| Users > Guest Users..... | 219 |
| Users > Tags..... | 221 |
| View AP Credentials | 142 |
| VisualRF | 25 |
| OV3600 RAPIDs | 12 |
| OV3600 VisualRF..... | 11 |

P

| | |
|-------------------------------------|-----|
| password | |
| changing default root..... | 19 |
| PCI Compliance | |
| Default Credential Compliance | 69 |
| PCI Requirements..... | 68 |
| protocol and port diagram | 20 |
| Proxim 4900 | 98 |
| Proxim/Avaya | 82 |
| PTMP..... | 105 |

R

| | |
|--|---------|
| radio settings | |
| configuring for groups | 93 |
| RADIUS | 92 |
| accounting | 57 |
| adding a server | 92 |
| authentication | 53 |
| configuring authentication and authorization | 55 |
| integrating with OV3600 | 57 |
| RAPIDS..... | 25, 183 |
| reports | 247 |
| creating, running, and emailing..... | 247 |
| defining custom reports..... | 274 |
| rogue classification..... | 183 |
| rogue devices | |
| configuring WLSE scanning..... | 58 |
| WLSE rogue scanning | 58 |
| root password | 19 |
| routers and switches | |
| adding with a CSV file..... | 131 |

S

| | |
|---|-----|
| scanning | |
| defining credentials..... | 124 |
| security | |
| auditing PCI compliance..... | 67 |
| configuring ACS servers | 64 |
| configuring group security settings | 85 |
| configuring group SSIDs and VLANs..... | 87 |
| configuring RADIUS..... | 53 |
| configuring TACACS+..... | 53 |

| | |
|--------------------------------------|-----|
| integrating NMS..... | 65 |
| RAPIDS and rogue classification..... | 183 |
| using triggers and alerts..... | 202 |
| servers | |
| specifying general settings..... | 32 |
| Smarthost | 278 |

SNMP

| | |
|---------------------|---------|
| polling period..... | 79 |
| SSIDs | 87 |
| Symbol..... | 99, 164 |
| Symbol/Intel..... | 83 |

T

| | |
|--------------------------------------|----------|
| TACACS+..... | 92 |
| adding a server..... | 92 |
| configuring authentication | 53 |
| integrating..... | 53 |
| templates | 164 |
| adding..... | 167, 180 |
| configuring a global template..... | 180 |
| configuring Cisco IOS templates..... | 175 |
| configuring for groups | 164 |
| global template variables | 181 |
| variables | 181 |
| Trapeze | 164 |

U

| | |
|---------------|----|
| user roles | |
| creating..... | 42 |
| users | |
| creating..... | 40 |

V

| | |
|----------------|----|
| VisualRF | 25 |
| VLANs | 87 |

W

| | |
|---------------------------|-----|
| WiMAX | 105 |
| Wireless LAN | |
| components..... | 13 |
| WLSE | |
| configuring..... | 58 |
| WLSE rogue scanning | 58 |

Y

| | |
|----------|-----|
| Yum..... | 287 |
|----------|-----|

