OmniVista 3600 Air Manager

User Guide

Version 6.1

© 2008 Alcatel-Lucent. Alcatel-Lucent, and the Alcatel-Lucent logo are trademarkes 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.

Introduction

Thank you for choosing the OmniVista 3600 Air Manager (**OV3600**). OV3600 is the centerpiece of the OmniVista 3600 Air Manager. OV3600 makes it easy and efficient to manage your wireless network by combining industry-leading functionality with an intuitive user interface, enabling network administrators and helpdesk staff to support and control even the largest wireless networks in the world.

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

The OmniVista 3600 Air Manager supports hardware from leading wireless vendors, including Aruba Networks, Alcatel-Lucent, Avaya, Cisco (Aironet and Airespace), Colubris Networks, Enterasys, Juniper Networks, LANCOM Systems, Meru, Nomadix, Nortel, ProCurve by HP, Proxim, Symbol, Trapeze, Tropos, and many others. The core components of the OmniVista 3600 Air Manager are:

- **OmniVista 3600 Air Manager** (OV3600) wireless network management software
- **VisualRF** location and RF mapping software module
- **RAPIDS** rogue access point detection software module
- **OmniVista 3600 Air Manager Master Console and Failover Servers** for scalability and high-availability

OmniVista 3600 Air Manager

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

VisualRF™

- Accurate location information for all wireless users and devices
- Up-to-date heatmaps and channel maps for RF diagnostics
    - Adjusts for building materials
    - Supports multiple antenna types
- 3-D campus and building views
- Visual display of errors and alerts
- Easy import of existing floorplans and building maps

RAPIDs™

- Automatic detection of unauthorized wireless devices
- Wireless detection
    - Uses authorized wireless APs to report other devices within range
    - Calculates and displays rogue location on VisualRF map
- Wired network detection
    - Discovers Rogue APs located beyond the range of authorized APs/sensors
    - Queries routers & switches
    - Ranks devices according to the likelihood they are rogues
    - Multiple tests to eliminate ‘false positive’ results
    - Provides rogue switch port

Master Console & Failover

- Provides network-wide visibility, even when the WLAN grows to 25,000+ devices.
- Executive Portal allows executives to view high-level usage and performance data
- Aggregated Alerts
- Failover
    - Many-to-one failover
    - One-to-one failover

This User Guide provides instructions for the installation, configuration, and operation of the OmniVista 3600 Air Manager. If you have any questions or comments, please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com.

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 will communicate 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 utilizing NAT. OV3600 communicates over-the-air or over-the-wire utilizing a variety of protocols.

Components of a Wireless LAN	
• 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, etc.)
• 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's database of managed APs

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

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

Hardware Requirements

OV3600's installation CD includes all software (including the Linux OS) required to complete the installation of the OmniVista 3600 Air Manager. OV3600 supports any hardware that is RedHat Enterprise Linux 5 certified.

OV3600 hardware requirements vary by version. As additional features are added to OV3600 increased hardware resources will be necessary. For the most recent hardware requirements, please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com.

Installing Linux CentOS 5 (Phase 1)

- Insert the OV3600 installation CD and boot the server.

! ***Warning – The following step will erase the server's hard drive(s).***

- The following message is displayed on the screen. If this is a new installation of OV3600 software, type `install` and press <Enter> to continue with the install. *NOTE: When you hit <Enter>, all the existing data on the hard drive will be erased.* To manually configure the partitions type 'expert' and press <Enter>.
- 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.

```
              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:
```

- Installing the CentOS software (Phase I) takes 10 - 20 minutes to complete. It will format the hard drive and launch Anaconda to install all necessary packages. Anaconda will gauge the progress of the installation.

- Upon completion, the system will automatically reboot and eject the installation CD.

- Remove the CD.

Installing OV3600 Software (Phase 2)

Getting Started

- After the reboot, OV3600’s GRUB screen will appear. Hit <ENTER> or wait 6 seconds, and the system will automatically load the “smp” kernel.

- When the kernel is loaded, log into the server using the following credentials:
    - login = “*root*”
    - password = “*admin*”

- Start OV3600’s software installation script by executing `./OV3600-install`. Type ‘./OV3600-install’ at the command prompt and hit enter to execute the script.

Step 1: Configuring Date and Time

The following message is displayed onscreen to ensure the proper time is set on the server.

```
------------------------ Date and Time Configuration ------------------

         Current Time: Fri Jul 26 09:18:12 PDT 2007


         1)  Change Date and Time
         2)  Change Time Zone

         0)  Finish
```

Ensure that the accurate date and time are entered. There will be errors during the install if the specified date varies significantly from the actual date. Select 1 to set the date and 2 to set the time zone. Changing these settings after the installation can cause a loss of graphical data and should be avoided.

Step 2: Checking for Previous OV3600 Installations

The following message is displayed onscreen.

```
      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 will automatically proceed to Step 3 below. If a previous version of the software **is** discovered, the following message displays 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)? y
```

! ***Warning – This will erase the current database including all historical information. To ensure that OV3600’s database is backed up prior to reinstallation, answer `n` and contact support.***

Step 3: Installing OV3600 Software

The following message is displayed on the screen 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 non-interactive step requires no user input. To view detailed output from OV3600’s software installer, press ‘*Alt-F9*’ or ‘*Ctrl-Alt-F9*’. Hitting ‘*Alt-F1*’ or ‘*Ctrl-Alt-F1*” will return you to the main console.

Step 4: Checking OV3600 Installation

The following message is displayed on the screen.

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

This non-interactive step requires no user input.

Step 5: Assigning OV3600’s IP Address

While OV3600’s primary network interface will initially accept a DHCP address during installation, OV3600 will not function unless a static IP is assigned.

The following message displays on the screen:

```
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
```

- Enter the network information. *Note: ‘Secondary DNS’ is an optional field.*
- Commit the changes by typing `9` and pressing <ENTER>. To discard the changes, type `0` and press <ENTER>.

Step 6: Naming OV3600

The following message is displayed on the screen.

```
STEP 5:  Naming OV3600
 OV3600’s name is currently set to: New OmniVista 3600 Air Manager
 Please enter a name for your OV3600:
```

- Enter a name for your OV3600 server and press <ENTER>.

Step 7: Assigning OV3600's Host Name

The following message is displayed on the screen.

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

- If OV3600 does **not** have a valid host name on the network, enter `*n*` at the prompt. The following message is displayed on the screen.

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

- If OV3600 **does** have a valid host name on the network, enter `*y*` at the prompt. The following message is displayed on the screen.

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

Type OV3600's DNS name and hit <ENTER>. The following message is displayed on the screen:

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

Step 8: Changing the Default Root Password

The following message is displayed on the screen.

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

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

- Enter the new root password. 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. It is recommended that you keep this password as secure as possible since it will allow full access to the machine. This password will not be needed on a day to day basis but will be required to perform OV3600 upgrades and advanced troubleshooting. If you lose this password please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com.

Completing the Installation

Upon completion after Step 8, the following message is displayed onscreen.

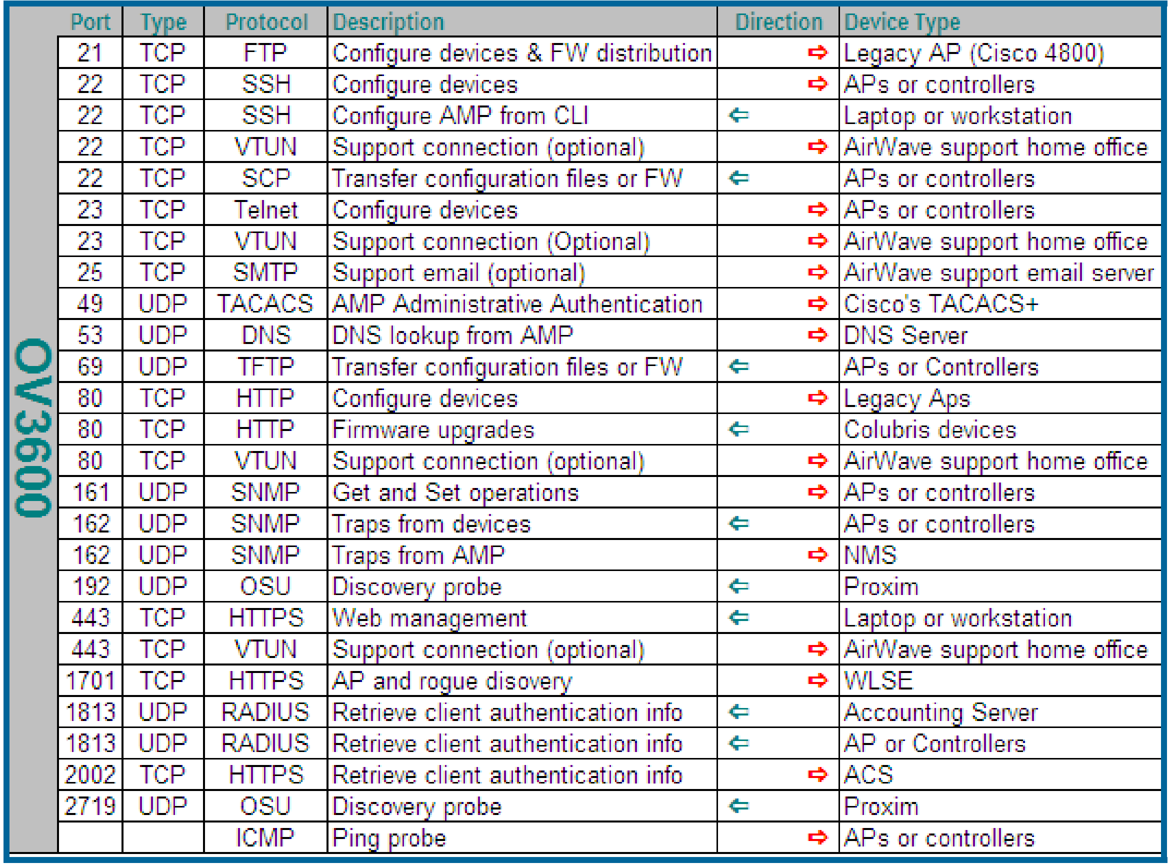
```
CONGRATULATIONS!  OV3600 is configured properly.
To access OV3600 web console, browse to https://<IP ADDRESS>
Login with the following credentials:
Username: admin
Password: admin
```

- 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's GUI enter OV3600's IP in the address bar of any modern browser. The OV3600 GUI will then prompt for your license key. If you are entering a dedicated Master Console or OV3600 Failover license please see the Maser Console or OV3600 Failover sections of the OV3600 User Guide.

Configuring the Firewall

The following diagram details the communication protocols and ports necessary for OV3600 to communicate with wireless LAN infrastructure devices, including APs, controllers, routers & switches, and RADIUS servers.

Figure 5. OV3600 Protocol and Port Diagram

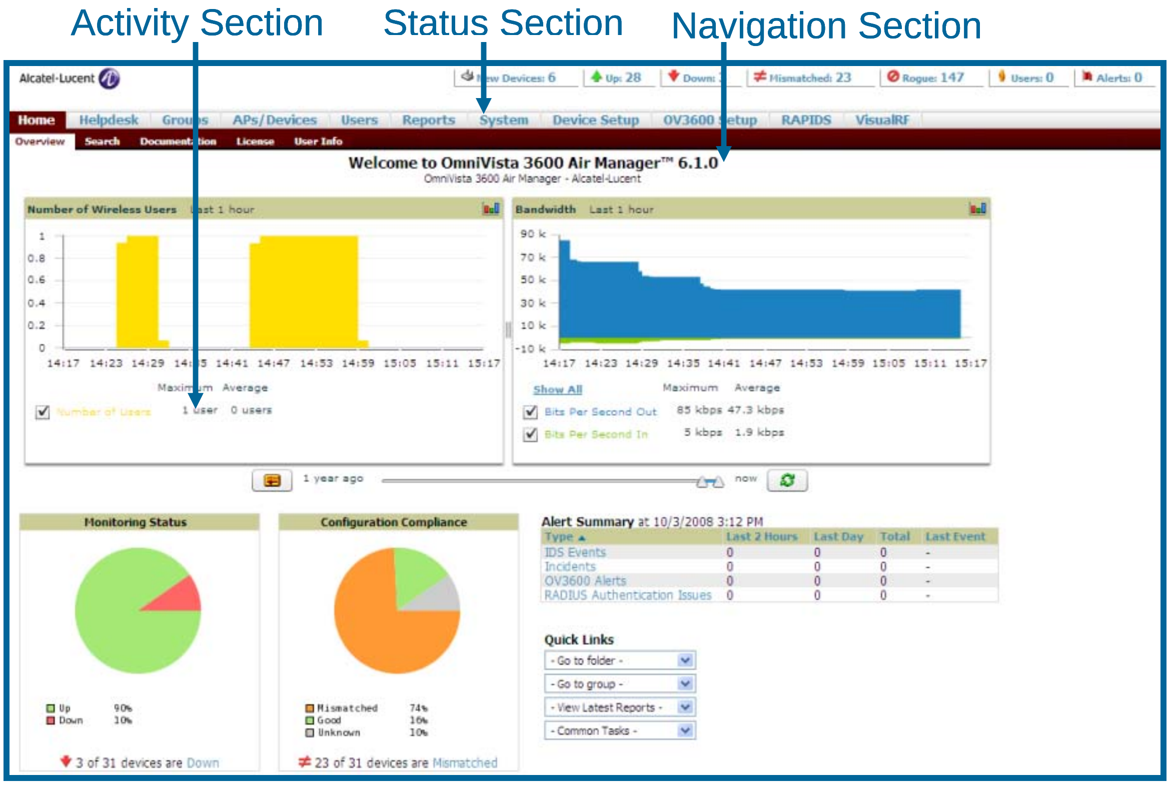


	Port	Type	Protocol	Description	Direction	Device Type
OV3600	21	TCP	FTP	Configure devices & FW distribution	⇨	Legacy AP (Cisco 4800)
	22	TCP	SSH	Configure devices	⇨	APs or controllers
	22	TCP	SSH	Configure AMP from CLI	⇐	Laptop or workstation
	22	TCP	VTUN	Support connection (optional)	⇨	AirWave support 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)	⇨	AirWave support home office
	25	TCP	SMTP	Support email (optional)	⇨	AirWave support email server
	49	UDP	TACACS	AMP Administrative Authentication	⇨	Cisco's TACACS+
	53	UDP	DNS	DNS lookup from AMP	⇨	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)	⇨	AirWave 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 AMP	⇨	NMS
	192	UDP	OSU	Discovery probe	⇐	Proxim
	443	TCP	HTTPS	Web management	⇐	Laptop or workstation
	443	TCP	VTUN	Support connection (optional)	⇨	AirWave support home office
	1701	TCP	HTTPS	AP and rogue disovery	⇨	WLSE
	1813	UDP	RADIUS	Retrieve client authentication info	⇐	Accounting Server
	1813	UDP	RADIUS	Retrieve client authentication info	⇐	AP or Controllers
	2002	TCP	HTTPS	Retrieve client authentication info	⇨	ACS
	2719	UDP	OSU	Discovery probe	⇐	Proxim
			ICMP	Ping probe	⇨	APs or controllers

OV3600 Navigation Basics

Every OV3600 page contains three basic sections: (1) Status Section, (2) Navigation Section, and (3) Activity Section. OV3600 pages also contain Help links with page-specific help information and certain standard action buttons.

Figure 6. OV3600 User Interface – Basic Sections



Alert Summary at 10/3/2008 3:12 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	-

Status Section

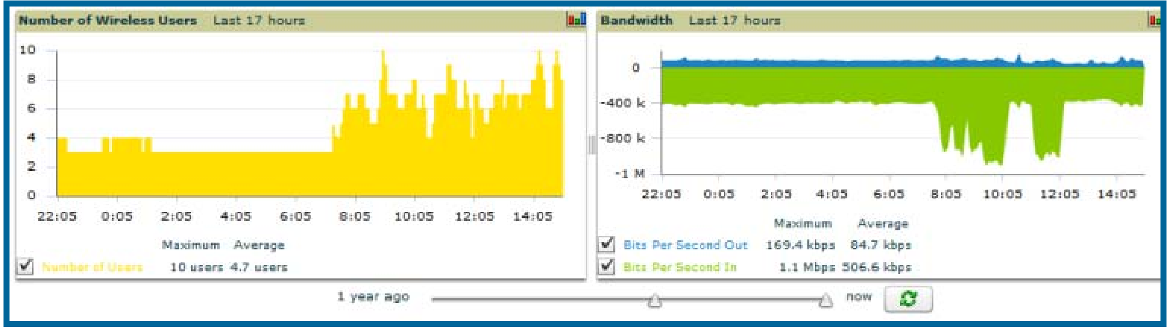
The Status Section provides a snapshot view of overall WLAN performance and provides direct links for immediate access to key system components.

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 will direct you to a page displaying a detailed list of devices awaiting authorization.
Up	The number of managed, authorized devices that are currently responding to OV3600's requests. When you click this link, OV3600 will direct you to a page displaying a detailed list of all "Up" devices.
Down	The number of managed, authorized devices that are **not** currently responding to OV3600's SNMP requests. When you click this link, OV3600 will direct you to a page displaying a detailed list of all "Down" devices.
Mismatched	The total number of Mismatched APs. An AP is considered mismatched when the desired configuration in OV3600 does not match the actual device configuration read off of the AP.

Rogue	The number of unknown APs detected on the network by OV3600 with a score of five. A score of five means the rogues were discovered via wireless or wireline fingerprint scanning techniques. When you click this link, OV3600 will direct you to a page displaying a detailed list of all “Rogue” APs. *NOTE: A newly discovered AP is considered a “Rogue” if it is not a supported AP that OV3600 can manage and monitor. If the newly discovered AP is capable of being managed and monitored by OV3600 it will be classified as a “New” device rather than a “Rogue.”*
Users	The number of wireless users currently associated to the wireless network via all the APs managed by OV3600. When you click this link, OV3600 will direct you to a page containing a list of users currently associated.
Alerts	The number of non-acknowledged OV3600 alerts generated by user-configured triggers. When you click this link, OV3600 will direct 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 will appear at the right of the Status field in bold red font. Only users configured on the **Home→User Info** page to view critical alerts can see Severe Alerts. The functionality of Severe Alerts is the same as that described above for Alerts. Unlike Alerts, the Severe Alerts section will be hidden if there are no Severe Alerts.
Search	Search performs partial string searches on a large number of fields including the notes, version, secondary version, radio serial number, device serial number, LAN MAC, radio MAC and apparent IP of all the APs as well as the client MAC, VPN user, LAN IP, VPN IP fields.

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

Figure 7. Flash graphs on the OV3600’s Home→Overview Page



Drag the slider at the bottom of the screen to move the scope of the graph between one year ago and the current time. Uncheck the boxes to change the data displayed on each graph. The button with green arrows refreshes data on the graph. Once a change to the slider bars or to the display boxes has been made, the same change can be applied to all other flash graphs with an apply button (appears on mouseover 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 interface is available if desired; instead of flash it uses the RRD graphs that were used in OV3600 through the 5.3 release. Contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com. for more information on activating this feature in the OV3600 database.

Navigation Section

The Navigation Section displays tabs to all main UI pages within OV3600. The top bar is a static navigation bar containing tabs for the main components of OV3600, while the lower bar is context-sensitive and displays the sub-menus for the highlighted tab.

Main Tab	Description	Sub-Menus
Home	The **Home** page provides basic OV3600 information, including system name, host name, IP address, current time, running time, and software version.	• Overview • Search • Documentation • License • User Info
Groups	The **Groups** page provides information on the logical "groups" of devices that have been established for efficient monitoring and configuration. (See "Configuring Groups" section below) *Note: Some of the tabs will not appear for all groups. Tabs are visible based on the device type field on the **Groups→Basic** page.*	• List • Focused Sub-Menus o Monitor o Basic o Templates o Security o SSIDs o RADIUS o Radio o Airespace Radio o LWAPP APs o WiMAX o Proxim Mesh o Colubris o MAC ACL o Firmware
APs/Devices	The **APs/Devices** page provides detailed information about all authorized APs and wireless LAN switches/controllers on the network, including all configuration and current monitoring data. *NOTE: Group-level settings are default values that are overridden by device-level settings when specified.*	• List • New • Up • Down • Mismatched • Ignored • Focused Sub-Menus o Monitor o Manage o Audit
Users	The **Users** page provides detailed information on all client devices and users currently associated to the WLAN.	• Connected • All • RFID Tags
Reports	The **Reports** page lists all the standard and custom reports generated by OV3600.	• List • Focused Sub-Menus o Detail
System	The **System** page provides information related to OV3600 operation and administration (including overall system status, the job scheduler, trigger/alert administration, etc.)	• Status • Scheduling • Event Log • Triggers • Alerts • Backups • Firmware Upgrade Jobs • Performance
Device Setup	The **Device Setup** page provides information related to the configurations of devices on the WLANs, including AP discovery parameters, firmware management, VLAN definition, etc.	• Discover • Add • Communication

Main Tab	Description	Sub-Menus
		• Firmware Files
OV3600 Setup*	**OV3600 Setup** page provides all information relating to the configuration of OV3600 itself and its connection to your network.	• General • Network • Users • Roles • TACACS+ • Routers and Switches • WLSE • ACS • NMS • RADIUS Accounting
RAPIDS*	The **RAPIDS** page provides all information relating to rogue access points. Including methods of discovery and lists of discovered and possible rogues.	• Overview • Rogue APS • Setup • Score Override
VisualRF*	**VisualRF** pages provide access to floor plans, client location, and RF visualization.	• Overview • Floors • COV3600us/Building • Setup
Master Console*	The **Management Console** page provides a centralized location to manage multiple OV3600s.	• Overview • Managed OV3600s • Alerts • Search

*Note: The OV3600 Setup tab will vary based on the user's role. The Master Console, RAPIDS and VisualRF tabs appear based on the license entered on the **Home→License** page and might not be visible on your OV3600.*

Activity Section

The Activity Section displays all detailed configuration and monitoring information, and is where changes will be implemented.

Help Pages

The Help link is available on every page within OV3600. When clicked it opens a help page with information related to the OV3600 page that is currently displayed.

Note: Acrobat Reader must be installed to view the .PDF help file.

Buttons and Icons

Standard buttons and icons are used consistently from screen to screen throughout OV3600's user interface:

Buttons and Icons	Description
Acknowledge	Acknowledge and clear an OV3600 alert.
Add	Add the object to both OV3600's database and the onscreen display list.
Add Folder	Add a new folder to hierarchically organize APs.
Alert	Indicates an alert.
Apply	Apply all "saved" configuration changes to devices on the WLAN.
Attach	Attach a snapshot of an OV3600 screen to a Helpdesk incident.
Audit	Read device configuration, compare to desired, and update status.
Bandwidth	Current bandwidth for group.
Choose	Choose a new Helpdesk incident to be the Current Incident.
Create	Create a new Helpdesk incident.
Customize	Ignore selected settings when calculating the configuration status.
Delete	Delete an object from OV3600's database.
Down	Indicate down devices and radios.
Duplicate	Duplicate or makes a copy of the configuration of an OV3600 object.
Edit	Edit the object properties.
Email	Link to email reports.
Filter	Filter rogue list by score and/or ad hoc status.
Google Earth	View device's location in Google Earth (requires plug-in).
Manage	Manage the object properties.
Monitor	Indicates an access point is in "monitor only" mode.
Ignore	Ignore specific device(s) – devices selected with check boxes.
Import	Update a Group's desired settings to match current settings.
Mismatched	Indicates mismatched access points.
New Devices	Indicates new access points and devices.
Poll Now	Poll device (or controller) immediately, override group polling settings.
Preview	Display a preview of changes applicable to multiple groups.
Print	Print the report.
Reboot	Reboot devices or OV3600.
Relate	Relates an AP, Group or Client to a Helpdesk incident.
Replace Hardware	Confers configuration and history of one AP to a replacement device.
Revert	Return all configurable data on the screen to its original status.
Rogue	Indicates a Rogue access point.
Run	Run a new user-defined report.
Save	Save the information on the page in OV3600's database.
Save & Apply	Save changes to OV3600's database and apply all changes to devices.
Scan	Scans for devices and rogues using selected networks.
Schedule	Schedule a window for reports, device changes, or maintenance.
Search	Searche OV3600 for the specified name, MAC or IP.
Up	Indicates access points which are in the up status.
Update Firmware	Apply a new firmware image to an AP/device.
User	Indicates a user.
VisualRF	Link to VisualRF – real time visualization.
XML	Link to export XHTML versions of reports.

Getting Started

Initial Login

Use your browser to navigate to the static IP assigned to OV3600’s internal interface. When presented with the OV3600 Authentication Dialogue Box:

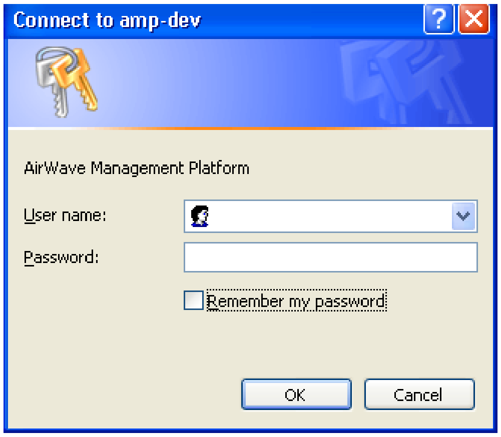
- Enter *User name*: “admin”
- Enter *Password:* “admin”
- Click “OK.”

NOTE: OV3600 pages are protected via SSL.

After successful authentication, your browser will launch OV3600’s **Home→Overview** page.

*NOTE: It is recommended that you change the default login and password on the **OV3600 Setup→Users** page. See the “Creating OV3600 Users” section for more information.*

Figure 8. OV3600 Authentication Dialogue



Connect to amp-dev

AirWave Management Platform

User name:

Password:

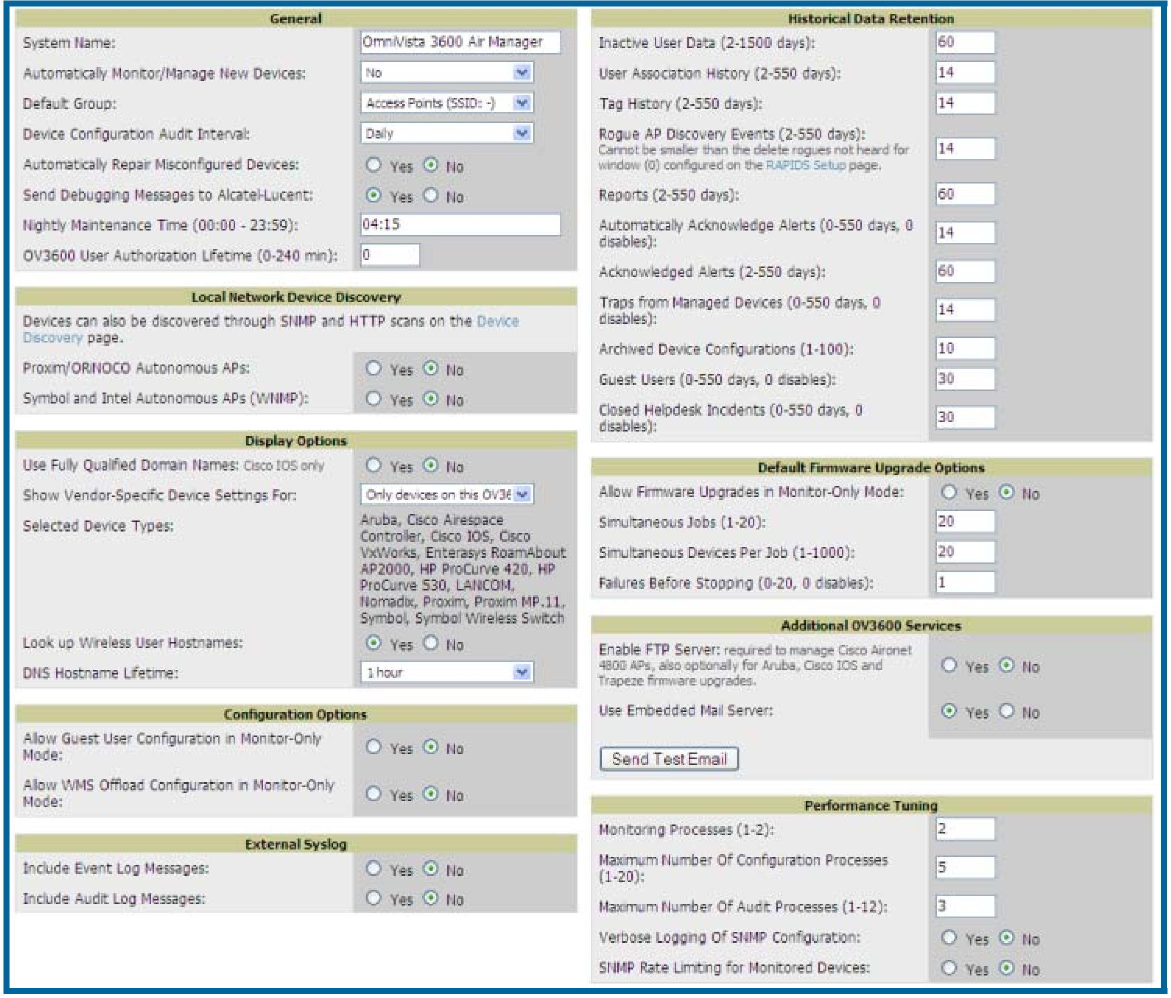
□ Remember my password

Configuring OV3600 on Your Network

General OV3600 Configuration Settings

The first step in configuring OV3600 is specifying the general settings for the OV3600 server.

Figure 9. "OV3600 Setup→General" Page Activity Section



General

System Name:	OmniVista 3600 Air Manager
Automatically Monitor/Manage New Devices:	No
Default Group:	Access Points (SSID: -)
Device Configuration Audit Interval:	Daily
Automatically Repair Misconfigured Devices:	○ Yes ● No
Send Debugging Messages to Alcatel-Lucent:	● Yes ○ No
Nightly Maintenance Time (00:00 - 23:59):	04:15
OV3600 User Authorization Lifetime (0-240 min):	0

Local Network Device Discovery

Devices can also be discovered through SNMP and HTTP scans on the Device Discovery page.

Proxim/ORINOCO Autonomous APs:	○ Yes ● No
Symbol and Intel Autonomous APs (WNMP):	○ Yes ● No

Display Options

Use Fully Qualified Domain Names: Cisco IOS only	○ Yes ● No
Show Vendor-Specific Device Settings For:	Only devices on this OV36
Selected Device Types:	Aruba, Cisco Airespace Controller, Cisco IOS, Cisco VxWorks, Enterasys RoamAbout AP2000, HP ProCurve 420, HP ProCurve 530, LANCOM, Nomadix, Proxim, Proxim MP.11, Symbol, Symbol Wireless Switch
Look up Wireless User Hostnames:	● Yes ○ No
DNS Hostname Lifetime:	1 hour

Configuration Options

Allow Guest User Configuration in Monitor-Only Mode:	○ Yes ● No
Allow WMS Offload Configuration in Monitor-Only Mode:	○ Yes ● No

External Syslog

Include Event Log Messages:	○ Yes ● No
Include Audit Log Messages:	○ Yes ● No

Historical Data Retention

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

Default Firmware Upgrade Options

Allow Firmware Upgrades in Monitor-Only Mode:	○ Yes ● No
Simultaneous Jobs (1-20):	20
Simultaneous Devices Per Job (1-1000):	20
Failures Before Stopping (0-20, 0 disables):	1

Additional OV3600 Services

Enable FTP Server: required to manage Cisco Aironet 4800 APs, also optionally for Aruba, Cisco IOS and Trapeze firmware upgrades.	○ Yes ● No
Use Embedded Mail Server:	● Yes ○ No

Performance Tuning

Monitoring Processes (1-2):	2
Maximum Number Of Configuration Processes (1-20):	5
Maximum Number Of Audit Processes (1-12):	3
Verbose Logging Of SNMP Configuration:	○ Yes ● No
SNMP Rate Limiting for Monitored Devices:	○ Yes ● No

- Browse to **OV3600 Setup→General** page, locate the "General" area, and enter the following information:

Setting	Default	Description
System Name	"OV3600"	User-definable name for OV3600 server (max. 20 characters)
Console Refresh Rate	60	Drop down menu that specifies the number of seconds (5, 10, 15, 30, 60, 120 and never) between screen refreshes on OV3600 monitoring screens.

Setting	Default	Description
Automatically Monitor/Manage New Devices	No	Drop down menu that specifies the behavior OV3600 should follow when it discovers a new device. Devices will be placed in the default group which is defined on the Groups→List page. No: new devices will remain on the New Devices page until manually added to the OV3600. Monitor Only: newly discovered devices will be automatically added to the default group in Monitor Only mode. Manage Read/Write : newly discovered devices will be added to the default group in Managed mode. ***Caution should be exercised when selected managed mode since it will overwrite the config of any newly discovered device.***
*Default Folder**	NA	The folder used when automatically monitoring or managing new devices. The default folder is the top folder of the default group. It is calculated as the lowest folder that is still able to view all of the APs in a group. *Note: The Default Folder field is only visible when OV3600 is set to Automatically Monitor or Manage New Devices.*
Device Configuration Audit Interval	Daily	If enabled, OV3600 will query each device at the selected interval and compare actual device settings to the Group configuration policies stored in OV3600's database. If the settings do not match the AP will be flagged as mismatched and OV3600 will send an alert via email, log, or SNMP. *Note: It is recommended that you enable this feature with a frequency of "Daily" or greater to ensure that your AP configurations comply with your established policies.*
Automatically Repair Misconfigured Devices	Disabled	If enabled, OV3600 will automatically reconfigure the settings on the device when it detects a variance between actual device settings and the Group configuration policy in OV3600's database.
Nightly Maintenance Time (00:00 – 23:59)	04:15	OV3600 performs maintenance on a daily basis. This field specifies the time of day OV3600 should perform the maintenance. During maintenance OV3600 cleans the database, performs backups and completes a few other housekeeping tasks.
OV3600 Authorization Lifetime (0-240 min)	120	The amount of time, in minutes, that an OV3600 user session will last before the user must authenticate when a new browser window is opened. Setting the lifetime to 0 will require the user to login every time a new browser window is opened.
DNS Lookup of User Hostnames	Yes	OV3600 will automatically look up DNS for new user hostnames. This can be turned off to troubleshoot performance issues.
DNS Cleanup Period	1 hour	The period after which OV3600 refreshes the DNS lookup.

- On the **OV3600 Setup→General** page, locate the "Auto-Discovery" area, and indicate whether or not you want to use the specified local broadcast protocols for discovering new and rogue Devices. *NOTE: Local broadcast protocols typically work only on the local subnet to which OV3600 is connected. CDP (Cisco Discovery Protocol) will work on both local and remote subnets when it is enabled and OV3600 is configured to access (read only) CDP information from the appropriate routers and switches.*

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

- On the **OV3600 Setup→General** page locate the Default Group Display Options section. The Default Group Display Options will configure which Group tabs and options appear by default in new groups. Changes to this section are OV3600-wide. They will affect all users and new groups.

Setting	Default	Description
Show Device Settings For:	All Devices	Drop down menu that determines which Group tabs and options will be viewable by default in new groups: All Devices: OV3600 will display all Group tabs and setting options. Only Devices on this OV3600: OV3600 will hide all options and tabs that do not apply to the APs and devices currently on OV3600. Selected device types: Allows the user to specify the device types for which OV3600 will display Group settings.
Selected Device Types	None	Select the device types that are likely to be in a group. OV3600 will only display configuration information related to the selected device types.

- On the **OV3600 Setup→General** page locate the Configuration Options section. The Configuration Options will configure whether certain changes can be pushed to devices in monitor-only mode.

Setting	Default	Description
Allow Guest User Configuration in Monitor-Only Mode	No	When “Yes,” new Airespace 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 will not reboot as a result of the push.
Allow WMS Offload Configuration in Montior-Only Mode (for Aruba/Alcatel-Lucent WLAN switches only)	No	When “Yes,” the WMS offload feature on the **Groups→Basic** page can be enabled for Aruba/Alcatel-Lucent WLAN switches in monitor-only mode. Enabling WMS offload will not cause a controller to reboot.

- On the **OV3600 Setup→General** page locate the Historical Data section and specify the number of days you wish to keep client session records and rogue discovery events.

Setting	Default	Description
Inactive User Data (2-1500 days)	60	The number of days OV3600 will store basic information about inactive users. It is recommended that you use 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 will need.
User Association History (2-550 days)	14	The number of days OV3600 will store client session records. The longer you store client session records the more hard disk space you will need.
Rogue AP Discovery Events (2-550 days)	14	The number of days OV3600 will store Rogue Discovery Events. The longer you store discovery event records the more hard disk space you will need.
Reports (2-550 days)	60	The number of days OV3600 will store Reports. Large numbers of reports, over 1000, can cause the **Reports→List** page to be slow to respond.
Acknowledged Alerts (2-550 days)	60	The number of days OV3600 will retain information about acknowledged alerts. Large numbers of Alerts, over 2000, can cause the **System→Alerts** page to be slow to respond.
Traps from Managed Devices (0-550 days, 0 disables)	14	The number of days OV3600 will retain information about traps from Managed Devices.

- On the **OV3600 Setup→General** page, locate the Default Firmware Upgrade Options section. This section allows you to configure the default firmware upgrade behavior for OV3600.

Setting	Default	Description
Allow Firmware upgrades in Monitor-Only mode	No	If yes is selected OV3600 will upgrade the firmware for APs in Monitor-Only mode. When OV3600 upgrades the firmware in monitor only mode the desired configuration will not be pushed to OV3600. Only the firmware will be applied. The firmware upgrade may result in configuration changes. OV3600 will not correct those changes when the AP is in Monitor Only mode.
Number of Simultaneous Jobs (1-20)	20	The number of jobs OV3600 will run at the same time. A job can include multiple APs.
Default number of devices to be upgraded simultaneously (1-1000)	20	The number of devices that can be in the process of upgrading at the same time. **OV3600 will only run one tftp transfer at a time.** As soon as the transfer to a device has completed the next transfer will begin, even if the first device is still in the process of rebooting or verifying configuration.
Default number of failures before stopping	1	The default number of upgrade failures before OV3600 pauses the upgrade process. User intervention is required to resume the upgrade process.
Serve firmware files from this interface	Primary	This is the address that the devices will use to fetch the firmware file.

- *On the **OV3600 Setup→General** page, locate the Display Options section.*

Setting	Default	Description

Setting	Default	Description
Use Fully Qualified Domain Names	Enabled	Use fully qualified domain names for APs in OV3600 instead of the AP name. For example, “testap.yourdomain.com” instead of “testap.”
Show Device Settings For	All Devices	Select the device types for which to use fully qualified domain names.

- On the **OV3600 Setup→General** page, locate the Additional OV3600 Services section.

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. It is recommended that you disable the FTP server if you do not have any Cisco Aironet 4800 APs.

- On the **OV3600 Setup→General** page, locate the Performance Tuning section. Performance tuning is unlikely to be necessary for many OV3600 customers and will likely show the most improvements for customers with extremely large Pro or Enterprise installations. Please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com.if you think you might need to change any of these settings.

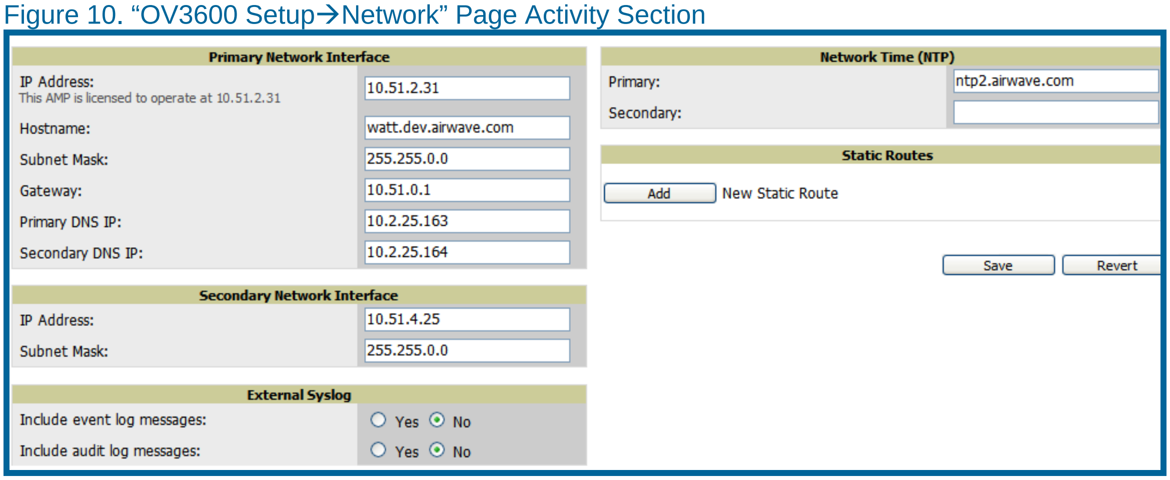
Setting	Default	Description
Monitoring Processes	Based on the number of cores for your sever	OV3600 gives you the option to configure the throughput of monitoring data. Increasing this setting can allow OV3600 to process more data per second, but it can take resources away from other OV3600 processes. Please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com. if you think you might need to increase this setting for your network.
Maximum number of configuration processes	5	OV3600 gives you the option to increase the number of processes that are pushing configurations to your devices. The optimal setting for your network depends on the resources available, especially ram. Please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com. if you think you might need to increase this setting for your network.
Maximum number of audit processes	3	OV3600 gives you the option to increase the number of processes that are auditing configurations for your devices. The optimal setting for your network depends on the resources available, especially ram. Please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com. if you think you might need to increase this setting for your network.

- Click “Save” when settings are completed.

Defining OV3600 Network Settings

The next step in configuring OV3600 is confirming OV3600's network settings.

Figure 10. "OV3600 Setup→Network" Page Activity Section



Primary Network Interface

IP Address: This AMP is licensed to operate at 10.51.2.31	10.51.2.31
Hostname:	watt.dev.airwave.com
Subnet Mask:	255.255.0.0
Gateway:	10.51.0.1
Primary DNS IP:	10.2.25.163
Secondary DNS IP:	10.2.25.164

Secondary Network Interface

IP Address:	10.51.4.25
Subnet Mask:	255.255.0.0

External Syslog

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

Network Time (NTP)

Primary:	ntp2.airwave.com
Secondary:	

Static Routes

- Browse to **OV3600 Setup→Network** page and locate the "Primary Network Interface" area. *The information in this section should match those defined during Initial Network Configuration and should not require changes.*

Setting	Default	Description
IP Address	None	The IP Address of OV3600's network interface. *NOTE: This address must be a statically assigned IP address.*
Hostname	None	The DNS name assigned to the OV3600 server.
Subnet Mask	None	The subnet mask for OV3600's primary network interface.
Gateway	None	The default gateway for OV3600's network interface.
Primary DNS IP	None	Primary DNS IP for OV3600's network interface.
Secondary DNS IP	None	Secondary DNS IP for OV3600's network interface.

- On the **OV3600 Setup→Network** page, locate the "Secondary Network Interface" area. *The information in this section only needs to be completed if the server running OV3600 is using a second network interface.*

Setting	Default	Description
IP Address	None	The IP Address of OV3600's secondary network interface. *NOTE: This address must be a statically assigned IP address.*
Subnet Mask	None	The subnet mask for OV3600's secondary network interface.

- On the **OV3600 Setup→Network** page, locate the "Network Time (NTP)" area. The Network Time Protocol is used to synchronize the time on OV3600 with your organization's reference server. *NOTE: Specifying NTP servers is optional. The servers synchronize the time on the OV3600 server, not individual access points. To disable NTP services, simply clear both the "Primary" and "Secondary" NTP server fields. Any problem related to communication between OV3600 and the NTP servers will create an entry in the event log.*

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

- On the OV3600 Setup→Network page, locate the "External Syslog" area. *Use this section to configure OV3600 to send audit and system events to an external syslog server.*

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

- On the **OV3600 Setup→Network** page, locate the "Static Routes" area. *Use this section when OV3600 needs to reach certain networks that are inaccessible through the default gateway. It is likely that you will leave this section blank.*

  - To **add** a new static route, click the add button. On the following screen enter the *Network* (IP Address), *Subnet Mask*, and *Gateway* information and click "Add."

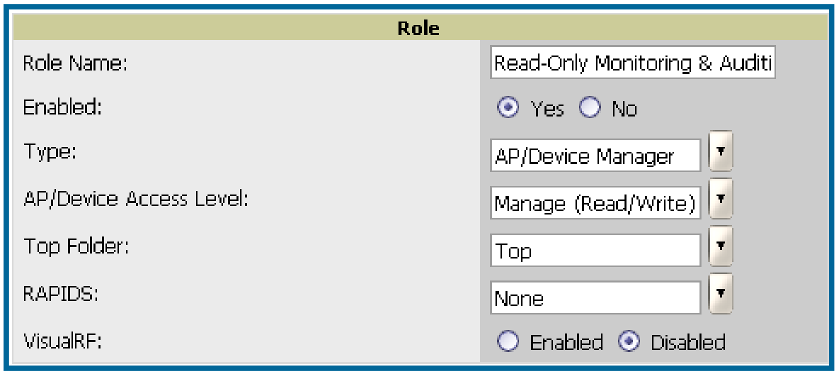
  - To **delete** an existing static route, check the box next to the static route you want to remove and click "Delete."

- Click "Save" when all changes have been completed. This will restart any affected services and may temporarily disrupt your network connection.

Creating OV3600 User Roles

The User Role defines the viewable devices, the operations that can be performed on devices, and general OV3600 access. VisualRF uses the same user roles as defined for OV3600 users can see floor plans that contain an AP that they have access to in OV3600 (although only visible APs will appear on the floorplan). They can also see any building that contains a visible floorplan, and any campus that contains a visible building. When a new role is added to OV3600, VisualRF must be restarted for the new user to be enabled.

Figure 11. “OV3600 Setup→Roles” Add page



Role	
Role Name:	Read-Only Monitoring & Auditi
Enabled:	● Yes ○ No
Type:	AP/Device Manager
AP/Device Access Level:	Manage (Read/Write)
Top Folder:	Top
RAPIDS:	None
VisualRF:	○ Enabled ● Disabled

- Roles define the type, privileges and the viewable groups/APs.

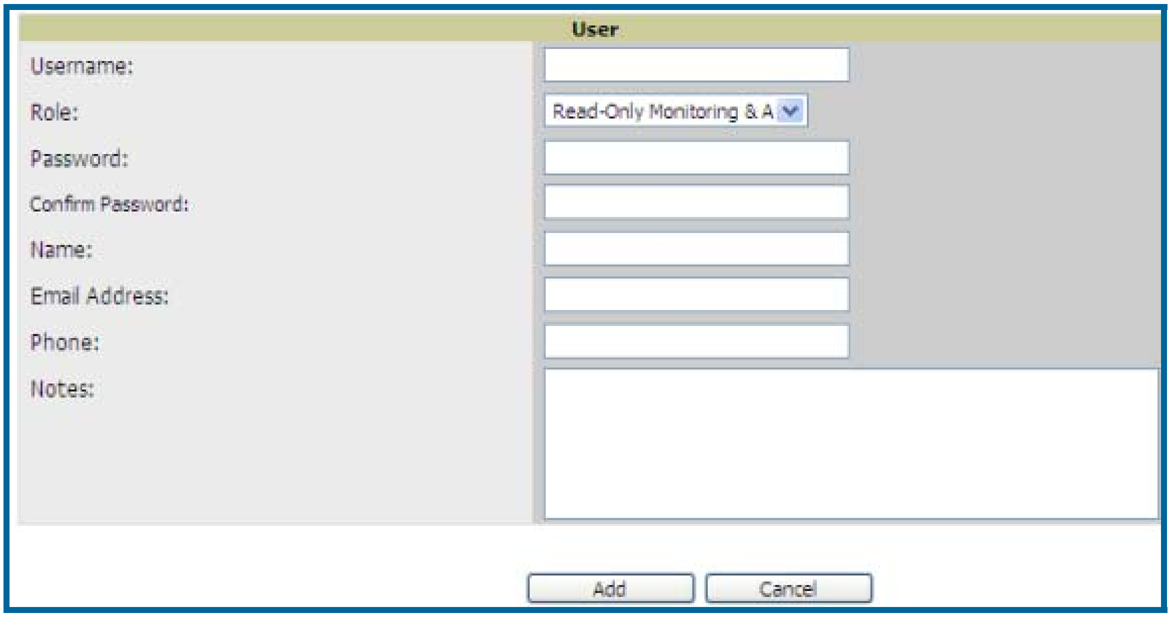
Setting	Default	Description
Role Name	None	Administrator definable string that names the role. It is recommended that the role name give an indication of the devices and Groups that are viewable as well as the privileges granted to the role.
Enabled	Yes	Disable or enable the role. Disabling a role will prevent all users of that role from logging in to OV3600.
Type	None	There are three types of roles in OV3600. 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 any of the OV3600 Setup pages. AP/Device Manager: AP/Device Managers have access to a limited number of devices and groups based on the Top folder and varying levels of control based on the Access Level.

Setting	Default	Description
Access Level	None	The privileges the role has over the viewable APs. 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 will have access to the **APs/Devices→Audit** page which may contain sensitive information including AP passwords. Monitor (Read Only): Monitor users have read only access to the devices and Groups. Monitor users can not view the **APs/Devices→Audit** page which may contain sensitive information including AP passwords.
Top Folder	None	The Top viewable folder for the role. The role will be able to view all devices and groups contained by the Top folder. The top folder and its sub folders must contain all of the devices in any of the groups it can view.
RAPIDS	None	The RAPIDS privileges are set separately from the APs/Devices. This field specifies the RAPIDS privileges for the role. Read/Write: The user may ignore, delete, override scores and perform OS scans. Read Only: The user can view the RAPIDS pages but cannot make any changes to rogue APs or perform OS scans. None: Cannot view the RAPIDS tab or any Rogue APs.
VisualRF	None	OV3600 Administrators will always have access to VisualRF. Read-Only users do not have access to VisualRF. Read/Write AP/Device Managers VisualRF permissions are decided by the radio button.

Creating OV3600 Users

OV3600 installs with only one user, the OV3600 administrator, “admin”. The Administrator is able to define additional users with varying levels of privileges. The admin can limit the viewable devices as well as the type of access a user has to the devices. For each user a Username, Password and a Role are defined. The username and password are used when logging in to the OV3600 GUI. It is helpful to use unique and meaningful usernames as they are recorded in the log files when changes are made in OV3600. The role defines the user type, access level and the top folder. Roles are defined on the **OV3600 Setup→Roles** page. The admin can optionally note additional information about the user including the user’s real name, email address, phone number etc.

Figure 12. “OV3600 Setup→Users” Add Page Section



User

Username:

Role: Read-Only Monitoring & A

Password:

Confirm Password:

Name:

Email Address:

Phone:

Notes:

- On the **OV3600 Setup→Users** page set and change Usernames, Passwords and Roles. Roles are defined on the **OV3600 Setup→Roles** page. The role defines the top viewable folder, type and access level of the user. The Name, E-Mail, Phone and Notes field are completely optional. They are provided to help administrators keep track of their users.

Setting	Default	Description
Username	None	The Username is used when logging in to OV3600 and in the log files.
Role	None	This setting specifies the User Role which defines the Top viewable folder, type and access level of the user.
Enabled	Yes	Displays the status of the Role. If a Role is disabled any users associated with it will not be able to login to OV3600. Roles are enabled from the **OV3600 Setup→Roles** page.
Type	None	There are three types of users in OV3600. OV3600 Administrator: The OV3600 Administrator has full access to OV3600 and all of the APs. The administrator can view and edit all settings and all APs in OV3600. Only the OV3600 Administrator can create new Users and acces all of the OV3600 Setup pages. AP/Device Manager: AP/Device Managers have access to a limited number of devices and groups based on the Top folder and varying levels of control based on the Access Level. AP/Device Managers are limited to the NMS sub tab of the OV3600 Setup pages
Access Level	None	Specifies the privileges an AP/Device Manager has over the viewable APs. Manage (Read/Write): Manage users have read/write access to the viewable APs and Groups. They can change all OV3600 settings for the APs and Groups they can view. Audit (Read Only): Audit users have read only access to the viewable APs and Groups. Audit users will have access to the **APs/Devices→Audit** page which may contain sensitive information including AP passwords. Monitor (Read Only): Similar to the Audit role, monitor users have read only access to the APs and Groups. However monitor users can not view the **APs/Devices→Audit** page which may contain sensitive information including AP passwords.
Top Folder	None	The Top viewable folder for the user. The user will be able to view all APs and groups contained by the Top folder. You can not assign a top folder that would give a user access to only part of a group. If the top folder and its sub folders contain one AP from a group they must contain all APs in that group.
RAPIDS	None	Specifies the RAPIDS privileges for the user's role. Read/Write: The user may Ignore, Delete, override scores and perform OS scans. Read Only: The user can view the RAPIDS pages but can not make any changes to rogue APs or perform OS scans. None: Can not view the RAPIDS tab or any Rogue APs.
Name	None	Optional text field used to take note of the user's actual name.

Setting	Default	Description
E-Mail	None	Optional text field used to take note of the user's email address.
Phone	None	Optional text field used to take note of the user's phone number.
Notes	None	Optional text field for any additional notes about the user including the reason they were granted access, user's department or job title.

Note: OV3600 installs with one default user "admin". Because the default user's password is identical to its name, it is strongly recommended that this password is changed.

! ***It is strongly recommended that you immediately change the default OV3600 "admin" password.***

Configuring TACACS+ integration (Optional)

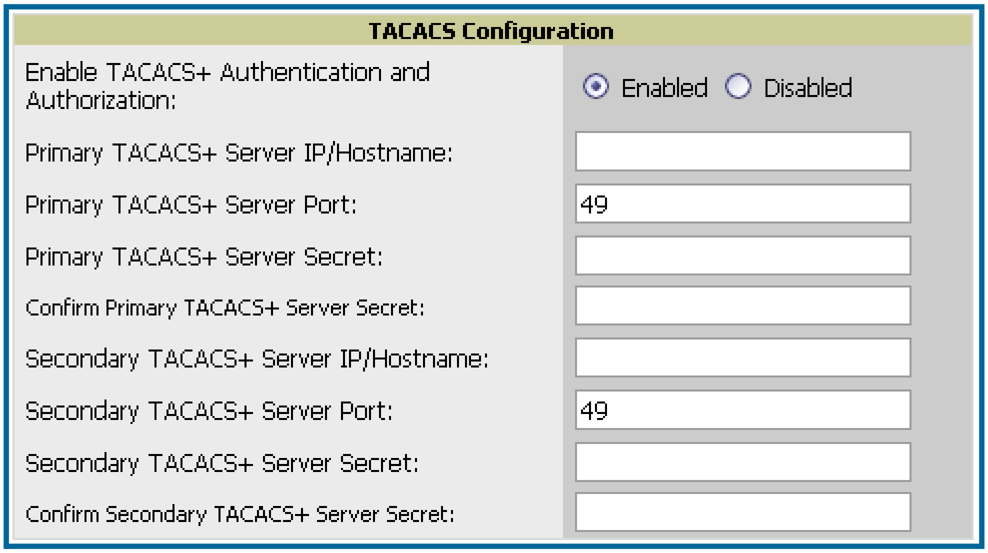
OV3600 can be configured to use an external user database to simplify password management for OV3600 admins and users. OV3600 needs to be configured with the IP/Hostname of the TACAS+ server, port and server secret.

To configure Cisco ACS to work with OV3600 you will need to define a new service named OV3600 that uses https on the ACS server. The OV3600 https service is added to the TACACS+ (Cisco) page under the Interface Configuration tab. Select a checkbox for a new service. Enter OV3600 in the service column and https in the protocol column.

Next you will need to edit the existing groups or users in TACACS to use the “OV3600 service” and define a role for the group or user. The role defined on the Group Setup page in ACS must exactly match name of the role defined on the **OV3600 Setup→Roles** page. The defined role should use the following format: role=<name_of_OV3600_role>. For exOV3600le: role=DormMonitoring. Like your routers and switches, OV3600 does not need to know anything about the usernames.

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. Select TACACS+ (Cisco IOS) in the “Authenticate Using” drop down menu and click submit + restart.

Figure 13. “OV3600 Setup→TACACS+” page



TACACS Configuration

Enable TACACS+ Authentication and Authorization:	● Enabled ○ Disabled
Primary TACACS+ Server IP/Hostname:	
Primary TACACS+ Server Port:	49
Primary TACACS+ Server Secret:	
Confirm Primary TACACS+ Server Secret:	
Secondary TACACS+ Server IP/Hostname:	
Secondary TACACS+ Server Port:	49
Secondary TACACS+ Server Secret:	
Confirm Secondary TACACS+ Server Secret:	

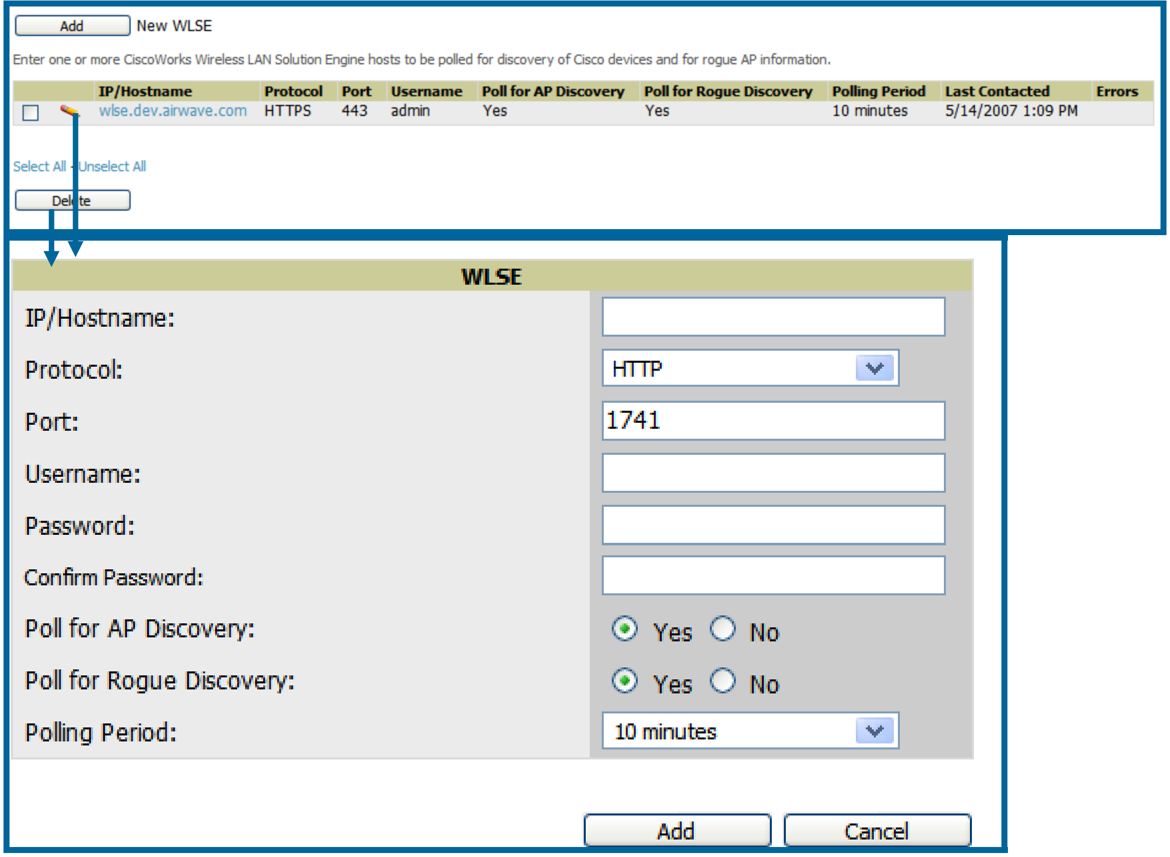
Note: OV3600 will check the local username/password store before checking with the TACACS+ server. If the user is found locally the local password and local role will apply.

Integrating with WLSE Rogue Scanning (Optional)

The **OV3600 Setup→WLSE** page allows OV3600 to integrate with Cisco's WLSE. OV3600 can discover APs and gather rogue scanning data from Cisco's WLSE. Please see **APPENDIX A** for instructions detailing how to configure the WLSE to communicate with OV3600.

- To add a WLSE server to OV3600 navigate to the **OV3600 Setup→WLSE** page and click on the add button.

Figure 14. "OV3600 Setup→WLSE" page



New WLSE

Enter one or more CiscoWorks Wireless LAN Solution Engine hosts to be polled for discovery of Cisco devices and for rogue AP information.

		IP/Hostname	Protocol	Port	Username	Poll for AP Discovery	Poll for Rogue Discovery	Polling Period	Last Contacted	Errors
□	✎	wlse.dev.airwave.com	HTTPS	443	admin	Yes	Yes	10 minutes	5/14/2007 1:09 PM	

WLSE

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

Setting	Default	Description
IP Address/ Hostname	None	The IP Address or DNS Hostname for the WLSE server.
Protocol	HTTP	Drop-down menu that specifies the protocol to be used when polling the WLSE.
Port	1741	The port OV3600 will use to communicate with the WLSE server.
Username	None	The username OV3600 will use 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. Due to a Cisco issue only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) will allow OV3600 to pull the necessary XML APIs.

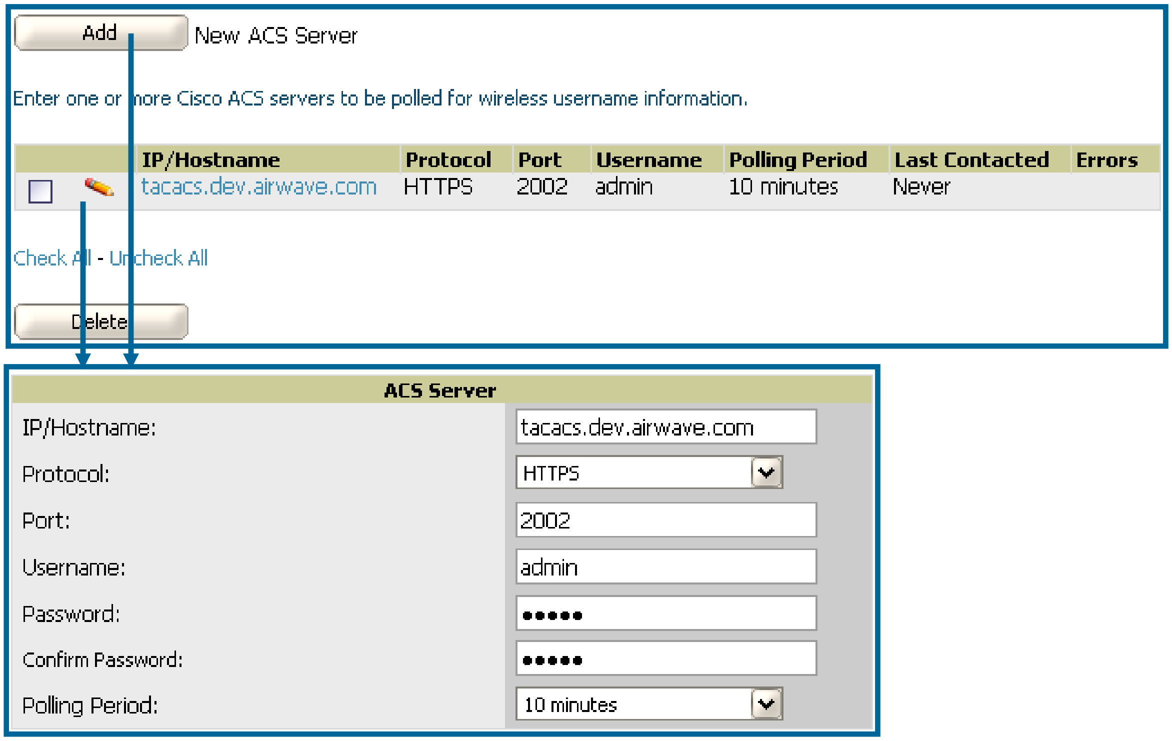
Setting	Default	Description
Password	None	The password OV3600 will use to communicate with the WLSE server. The username and password must be configured the same way on the WLSE server and on OV3600. Due to a Cisco issue only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) will allow OV3600 to pull the necessary XML APIs.
Poll for AP Discovery; Poll for Rogue Discovery	Yes	OV3600 will use WLSE to poll for discovery of new APs and/or new rogue devices on the network.
Last Contacted	None	The last time OV3600 was able to contact the WLSE server
Polling Period	10 minutes	Determines how frequently OV3600 will poll WLSE to gather rogue scanning data.
Error	None	Helpful error messages will appear in this field if errors occur to aid in debugging.

- After you have filled in all fields click the Save button. OV3600 is now configured to gather rogue information from WLSE rogue scans. Any Rogues found by WLSE will appear on the **RAPIDS→Rogue page.**

ACS Integration (Optional)

The **OV3600 Setup→ACS** page allows OV3600 to poll one or more Cisco ACS servers for wireless username information. When an ACS server is specified OV3600 is able to poll it for username information. The OV3600 Setup→ACS page is used to gather information about your networks wireless users. Please see the TACACS+ section if you want to use your ACS server to manage your OV3600 users.

Figure 15. "OV3600 Setup→ACS" page



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

		IP/Hostname	Protocol	Port	Username	Polling Period	Last Contacted	Errors
□	✎	tacacs.dev.airwave.com	HTTPS	2002	admin	10 minutes	Never	

ACS Server

IP/Hostname:	tacacs.dev.airwave.com
Protocol:	HTTPS
Port:	2002
Username:	admin
Password:	●●●●●
Confirm Password:	●●●●●
Polling Period:	10 minutes

- To specify one or more ACS servers OV3600 should communicate with, browse to **OV3600 Setup→ACS** page and provide the following information:

Setting	Default	Description
IP/Hostname	None	DNS name or the IP Address of the ACS Server.
Protocol	HTTP	Drop down menu specifying the protocol OV3600 will use when it polls the ACS server.
Port	2002	The port through which OV3600 will communicate with the ACS. *(NOTE: OV3600 will generally communicate via SNMP traps on port 162).*
Username	None	The Username of the account OV3600 will use to poll the ACS server.
Password	None	The Password of the account OV3600 will use to poll the ACS server.
Polling Period	10 min	Drop down menu that specifies how frequently OV3600 will poll the ACS server for username information.

- The ACS server must have logging enabled for passed authentications. To configure your ACS server to log the required information you will need to enable the “Log to CSV Passed Authentications report” option. To enable it, login to the ACS server, click on System Configuration, then in the select frame click on the Logging link. Under Enable Logging click on the CSV Passed Authentications link. The default logging options will work. They include the 2 columns which we require, User-Name and Caller-ID.

Integrating with an Existing Network Management Solution (Optional)

The **OV3600 Setup→NMS** page allows OV3600 to integrate with other Network Management Solution (NMS) consoles.

- OV3600 can be configured to forward WLAN-related SNMP traps to the NMS, or to send SNMPv1 or SNMPv2 traps to NMS. OV3600 can be used in conjunction with HP's ProCurve Manager. The necessary files can be downloaded from the **OV3600 Setup → NMS** page.

NOTE: This is an optional step to enable the advanced functionality described above.

- To specify the NMS server with which OV3600 should communicate, browse to **OV3600 Setup→NMS** page, click add and provide the following information:

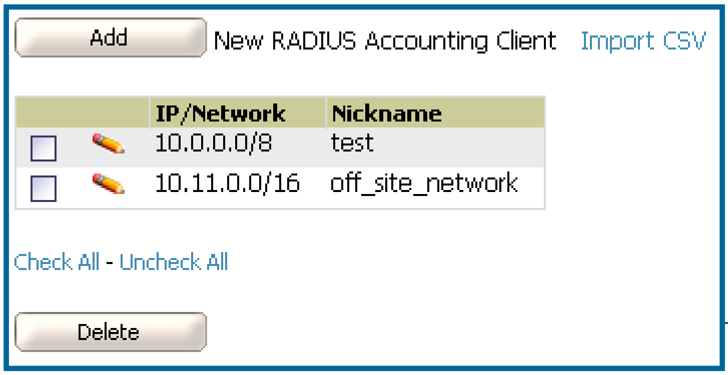
Setting	Default	Description
Host	None	DNS name or the IP Address of the NMS.
Port	162	The port OV3600 will use to communicate with the NMS. *(NOTE: OV3600 will generally communicate via SNMP traps on port 162).*
Community String	None	The community string used to communicate with the NMS.
SNMP Version	v2C	The SNMP version of the traps sent to the Host.
Enabled	Yes	Radio button to enable or disable trap logging to the specified NMS.
Role	None	NMS servers can be restricted by role (**OV3600 Setup→Users** page).

Integrating with a RADIUS Authentication Server (Optional)

The **OV3600 Setup→RADIUS Accounting** page allows OV3600 to receive RADIUS accounting records from a wide variety of RADIUS-based authentication servers and APs. OV3600 utilizes these records to correlate the MAC Address of each user associated to an AP with a user name from the authentication server. This allows OV3600 to monitor and track each user by name rather than by MAC Address.

NOTE: This is an optional step to enable the advanced functionality described above. It is not required for basic OV3600 operation.

Figure 17. "OV3600 Setup→RADIUS Accounting" page



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

- To specify the authentication server or network with which OV3600 should communicate, browse to the **OV3600 Setup→RADIUS Accounting** page and provide the following information:

Setting	Default	Description
Nickname	None	User-defined name for the authentication server.
IP/Network	None	List 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 (e.g. 10.51.0.0/24).
Shared Secret	None	The Shared Secret that will be used to establish communication between OV3600 and the RADIUS authentication server.

- Click “Save.”
- For additional information on configuring WLAN Gateways or WLAN Controllers such as BlueSocket, ReefEdge, or ProCurve wireless gateways please proceed to Appendix B.

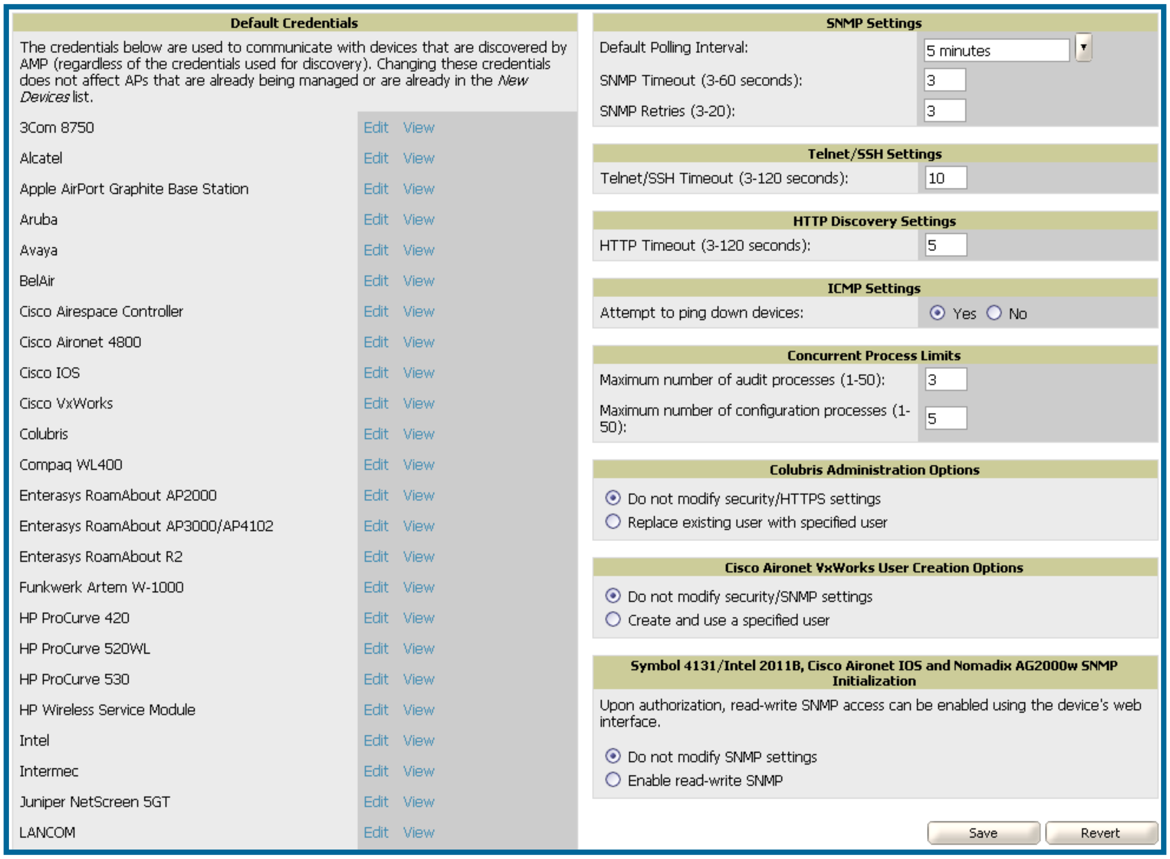
Enabling OV3600 to Manage Your Devices

Once OV3600 is configured and on the network, the next step is to define the basic settings that will allow OV3600 to communicate with and manage your devices.

Configuring OV3600 Discovered Devices Communication Settings

The first step is to configure OV3600 to communicate with your devices by defining default shared secrets and SNMP polling information.

Figure 18. "Device Setup→Communication" page



Default Credentials

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

3Com 8750	Edit	View
Alcatel	Edit	View
Apple AirPort Graphite Base Station	Edit	View
Aruba	Edit	View
Avaya	Edit	View
BelAir	Edit	View
Cisco Airespace Controller	Edit	View
Cisco Aironet 4800	Edit	View
Cisco IOS	Edit	View
Cisco VxWorks	Edit	View
Colubris	Edit	View
Compaq WL400	Edit	View
Enterasys RoamAbout AP2000	Edit	View
Enterasys RoamAbout AP3000/AP4102	Edit	View
Enterasys RoamAbout R2	Edit	View
Funkwerk Artem W-1000	Edit	View
HP ProCurve 420	Edit	View
HP ProCurve 520WL	Edit	View
HP ProCurve 530	Edit	View
HP Wireless Service Module	Edit	View
Intel	Edit	View
Intermec	Edit	View
Juniper NetScreen 5GT	Edit	View
LANCOM	Edit	View

SNMP Settings

Default Polling Interval:	5 minutes
SNMP Timeout (3-60 seconds):	3
SNMP Retries (3-20):	3

Telnet/SSH Settings

Telnet/SSH Timeout (3-120 seconds):	10

HTTP Discovery Settings

HTTP Timeout (3-120 seconds):	5

ICMP Settings

Attempt to ping down devices:	● Yes ○ No

Concurrent Process Limits

Maximum number of audit processes (1-50):	3
Maximum number of configuration processes (1-50):	5

Colubris Administration Options

● Do not modify security/HTTPS settings
○ Replace existing user with specified user

Cisco Aironet VxWorks User Creation Options

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

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

Upon authorization, read-write SNMP access can be enabled using the device's web interface.

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

- On the **Device Setup→Communication** page, locate the "Default Credentials" area. You will need to enter the credentials for each of the device models on your network. The default credentials are assigned to all newly discovered APs. To change the credentials of APs already managed/monitored by OV3600 use the **APs/Devices→Manage** page or the Modify these devices link.

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

- Browse to the **Device Setup→Communication** page, locate the "SNMP Settings" area, and enter the following information:

Setting	Default	Description
Default Polling Interval	5 minutes	Specifies the interval at which OV3600 will poll each device for all newly created groups (this default may be overridden on the Group management page). A frequent (short) polling interval will provide more up-to-date monitoring information but will also increase SNMP traffic on your network, especially on larger WLANs and increase the load placed on the OV3600 server. *It is recommended that you configure an initial 5-minute polling interval for most networks.*
SNMP Timeout	3	The time (in seconds), that OV3600 will wait for a response from a device after sending an SNMP request
SNMP Retries	3	The number of times OV3600 will try 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 will classify that device as "Down."

- On the **Device Setup→Communication page**, locate the Telnet/SSH Settings section.

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

- On the **Device Setup→Communication** page, locate the HTTP Discovery Settings section.

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

- On the **Device Setup→Communication** page, locate the ICMP Settings section.

Setting	Default	Description
Attempt to ping down APs:	Yes	When an AP is unreachable over SNMP, OV3600 will attempt to ping the device if yes is selected. If there are a large number of APs unreachable by ICMP (in excess of 100) the timeouts will start to negatively impact performance. Select "No" if performance is negatively affected. If ICMP is disabled on the network select "No" to avoid the performance penalty caused by numerous ping requests.

- On the **Device Setup→Communication** page, locate the Concurrent Process Limits section.

Setting	Default	Description
Maximum number of audit processes (1-50)	3	Defines the maximum number of configuration audit processes that will be run at once. It is recommended that you set this to one fewer than the number of CPU cores in the box. Adding additional process will speed up the configuration audit of multiple APs. Setting the maximum too high will result in diminished OV3600 performance.

Setting	Default	Description
Maximum number of configuration processes (1-50):	5	Defines the maximum number of configuration processes that will be run at once. The configuration processes are responsible for pushing configurations to devices. It is recommended that you set this to one more than the number of CPU cores in the box. Setting the maximum too high will result in diminished OV3600 performance.

- On the **Device Setup→Communication** page, locate the "Colubris Administration Options." *You only need to provide this information if you use Colubris APs on your network*. Select one of the three options listed:

Setting	Default	Description
Do Not Modify Security/HTTPS Settings	N/A	If selected, OV3600 will use only an existing user account on the AP (this user account must have all permissions set), as defined in the *Colubris Username/Password* section in the "Default Secrets" area.
Replace existing user with specified user	N/A	If selected, OV3600 will replace the existing user with a new user account (specified below) on each AP, with all permissions turned on.
New Colubris Username and Password	N/A	Specifies the username and password to be used only if *Replace existing user with specified user* is selected.

- On the **Device Setup→Communication** page, locate the "Cisco Aironet VxWorks User Creation Options." *You only need to provide this information if you use VxWorks-based Cisco APs (Aironet 340, 350, and 1200 models) on your network*. Select one of the three options listed:

Setting	Default	Description
Do Not Modify Security/SNMP Settings	N/A	If selected, OV3600 will use only an existing user account on the AP (this user account must have all permissions set), as defined in the *Cisco VxWorks Username/Password* section in the "Default Secrets" area.
Create and Use Specified User	N/A	If selected, OV3600 will create a new user account (specified below) on each AP, with all permissions turned on.
New Cisco Aironet Username/Password	N/A	Specifies the username and password to be created if *the Create and use specified user* is selected above.

- 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 two options listed:

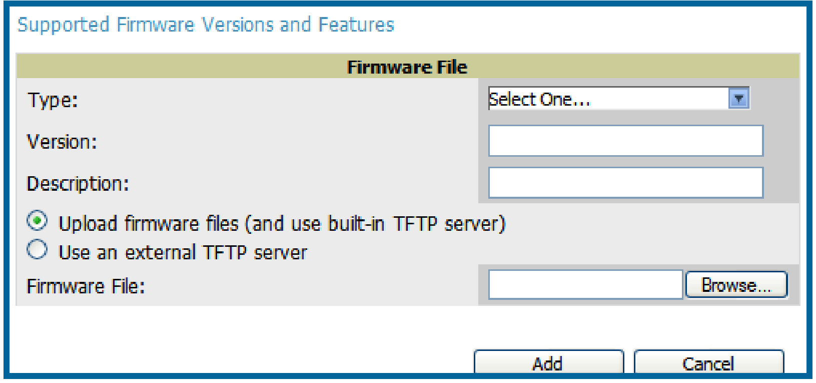
Setting	Default	Description
Do Not Modify SNMP Settings	Yes	If selected, OV3600 will not modify any SNMP settings. If SNMP is not already initialized on the Symbol, Intel, and Cisco IOS APs, OV3600 will not be able to manage them.

Setting	Default	Description
Enable Read-Write SNMP and Set Community String to Default	No	If selected, on networks where the Symbol, Intel, and Cisco IOS APs do not have SNMP initialized, OV3600 will enable SNMP so the devices can be managed by OV3600. OV3600 will set the SNMP community string to the default for that device type as defined on the left side of the page.

Loading Device Firmware onto OV3600 (Optional)

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→Firmware Files** page. Firmware files uploaded to OV3600 on this page will appear as options in the drop-down menus on the **Group→Firmware** page and on individual **AP/Device→Manage** pages, and can be applied automatically to devices through OV3600. Please see the **OV3600 Setup→General page** to configure OV3600-wide default firmware options.

Figure 19. "Device Setup→Firmware Files (Add)" page



Supported Firmware Versions and Features

Firmware File

Type: Select One...

Version:

Description:

● Upload firmware files (and use built-in TFTP server)

○ Use an external TFTP server

Firmware File: Browse...

Add Cancel

The **Device Setup→Firmware Files** page displays all of the firmware files that have been uploaded to OV3600.

Setting	Default	Description
Type	None	Drop-down list of the primary AP makes and models that OV3600 supports with automated firmware distribution.
Owner Role	None	The role that uploaded the firmware file. This is the role that has access to the file when an upgrade is attempted.
Version	None	User-configurable field to specify the firmware version number.
Description	None	User-configurable text description of the firmware file.
Filename	None	The name of the file that was uploaded to OV3600 and will be transferred to an AP when the file is used in an upgrade
MD5 Checksum	None	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.
File Size	None	The size of the firmware 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 can not delete a firmware file that is set as the desired firmware version for a group.

- Before you can upload a file to OV3600 you will need to download the appropriate firmware files from the manufacturer's website to a location on your network.

- To upload a new firmware file to OV3600, browse to the **Device Setup→Firmware Files** page and click the "Add" button. Enter the appropriate information and click the "Add" button. Click the "Supported Firmware Versions and Features" link to view a list of supported firmware versions. You can also import a CSV list of groups and their external TFTP firmware servers.

Setting	Default	Description
Type	None	The firmware file is used with the specified type. If you select an IOS device from the "Type" dropdown menu you will 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.
Version	None	User-configurable field to specify the firmware version number.
*HTML Version**	None	User-configurable field identifying the HTML firmware version for Symbol and Intel APs.
Description	None	User-configurable text description of the firmware file.
Use Built-in or External TFTP Server	Built-in	Select the TFTP server access points will use to download their firmware. The built-in TFTP server is recommended. If you choose to use an external TFTP server you will enter the File Server IP address and the Filename. You can also choose to assign the external TFTP server on a per-group basis. If you check that box you will need to enter the IP address on the **Groups→Firmware** page.
TFTP Server IP	None	Enter the IP of the External TFTP Server (Like SolarWinds) used for the firmware upgrade. This option is displayed when the user selects Use a Different TFTP server option.
Filename	None	Enter the filename of the firmware file that needs to be uploaded. Ensure that the firmware file is in the TFTP root directory.
*HTML File**	None	Click the "Browse" button to locate the appropriate Intel or Symbol HTML firmware file on your network.

**Note: Fields only appear for Intel and Symbol APs. Intel and Symbol distribute their firmware in two separate files, an image file and an HTML file. Both files must be uploaded to OV3600 for the firmware to be successfully distributed via OV3600.*

- Click the "View Certified Firmware Versions" to see a list of tested and supported firmware. Unsupported and untested firmware may cause device mismatches and other problems. Please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com. before installing non-certified firmware.

- To delete a firmware file that has already been uploaded to OV3600, 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. Select the file from the pick list window in the "Delete Firmware File" area and click the "Delete" button.

Helpdesk

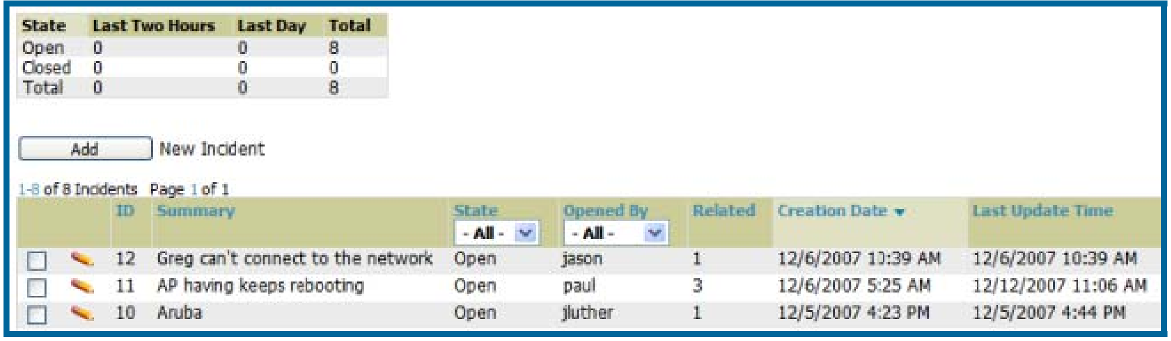
Overview

The Helpdesk module of the OmniVista 3600 Air Manager is designed to allow front-line technical support staff to take full advantage of the data available in the OmniVista 3600 Air Manager. If an external Remedy installation is available, the Helpdesk functionality can be disabled and 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.

The Helpdesk tab will appear to the right of the Home tab. By default, the option to use an external Remedy server is disabled; navigate to the **Helpdesk→Setup** page to enable Remedy (and see the section below for more information on how to configure OV3600 to integrate with a Remedy server). 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). Users with an Admin role have the Helpdesk option enabled by default.

The Helpdesk's functionality includes the ability to document incidents associated with users on the network. For a complete list of incidents, or to open a new incident, navigate to the **Helpdesk→Incidents** page.

Figure 20. "Helpdesk→Incidents" page



State	Last Two Hours	Last Day	Total
Open	0	0	8
Closed	0	0	0
Total	0	0	8

Add New Incident

1-8 of 8 Incidents Page 1 of 1

		ID	Summary	State - All -	Opened By - All -	Related	Creation Date ▾	Last Update Time
□	✎	12	Greg can't connect to the network	Open	jason	1	12/6/2007 10:39 AM	12/6/2007 10:39 AM
□	✎	11	AP having keeps rebooting	Open	paul	3	12/6/2007 5:25 AM	12/12/2007 11:06 AM
□	✎	10	Aruba	Open	jluther	1	12/5/2007 4:23 PM	12/5/2007 4:44 PM

The table at the top of the page shows the count of incidents by state and by time.

Column	Description
State	Open (currently under invstigation), Closed (resolved) and the total incident count
Period of time	Shows the count of incidents in the last two hours, the last day, and the total count

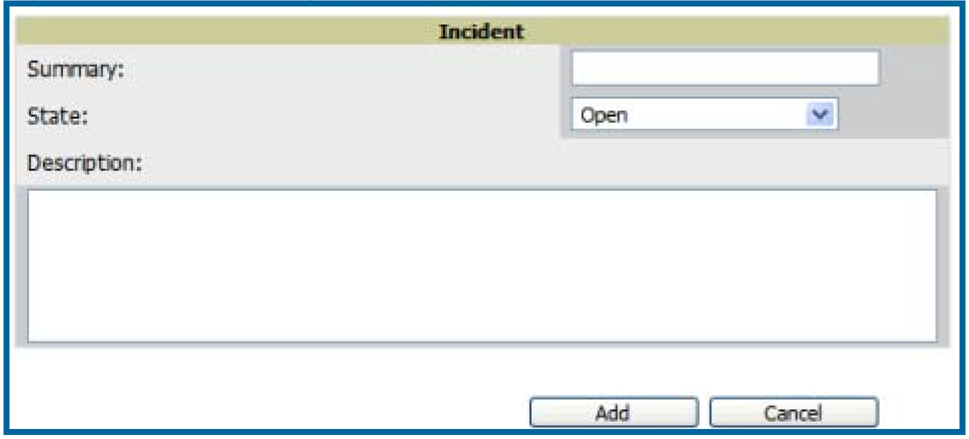
The table at the bottom of the page summarizes the incidents that have been reported so far. Clicking the pencil icon next to any incident will open an edit page where the incident can be modified. An incident can be deleted by selecting the check box next to it and clicking the delete button at the bottom of the table.

Column	Description
ID	The ID number of the incident, which is automatically assigned when the incident is logged.
Summary	Summary statement of the issue or problem; entered by the OV3600 user when the incident is created.

Column	Description
State	The current state of the incident – this can be either open or closed. The dropdown 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	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 (by clicking on the pencil icon next to a role on the **OV3600 Setup→Roles** page).
Related	The number of items that have been associated to the incident. These link different groups, APs or clients to the incident report.
Creation Date	The time and date the incident was created.
Last Update Time	The time and date the incident was last modified by an OV3600 user.

To create a new incident, click the “Add New Incident” button underneath the top table. This displays an incident edit page.

Figure 21. “Incident edit” page

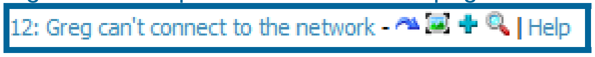


State: Open

Field	Description
Summary	User-inputted text that describes a short summary of the incident
State	Dropdown menu with the options “Open” or “Closed”
Description	Longer user-inputted text area for a thorough description of the incident.

Helpdesk icons appear at the top of other OV3600 pages, allowing screenshots and other records to be associated to existing incidents. They appear in the upper right-hand corner next to the “Help” link.

Figure 22. Helpdesk Icons on other pages in OV3600



12: Greg can't connect to the network - | Help

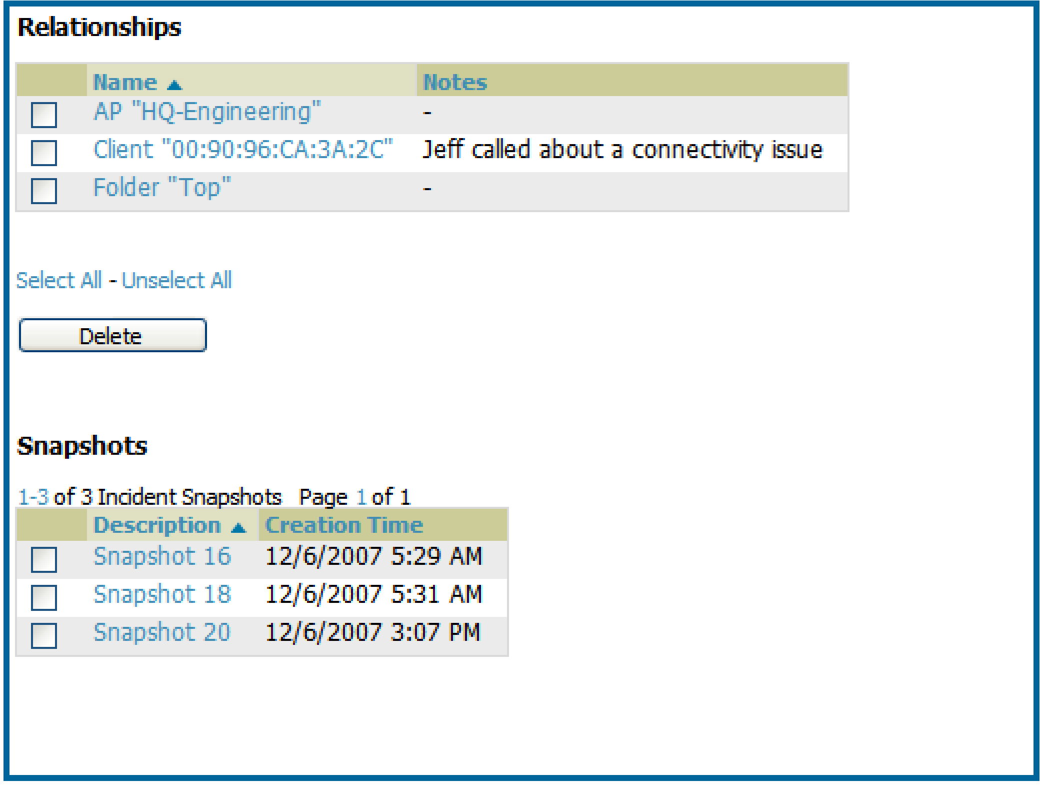
Icon	Description
Current Incident (ID number and description)	The current incident of focus in the Helpdesk header. Clicking on the link will bring up the Incident Edit page (see above). Mousing over the incident will bring up a summary popup of the incident.

Icon	Description
↷	Relates the device, group or client to the incident (see below for more details).
🖼	Attach 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 puroposes.
✚	Create a new incident report.
🔍	Choose a new incident from the list of created incidents to be the “Current Incident” (see description of icon above).

Snapshots or relationships can be created by clicking the Helpdesk header icon (see table above) on the screen that needs to be documented. They 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 on the snapshot description will open a popup window to display the screenshot.

Figure 23. Relationships and Snapshots on the "Incident Edit" page



Relationships

	Name ▲	Notes
□	AP "HQ-Engineering"	-
□	Client "00:90:96:CA:3A:2C"	Jeff called about a connectivity issue
□	Folder "Top"	-

Snapshots

1-3 of 3 Incident Snapshots Page 1 of 1

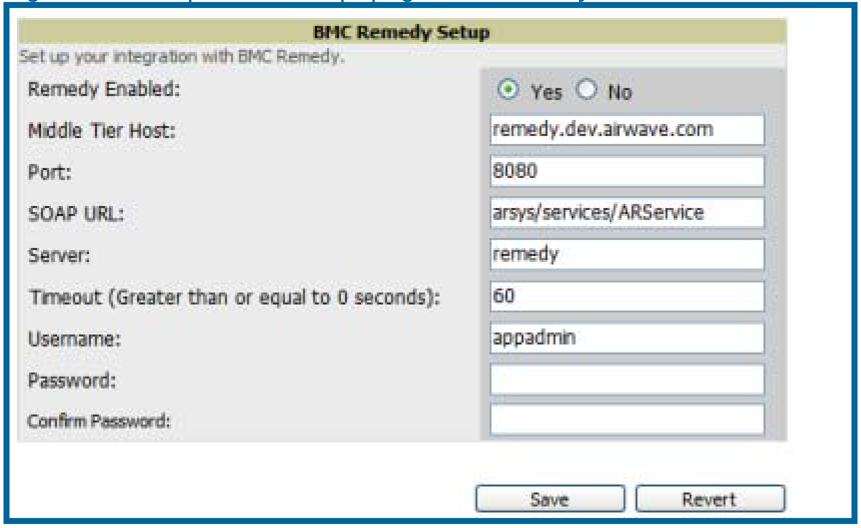
	Description ▲	Creation Time
□	Snapshot 16	12/6/2007 5:29 AM
□	Snapshot 18	12/6/2007 5:31 AM
□	Snapshot 20	12/6/2007 3:07 PM

Using the Helpdesk Tab with an Existing Remedy Server

If an external Remedy server exists, the OV3600's 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 will expose 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 above section for more details on how they work.

Figure 24. “Helpdesk→Setup” page with Remedy enabled



BMC Remedy Setup

Set up your integration with BMC Remedy.

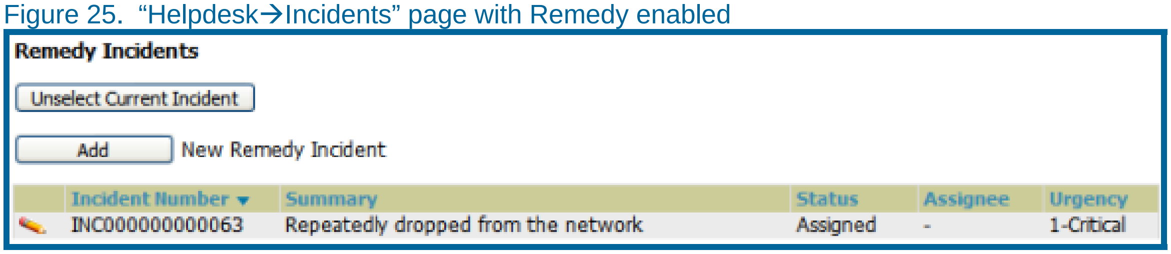
Remedy Enabled:	● Yes ○ No
Middle Tier Host:	remedy.dev.airwave.com
Port:	8080
SOAP URL:	arsys/services/ARService
Server:	remedy
Timeout (Greater than or equal to 0 seconds):	60
Username:	appadmin
Password:	
Confirm Password:	

Field	Description
Remedy Enabled	If “no” (default) is selected, OV3600’s existing helpdesk functionality is available. If “yes” is selected, OV3600’s helpdesk functionality is disabled and the Helpdesk tab can be configured for use with an existing Remedy server. Fields for server data appear only when Remedy is enabled.
Middle Tier Host	The location of the Remedy installation’s web server.
Port	The port for 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's Helpdesk functionality will be disabled. OV3600 will now display 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 25. "Helpdesk→Incidents" page with Remedy enabled



Remedy Incidents

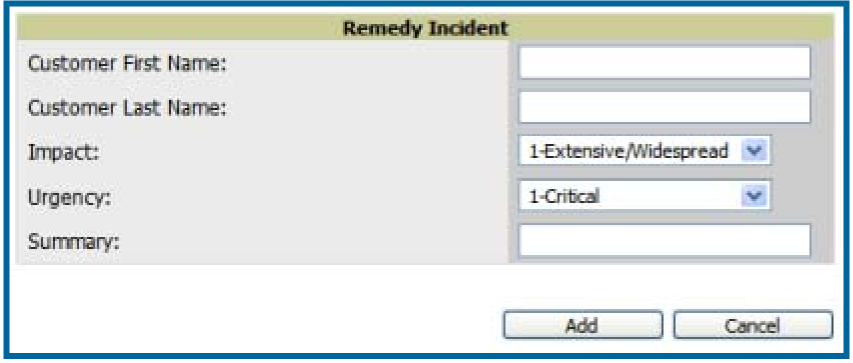
New Remedy Incident

	Incident Number ▾	Summary	Status	Assignee	Urgency
✎	INC000000000063	Repeatedly dropped from the network	Assigned	-	1-Critical

Field	Description
Incident Number	Unique identifier for each incident; assigned by the Remedy installation.
Summary	Brief incident summary as entered by OV3600 or Remedy user.
Status	Chosen by OV3600 or Remedy user: New, Assigned, In Progress, Pending, Resolved, Closed, Cancelled.
Assignee	Assigned by Remedy installation; cannot be changed in OV3600.
Urgency	Chosen by OV3600 or Remedy User: 1 – Critical, 2 – High, 3 – Medium, 4 – Low.

To change the current incident in the Helpdesk header, click the "Unselect Current Incident" button. To add a new Remedy incident, click the "Add" button. To edit an existing Remedy incident, click the pencil icon next to the incident you wish to edit.

Figure 26. "Helpdesk→Incidents" Add a new Remedy Incident



Remedy Incident

Customer First Name:	
Customer Last Name:	
Impact:	1-Extensive/Widespread
Urgency:	1-Critical
Summary:	

Field	Description
Customer First and Last Name	These must match exactly a customer that already exists on the Remedy server. There is no way to create a new customer from OV3600 or to search Remedy customers remotely.
Impact	1 – Extensive/Widespread (default), 2 – Signficant/Large, 3 – Moderate/Limited, 4 – Minor/Localized.
Urgency	1 – Critical (default), 2 – High, 3 – Medium, 4 – Low.
Summary	Free-form text field.

Note that a new incident will not be created if the customer first and last name do not exist on the Remedy server. However, there will be 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.

Configuring Groups

Overview

Enterprise-class APs and controllers are complex devices with hundreds of variable settings that must be configured precisely to achieve optimal performance and network security. Configuring all settings on each device individually is time-consuming and prone to human error. OV3600 addresses this problem by automating the processes of device configuration and compliance auditing.

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 (“5th Floor APs”), usage or security policies (“Guest Access APs”), function (“Manufacturing APs”), or any other variable appropriate for your business needs. Devices within a Group may be from different manufacturers or hardware models – all that matters is that they share certain basic configuration settings.

Typical Group configuration variables include basic settings (SSID, SNMP polling interval, etc.), security settings (VLANs, WEP, 802.1x, ACLs, etc.), and some radio settings (data rates, fragmentation threshold, RTS threshold, DTIM, preamble, etc.). When configuration changes are applied at a Group level, they are automatically assigned to every device within that Group and applied to every device in “Managed” mode. “Individual device” settings – such as device name, RF channel selection, RF transmission power, antenna settings, etc. - typically cannot and should not be managed at a Group level and must be configured individually to achieve optimal performance. AP level settings are configured on the **APs/Devices→Manage** page.

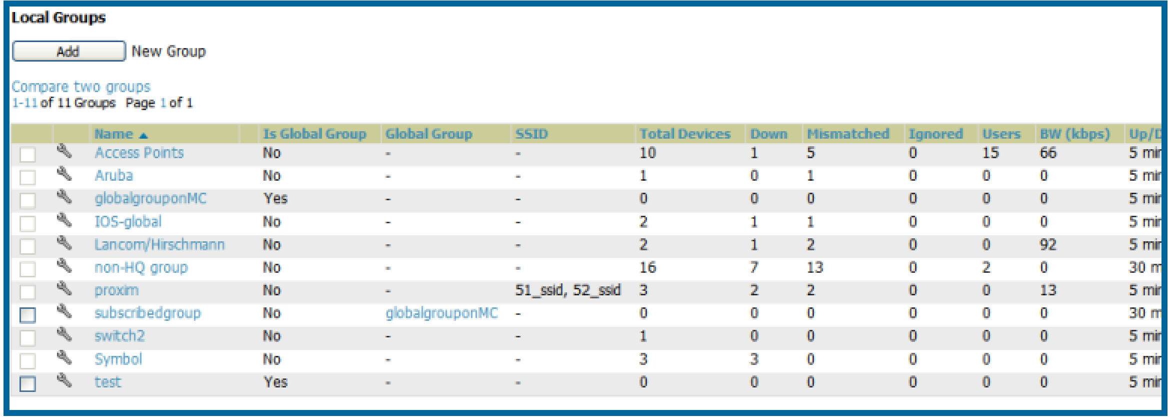
With OV3600, you can create as many different groups as required. OV3600 users usually establish groups that range in size from 5 to 100 wireless devices.

Group configuration can be enhanced with OV3600’s Global Groups feature, which allows the user to create global groups with master configurations that are pushed to individual subscriber groups. More information is available in the “Global Groups” part of this section, as well as in the section on the Master Console.

Viewing All Defined Device Groups

To see a list of all Groups that have been defined within OV3600, browse to the **Groups→List** page.

Figure 27. "Groups→List" page



Local Groups

1-11 of 11 Groups Page 1 of 1

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

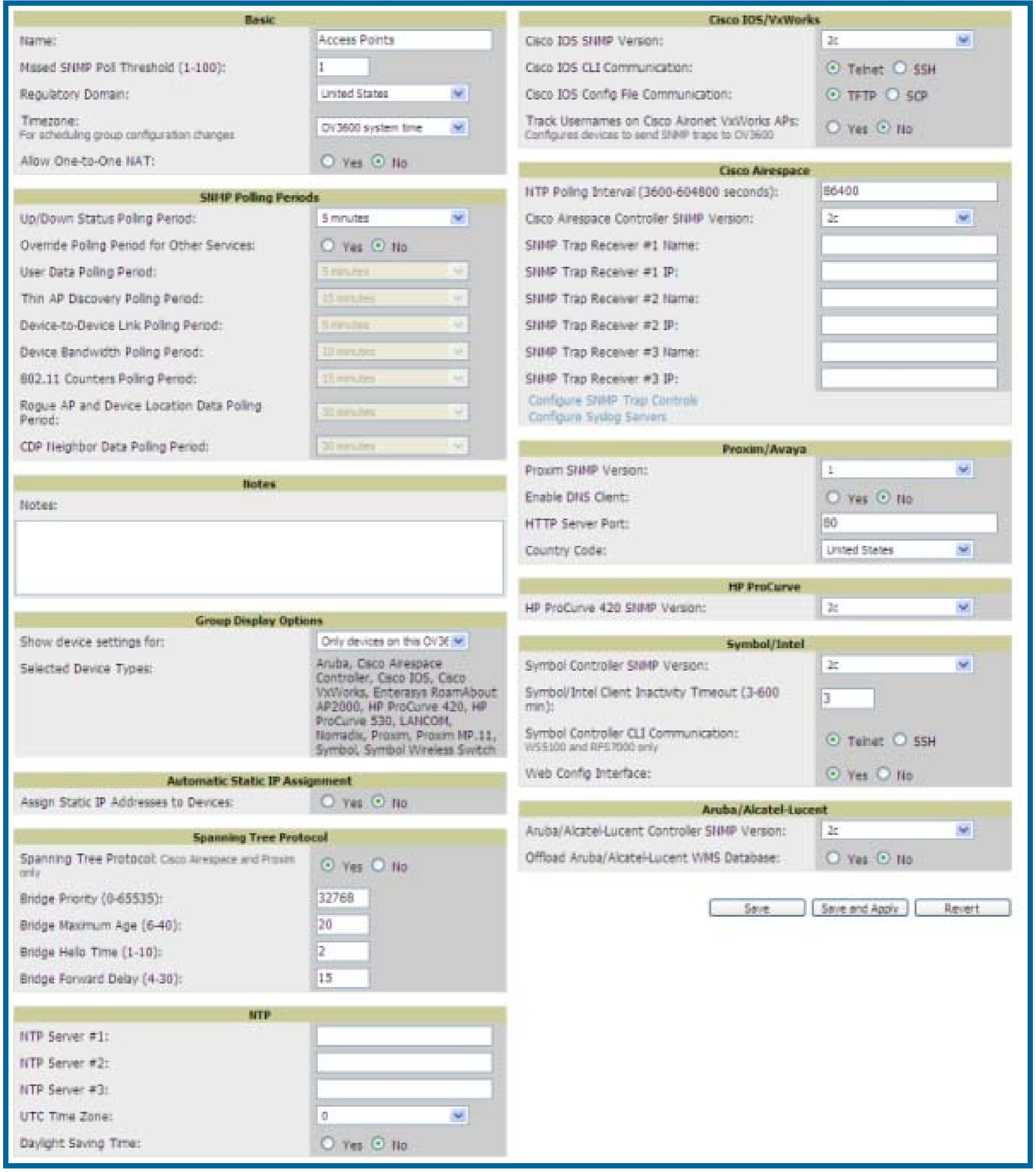
Column	Description
Add new group button	Links to a form to add a new group by name.
Manage	The pencil represents a hyperlink to **Group→Basic** page to begin editing Group configuration settings.
Default	Indicates the default group where devices are automatically assigned unless otherwise specified. If “Automatically Monitor/Manage New Devices” is enabled on **OV3600 Setup→General** page all newly, discovered devices will immediately transition into the default group. *Note: the default group cannot be deleted.*
Name	User-defined name that will uniquely identify the group by location, manufacturer, department or any other identifier (i.e., “Accounting APs,” “Floor 1 APs,” “Cisco APs,” “802.1x APs”).
Is Global Group	Identifies whether or not the group has been identified as a global group that can be used to configure subscriber groups. Global groups cannot contain APs and are visible by users of any role.
Global Group	Identifies the global group to which the group is subscribed, if any.
Unapplied Changes	Column is visible if configuration changes have been saved in the database, but the devices have not received the configuration changes.
SSID	Column represents the Service Set Identifier (SSID) assigned to all devices within the group.
Total Devices	Column represents the total number of access points contained in the group.
Down	Column represents the number of access points within the group, which are **not** reachable via SNMP.
Mismatched	Column represents the number of access points within the group that are in a mismatched state.
Users	Column represents the number of mobile users associated with all access points within the group.
BW (kbps)	Column represents a running average of the sum of bytes in and bytes out for the managed radio interface.
Up/Down Polling Interval	Column represents the time between Up/Down SNMP polling periods for each device in the group. By default, all SNMP polling periods will match the Up/Down period. Detailed SNMP polling period information is available on the **Groups→Basic** page.
Duplicate	Column represents a hyperlink, which will create a new group with the name “Copy of <Group Name>” with the same group configuration.

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

Configuring Basic Group Settings

The **Groups→Basic** page allows you to specify basic information about a Group, including the Group name. The first step in configuring your own Group on OV3600 is to edit the “default” group.

Figure 28. “Groups→Basic” page



Basic

Name:	Access Points
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	United States
Timezone: For scheduling group configuration changes	OV3600 system time
Allow One-to-One NAT:	○ Yes ● No

SNMP Polling Periods

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

Notes

Notes:

Group Display Options

Show device settings for:	Only devices on this OV3€
Selected Device Types:	Aruba, Cisco Airespace Controller, Cisco IOS, Cisco VxWorks, Enterasys RoamAbout AP2000, HP ProCurve 420, HP ProCurve 530, LANCOM, Nomadix, Proxim, Proxim MP.11, Symbol, Symbol Wireless Switch

Automatic Static IP Assignment

Assign Static IP Addresses to Devices:	○ Yes ● No

Spanning Tree Protocol

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

NTP

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

Cisco IOS/VxWorks

Cisco IOS SNMP Version:	2c
Cisco IOS CLI Communication:	● Telnet ○ SSH
Cisco IOS Config File Communication:	● TFTP ○ SCP
Track Usernames on Cisco Aironet VxWorks APs: Configures devices to send SNMP traps to OV3600	○ Yes ● No

Cisco Airespace

NTP Polling Interval (3600-604800 seconds):	86400
Cisco Airespace Controller SNMP Version:	2c
SNMP Trap Receiver #1 Name:	
SNMP Trap Receiver #1 IP:	
SNMP Trap Receiver #2 Name:	
SNMP Trap Receiver #2 IP:	
SNMP Trap Receiver #3 Name:	
SNMP Trap Receiver #3 IP:	

Configure SNMP Trap Controls
Configure Syslog Servers

Proxim/Avaya

Proxim SNMP Version:	1
Enable DNS Client:	○ Yes ● No
HTTP Server Port:	80
Country Code:	United States

HP ProCurve

HP ProCurve 420 SNMP Version:	2c

Symbol/Intel

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

Aruba/Alcatel-Lucent

Aruba/Alcatel-Lucent Controller SNMP Version:	2c
Offload Aruba/Alcatel-Lucent WMS Database:	○ Yes ● No

- Browse to the **Groups→List** page
- Click the “Access Points” link in the *Name* column. This will direct you to the **Groups→Monitoring** page.
- Select the **Groups→Basic** page in the Navigation Section.
- Edit the information on this page for your default Group:

Setting	Default	Description
Name	Access Points	User-defined name that will uniquely identify the group by location, manufacturer, department or any other identifier (i.e., "Accounting APs," "Floor 1 APs," "Cisco APs," "802.1x APs").
Missed SNMP Poll Threshold	1	Sets the number of Up/Down SNMP polls that must be missed before OV3600 will consider 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 timezone in which the access points are located.
Allow One-to-One NAT	No	Allows OV3600 to talk to the devices on a different address than the one configured in the device. *NOTE: If enabled, the LAN IP Address listed on the AP/Devices→Manage page under the "Settings" area will be different than the IP Address under the "Device Communication" area.*

- To configure the polling intervals for your devices in the group locate the "SNMP Polling Periods" section on the **Groups→Basic** page. The Group SNMP Polling Period information will override the default

Setting	Default	Description
Up/Down Status Polling Period	5 minutes	Time between Up/Down SNMP polling for each device in the group. *NOTE: The Group SNMP Polling Interval will override the global parameter configured on the **Device Setup→Communication** page. It is recommended that you configure an initial polling interval of 5 minutes for most networks.*
Override Polling Period for Other Services	No	Radio button that enables or disables overriding the base SNMP Polling Period.
User Data Polling Period	5 minutes	Time between SNMP polls for User Data for devices in the group.
Thin AP Discovery Polling Period	5 minutes	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	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	The interval at which OV3600 will poll for the bandwidth being used by a device.
802.11 Counters Polling Period	5 minutes	Time between SNMP polls for 802.11 Counter information.
Rogue AP and Device Location Data Polling Period	5 minutes	Time between SNMP polls for Rogue AP and Device Location Data polling.

- To record additional information and comments about the group locate the "Notes" section on the **Groups→Basic** page.

Setting	Default	Description
Notes	Blank	Free form text field.

- To configure which options and tabs are visiable for the group locate the "Group Display Options" section of the **Groups→Basic** page.

Setting	Default	Description
Show device settings for:	All Devices	Drop down menu that determines which Group tabs and options will be viewable by default in new groups: All Devices: OV3600 will display all Group tabs and setting options. Only Devices in this group: OV3600 will hide all options and tabs that do nat apply to the APs and devices currently in the group. Only Devices on this OV3600: OV3600 will hide 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 Setup→General** page Selected device types: Allows the user to specify the device types for which OV3600 will display Group settings.

- To dynamically assign 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** page.

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	The first address OV3600 will assign to the devices in the Group.
Number of Addresses	Blank	The number of addresses in the pool from which OV3600 can assign IP addresses.
Subnet Mask	Blank	Subnet Mask to be assigned to the devices in the Group.
Subnet Gateway	Blank	Gateway to be assigned to the devices in the Group.
Next IP Address	Blank	The next IP Address queued for assignment.

- To configure Spanning Tree Protocol on Airespace devices and Proxim APs locate the Spanning Tree Protocol section on the **Groups→Basic** page.

Setting	Default	Description
Spanning Tree Protocol	Enabled	Enables Spanning Tree Protocol on Airespace 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 will be 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	The maximum time, in seconds, that the device will store protocol information.
Bridge Hello Time	2	The time, in seconds, between Hello message broadcasts.

Setting	Default	Description
Bridge Forward Delay	15	The time, in seconds, that the port will spend in listening and learning mode if the spanning tree has changed.

- To configure NTP settings locate the NTP section on the **Groups→Basic** page.

Setting	Default	Description
NTP Server #1,2,3	None	The IP address of the NTP server that will be configured on the AP.
UTC Time zone	0	The hour offset from UTC time to local time for the AP. Times displayed in OV3600 graphs and logs use the time set on the OV3600 server.
Daylight Saving Time	Disabled	Enable the advanced daylight saving time settings in the Proxim and HP ProCurve 420 sections of the **Groups→Basic** page.

- To configure Cisco IOS/VxWorks specific settings locate the Cisco IOS/VxWorks section on the **Groups→Basic** page.

Setting	Default	Description
Cisco IOS SNMP Version	2c	Dropdown menu that specifies the version of SNMP used by OV3600 to communicate to the AP.
Cisco IOS CLI Communication	Telnet	Sets the protocol OV3600 uses to communicate with Cisco IOS devices. Selecting SSH will use the secure shell for command line interface (CLI) communication. Selecting telnet will send the data in clear text via telnet.
Cisco IOS File Communication	TFTP	Sets the protocol OV3600 uses to communicate with Cisco IOS devices. Selecting SCP will use 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	Configure VxWorks APs to send RADIUS accounting packets to OV3600. See the **OV3600 Setup→RADIUS Accounting** page to ensure OV3600 is accepting RADIUS accounting packets from the APs.

- To configure Cisco Airespace specific settings locate the Cisco Airespace section of the **Groups→Basic** page.

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

- To configure Proxim/Avaya specific settings locate the Proxim/Avaya section on the **Groups→Basic** page.

Setting	Default	Description
Proxim SNMP Version	2c	Dropdown menu that specifies the version of SNMP used by OV3600 to communicate to the AP.
Enable DNS Client (Proxim Only)	No	Enables the DNS client on the AP. Enabling the DNS client will allow you to set some values on the AP by hostname instead of IP.
Primary DNS server	Blank	The IP address of the Primary DNS server.
Secondary DNS server	Blank	The IP address of the Secondary DNS server.
Default DNS domains	Blank	The default DNS domain used by the AP.
HTTP Server Port	80	OV3600 will set this port as the HTTP server port on all Proxim APs in the group.
*DST Offset**	+1	Configures the amount of time, in hours, that will be jumped when entering/leaving daylight saving time.

*Note: DST Offset is only visible if Daylight Saving Time is enabled in the NTP section of the **Groups→Basic** page.*

- To configure HP ProCurve 420 specific settings locate the HP ProCurve 420 section on the **Groups→Basic** page.

Setting	Default	Description
Hp ProCurve 420 SNMP Version	2c	Dropdown menu that specifies the version of SNMP used by OV3600 to communicate to the AP.
*DST Start Month**	1	Specifies the month that begins daylight saving time. 1 is January and 12 is December.
*DST Start Day**	1	Specifies the day of the month that begins daylight saving time.
*DST End Month**	12	Specifies the month that ends daylight saving time. 1 is January and 12 is December.
*DST End Day**	31	Specifies the day of the month that ends daylight saving time.
ProCurve XLWeSM CLI Communication	Telnet	Sets the protocol OV3600 uses to communicate with ProCurve XLWeSM devices. Selecting SSH will use the secure shell for command line interface (CLI) communication. Selecting telnet will send the data in clear text via telnet.

*Note: 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** page.*

- To configure Symbol/Intel specific settings locate the Symbol/Intel section on the **Groups→Basic** page.

Setting	Default	Description
Symbol Controller SNMP Version	2c	Dropdown menu that specifies the version of SNMP used by OV3600 to communicate to the device.

Setting	Default	Description
Symbol/Intel Client Inactivity Timeout (3-600 min)	3	Minutes of inactivity after which a client associated to an Intel or Symbol AP will be considered "inactive." A lower value typically provides a more accurate representation of current WLAN usage. *NOTE: For other APs, OV3600 has more precise methods to determine when inactive clients are no longer associated to an AP.*
Web Config Interface	Enable	Enables or disables the http/https configuration interface for the Symbol 4131 and Intel 2011.

- To configure Aruba/Alcatel-Lucent-specific settings locate the Aruba/Alcatel-Lucent section on the **Groups→Basic** page.

Setting	Default	Description
Aruba/Alcatel-Lucent WLAN switch SNMP Version	2c	Dropdown menu that specifies the version of SNMP used by OV3600 to communicate to the AP.
Offload Aruba/ Alcatel-Lucent WMS database	No	When enabled allows OV3600 to display historical information for Aruba/Alcatel-Lucent WLAN switches. Changing the setting to "Yes" will push commands via SSH to all Aruba/Alcatel-Lucent WLAN switches in monitor-only mode without rebooting the device. The command can be pushed to WLAN switches in manage mode (also without rebooting the device) if the "Allow WMS Offload" setting on the **OV3600 Setup→General** page is changed to "Yes".

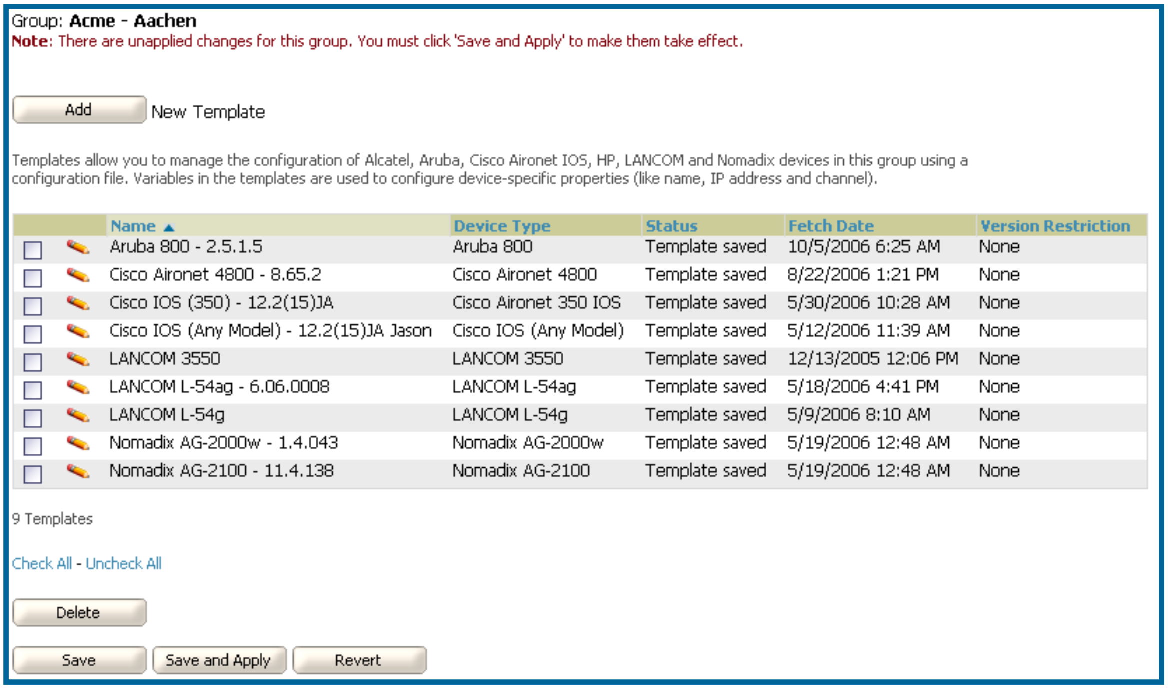
- Click "Save" when completed.

Configuring Group Templates

The **Groups→Templates** page allows you to create configuration templates for Alcatel-Lucent, Aruba, Cisco IOS, HP ProCurve, Hirschmann, Lancom, Symbol and Nomdix, and Trapeze APs. Templates are powerful configuration constructs that allow OV3600 to manage virtually all settings on an AP. The template uses variables to adjust for minor configuration differences between devices. The template understands many variables including, %channel%, %ofdmpower%, %ip_address%, %hostname%. The variables are populated with the corresponding values on the **APs/Devices →Manage** page of the specific AP that is getting configured. Please see the "Configuring Cisco IOS Templates" section below for template and variable details. Please see the section below for information about creating global templates for subscriber groups.

NOTE: Changes made on OV3600's standard Group configuration pages (Basic, Radio, Security, VLANs, etc.) will not be applied to any template based devicesAPs..

Figure 29. "Groups→Templates" page



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

Templates allow you to manage the configuration of Alcatel, Aruba, Cisco Aironet IOS, HP, LANCOM and Nomadix 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).

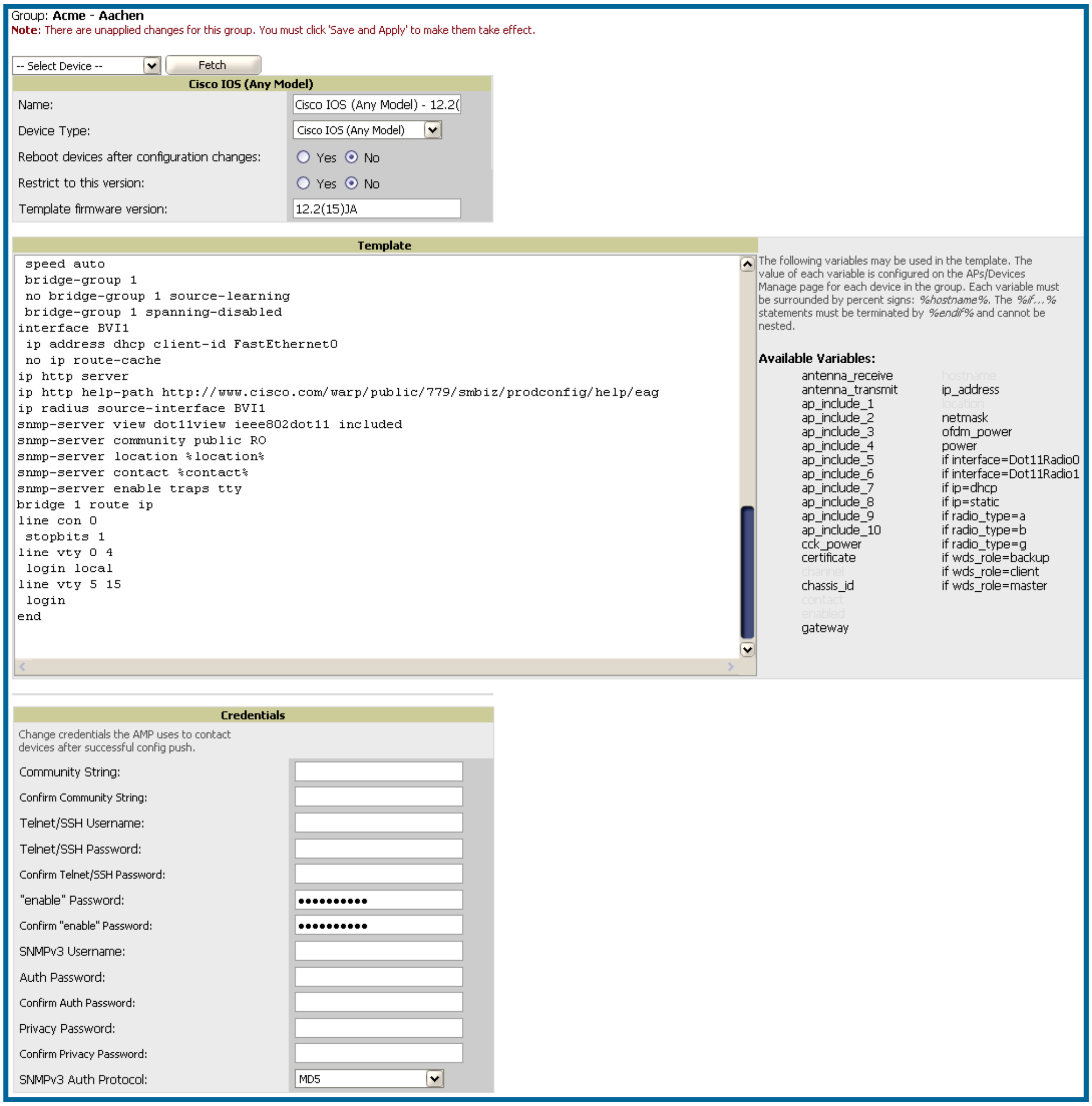
		Name ▲	Device Type	Status	Fetch Date	Version Restriction
□	✎	Aruba 800 - 2.5.1.5	Aruba 800	Template saved	10/5/2006 6:25 AM	None
□	✎	Cisco Aironet 4800 - 8.65.2	Cisco Aironet 4800	Template saved	8/22/2006 1:21 PM	None
□	✎	Cisco IOS (350) - 12.2(15)JA	Cisco Aironet 350 IOS	Template saved	5/30/2006 10:28 AM	None
□	✎	Cisco IOS (Any Model) - 12.2(15)JA Jason	Cisco IOS (Any Model)	Template saved	5/12/2006 11:39 AM	None
□	✎	LANCOM 3550	LANCOM 3550	Template saved	12/13/2005 12:06 PM	None
□	✎	LANCOM L-54ag - 6.06.0008	LANCOM L-54ag	Template saved	5/18/2006 4:41 PM	None
□	✎	LANCOM L-54g	LANCOM L-54g	Template saved	5/9/2006 8:10 AM	None
□	✎	Nomadix AG-2000w - 1.4.043	Nomadix AG-2000w	Template saved	5/19/2006 12:48 AM	None
□	✎	Nomadix AG-2100 - 11.4.138	Nomadix AG-2100	Template saved	5/19/2006 12:48 AM	None

9 Templates

Setting	Description
Name	The template name.
Device Type	The template will apply to APs or devices of the specified type. If "Cisco IOS (Any Model)" is selected the template will apply to all IOS APs that do not have a version specific template defined. If there are two templates that might apply to a device the template with the most restrictions takes precedence.
Status	Displays the status of the template.
Fetch Date	The date that the template was originally fetched from a device.

Setting	Description
Version Restriction	The template will only apply to APs running the version of firmware specified. If the restriction is “None” then the template will apply 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.

Figure 30. “Groups→Templates Add” page



Group: **Acme - Aachen**

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

Cisco IOS (Any Model)

Name:	Cisco IOS (Any Model) - 12.2(
Device Type:	Cisco IOS (Any Model)
Reboot devices after configuration changes:	○ Yes ● No
Restrict to this version:	○ Yes ● No
Template firmware version:	12.2(15)JA

Template

```
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
interface BVI1
 ip address dhcp client-id FastEthernet0
 no ip route-cache
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
snmp-server view dot11view ieee802dot11 included
snmp-server community public RO
snmp-server location %location%
snmp-server contact %contact%
snmp-server enable traps tty
bridge 1 route ip
line con 0
 stopbits 1
line vty 0 4
 login local
line vty 5 15
 login
end
```

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

Available Variables:

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

Credentials

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

Community String:	
Confirm Community String:	
Telnet/SSH Username:	
Telnet/SSH Password:	
Confirm Telnet/SSH Password:	
"enable" Password:	••••••••••
Confirm "enable" Password:	••••••••••
SNMPv3 Username:	
Auth Password:	
Confirm Auth Password:	
Privacy Password:	
Confirm Privacy Password:	
SNMPv3 Auth Protocol:	MD5

Setting	Default	Description
Use Global Template	No	Use a global template that has been previously configured on the **Groups→Templates** page. Available templates will appear in the dropdown menu. If “Yes” is selected you can also configure global template variables. For Symbol devices you can select the groups of thin APs to which the template should be applied. For more information about global templates see the **Groups→Templates** section of the User Guide.
Fetch	None	Select 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 will be filled with the data on the **APs/Devices→Manage** page for each AP.

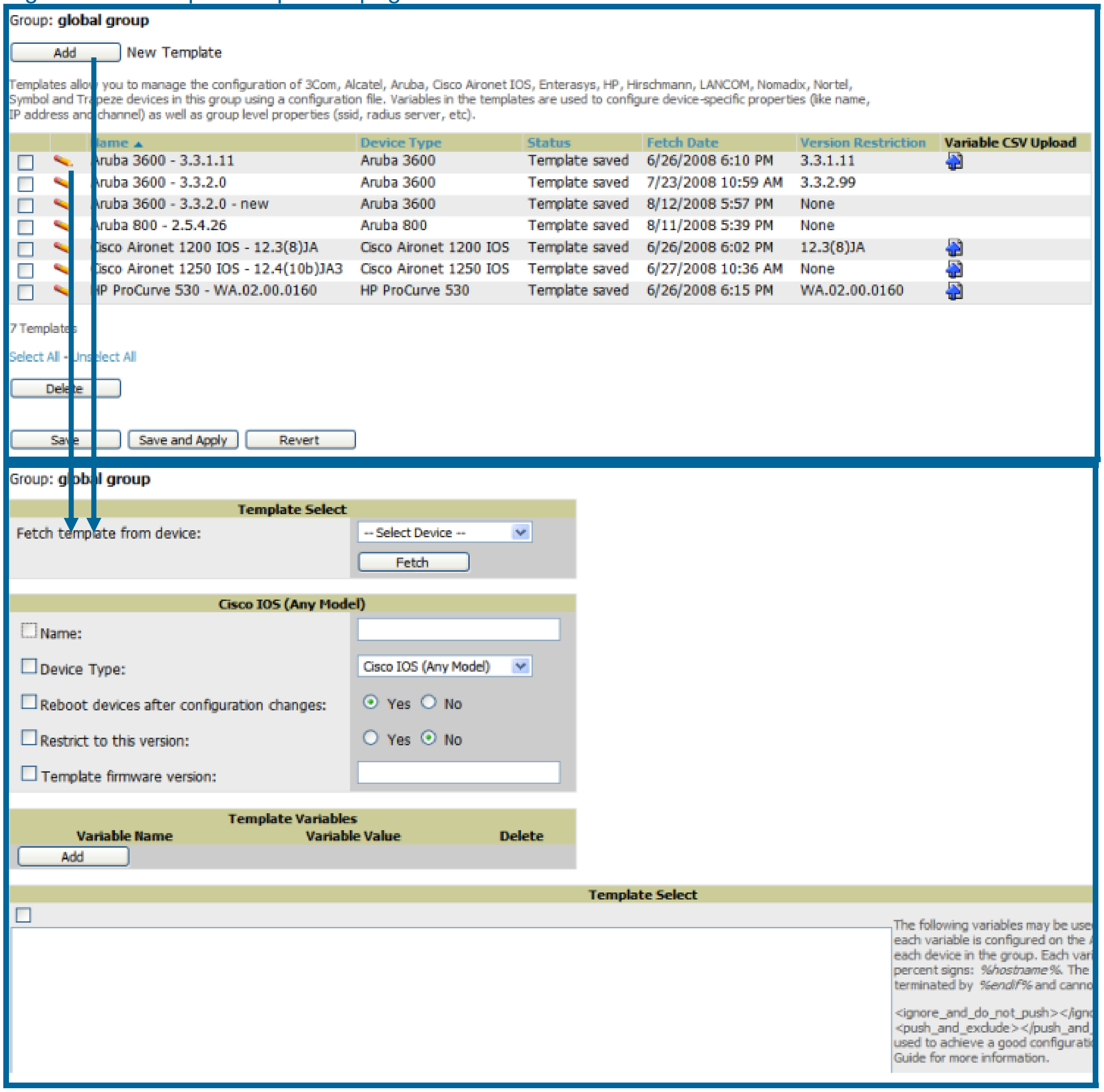
Setting	Default	Description
Name	None	The template display name.
AP Type	Cisco IOS (Any Model)	The template will apply to APs or devices of the specified type. If "Cisco IOS (Any Model)" is selected the template will apply to all IOS APs that do not have a version specific template specified.
*Reboot APs After Configuration Changes **	No	When OV3600 applies the template it copies the new config to the startup config on the AP. If "No" is selected OV3600 will use the AP to merge the startup and running configurations. If "Yes" is selected the configuration will be copied to the startup config and the AP will be 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 will only apply to APs on the version of firmware specified in the "Template Firmware Version" field.
Template firmware version	None	The template will only apply 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 will update 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 will update 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 will update 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 will update 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 will update 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 will update 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 will update the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Auth Protocol	MD5	Specify the SNMPv3 Auth protocol, either MD5 or SHA-1.

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, turning settings like group RADIUS servers and encryption keys into variables that can be configured on a per-group basis.

To create a global template, or to view or edit an existing global template, navigate to the **Group→Templates** page for the global group that owns it. Click the Add button to add a new template, or click the pencil icon next to an existing template to edit that template.

Figure 31. “Group→Templates” page



Group: **global group**

New Template

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

		Name ▲	Device Type	Status	Fetch Date	Version Restriction	Variable CSV Upload
□	✎	Aruba 3600 - 3.3.1.11	Aruba 3600	Template saved	6/26/2008 6:10 PM	3.3.1.11	⇪
□	✎	Aruba 3600 - 3.3.2.0	Aruba 3600	Template saved	7/23/2008 10:59 AM	3.3.2.99	
□	✎	Aruba 3600 - 3.3.2.0 - new	Aruba 3600	Template saved	8/12/2008 5:57 PM	None	
□	✎	Aruba 800 - 2.5.4.26	Aruba 800	Template saved	8/11/2008 5:39 PM	None	
□	✎	Cisco Aironet 1200 IOS - 12.3(8)JA	Cisco Aironet 1200 IOS	Template saved	6/26/2008 6:02 PM	12.3(8)JA	⇪
□	✎	Cisco Aironet 1250 IOS - 12.4(10b)JA3	Cisco Aironet 1250 IOS	Template saved	6/27/2008 10:36 AM	None	⇪
□	✎	HP ProCurve 530 - WA.02.00.0160	HP ProCurve 530	Template saved	6/26/2008 6:15 PM	WA.02.00.0160	⇪

7 Templates

Select All - Unselect All

Group: **global group**

Template Select

Fetch template from device: -- Select Device --

Cisco IOS (Any Model)

□ Name:	
□ Device Type:	Cisco IOS (Any Model)
□ Reboot devices after configuration changes:	● Yes ○ No
□ Restrict to this version:	○ Yes ● No
□ Template firmware version:	

Template Variables

Variable Name	Variable Value	Delete

Template Select

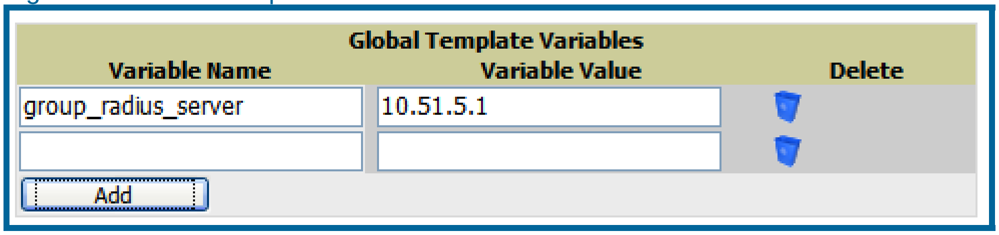
□

The following variables may be use each variable is configured on the each device in the group. Each var percent signs: *%hostname%*. The terminated by *%endif%* and canno

<ignore_and_do_not_push></ign <push_and_exclude></push_and used to achieve a good configurati Guide for more information.

Use the dropdown menu to select a device from which to build the global template and click the "Fetch" button. The dropdown menus are populated with all devices that are contained in any group that subscribes to the global group. The fetched configuration will populate the template field. Global template variables can be configured with the "Add" button in the Global Template Variables box.

Figure 32. Global Template Variables box



Global Template Variables

Variable Name	Variable Value	Delete
group_radius_server	10.51.5.1	🗑
		🗑

The variable name cannot have any spaces or non-alphanumeric characters. The initial variable value entered will be 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).

Once you have configured your global template, click the "Add" button at the bottom of the page. You will be taken to a confirmation page where you can review your changes. 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 on the confirmation page will cause the template and all of the template variables to be lost.

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** 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 filled in.

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

For exOV3600le, for a global template with a variable called "ssid_1", the CSV file might look like:

```
Group Name, ssid_1
Subscriber 1, Value 0
```

Once you have defined a global template, it will be available for use by any local group that subscribes to the global group. Navigate to the **Groups→Template** page for the local group and click the pencil icon next to the name of the global template in the list.

You will not be able to edit the template itself from the subscriber group's **Groups→Templates** tab; to make changes navigate to the **Groups→template** page for the global group and click the pencil icon next to the template you wish to edit.

If group template variables have been defined, you'll be able to edit the value for the group on the **Groups→Template** add page in the "Group Template Variables" box. For Symbol devices, you'll also be able to define the template per group of APs.

For more information on using templates in OV3600, see the previous section of the User Guide. It is also possible to create local templates in a subscriber group – using global groups does not mean that global templates are mandatory.

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** page, which defines the startup-config of the devices rather than utilizing OV3600's normal Group configuration pages. OV3600 no longer supports making changes for these devices via the browser-based interface, but rather uses templates to configure all settings, including settings that were formally controlled on the OV3600's Group configuration pages.

STEP ONE: Defining a Model AP

Navigate to the Groups→Template page of a group containing an IOS device. Click "Fetch" to create a template based on the running configuration of a "model" access point. OV3600 will replace some settings with variables so that the template is able to apply to all devices in the group even though some of their individual settings may vary. Some of the settings that are turned into variables include channel, transmit power, IP address and most settings that change per device

STEP TWO: Creating a Template

OV3600 provides a text-based template editor allowing you to modify the template created by fetching the device configuration to create a template that defines Group settings to be applied to all APs in the Group (security, VLANs, etc.) while enabling other settings (like channel and antenna configuration) to be managed on an AP-by-AP basis.

STEP THREE: Generating Startup-config Files

OV3600 replaces all variables with the ap specific settings from the APs/Devices→Manage page to create a unique startup-config file for each IOS access point in the group.

STEP FOUR: Applying Startup-config Files

OV3600 instructs each of the APs in the Group to copy its unique startup-config from OV3600 via TFTP or SCP. If the "Reboot Devices after Configuration Changes" option is selected then OV3600 will instruct the AP to copy the configuration from OV3600 to the startup config of the AP and reboot the AP. If the "Reboot Devices after Configuration Changes" option is not selected then OV3600 will instruct the AP to copy the configuration to the startup config and then tell the AP to copy the startup config to the running config. It is recommended that you use the reboot option when possible. Copying the configuration from startup to running merges the two configurations and can cause undesired configuration lines to remain active on the AP.

Please see Appendix D – Access Point Notes for a full Cisco IOS template.

NOTE: Changes made on OV3600's standard Group configuration pages (Basic, Radio, Security, VLANs, etc.) will not be applied to any template-based APs..

Configuration Procedure

To use Templates configuration within a Group:

- Select a Group to configure. *NOTE: It is recommended that you start with a small group of access points and placing these APs in "Monitor Only" (read only) via the "Modify Devices" link until you are fully familiar with the template configuration process. This will prevent configuration changes from being applied to the APs until you are sure you have the correct configuration specified.*

- 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 currently configured 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 properly.

- Navigate to the **Groups→Templates** page. Click "Add" to add a new template.

- Select the model AP from the drop-down list, and click "Fetch".

- OV3600 will automatically attempt 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 (see **Template Syntax** below). These variables are always encapsulated between % signs. On the right side of the page you will see a section labeled "Additional Variables". 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. Doublecheck 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 support@ind.alcatel.com before proceeding.

- Specify the device types for the template. The template will only apply to devices of the specified type.

- Specify if OV3600 should reboot the devices after a configuration push. If the "Reboot Devices after Configuration Changes" option is selected then OV3600 will instruct the AP to copy the configuration from OV3600 to the startup config of the AP and reboot the AP. If the "Reboot Devices after Configuration Changes" option is not selected then will instruct the AP to copy the configuration to the startup config and then tell the AP to copy the startup config to the running config. It is recommended that you use the reboot option when possible. Copying the configuration from startup to running merges the two configurations and can cause undesired configuration lines to remain active on the AP.

- Restrict the template to only apply 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.

- Click the "Save and Apply" button to instruct OV3600 to re-verify the configuration of each AP in the Group. *NOTE: If you set the reboot flag to "No" then some changes could result in configuration mismatches until the AP is rebooted. For exOV3600le, changing the "SSID" on Cisco IOS APs requires the AP to be rebooted. Logging and NTP service are other settings that require the AP to be rebooted to implement a configuration change and will result in a configuration mismatch 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 config mismatch like this if the AP is not rebooted:*

IOS config template:

```
…
(no logging queue-limit)
…
```

Device Config on APs->Audit 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
…
```

- Once the template is correct and all mismatches are verified on AP Audit page, use the “Modify Devices” link on the **Groups→Monitor** page to place the desired devices into “Management” mode. This removes the APs from Monitor mode (read-only) and will instruct AP to pull down its new startup-config from OV3600.

Note: Devices can be placed into “Management” mode individually from the ***APs/Devices→Manage page*****.**

Template Syntax

AP-Specific Variables

When a template is applied to an AP all variables are replaced with the corresponding settings from the APs/Devices→Manage 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 page. Variables are always encapsulated between % signs. ExOV3600les:

```
hostname %hostname%
…
interface Dot11Radio0
…
 power local cck %CCK_POWER%
 power local ofdm %OFDM_POWER%
 channel %CHANNEL%
…
```

The hostname line sets the APs 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.

Using Directives to Eliminate Reporting of Specified 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 interface.

However, when using the templates configuration function, there will be times when the running-config and the startup-config will not match under normal circumstances. For exOV3600le, the "ntp clock-period" setting will almost never be identical in the running-config and the startup-config. 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 to send to each AP and whether it reports variances between the running-config and the startup-config as "configuration mismatches." Lines enclosed in <push_and_exclude> will be included in the AP's startup-config but OV3600 will ignore them when verifying configurations. Lines enclosed in <ignore_and_do_not_push> will 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. Lines enclosed in the ignore and do not push directive will not be included in the startup-config that is copied to each AP. When OV3600 is comparing the running-config to the startup-config for configuration verification, it will ignore any lines in the running-config that start with the text within the directive. Lines belonging to an ignored and unpushed line, the lines immediately below the line and indented, will be ignored as well. In the exOV3600le below if you were to bracket ntp server the ntp clock period would behave as if it were bracketed because it belongs or is associated with the ntp server line.

NOTE: The line **<ignore_and_do_not_push>***ntp clock-period***</ignore_and_do_not_push>** *will cause lines starting with "ntp clock-period" to be ignored. However, the line* **<ignore_and_do_not_push>***ntp* **</ignore_and_do_not_push>** *will cause 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. For exOV3600le, some "no" commands that are used to remove SSIDs or unset configuration parameters will not appear in the running-config of a device. A command inside the push and exclude directive will be included in the startup-config pushed to a device, but OV3600 will exclude them when calculating and reporting configuration mismatches.

NOTE: The opening tag may have leading spaces.

ExOV3600les:

```
…
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
```

Conditional Variables

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 exOV3600le, 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:

```
 %if variable=value%
…
%endif%
```

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** page for the device.
	client	
	master	
IP	Static	IP address of the device is set statically on the AP Manage page
	DHCP	IP address of the device is set dynamically using DHCP

Substitution Variables

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 2 will be substituted with values specified on each access point's **APs/Devices→Manage** page within the OV3600 user interface.

Sometimes, the running-config on the AP will not include the command for one of these variables because the value is set to the default. For exOV3600le, when the "transmission power" is set to *maximum (the default)*, the line "power local maximum" will not appear in the AP's running-config, although it will appear in the startup-config. OV3600 would typically detect and flag this variance between the running-config and startup-config as a configuration mismatch. To prevent OV3600 from reporting a configuration mismatch between the desired startup-configuration and the running-config 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 will cause lines to be suppressed in this way when reporting configuration mismatches.

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 transmit	diversity

Variable	Meaning	Command	Suppressed Default
	antenna	%antenna_transmit%	
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 AP include	The SSL Certificate used by the AP The AP include fields allow for configurable variables. Any lines placed in the AP Include field on the **APs/Devices→ Manage** page will replace this variable.	%certificate% %ap_include_1%	- -

WDS Settings

Template supports Cisco WDS settings. APs functioning in a WDS environment communicate with the 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** page select the proper role for the AP in the WDS Role drop down menu.

ExOV3600le – setting an AP as a **WDS Slave** the following lines:

```
%if wds_role=client%
wlccp ap username wlse password 7 XXXXXXXXXX
%endif%
```

ExOV3600le – setting an AP as a **WDS Master** the following lines:

```
%if wds_role=master%
aaa authentication login method_wds group wds
aaa group server radius wds server
10.2.25.162 auth-port 1645 acct-port 1646
wlccp authentication-server infrastructure method_wds
wlccp wds priority 200 interface BVI1
wlccp ap username wlse password 7 095B421A1C
%endif%
```

ExOV3600le – setting an AP as a **WDS Master Backup** 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

A few things must be setup before enabling SCP on the **Groups→Basic** page. The credentials used by OV3600 to login to the AP must have level 15 privileges. Without them OV3600 will not be able to communicate with the AP via SCP. The line “aaa authorization exec default local” must be in the AP’s config and the AP must have the SCP server enabled. These three settings correspond to the following lines in the AP’s config.

```
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** page without problems.

Common Scenarios

Supporting Multiple Radio Types via a Single IOS Template

Some lines in an IOS configuration file should only apply to certain radio types (i.e., 802.11g vs. 802.11b). For instance, lines related to speed rates that mention rates above 11.0Mb/s will 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 config template to configure APs with different radio types within the same Group.

ExOV3600les:

```
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 Both 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. ExOV3600le:

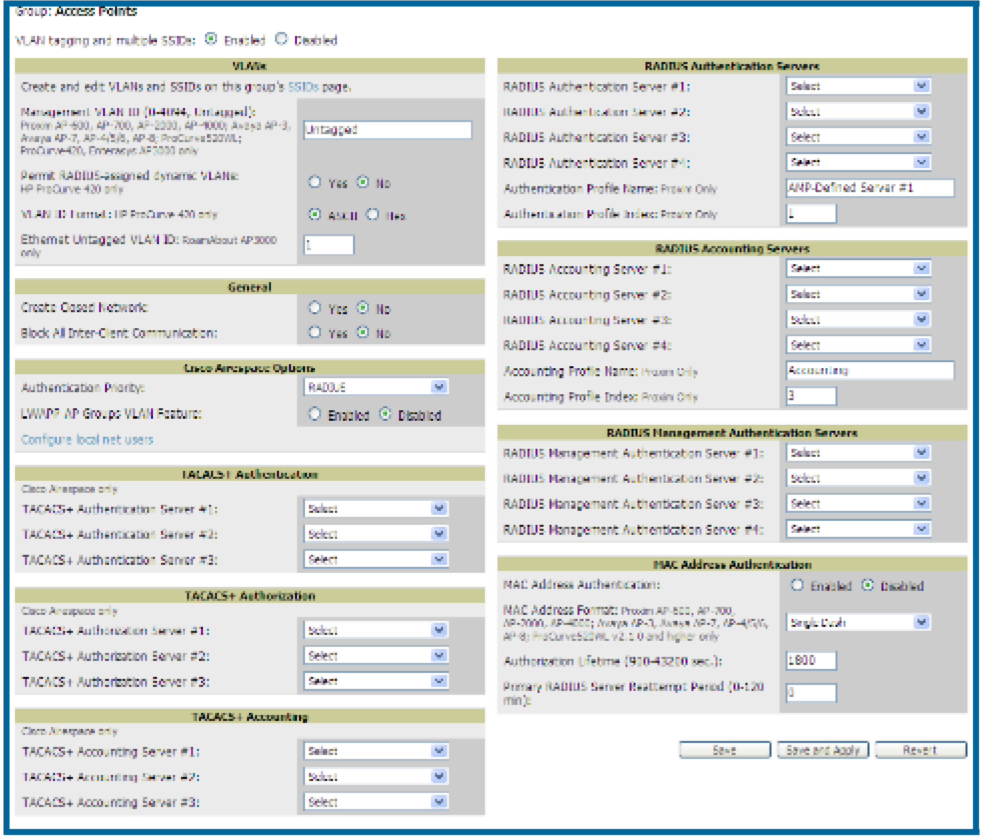
```
%IF interface=Dot11Radio1%
interface Dot11Radio1
 bridge-group 1
 bridge-group 1 block-unknown-source
 bridge-group 1 spanning-disabled
 bridge-group 1 subscriber-loop-control
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 no ip address
 no ip route-cache
 rts threshold 2312
 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 Group Security Settings

The **Groups→Security** page allows you to specify critical security policies for APs in the Group.

- Browse to the **Groups→Security** page to enable wireless security coupled or decoupled with VLANs.

Figure 34. “Groups→Security” page



Group: Access Points

VLAN tagging and multiple SSIDs: ● Enabled ○ Disabled

VLANs

Create and edit VLANs and SSIDs on this group's SSIDs page.

Management VLAN ID (0-4094, Untagged): Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL; ProCurve420, Enterasys AP3000 only	Untagged
Permit RADIUS-assigned Dynamic VLANs: HP ProCurve 420 only	○ Yes ● No
VLAN ID Format: HP ProCurve 420 only	● ASCII ○ Hex
Ethernet Untagged VLAN ID: RoamAbout AP3000 only	1

General

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

Cisco Airespace Options

Authentication Priority:	RADIUS
LWAPP AP Groups VLAN Feature:	○ Enabled ● Disabled

Configure local net users

TACACS+ Authentication

Cisco Airespace only

TACACS+ Authentication Server #1:	Select
TACACS+ Authentication Server #2:	Select
TACACS+ Authentication Server #3:	Select

TACACS+ Authorization

Cisco Airespace only

TACACS+ Authorization Server #1:	Select
TACACS+ Authorization Server #2:	Select
TACACS+ Authorization Server #3:	Select

TACACS+ Accounting

Cisco Airespace only

TACACS+ Accounting Server #1:	Select
TACACS+ Accounting Server #2:	Select
TACACS+ Accounting Server #3:	Select

RADIUS Authentication Servers

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

RADIUS Accounting Servers

RADIUS Accounting Server #1:	Select
RADIUS Accounting Server #2:	Select
RADIUS Accounting Server #3:	Select
RADIUS Accounting Server #4:	Select
Accounting Profile Name: Proxim Only	Accounting
Accounting Profile Index: Proxim Only	3

RADIUS Management Authentication Servers

RADIUS Management Authentication Server #1:	Select
RADIUS Management Authentication Server #2:	Select
RADIUS Management Authentication Server #3:	Select
RADIUS Management Authentication Server #4:	Select

MAC Address Authentication

MAC Address Authentication:	○ Enabled ● Disabled
MAC Address Format: Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL v2.1.0 and higher only	Single Dash
Authorization Lifetime (900-43200 sec.):	1800
Primary RADIUS Server Reattempt Period (0-120 min):	0

- Locate the “General” area on the **Groups→Security** page.

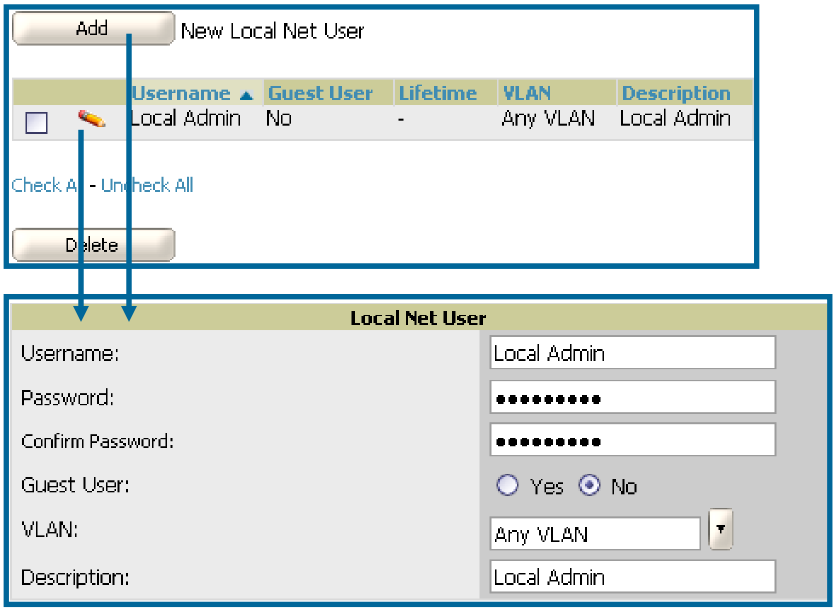
Setting	Default	Description
Create Closed Network	No	If enabled, the APs in the Group will not broadcast their SSIDs. *NOTE: It is recommended that you create a closed network to make it more difficult for intruders to detect your wireless network.*
Block All Inter-Client Communication	No	If enabled, 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.*

- Locate the “Cisco Airespace Options” area on the **Groups→Security** page.

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

- To configure local net users on Cisco Airespace controllers click the “Configure local net users” link in the Cisco Airespace Options area on the **Groups→Security** page.

Figure 35. “Groups→Security Configure Local Net Users” page



	Username ▲	Guest User	Lifetime	VLAN	Description
□	Local Admin	No	-	Any VLAN	Local Admin

Local Net User

Username:	Local Admin
Password:	●●●●●●●●●
Confirm Password:	●●●●●●●●●
Guest User:	○ Yes ● No
VLAN:	Any VLAN
Description:	Local Admin

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

- Locate the “EAP Options” area on the **Groups→Security** page.

Setting	Default	Description
WEP Key Rotation Interval (seconds)	120	Time (in seconds) at which the AP will rotate between WEP keys.
Session Key Refresh Rate (0-1440 min) (HP ProCurve 420 only)	0	The time, in minutes, between session key refreshes.
Session Timeout (0-65535 sec.) (HP ProCurve 420 only)	0	Allows you to specify the time, in seconds, before users are forced to re-authenticate.
Cisco Temporal Key Integrity Protocol (TKIP)	Disabled	If enabled, TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP. *NOTE: TKIP can only be enabled when EAP-based security is used.*
Cisco Message Integrity Check (MIC)	Disabled	If enabled, MIC adds several bytes per packet to make it more difficult to tOV3600er with the packets.

- Locate “RADIUS Accounting Servers” area on the **Groups→Security** page. These RADIUS servers dictate where the AP will send RADIUS accounting packets. Once the RADIUS Accounting servers are configured on the **Group→AAA Servers** page they will appear in the dropdown menus. Configuring the AP to send RADIUS accounting packets directly to OV3600 allows OV3600 to pull usernames from the packets. The usernames are then correlated with MAC addresses and displayed in OV3600. To Configure OV3600 to accept the RADIUS accounting packets from APs please see the **OV3600 Setup→RADIUS Accounting** page.

Setting	Default	Description
RADIUS Accounting Server 1-4	None	Pull-down menu to select RADIUS Accounting servers previously entered on the **Group → AAA** page. These RADIUS servers dictate where the AP will send RADIUS Accounting packets
Accounting Profile Name	Accounting	The Accounting Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.
Accounting Profile Index	1	The Accounting Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.

- Locate “RADIUS Authentication Servers” area on the **Groups→Security** page. These RADIUS servers dictate how wireless clients will authenticate onto the network. For RADIUS-based authentication, every AP must be configured to authenticate associated users to a specific RADIUS server. RADIUS servers need to be configured on the **Group→AAA Servers** page to appear in the dropdown menus.

Setting	Default	Description
RADIUS Authentication Server 1-4	None	Pull-down menu to select RADIUS Authentication servers previously entered on the **Group → RADIUS** page. These RADIUS servers dictate how wireless clients will authenticate onto the network.
Authentication Profile Name	OV3600-Defined Server #1	The Authentication Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.

Setting	Default	Description
Authentication Profile Index	1	The Authentication Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.

- Locate "RADIUS Management Servers" area on the **Groups→Security** page. These RADIUS servers dictate who can login to the APs/Devices. RADIUS servers need to be configured on the **Group→AAA Servers** page to appear in the dropdown menus.

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

- Locate "MAC Address Authentication" area on the **Groups→Security** page.

Setting	Default	Description
MAC Authentication	Disabled	If enabled, only MAC addresses known to the RADIUS server will be permitted to associate to APs in the Group.
MAC Address Format(Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8, HP ProCurve 520WL, ProCurve 420 v2.1.0 and higher)	Dash Delimited	It allows selection of the format for MAC addresses used in RADIUS authentication and accounting requests: Dash Delimited: xx-xx-xx-xx-xx-xx (default) Colon Delimited: xx:xx:xx:xx:xx:xx Single-Dash: xxxxxx-xxxxxx No Delimiter: xxxxxxxxxxxx
Authorization Lifetime (900 – 432000 seconds)	1800	The amount of time a user can be connected before reauthorization is required.
Primary RADIUS Server Reattempt Period (minutes)	0	Specifies the time (in minutes) that the AP will await responses from the primary RADIUS server before communicating with the secondary RADIUS server, etc.

- Locate the TACACS+ Authentication, Authorization and Accounting areas on the **Groups→Security** page (this area is for Airespace devices only). These settings configure TACACS+ servers on the controller, which control users logging in to the controller. TACACS+ servers need to be configured on the **Group→AAA Servers** page to appear in the dropdown menus.

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

- If you are using VLAN tagging, select *Enable VLAN Tagging* at the top of the page. Please see the **Groups→SSIDS** page to configure individual SSIDs and VLANs.

Setting	Default	Description
Management VLAN ID (0-4094)	Untagged	Sets the management VLAN on the Device
Permit RADIUS-assigned Dynamic VLANs (HP ProCurve 420)	No	Allows or denies RADIUS-assigned Dynamic VLANs on HP ProCurve 420s.
VLAN ID Format (HP ProCurve420)	ASCII	Sets the VLAN ID format to ASCII or Hex for HP ProCurve 420s.
Ethernet Untagged VLAN ID (RoamAbout AP3000)	1	Defines the untagged VLAN ID for the RoamAbout AP3000.

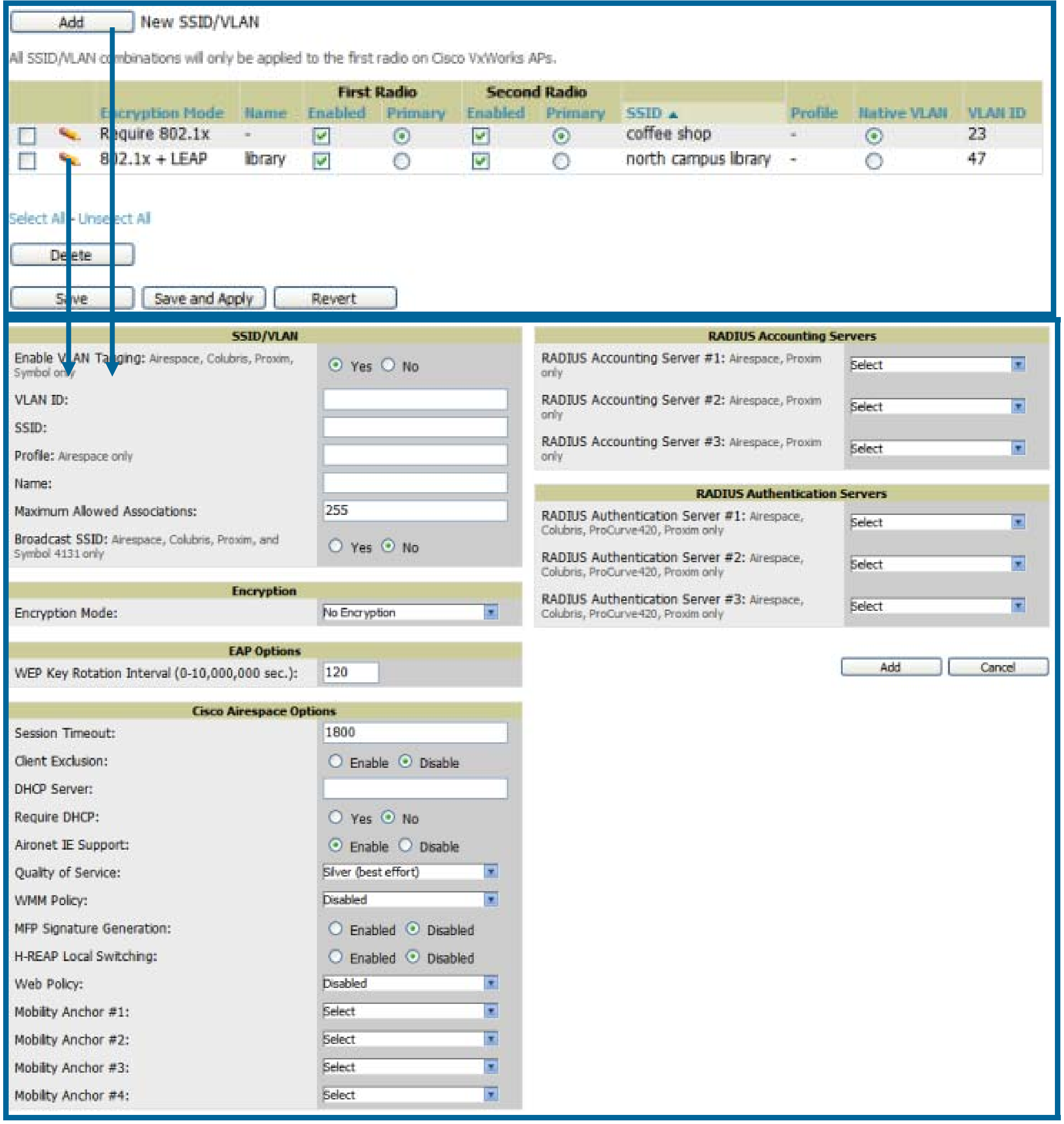
- See tables above for detailed descriptions of fields under General or RADIUS Servers.

Configuring Group SSIDs Settings (Optional)

The **Groups→SSIDs** page allows you to create and edit VLANs associated with the group of access points. Multiple VLANs and SSIDs are only supported on Cisco and Colubris access points.

- Browse to the **Groups→SSIDs** page to create and edit the group's VLANs.

Figure 37. "Groups→SSIDS" page (Create & Edit VLANs on this page)



All SSID/VLAN combinations will only be applied to the first radio on Cisco VxWorks APs.

				First Radio		Second Radio					
		Encryption Mode	Name	Enabled	Primary	Enabled	Primary	SSID ▲	Profile	Native VLAN	VLAN ID
□		Require 802.1x	-	☑	●	☑	●	coffee shop	-	●	23
□		802.1x + LEAP	library	☑	○	☑	○	north campus library	-	○	47

SSID/VLAN

Enable VLAN Tagging: Airespace, Colubris, Proxim, Symbol only	● Yes ○ No
VLAN ID:	
SSID:	
Profile: Airespace only	
Name:	
Maximum Allowed Associations:	255
Broadcast SSID: Airespace, Colubris, Proxim, and Symbol 4131 only	○ Yes ● No

Encryption

Encryption Mode:	No Encryption

EAP Options

WEP Key Rotation Interval (0-10,000,000 sec.):	120

Cisco Airespace Options

Session Timeout:	1800
Client Exclusion:	○ Enable ● Disable
DHCP Server:	
Require DHCP:	○ Yes ● No
Aironet IE Support:	● Enable ○ Disable
Quality of Service:	Silver (best effort)
WMM Policy:	Disabled
MFP Signature Generation:	○ Enabled ● Disabled
H-REAP Local Switching:	○ Enabled ● Disabled
Web Policy:	Disabled
Mobility Anchor #1:	Select
Mobility Anchor #2:	Select
Mobility Anchor #3:	Select
Mobility Anchor #4:	Select

RADIUS Accounting Servers

RADIUS Accounting Server #1: Airespace, Proxim only	Select
RADIUS Accounting Server #2: Airespace, Proxim only	Select
RADIUS Accounting Server #3: Airespace, Proxim only	Select

RADIUS Authentication Servers

RADIUS Authentication Server #1: Airespace, Colubris, ProCurve420, Proxim only	Select
RADIUS Authentication Server #2: Airespace, Colubris, ProCurve420, Proxim only	Select
RADIUS Authentication Server #3: Airespace, Colubris, ProCurve420, Proxim only	Select

- The initial **Groups→SSIDs** page provides the ability to add, modify, or delete VLANs.

Setting	Description
Encryption Mode	The encryption set on the VLAN.
Name	The name of the VLAN.
First or Second Radio Enabled	Checkbox used to enable the VLAN, SSID and Encryption Mode on the radio.
First or Second Radio Primary	Specifies which VLAN will 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 will be broadcast.*
SSID	The SSID associated with the VLAN.
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 will need to create a dummy VLAN, disable it on both radios and ensure that it has the highest VLAN ID.
VLAN ID	Identifies the number of the primary VLAN SSID on which encrypted or unencrypted packets can pass between the AP and the switch.

- Locate “SSID/VLAN” area on the **Groups→SSIDS** page by clicking on the “manage” icon. This section encompasses the basic VLAN configuration.

Setting	Default	Description
Enable VLAN Tagging (Airespace, Colubris and Symbol only)	Yes	Enables or disables VLAN tagging on the AP.
VLAN ID	None	Indicates the number of the VLAN designated as the “Native VLAN,” typically for management purposes
SSID	None	Service Set Identifier (SSID) is a 32-character user-defined identifier attached to the header of packets sent over a WLAN. It acts as a password when a mobile device tries to connect to the network through the AP, and a device will not be permitted to join the network unless it can provide the unique SSID.
Profile (Airespace only)	None	This setting allows the same SSID to be defined with up to four different security settings (Cisco Airespace only).
Name	None	User-definable name associated with SSID/VLAN combination.
Service Priority (VxWorks only)	None	Identifies the delivery priority which packets receive on the VLAN/SSID (VxWorks only).
Maximum Allowed Associations	255	Indicates the maximum number of mobile users which can associate with the specified VLAN/SSID. *Note: 0 means unlimited for Cisco and none for Colubris.*

Setting	Default	Description
Broadcast SSID (Airspace, Colubris and Proxim only)	No	Enables the AP to broadcast the SSID for the specified VLAN/SSID. This setting works in conjunction with the "Creat Closed Network" setting on the **Groups→Security** page. Proxim devices support a maximum of four SSIDs. *Note: This option should be enabled to ensure support of legacy users.*
Unique Beacon (Proxim only)	Disabled	If more than one SSID is enabled, they can be sent in separate beacons.
Closed Partial Beacon (Proxim only)	Disabled	AP will send its SSID in every beacon but will not respond to any probe requests.

-
- Locate "Encryption" area on the **Groups→SSIDS** page.

Setting	Default	Description
Encryption Mode	None	Pull-down menu that determines the level of encryption required for devices to associate to the APs (i.e., "Optional WEP", Require WEP", "Require 802.1x", "Require Leap", "802.1x+WEP", "LEAP+WEP", "WPA", "WPA/PSK").
WPA2 WPA Compatibility Mode	Enabled	Enable compatibility mode. In compatibility mode WPA clients will be able to associate to the AP
WPA2 Allow TKIP	Enabled	Allow TKIP encryption. Typically WPA2 only allows AES encryption.
WPA Preshared Key (Cisco IOS, HP ProCurve 420, Colubris, Symbol)	None	Allows specification of a pre-shared key material for securing the wireless connection. *This will only appear when WPA/PSK is selected on the Encryption Mode pull-down menu.* *NOTE: This is not recommended for high security enterprise connectivity.*

- Locate "EAP Options" area on the **Groups→SSIDS** page.

Setting	Default	Description
WEP Key Rotation Interval (seconds)	120	Time (in seconds) between WEP key rotation on the AP.
Cisco Temporal Key Integrity Protocol (TKIP)	Disabled	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 (Message Integrity Check)	Disabled	If enabled, MIC adds several bytes per packet to make it more difficult to tOV3600er with the packets.

- Locate the “RADIUS Accounting Servers” area on the **Groups→SSIDS** page.

Setting	Default	Description
RADIUS Accounting Server 1-2	None	Pull-down menu to select RADIUS Accounting servers previously entered on the Group → RADIUS page. These RADIUS servers dictate where the AP will send RADIUS Accounting packets for this SSID/VLAN.
Accounting Profile Name	None	The Accounting Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.
Accounting Profile Index	None	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.

- Locate “RADIUS Authentication Servers” area on the **Groups→SSIDS** page.

Setting	Default	Description
RADIUS Authentication Server 1-2	None	Pull-down menu to select RADIUS Authentication servers previously entered on the Group → RADIUS page. These RADIUS servers dictate how wireless clients will authenticate onto the network.
Authentication Profile Name	None	The Authentication Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.
Authentication Profile Index	None	The Authentication Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.

- Locate “Cisco Airespace Options” area on the **Groups→SSIDS** page.

Setting	Default	Description
Session Timeout	1800	Configures the session timeout option on the Airespace controllers in the group.
Client Exclusion	60	Configures the Client Exclusion option on the Airespace controllers in the group.
DHCP Server	None	Defines the DHCP server for the Airespace controllers in the group.
Require DHCP	No	*Enables or disables the Require DHCP command line setting. Sets DHCP Addr. Assignment to Required.*
Aironet IE Support	Enable	Enables or disables Aironet IE support.
Quality of Service	Silver (Best Effort)	Defines the QOS for the network or VLAN.
WMM Policy	Disabled	Enables or disables the WMM policy.
MFP Signature Generation	Enabled	Enables or disables MFP signature generation.
H-REAP Local Switching	Disabled	Enables or disables H-REAP local switching.

Setting	Default	Description
Web Policy	Disabled	Dropdown menu that specifies the web authentication policy. Disabled: No web authentication. Authentication: Will prompt the user for a login and password when they connect to the network Passthrough: The user will be able to access the network without entering an email or password.
Email Input	Enabled	Prompts the user for their email address before allowing them to access the network. *Note: This field is only visible if the Web Policy setting is set to Passthrough.*
Mobility Anchor	N/A	Select the mobility Anchors for this VLAN/SSID.

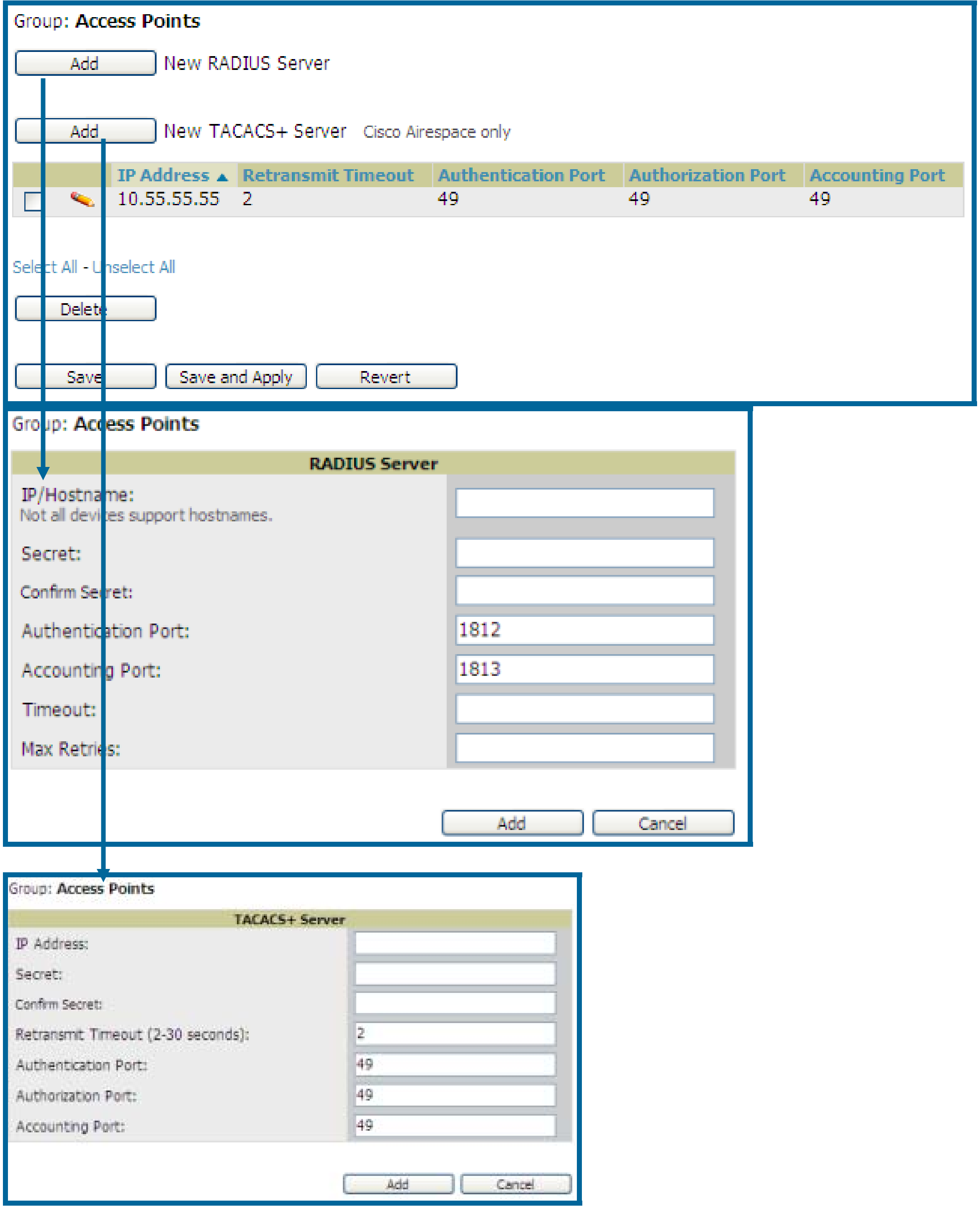
- Click "Save" when completed.

NOTE: You may need to return to the Security Page in order to configure or reconfigure RADIUS servers.

Configuring Group AAA Servers

RADIUS and TACACS+ servers get defined get defined on the **Group→AAA Servers** page. Once defined on this page they will be selectable in the drop down menus on the **Groups→Security** page. TACACS+ servers are configurable for Cisco Airespace devices only.

Figure 38. Adding a RADIUS or TACACS+ server



Group: **Access Points**

		IP Address ▲	Retransmit Timeout	Authentication Port	Authorization Port	Accounting Port
□	✎	10.55.55.55	2	49	49	49

Group: **Access Points**

RADIUS Server

IP/Hostname: Not all devices support hostnames.	
Secret:	
Confirm Secret:	
Authentication Port:	1812
Accounting Port:	1813
Timeout:	
Max Retries:	

Group: **Access Points**

TACACS+ Server

IP Address:	
Secret:	
Confirm Secret:	
Retransmit Timeout (2-30 seconds):	2
Authentication Port:	49
Authorization Port:	49
Accounting Port:	49

- Click the “Add” button to add a new TACACS+ Server (for Cisco Airespace devices only)

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

- Click the “Add” button to add a new RADIUS server

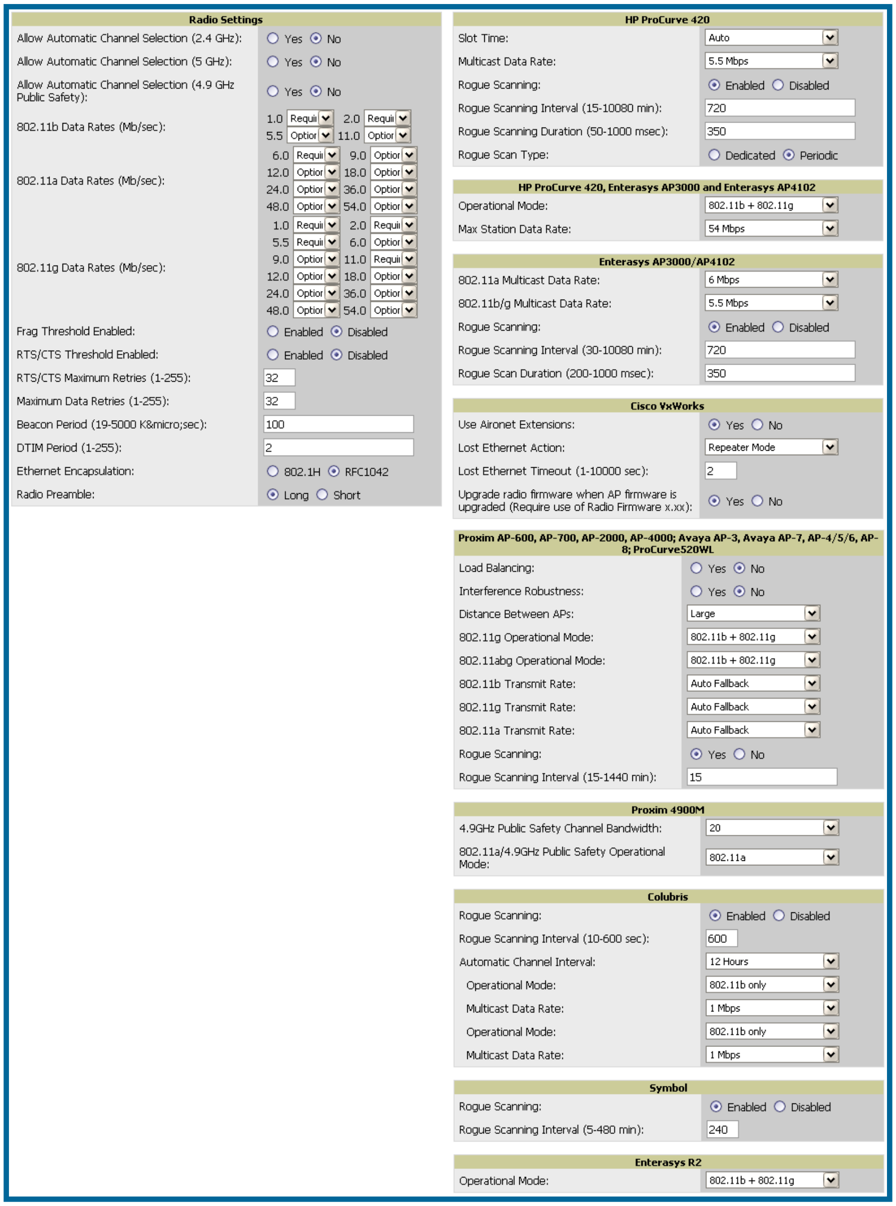
Setting	Default	Description
IP/Hostname	None	IP Address or DNS name for RADIUS Server. *Note: IP Address is required for Proxim/ORiNOCO and Cisco Aironet IOS APs.*
Secret & *Confirm Secret*	None	The shared secret that will be used to establish communication between OV3600 and the RADIUS server. *NOTE: The shared secret entered in OV3600 must match the shared secret on the server.*
Authentication Port	1812	The port used for communication between the AP and the RADIUS authentication server. *NOTE: The default 1812 should not be changed unless using older versions of RADIUS 1645.*
Accounting Port	1813	The port used for communication between the AP and the RADIUS accounting server.
Timeout (Seconds)	None	The time (in seconds) that the access point will wait for a response from the RADIUS server.
Max Retries (0-20)	None	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.*

Configuring Group Radio Settings

The **Groups→Radio** 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.

- Browse to the **Groups→Radio** page and locate the “Radio Settings” area onscreen:

Figure 39. “Groups→Radio” page



Radio Settings

Allow Automatic Channel Selection (2.4 GHz):	○ Yes ● No
Allow Automatic Channel Selection (5 GHz):	○ Yes ● No
Allow Automatic Channel Selection (4.9 GHz Public Safety):	○ Yes ● No
802.11b Data Rates (Mb/sec):	1.0 Requi 2.0 Requi 5.5 Optior 11.0 Optior
802.11a Data Rates (Mb/sec):	6.0 Requi 9.0 Optior 12.0 Optior 18.0 Optior 24.0 Optior 36.0 Optior 48.0 Optior 54.0 Optior
802.11g Data Rates (Mb/sec):	1.0 Requi 2.0 Requi 5.5 Requi 6.0 Optior 9.0 Optior 11.0 Requi 12.0 Optior 18.0 Optior 24.0 Optior 36.0 Optior 48.0 Optior 54.0 Optior
Frag Threshold Enabled:	○ Enabled ● Disabled
RTS/CTS Threshold Enabled:	○ Enabled ● Disabled
RTS/CTS Maximum Retries (1-255):	32
Maximum Data Retries (1-255):	32
Beacon Period (19-5000 K&micro;sec):	100
DTIM Period (1-255):	2
Ethernet Encapsulation:	○ 802.1H ● RFC1042
Radio Preamble:	● Long ○ Short

HP ProCurve 420

Slot Time:	Auto
Multicast Data Rate:	5.5 Mbps
Rogue Scanning:	● Enabled ○ Disabled
Rogue Scanning Interval (15-10080 min):	720
Rogue Scanning Duration (50-1000 msec):	350
Rogue Scan Type:	○ Dedicated ● Periodic

HP ProCurve 420, Enterasys AP3000 and Enterasys AP4102

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

Enterasys AP3000/AP4102

802.11a Multicast Data Rate:	6 Mbps
802.11b/g Multicast Data Rate:	5.5 Mbps
Rogue Scanning:	● Enabled ○ Disabled
Rogue Scanning Interval (30-10080 min):	720
Rogue Scan Duration (200-1000 msec):	350

Cisco VxWorks

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

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

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

Proxim 4900M

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

Colubris

Rogue Scanning:	● Enabled ○ Disabled
Rogue Scanning Interval (10-600 sec):	600
Automatic Channel Interval:	12 Hours
Operational Mode:	802.11b only
Multicast Data Rate:	1 Mbps
Operational Mode:	802.11b only
Multicast Data Rate:	1 Mbps

Symbol

Rogue Scanning:	● Enabled ○ Disabled
Rogue Scanning Interval (5-480 min):	240

Enterasys R2

Operational Mode:	802.11b + 802.11g

Setting	Default	Description
Allow Auto Channel Select (2.4, 5 GHz and 4.9GH Public Safety)	No	If enabled, whenever the AP is rebooted it will use 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 will automatically reboot the APs in the group when the change is implemented.*
802.11b Data Rates (Mb/sec)	Required: 1.0 2.0 Optional: 5.5 11.0	Pull-down menus for various data rates for transmitting data. The three values in each of the pull-down menus are: Required - The AP transmits only unicast packets at the specified data rate; multicast packets will be sent at a higher data rate set to optional. (Corresponds to a setting of 'yes' on Cisco APs.) Optional - The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of 'basic' on Cisco APs.) Not Used - The AP does not transmit data at the specified data rate. (Corresponds to a setting of 'no' on Cisco APs.)
802.11a Data Rates (Mb/sec)	Required: 6.0 9.0 12.0 Optional: 18.0 24.0 36.0 48.0 54.0	Pull-down menus for various data rates for transmitting data. The three values in each of the pull-down menus are: Required - The AP transmits only unicast packets at the specified data rate; multicast packets will be sent at a higher data rate set to optional. (Corresponds to a setting of 'yes' on Cisco APs.) Optional - The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of 'basic' on Cisco APs.) Not Used - The AP does not transmit data at the specified data rate. (Corresponds to a setting of 'no' on Cisco APs.)
802.11g Data Rates (Mb/sec)	Required: 1.0 2.0 5.5 6.0 9.0 Optional: 11.0 12.0 18.0 24.0 36.0 48.0 54.0	Pull-down menus for various data rates for transmitting data. The three values in each of the pull-down menus are: Required - The AP transmits only unicast packets at the specified data rate; multicast packets will be sent at a higher data rate set to optional. (Corresponds to a setting of 'yes' on Cisco APs.) Optional - The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of 'basic' on Cisco APs.) Not Used - The AP does not transmit data at the specified data rate. (Corresponds to a setting of 'no' on Cisco APs.)
Fragmentation Threshold Enabled	Disabled	If enabled, this setting enables packets to be sent as several pieces instead of as one block. *In most cases, it is recommended that you leave this option disabled.*
Fragmentation Threshold Value	2337	If Fragmentation Threshold is enabled, this specifies the size (in bytes) at which packets are fragmented. *A lower Fragmentation Threshold setting might be required if there is a great deal of radio interference.*

Setting	Default	Description
RTS/CTS Threshold Enabled	Disabled	If enabled, this setting will configure the AP to issue a RTS (Request to Send) before sending a packet. *In most cases, it is recommended that you leave this option disabled.*
RTS/CTS Threshold Value	2338	If RTS/CTS is enabled, this specifies the size of the packet (in bytes) at which the AP will send the RTS before sending the packet.
RTS/CTS Maximum Retires	32	If RTS/CTS is enabled, this specifies the maximum number of times the AP issues an RTS before stopping the attempt to send the packet through the radio. Acceptable values range from 1 to 128.
Maximum Data Retries	32	The maximum number of attempts the AP makes to send a packet before giving up and dropping the packet.
Beacon Period (19-5000 Kµsec)	100	Time between beacons (in kilo microseconds).
DTIM Period (1-255)	2	DTIM alerts power-save devices that a packet is waiting for them. This setting configures DTIM packet frequency as a multiple of the number of beacon packets. The DTIM Interval indicates how many beacons equal one cycle.
Ethernet Encapsulation	RFC1042	This setting selects either the RFC1042 or 802.1h Ethernet encapsulation standard for use by the group.
Radio Preamble	Long	This setting determines whether the APs will use a "short" or "long" preamble. The preamble is generated by the AP and attached to the packet prior to transmission. The short preamble is 50 percent shorter than the long preamble and thus may improve wireless network performance. *NOTE: Because older WLAN hardware may not support the "short" preamble, the "long" preamble is recommended as a default setting in most environments.*

- Certain wireless access points offer proprietary settings or advanced functionality that differ from prevailing industry standards. If you utilize these APs in the Group, you may wish to take advantage of this proprietary functionality. To configure these settings, locate the "Proprietary Settings" area on the **Groups→Radio** page. *NOTE: Proprietary settings will <u>only</u> be applied to APs in the group from the specific manufacturer and will not be configured on APs from manufacturers that do not support the functionality.*

- To configure HP ProCurve 420 only settings locate the HP ProCurve 420 section of the Proprietary Settings area.

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.*

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

- To configure the HP ProCurve 240, Enterasys AP 3000 and AP 4102 Operational Mode and Max Station Data Rate please locate the HP ProCurve 240, Enterasys AP 3000 and AP 4102 section of the Proprietary Settings area.

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

- To configure Enterasys AP3000 and Enterasys AP4102 specific settings locate the Enterasys AP3000 and Enterasys AP4102 section of the Proprietary Settings area.

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 will listen to rogues before returning to normal operation.

- Airespace radio settings are configured on the **Groups→Airespace Radio** page. See the Configuring Airespace Radio section below for details.
- To configure settings that apply to the LWAPP APs in the group, including WLAN override, controller assignment settings and HREAP options navigate to the Groups→LWAPP APs page. See the Configuring Cisco LWAPP page below for details.

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: Load balancing – allows the access point to direct Aironet clients to the optimum access point. Message Integrity Check (MIC) – protects against bit-flip attacks Temporal Key Integrity Protocol (TKIP) – key hashing algorithm that protects against IV attacks.
Lost Ethernet Action (Cisco VxWorks Only)	Repeater Mode	Pull-down menu that specifies the action to take when the *Lost Ethernet Timeout* threshold is exceeded: 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 will wait prior to taking action when its backbone connectivity is down. Actions are defined in the *Lost Ethernet Action* field.
Short Slot-Time	Enabled	If enabled the Cisco devices will use the short slot time which may slightly increase throughput. This setting can cause compatibility problems with certain radios.
Upgrade radio firmware when AP firmware is upgraded (Require Use of Radio Firmware x.xx) (Cisco Only)	Yes	If enabled, this setting mandates that the radio firmware be upgraded to a firmware version compatible with the current version of AP firmware.

- To configure settings specific to the Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3/4/5/6//7/8; and ProCurve 520WL locate the appropriate section of the Proprietary Settings area.

Setting	Default	Description
Load Balancing	No	If enabled, this setting allows client devices associating to an AP with two radio cards to determine which card to associate with, based on the load (# of clients) on each card. *NOTE: This feature is only available when two 802.11b wireless cards are used in an AP-2000.*

Setting	Default	Description
Interference Robustness	No	If enabled, this option will fragment packets greater than 500 bytes in size to reduce the impact of radio frequency interference on wireless data throughput.
Distance Between APs	Large	This setting adjusts the receiver sensitivity. Reducing receiver sensitivity from its maximum may help reduce the amount of crosstalk between wireless stations to better support roaming users. Reducing the receiver sensitivity, user stations will be more likely to connect with the nearest access point.
802.11g Operational Mode	802.11b +802.11g	This setting sets the operational mode of all g radios in the group to either b only, g only or b + g.
802.11abg Operational Mode	802.11b +802.11g	This setting sets the operational mode of all abg radios in the group to either a only, b only, g only or b + g.
802.11b Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
802.11g Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
802.11a Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
Rogue Scanning	Disabled	If enabled, any ORiNOCO, or Avaya access points in the group (with the appropriate firmware) will passively scan for rogue access points at the specified interval. This rogue scan will not break users' association to the network. *NOTE: This feature can affect the data performance of the access point.*
Rogue Scan Interval	15 minutes	If rogue scanning is enabled, this setting controls the frequency with which scans are conducted (in minutes). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan.

- To Configure Proxim Mesh settings please click the “Configure settings on the Proxim Mesh page” link.

- To configure settings specific to the Proxim 4900M settings locate the appropriate section of the Proprietary settings area.

Setting	Default	Description
4.9GHz Public Saftey 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.

- To configure Colubris only settings locate the Colubris section of the Proprietary Settings area.

Setting	Default	Description
Rogue Scanning	Disabled	If enabled, Colubris 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	600 seconds	If rogue scanning is enabled, this setting controls the frequency with which scans are conducted (in seconds). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan.
Automatic Channel Interval	12 Hours	Sets the amount of time in between automatic channel selections on Colubris APs.
First or Second Radio: Operational Mode	802.11b only	Specify the Operational Modes for the first or second radio.
First or Second Radio: Multicast Data Rate	1 Mbps	Select the Multicast Data Rate for the first or second radio.

- To configure Symbol only settings locate the Symbol section of the Proprietary Settings area.

Setting	Default	Description
Rogue Scanning (Symbol Access Points with 3.9.2 firmware or above)	Disabled	If enabled, Symbol access points with 3.9.2 or later firmware in the group will passively scan for rogue access points at the specified interval. This rogue scan will not break users' 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.

- To configure Enterasys R2 only settings locate the Enterasys R2 section of the Proprietary Settings area.

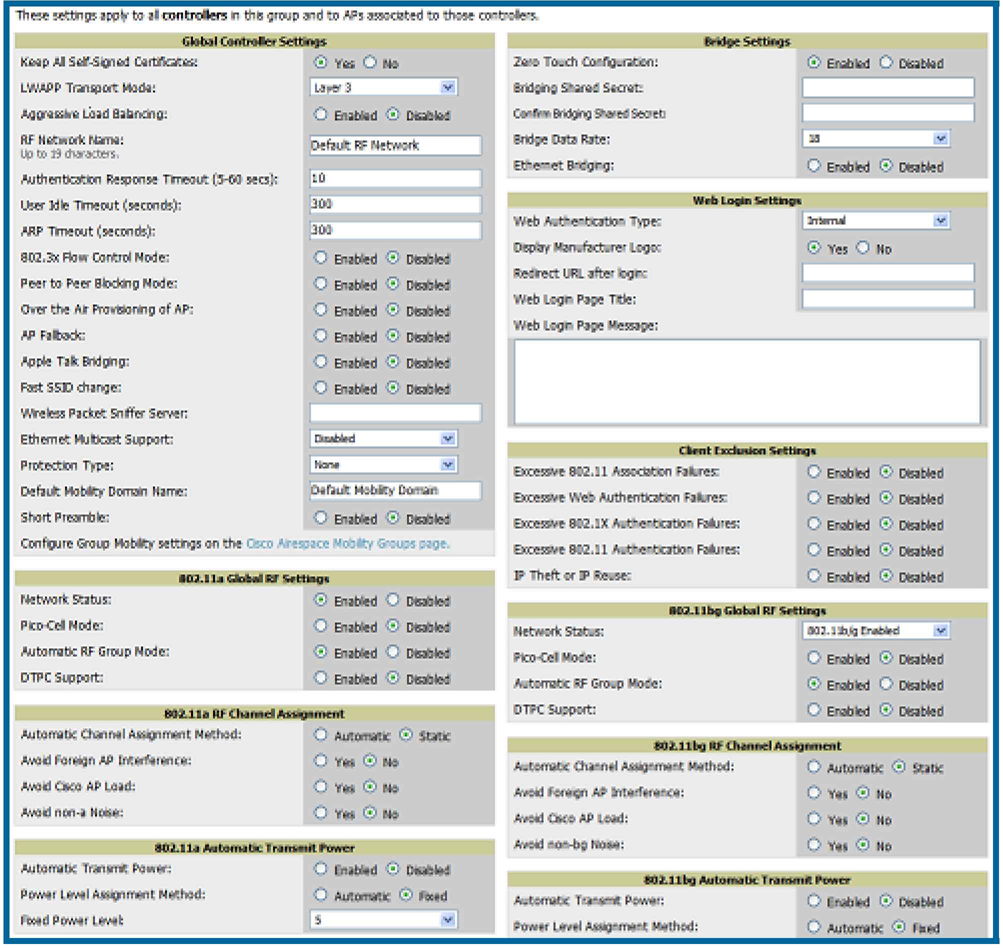
Setting	Default	Description
Operational Mode	802.11b + 802.11g	Specify the Operational Mode of the R2, either 802.11b only, 802.11g only, 802.11a only, or 802.11b + 802.11g.

- Click "Save" when completed.

Configuring Airespace Radio Settings

Navigate to the **Groups→Airespace Radio Settings** page. The Groups→Airespace Radio page configures the radio settings on Airespace controllers. All APs take their radio settings from their controllers even if the thin APs are in another group in OV3600.

Figure 40. "Groups→Airespace Radio Settings" top of page



These settings apply to all **controllers** in this group and to APs associated to those controllers.

Global Controller Settings	
Keep All Self-Signed Certificates:	● Yes ○ No
LWAPP Transport Mode:	Layer 3
Aggressive Load Balancing:	○ Enabled ● Disabled
RF Network Name: Up to 19 characters.	Default RF Network
Authentication Response Timeout (5-60 secs):	10
User Idle Timeout (seconds):	300
ARP Timeout (seconds):	300
802.3x Flow Control Mode:	○ Enabled ● Disabled
Peer to Peer Blocking Mode:	○ Enabled ● Disabled
Over the Air Provisioning of AP:	○ Enabled ● Disabled
AP Fallback:	○ Enabled ● Disabled
Apple Talk Bridging:	○ Enabled ● Disabled
Fast SSID change:	○ Enabled ● Disabled
Wireless Packet Sniffer Server:	
Ethernet Multicast Support:	Disabled
Protection Type:	None
Default Mobility Domain Name:	Default Mobility Domain
Short Preamble:	○ Enabled ● Disabled

Configure Group Mobility settings on the Cisco Airespace Mobility Groups page.

802.11a Global RF Settings	
Network Status:	● Enabled ○ Disabled
Pico-Cell Mode:	○ Enabled ● Disabled
Automatic RF Group Mode:	● Enabled ○ Disabled
DTPC Support:	○ Enabled ● Disabled

802.11a RF Channel Assignment	
Automatic Channel Assignment Method:	○ Automatic ● Static
Avoid Foreign AP Interference:	○ Yes ● No
Avoid Cisco AP Load:	○ Yes ● No
Avoid non-a Noise:	○ Yes ● No

802.11a Automatic Transmit Power	
Automatic Transmit Power:	○ Enabled ● Disabled
Power Level Assignment Method:	○ Automatic ● Fixed
Fixed Power Level:	5

Bridge Settings	
Zero Touch Configuration:	● Enabled ○ Disabled
Bridging Shared Secret:	
Confirm Bridging Shared Secret:	
Bridge Data Rate:	18
Ethernet Bridging:	○ Enabled ● Disabled

Web Login Settings	
Web Authentication Type:	Internal
Display Manufacturer Logo:	● Yes ○ No
Redirect URL after login:	
Web Login Page Title:	
Web Login Page Message:	

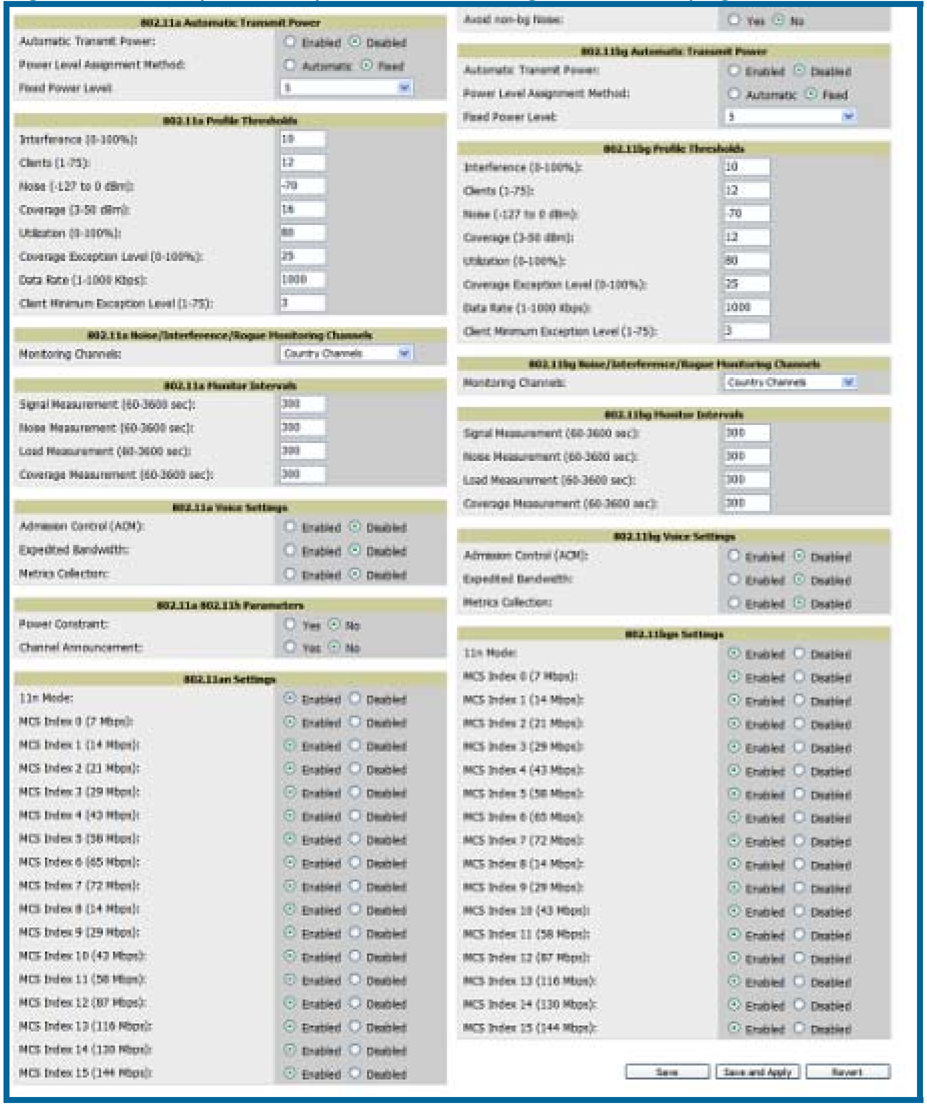
Client Exclusion Settings	
Excessive 802.11 Association Failures:	○ Enabled ● Disabled
Excessive Web Authentication Failures:	○ Enabled ● Disabled
Excessive 802.1X Authentication Failures:	○ Enabled ● Disabled
Excessive 802.11 Authentication Failures:	○ Enabled ● Disabled
IP Theft or IP Reuse:	○ Enabled ● Disabled

802.11bg Global RF Settings	
Network Status:	802.11b/g Enabled
Pico-Cell Mode:	○ Enabled ● Disabled
Automatic RF Group Mode:	● Enabled ○ Disabled
DTPC Support:	○ Enabled ● Disabled

802.11bg RF Channel Assignment	
Automatic Channel Assignment Method:	○ Automatic ● Static
Avoid Foreign AP Interference:	○ Yes ● No
Avoid Cisco AP Load:	○ Yes ● No
Avoid non-bg Noise:	○ Yes ● No

802.11bg Automatic Transmit Power	
Automatic Transmit Power:	○ Enabled ● Disabled
Power Level Assignment Method:	○ Automatic ● Fixed

Figure 41. “Groups→Airespace Radio Settings” bottom of page



802.11a Automatic Transmit Power

Automatic Transmit Power:	○ Enabled ● Disabled
Power Level Assignment Method:	○ Automatic ● Fixed
Fixed Power Level:	1

802.11a Profile Thresholds

Interference (0-100%):	10
Clients (1-75):	12
Noise (-127 to 0 dBm):	-70
Coverage (3-50 dBm):	16
Utilization (0-100%):	80
Coverage Exception Level (0-100%):	25
Data Rate (1-1000 Kbps):	1000
Client Minimum Exception Level (1-75):	3

802.11a Noise/Interference/Rogue Monitoring Channels

Monitoring Channels:	Country Channels

802.11a Monitor Intervals

Signal Measurement (60-3600 sec):	300
Noise Measurement (60-3600 sec):	300
Load Measurement (60-3600 sec):	300
Coverage Measurement (60-3600 sec):	300

802.11a Voice Settings

Admission Control (ACM):	○ Enabled ● Disabled
Expedited Bandwidth:	○ Enabled ● Disabled
Metrics Collection:	○ Enabled ● Disabled

802.11a 802.11h Parameters

Power Constraint:	○ Yes ● No
Channel Announcement:	○ Yes ● No

802.11an Settings

11n Mode:	● Enabled ○ Disabled
MCS Index 0 (7 Mbps):	● Enabled ○ Disabled
MCS Index 1 (14 Mbps):	● Enabled ○ Disabled
MCS Index 2 (21 Mbps):	● Enabled ○ Disabled
MCS Index 3 (29 Mbps):	● Enabled ○ Disabled
MCS Index 4 (43 Mbps):	● Enabled ○ Disabled
MCS Index 5 (58 Mbps):	● Enabled ○ Disabled
MCS Index 6 (65 Mbps):	● Enabled ○ Disabled
MCS Index 7 (72 Mbps):	● Enabled ○ Disabled
MCS Index 8 (14 Mbps):	● Enabled ○ Disabled
MCS Index 9 (29 Mbps):	● Enabled ○ Disabled
MCS Index 10 (43 Mbps):	● Enabled ○ Disabled
MCS Index 11 (58 Mbps):	● Enabled ○ Disabled
MCS Index 12 (87 Mbps):	● Enabled ○ Disabled
MCS Index 13 (116 Mbps):	● Enabled ○ Disabled
MCS Index 14 (130 Mbps):	● Enabled ○ Disabled
MCS Index 15 (144 Mbps):	● Enabled ○ Disabled

Avoid non-bg Noise:	○ Yes ● No

802.11bg Automatic Transmit Power

Automatic Transmit Power:	○ Enabled ● Disabled
Power Level Assignment Method:	○ Automatic ● Fixed
Fixed Power Level:	5

802.11bg Profile Thresholds

Interference (0-100%):	10
Clients (1-75):	12
Noise (-127 to 0 dBm):	-70
Coverage (3-50 dBm):	12
Utilization (0-100%):	80
Coverage Exception Level (0-100%):	25
Data Rate (1-1000 Kbps):	1000
Client Minimum Exception Level (1-75):	3

802.11bg Noise/Interference/Rogue Monitoring Channels

Monitoring Channels:	Country Channels

802.11bg Monitor Intervals

Signal Measurement (60-3600 sec):	300
Noise Measurement (60-3600 sec):	300
Load Measurement (60-3600 sec):	300
Coverage Measurement (60-3600 sec):	300

802.11bg Voice Settings

Admission Control (ACM):	○ Enabled ● Disabled
Expedited Bandwidth:	○ Enabled ● Disabled
Metrics Collection:	○ Enabled ● Disabled

802.11bgn Settings

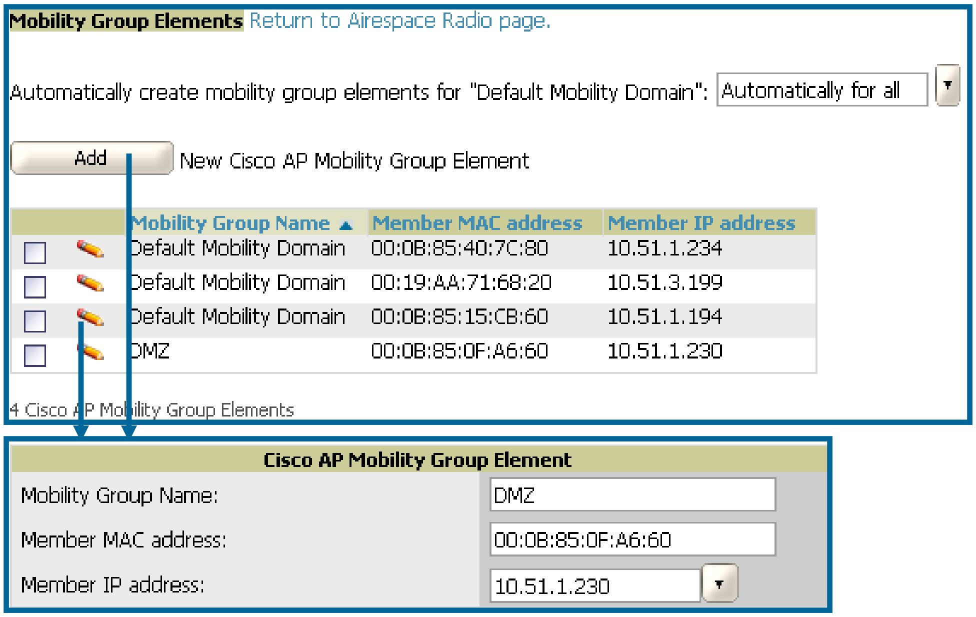
11n Mode:	● Enabled ○ Disabled
MCS Index 0 (7 Mbps):	● Enabled ○ Disabled
MCS Index 1 (14 Mbps):	● Enabled ○ Disabled
MCS Index 2 (21 Mbps):	● Enabled ○ Disabled
MCS Index 3 (29 Mbps):	● Enabled ○ Disabled
MCS Index 4 (43 Mbps):	● Enabled ○ Disabled
MCS Index 5 (58 Mbps):	● Enabled ○ Disabled
MCS Index 6 (65 Mbps):	● Enabled ○ Disabled
MCS Index 7 (72 Mbps):	● Enabled ○ Disabled
MCS Index 8 (14 Mbps):	● Enabled ○ Disabled
MCS Index 9 (29 Mbps):	● Enabled ○ Disabled
MCS Index 10 (43 Mbps):	● Enabled ○ Disabled
MCS Index 11 (58 Mbps):	● Enabled ○ Disabled
MCS Index 12 (87 Mbps):	● Enabled ○ Disabled
MCS Index 13 (116 Mbps):	● Enabled ○ Disabled
MCS Index 14 (130 Mbps):	● Enabled ○ Disabled
MCS Index 15 (144 Mbps):	● Enabled ○ Disabled

Setting	Default	Description
LWAPP Transport Mode	Layer 3	Specifies the layer that the controller will use to communicate with the APs. In Layer 2 mode the controller uses a proprietary protocol to communicate with the APs. In layer 3 mode the controller will use IP addresses to communicate to the APs.
Aggressive Load Balancing	Disabled	Enable or Disable Aggressive Load Balancing.
RF Network Name	Default RF Network	The RF Network Name determines which Radio Resource Management packets will be accepted by the AP. For the receiving AP to accept a RRM packet the RF Network Name must be the same as the transmitting AP.
Authentication Response Timeout (5-60 secs)	10	The amount of time, in seconds, before an authentication response times out.

Setting	Default	Description
User Idle Timeout (seconds)	300	The amount of time, in seconds, a user must idle before the controller will disassociate them.
ARP Timeout (seconds)	300	The lifetime, in seconds, of ARP information.
802.3x Flow Control Mode	Disabled	Enable or disable 802.3x Flow Control.
Peer to Peer Blocking Mode	Disabled	Enable or disable Peer to Peer Blocking mode. When disabled the Airespace switch will route traffic between local clients. When disabled the controller will send data through a higher level router even if both clients are connected to it.
Over the Air Provisioning of AP	Disabled	Enable or disable provisioning APs over the air.
AP Fallback	Disabled	Determines the behavior of the AP when communication with the controller is lost.
Apple Talk Bridging	Disabled	Enable or disable Apple talk bridging.
Fast SSID change	Disabled	Enable or disable Fast SSID changing. Users will not get new IPs from the DHCP server when they change SSIDs if enabled.
Wireless Packet Sniffer Server	None	Specifies the address of a Wireless Packet Sniffer Server for use with the controller.
Ethernet Multicast Support	Disabled	Enable or disable support for Ethernet multicasting.
Protection Type	None	Defines the wireless Protection Type.
*AP Neighbor Authentication Trigger Threshold **	1	Defines the trigger threshold for AP Neighbor authentication when Protection type AP Authentication is selected. *Note: This field is only visible if Protection Type "AP Authentication" is selected.*
Default Mobility Domain Name	Default Mobility Domain	User defined name for the Mobility Group.
Short Preamble	Enabled	A short preamble may improve throughput performance, but a long preamble is more likely to be compatible with older devices.

- To Configure Group Mobility settings locate the "Global Controller Settings" area on the **Groups→Airespace Radio** page. Click the "Cisco Airespace Mobility Groups Page" link.

Figure 42. "Groups→Airespace Radio Settings" page



Mobility Group Elements Return to Airespace Radio page.

Automatically create mobility group elements for "Default Mobility Domain": Automatically for all

Add New Cisco AP Mobility Group Element

		Mobility Group Name ▲	Member MAC address	Member IP address
□	✎	Default Mobility Domain	00:0B:85:40:7C:80	10.51.1.234
□	✎	Default Mobility Domain	00:19:AA:71:68:20	10.51.3.199
□	✎	Default Mobility Domain	00:0B:85:15:CB:60	10.51.1.194
□	✎	DMZ	00:0B:85:0F:A6:60	10.51.1.230

4 Cisco AP Mobility Group Elements

Cisco AP Mobility Group Element

Mobility Group Name:	DMZ
Member MAC address:	00:0B:85:0F:A6:60
Member IP address:	10.51.1.230

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

- To configure Bridge settings locate the Bridge settings section of the **Groups→ Airespace Radio** page.

Setting	Default	Description
Zero Touch Configuration	Enabled	Enable or disable Cisco's "Zero Touch Configuration" on the controller. Zero Touch Configuration will configure numerous settings including if the device should be a RAP or a PAP, backhaul interface and channel and security options between the controller and AP.
Bridge Shared Secret	None	The shared secret used by Bridges in the group.
Bridge Data Rate	18	The data rate used by bridges in the group.
Ethernet Bridging	Disabled	Enables or disables Ethernet bridging.

- To configure Web Login Settings locate the "Web Login Settings" section of the **Groups→Airespace Radio** page.

Setting	Default	Description
Web Authentication Type	Internal	Dropdown menu that defines the Web Authentication type. *Internal:* Web login information is authenticated locally on the controller. *External:* Web login information is authenticated against an external authentication server.
Display Manufacturer Logo	Yes	Enables or disables displaying the Manufacturers logo on the web authentication page.
Redirect URL after login	None	The URL users will be redirected to after they have logged in.
Web Login Page Title	None	The title displayed for the web login page.
Web Login Page Message	None	The message displayed to users on the web login page.
Web Authentication URL	None	The web authentication URL users visit when logging in.
External Web Authentication Server 1-4	None	The IP address or Hostname of the external web authentication servers.

- To configure Global RF settings locate the Global RF settings section of the **Groups→Airespace Radio** page.

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

- To configure RF Channel Assignment settings locate the RF Channel Assignment section of the **Groups→Cisco Airespace Radio** page.

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

- To configure Automatic Transmit Power settings locate the Automatic Transmit Power section of the **Groups→Cisco Airespace Radio** page.

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

- To configure Automatic Transmit Power settings locate the Automatic Transmit Power section of the **Groups→Cisco Airespace Radio** page.

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

- To configure Noise/Interference/Rogue Monitoring Channels locate the Noise/Interference/Rogue Monitoring Channels section of the **Groups→Cisco Airespace Radio** page.

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

- To configure the Monitor intervals locate the Monitor Intervals section of the **Groups→Cisco Airespace Radio** page.

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

Setting	Default	Description
Coverage Measurement (60-3600 sec)	300	Specifies how often the controller should monitor the AP Coverage measurements.

- To configure the Voice Settings locate the Voice Settings section of the **Groups→Cisco Airespace Radio** page.

Setting	Default	Description
Admission Control	Disabled	Denies network access under congestion conditions.
Max RF Bandwidth	75%	Range from 40 to 85%; AP rejects new calls on this radio band after this value is reached.
Reserved Roaming Bandwidth	6%	Range from 0 to 25%; reserved for roaming voice clients.
Metrics Collection	Disabled	Collects traffic stream metrics between AP and client.

- To configure 802.11h parameters locate the “802.11a 802.11h Parameters” section of the **Groups→Cisco Airespace Radio** page. 802.11h settings are only neccassary in Europe.

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

- Click “Save” when completed.

- To configure 802.11an and 802.11bgn parameters locate the “802.11an/bng Parameters” section of the **Groups→Cisco Airespace Radio** page.

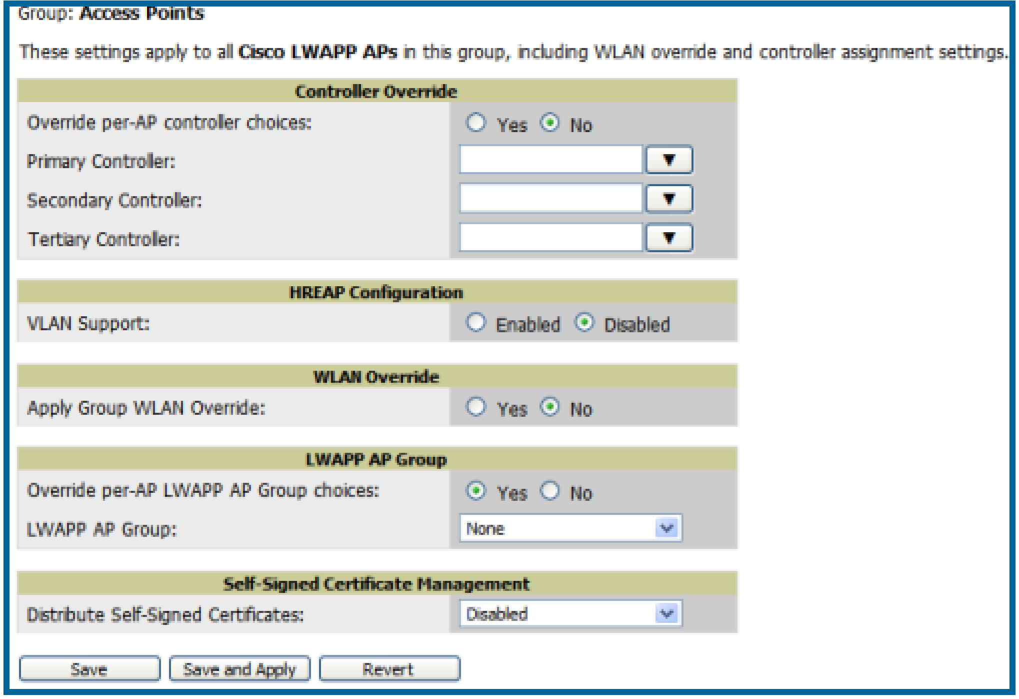
Setting	Default	Description
11n Mode	Enabled	Enables or disables the 802.11nt option on the controller.
MCS Index (0-15)	Enabled	Enables or disables the MCS index on the controller.

- Click “Save” when completed.

Configuring LWAPP AP Settings

Navigate to the **Groups→LWAPP AP Settings** page to configure LWAPP AP specific settings. The settings on this page will apply to all thin APs in the group even if the controller is in another group.

Figure 43. "Groups→LWAPP AP Settings" page



Group: **Access Points**

These settings apply to all **Cisco LWAPP APs** in this group, including WLAN override and controller assignment settings.

Controller Override	
Override per-AP controller choices:	○ Yes ● No
Primary Controller:	
Secondary Controller:	
Tertiary Controller:	

HREAP Configuration	
VLAN Support:	○ Enabled ● Disabled

WLAN Override	
Apply Group WLAN Override:	○ Yes ● No

LWAPP AP Group	
Override per-AP LWAPP AP Group choices:	● Yes ○ No
LWAPP AP Group:	None

Self-Signed Certificate Management	
Distribute Self-Signed Certificates:	Disabled

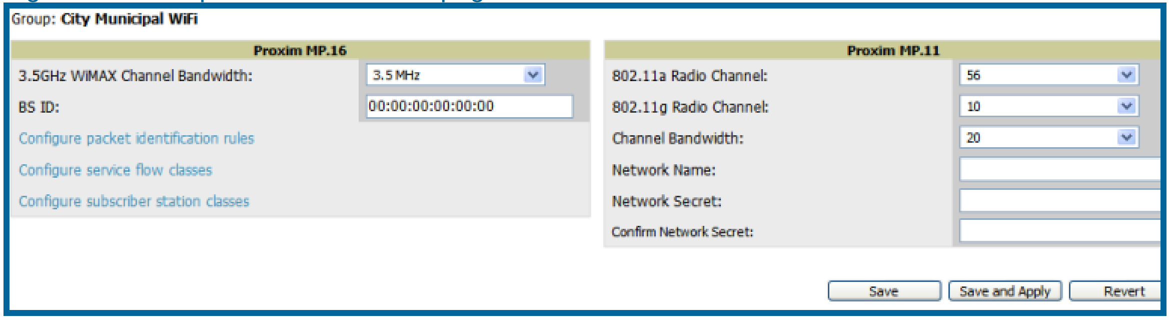
Setting	Default	Description
Override per-AP controller choices	No	Allows you to define the primary, secondary and tertiary controller for all of the APs in the group.
Primary/Secondary/Tertiary Controller	None	Dropdown menu allowing you to specify the primary, secondary and tertiary controller for all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

Setting	Default	Description
Distribute Self-Signed Certificates	Disabled	Enabled distribution by groups of controllers, mobility groups or primary/secondary/tertiary controllers.

Configuring Group PTMP/WiMAX Settings

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

Figure 44. "Groups→PTMP/WiMAX" page



Group: City Municipal WiFi

Proxim MP.16

3.5GHz WiMAX Channel Bandwidth: 3.5 MHz

BS ID: 00:00:00:00:00:00

Configure packet identification rules

Configure service flow classes

Configure subscriber station classes

Proxim MP.11

802.11a Radio Channel: 56

802.11g Radio Channel: 10

Channel Bandwidth: 20

Network Name:

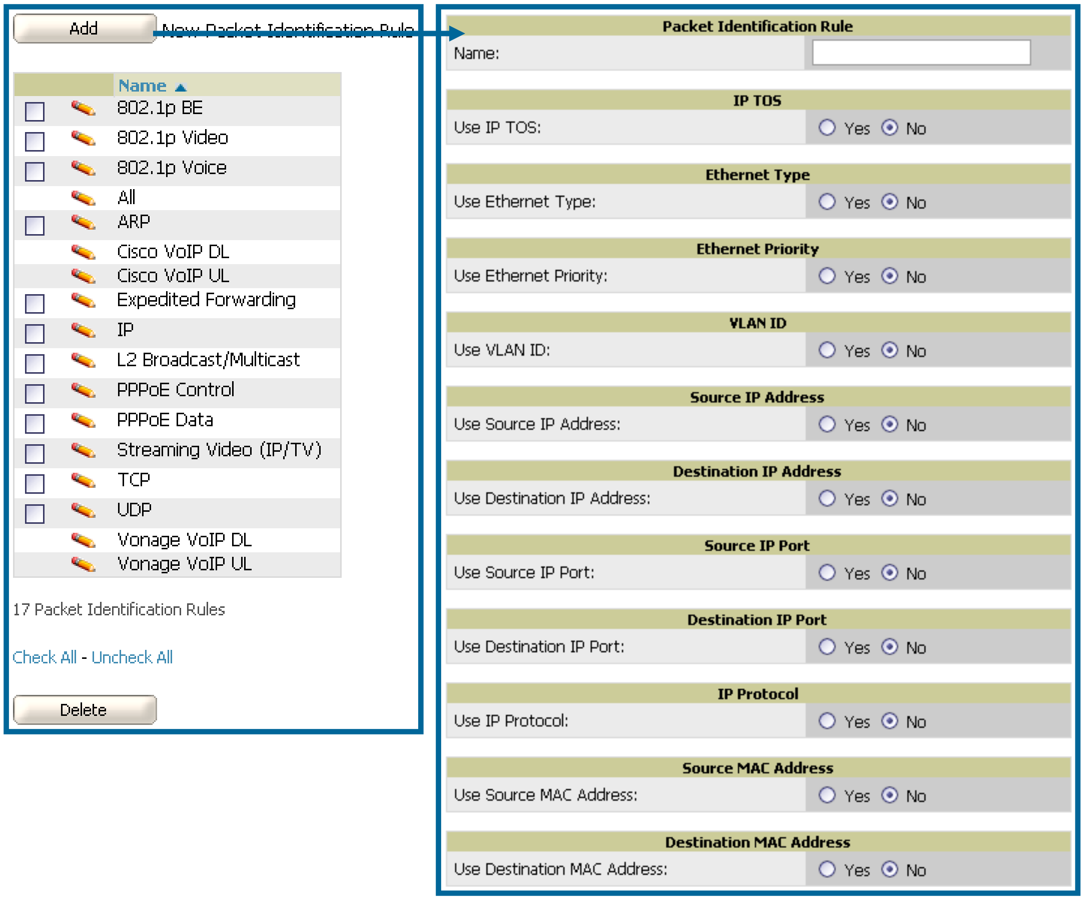
Network Secret:

Confirm Network Secret:

Setting	Default	Description
3.5GHz WiMAX Channel Bandwidth (Proxim MP.16)	3.5GHz	The frequency used by the WiMAX devices in the group.
BSID (Proxim MP.16)	00:00:00:00:00:00	The BSID used by the subscriber stations in the group. To define the BSID for a base station please see its APS/Devices→Manage page.
802.11a Radio Channel (Proxim MP.11)	56	The channel used for 802.11a radios by the devices in this group.
802.11g Radio Channel (Proxim MP.11)	10	The channel used for 802.11g radios by the devices in this group.
Channel Bandwidth (Proxim MP.11)	20	The channel bandwidth used by the devices in this group.
Network Name (Proxim MP.11)	None	Network name (two to 32 characters in length).
Network Secret and Confirm Network Secret (Proxim MP.11)	None	Shared password to authenticate to network.

- To configure packet identification rules please click the "Configure packet identification rules" link on the **Groups→PTMP/Wimax** page. Packet identification rules are used to define which packets will match a subscriber station class.

Figure 45. “Groups→PTMP/WiMAX Configuring Packet Identification Rules” page



Add New Packet Identification Rule

		Name ▲
□	✎	802.1p BE
□	✎	802.1p Video
□	✎	802.1p Voice
	✎	All
□	✎	ARP
	✎	Cisco VoIP DL
	✎	Cisco VoIP UL
□	✎	Expedited Forwarding
□	✎	IP
□	✎	L2 Broadcast/Multicast
□	✎	PPPoE Control
□	✎	PPPoE Data
□	✎	Streaming Video (IP/TV)
□	✎	TCP
□	✎	UDP
	✎	Vonage VoIP DL
	✎	Vonage VoIP UL

17 Packet Identification Rules

Check All - Uncheck All

Delete

Packet Identification Rule

Name:

IP TOS

Use IP TOS: ○ Yes ◉ No

Ethernet Type

Use Ethernet Type: ○ Yes ◉ No

Ethernet Priority

Use Ethernet Priority: ○ Yes ◉ No

VLAN ID

Use VLAN ID: ○ Yes ◉ No

Source IP Address

Use Source IP Address: ○ Yes ◉ No

Destination IP Address

Use Destination IP Address: ○ Yes ◉ No

Source IP Port

Use Source IP Port: ○ Yes ◉ No

Destination IP Port

Use Destination IP Port: ○ Yes ◉ No

IP Protocol

Use IP Protocol: ○ Yes ◉ No

Source MAC Address

Use Source MAC Address: ○ Yes ◉ No

Destination MAC Address

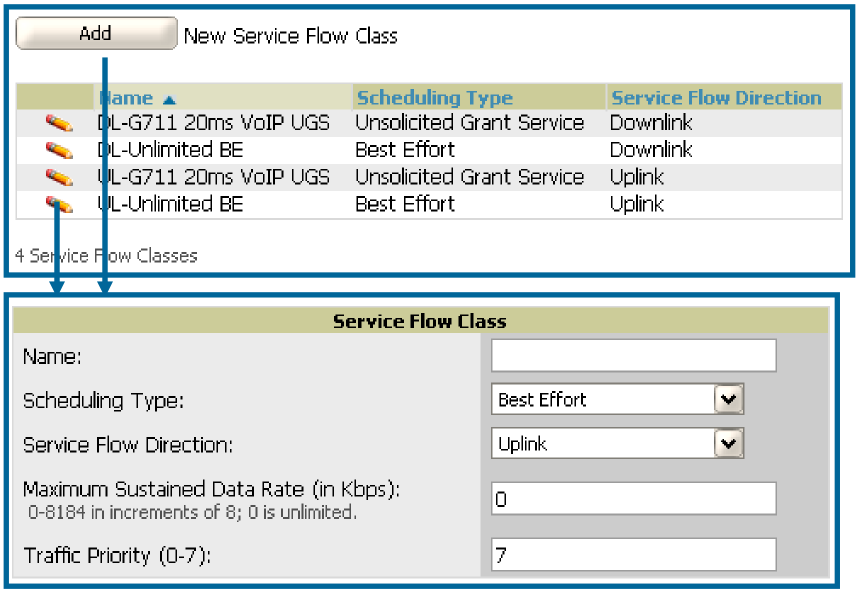
Use Destination MAC Address: ○ Yes ◉ No

Setting	Default	Description
Name	None	Text field that defines a name for the PIR. The name should be meaningful and descriptive. The name will be used to define the subscriber station class.
Use IP TOS	No	Identify packets based on IP Type-of-Service for the PIR.
Minimum TOS Value (positive integer)	0	Specifies the minimum TOS used to identify packets.
Maximum TOS Value (positive integer)	0	Specifies the maximum TOS used to identify packets
Mask (positive integer)	0	Specifies the TOS mask used to identify packets.
Use Ethernet Type	No	Identify packets based on Ethernet type settings.
Ethernet Type	DIX SNAP	Dropdown menu used to specify the Ethernet types used to identify a packet.
Ethernet Value (positive integer)	0	Identify packets that have a specific ethernet value.
Ethernet Priority	No	Identify packets based on Ethernet Priority settings.
Ethernet Priority Minimum (0-7)	None	Identify packets that meet a minimum priority.

Setting	Default	Description
Ethernet Priority Maximum (0-7)	0	Identify packets that meet a maximum priority.
Use VLAN ID	No	Identify 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	Identify 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	Identify 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	Identify packets based on IP protocol.
IP Protocol (0-255)	None	Identify packets that have a specific IP Protocol value.
Use Source MAC Address	No	Identify packets based on Source MAC address.
Source MAC Address	None	Packets from this MAC address will match this PIR.
Use Destination MAC Address	No	Identify packets based on Destination MAC address
Destination MAC Address	None	Packets to this destination MAC address will match this PIR.

- To configure service flow classes please click the “Configure service flow classes” link on the **Groups→PTMP/Wimax** page. Service flow classes are used to describe how the device will handle traffic.

Figure 46. “Groups→PTMP/WiMAX Configuring Service Flow Classes” page



	Name ▲	Scheduling Type	Service Flow Direction
✎	DL-G711 20ms VoIP UGS	Unsolicited Grant Service	Downlink
✎	DL-Unlimited BE	Best Effort	Downlink
✎	UL-G711 20ms VoIP UGS	Unsolicited Grant Service	Uplink
✎	UL-Unlimited BE	Best Effort	Uplink

4 Service Flow Classes

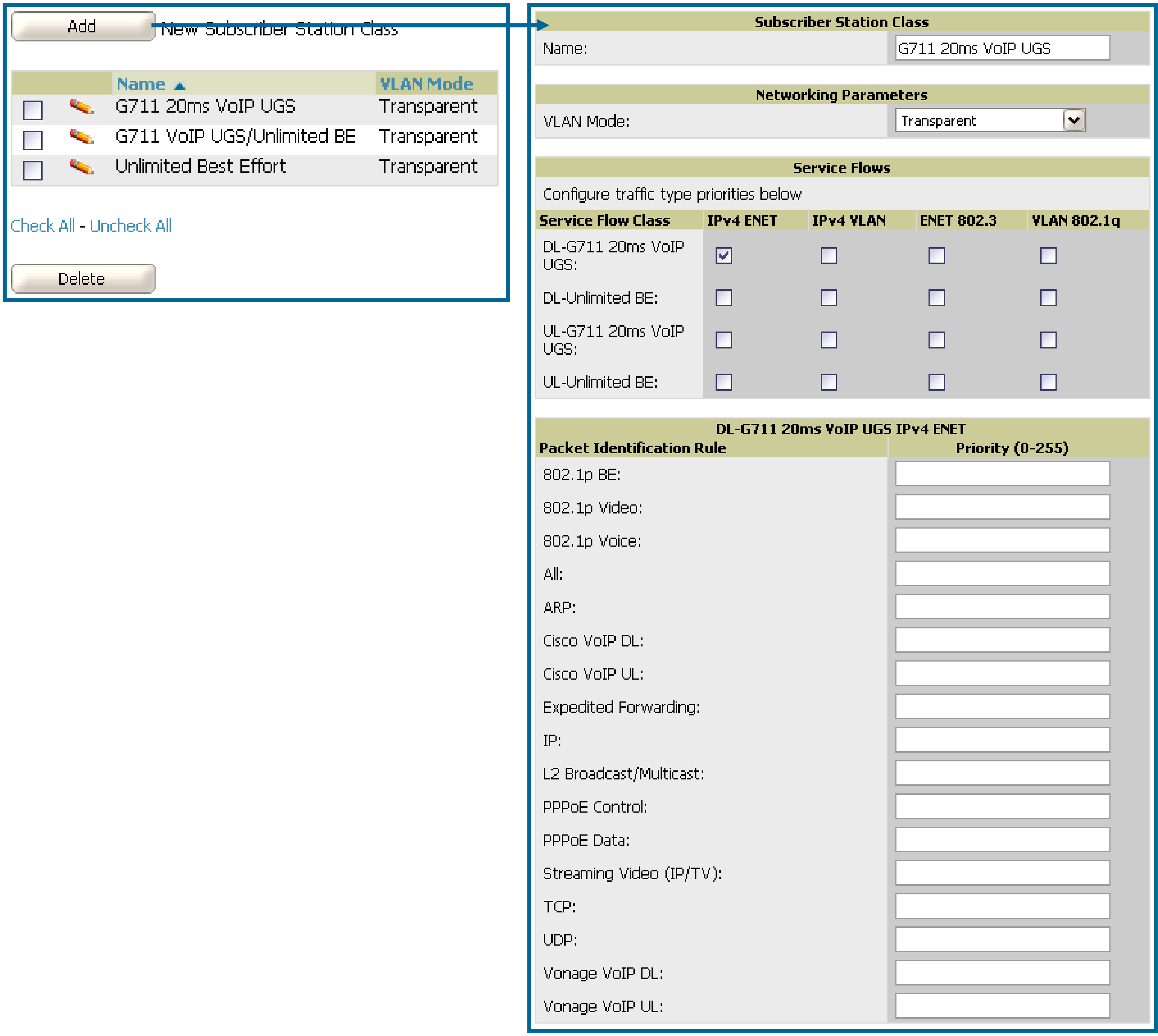
Service Flow Class

Name:	
Scheduling Type:	Best Effort
Service Flow Direction:	Uplink
Maximum Sustained Data Rate (in Kbps): 0-8184 in increments of 8; 0 is unlimited.	0
Traffic Priority (0-7):	7

Setting	Default	Description
Name	None	Text field that defines the name of the Service Flow Class. The name should be meaningful and descriptive. The name will be used to define the subscriber station class.
Scheduling Type	Best Effort	Dropdown menu that specifies the scheduling priority for the Service Flow Class. Best Effort: Maximum sustained data rate and traffic priority Unsolicitied Grant Servece: Maximum sustained data rate, maximum latency and tolerable jitter.
Service Flow Direction	Uplink	Defines the direction of service.
Maximum Sustained Data Rate (in Kbps)	0	The maximum sustained data rate for this service class. The base station will not allow the data rate to exceed this value.
Traffic Priority (0-7)	7	The priority of the traffic from 0 – 7 with 7 getting the highest priority.

- To configure subscriber station classes please click the "Configure subscriber station classes" link on the **Groups→PTMP/Wimax** page. Subscriber station classes link packet identification rules and service flow classes.

Figure 47. “Groups→PTMP/WiMAX Configuring Subscriber Station Classes” page



		Name ▲	VLAN Mode
□	✎	G711 20ms VoIP UGS	Transparent
□	✎	G711 VoIP UGS/Unlimited BE	Transparent
□	✎	Unlimited Best Effort	Transparent

Subscriber Station Class

Name: G711 20ms VoIP UGS

Networking Parameters

VLAN Mode: Transparent

Service Flows

Configure traffic type priorities below

Service Flow Class	IPv4 ENET	IPv4 VLAN	ENET 802.3	VLAN 802.1q
DL-G711 20ms VoIP UGS:	☑	□	□	□
DL-Unlimited BE:	□	□	□	□
UL-G711 20ms VoIP UGS:	□	□	□	□
UL-Unlimited BE:	□	□	□	□

DL-G711 20ms VoIP UGS IPv4 ENET

Packet Identification Rule	Priority (0-255)
802.1p BE:	
802.1p Video:	
802.1p Voice:	
All:	
ARP:	
Cisco VoIP DL:	
Cisco VoIP UL:	
Expedited Forwarding:	
IP:	
L2 Broadcast/Multicast:	
PPPoE Control:	
PPPoE Data:	
Streaming Video (IP/TV):	
TCP:	
UDP:	
Vonage VoIP DL:	
Vonage VoIP UL:	

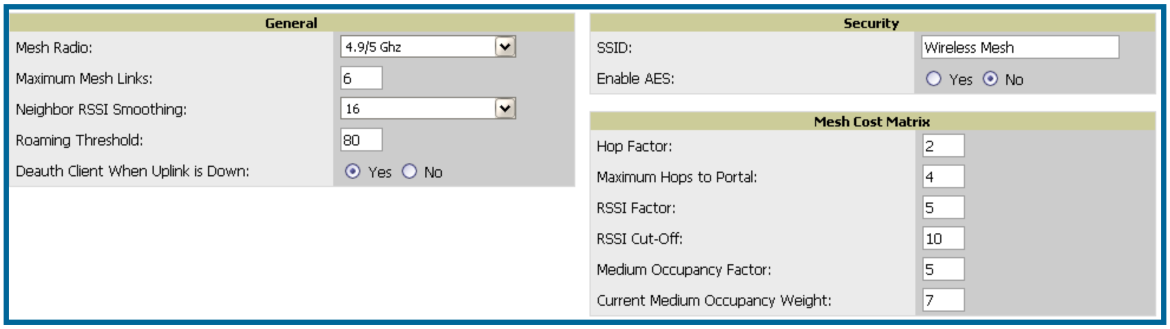
Setting	Default	Description
Name	None	Text field that defines the name of the Subscriber Station Class. The name should be meaningful and descriptive.
VLAN Mode	Transparent	Defines the VLAN mode.

Setting	Default	Description
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.

Configuring Mesh Radio Settings

Navigate to the **Groups→Proxim Mesh Radio Settings** page to configure Mesh specific radio settings.

Figure 48. "Groups→Mesh Radio Settings" page



General

Mesh Radio:	4.9/5 Ghz
Maximum Mesh Links:	6
Neighbor RSSI Smoothing:	16
Roaming Threshold:	80
Deauth Client When Uplink is Down:	● Yes ○ No

Security

SSID:	Wireless Mesh
Enable AES:	○ Yes ● No

Mesh Cost Matrix

Hop Factor:	2
Maximum Hops to Portal:	4
RSSI Factor:	5
RSSI Cut-Off:	10
Medium Occupancy Factor:	5
Current Medium Occupancy Weight:	7

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

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

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

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

- The Mesh Count Matrix sections contains settings for hop factor and maximum hops to portal, RSSI factor and cut-off, medium occupancy factor and current medium occupance weight.

Setting	Default	Description

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.

Configuring Colubris Advanced Settings (Optional)

The **Groups→Colubris** page provides a mechanism to fetch a “master” AP’s configuration and apply that configuration to all access points that match the “master’s” model in the group. The **Groups→Colubris Advanced** page requires that Colubris APs be present in the group. If Colubris APs are not yet discovered or placed in the group please see the Discovery of APs section of the User’s Guide.

- OV3600 fetches five categories of configuration items from the master AP:
  1. Configuration items that are read-only (e.g., serial number).
  2. Configuration items that are AP specific (e.g., primary IP address).
  3. Configuration items that are configurable on the **APs/Devices→Manage** page or on the group management pages.
  4. Configuration items that should always be applied to all the APs in the Group.
  5. Configuration items that should only be applied to all the APs in the group in certain situations.

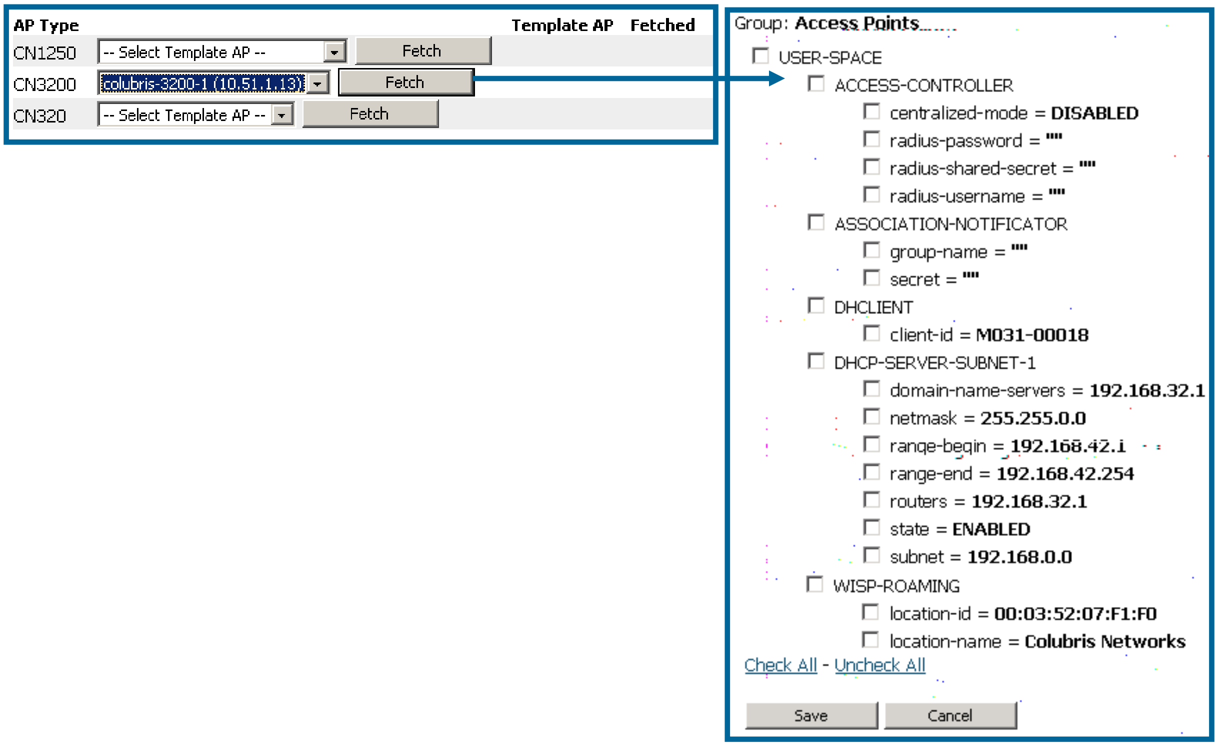
  This page displays the configuration items in category 5. Select the items that should be applied to all APs in this group.

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

- Browse to the **Groups→List** page and select the group you wish to manage and then navigate to the **Groups→Colubris** page.

- Select the “master” AP in the drop down menu whose configuration you wish to apply to all applicable APs in the group. The Fetch button instructs OV3600 to immediately fetch the “master” AP’s configuration.

Figure 49. Fetching a Colubris Template



AP Type	Template AP		Fetched
CN1250	-- Select Template AP --	Fetch	
CN3200	colubris-3200-1 (10.51.1.13)	Fetch	
CN320	-- Select Template AP --	Fetch	

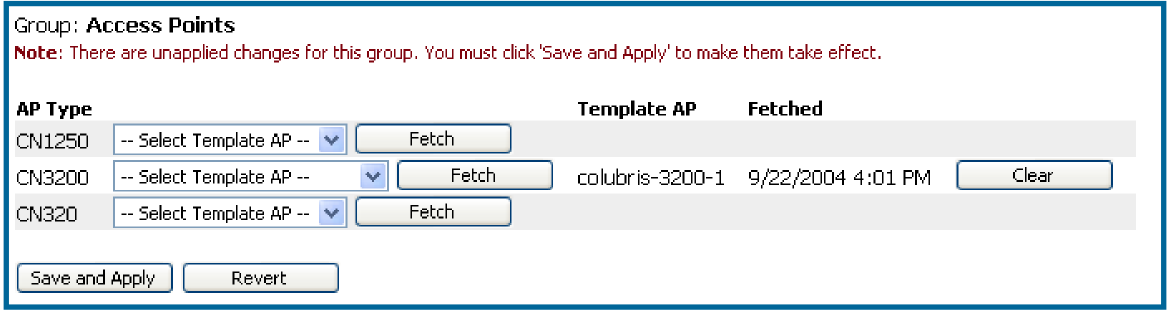
Group: **Access Points**

- □ USER-SPACE
  - □ ACCESS-CONTROLLER
    - □ centralized-mode = **DISABLED**
    - □ radius-password = **""**
    - □ radius-shared-secret = **""**
    - □ radius-username = **""**
  - □ ASSOCIATION-NOTIFICATOR
    - □ group-name = **""**
    - □ secret = **""**
  - □ DHCLIENT
    - □ client-id = **M031-00018**
  - □ DHCP-SERVER-SUBNET-1
    - □ domain-name-servers = **192.168.32.1**
    - □ netmask = **255.255.0.0**
    - □ range-begin = **192.168.42.1**
    - □ range-end = **192.168.42.254**
    - □ routers = **192.168.32.1**
    - □ state = **ENABLED**
    - □ subnet = **192.168.0.0**
  - □ WISP-ROAMING
    - □ location-id = **00:03:52:07:F1:F0**
    - □ location-name = **Colubris Networks**

Check All - Uncheck All

- Click the Save button to save the configuration items in category 4, and any items from category 5 you selected. OV3600 will automatically redirect you back to the **Groups→Colubris** page.

Figure 50. "Groups→Colubris" page



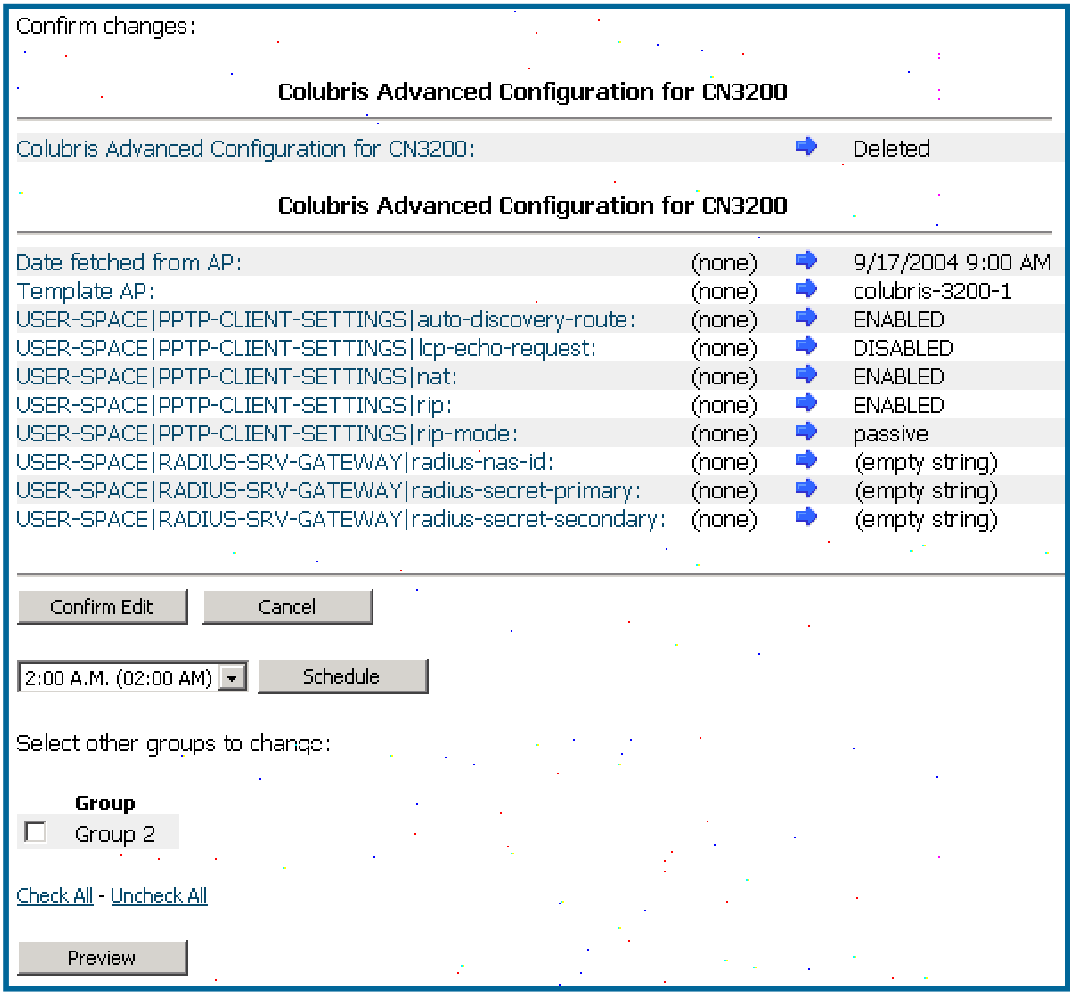
Group: **Access Points**

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

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

- Click the Save and Apply button to see the list of configuration items you selected from category 4.

Figure 51. Confirming changes



Confirm changes:

Colubris Advanced Configuration for CN3200

Colubris Advanced Configuration for CN3200:		→	Deleted

Colubris Advanced Configuration for CN3200

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

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

Select other groups to change:

	Group
☐	Group 2

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

Configuring Group MAC Access Control Lists (Optional)

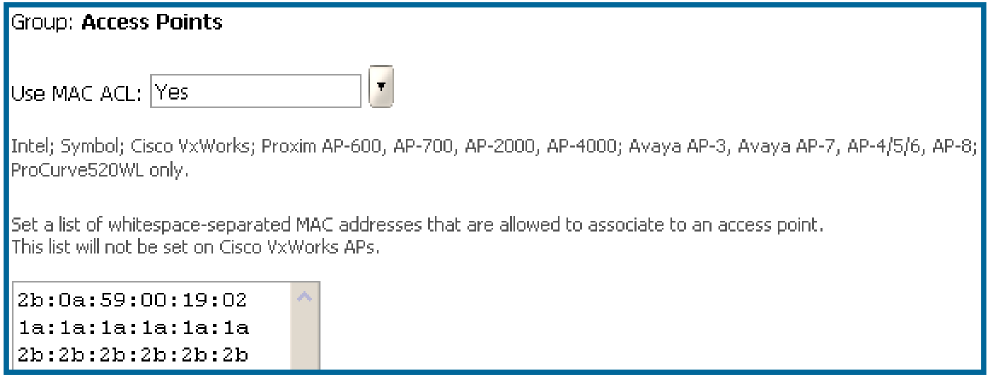
If you use Symbol 4121/4131, Intel 2011/2011b, Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP-3/4/5/6/7/8, or ProCurve 520WL wireless access points, OV3600 enables you to specify the MAC Addresses of devices that are permitted to associate with APs in the Group. Other devices will not be able to associate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

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

To use the MAC ACL function:

- Browse to the **Groups→MAC ACL** page

Figure 52. "Groups→MAC ACL" page



Group: **Access Points**

Use MAC ACL: Yes

Intel; Symbol; Cisco VxWorks; Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL only.

Set a list of whitespace-separated MAC addresses that are allowed to associate to an access point.
This list will not be set on Cisco VxWorks APs.

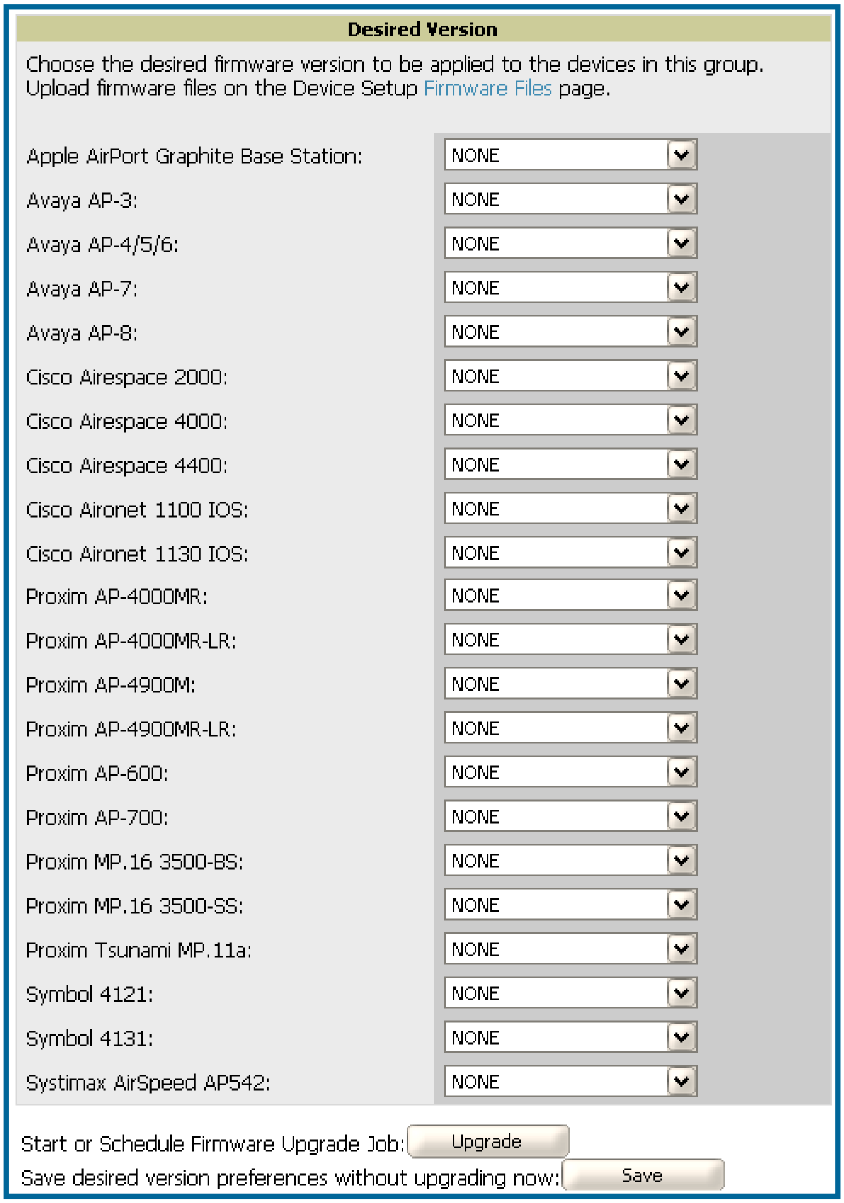
```
2b:0a:59:00:19:02
1a:1a:1a:1a:1a:1a
2b:2b:2b:2b:2b:2b
```

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

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

OV3600 allows you to define the minimum firmware version for each AP type in a group on the **Groups→Firmware** page. At the time that you define the minimum version, OV3600 will automatically upgrade all eligible APs. When you add APs into the group in the future you will be able to upgrade manually upgrade APs. An AP's firmware is not automatically upgraded when it is added to a group.

Figure 53. "Groups→Firmware" page



Desired Version

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

Apple AirPort Graphite Base Station:	NONE
Avaya AP-3:	NONE
Avaya AP-4/5/6:	NONE
Avaya AP-7:	NONE
Avaya AP-8:	NONE
Cisco Airespace 2000:	NONE
Cisco Airespace 4000:	NONE
Cisco Airespace 4400:	NONE
Cisco Aironet 1100 IOS:	NONE
Cisco Aironet 1130 IOS:	NONE
Proxim AP-4000MR:	NONE
Proxim AP-4000MR-LR:	NONE
Proxim AP-4900M:	NONE
Proxim AP-4900MR-LR:	NONE
Proxim AP-600:	NONE
Proxim AP-700:	NONE
Proxim MP.16 3500-BS:	NONE
Proxim MP.16 3500-SS:	NONE
Proxim Tsunami MP.11a:	NONE
Symbol 4121:	NONE
Symbol 4131:	NONE
Systimax AirSpeed AP542:	NONE

Start or Schedule Firmware Upgrade Job:

Save desired version preferences without upgrading now:

- Browse to the **Groups→Firmware** page
- 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 need to browse to the **Device Setup→Firmware** page to upload the firmware files to OV3600.

- Click “Upgrade” to apply firmware preferences to devices in the group. Please see the firmware upgrade help under APs/Devices→Manage page for detailed help on Firmware job options
- Click “Save” to save the firmware file as the desired version for the group.
- If you have opted to assign an external TFTP server on a per-group basis on the **Device Setup→Firmware** page you can enter the IP address in the “Firmware Upgrade Options” field on the top of this page.

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 will automatically be placed in the default group if OV3600 is set to “Automatically Monitor/Manage New Devices” on the **OV3600 Setup→General** page.

- Browse to the **Groups→List** page (see Figure 27. "Groups→List" page above).
- From the list of Groups, check the *Default* radio button next to the Group you would like to make the default.

Creating New Groups

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

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

To create a new Group by duplicating an existing Group:

- Browse to the **Groups→List** page
- Select the existing Group to be duplicated and click the *Duplicate* link.
- OV3600 will automatically create a new Group with the name “Copy of [Group Name]” and will direct you to the **Groups→Basic** page for you to review and modify any settings.

To create an entirely new Group:

- Browse to the **Groups→Create** page
- Enter a name for the new Group in the *Name* field and click “Create Group”
- OV3600 will automatically create a new Group with the specified name and will direct you to the **Groups→Basic** page. All configurations settings will be set to the default values.

Deleting a Group

To delete an existing Group from OV3600’s database:

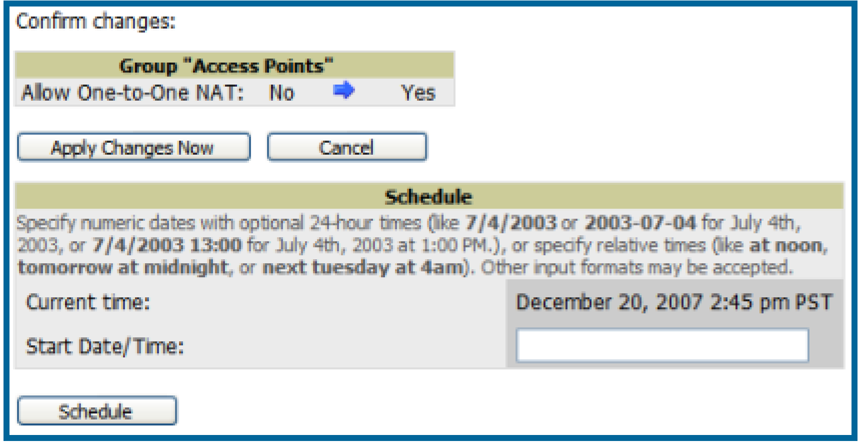
- Browse to the **Groups→List** page
- Ensure that the Group you wish to delete is not marked as the “default” group. *OV3600 will not permit you to delete the current default Group.*
- Ensure there are no devices in the Group you wish to delete. *OV3600 will not permit you to delete a Group that still contains managed devices. You must move all devices to other Groups before deleting a Group.*
- Select the checkbox and click delete.

Changing Multiple Group Configurations

To make any changes to an existing Group's configuration:

- Browse to the **Groups→List** page
- Click the Manage link 🔧 for the Group you wish to edit.
- OV3600 will automatically direct you to the **Groups→Basic** page.
- Select the fields to be edited on the Basic page or navigate to Radio, Security, VLANs, or MAC ACL and edit fields on these pages. Use the "Save" button to store the changes prior to applying them.
- When all changes for the group are complete click the "Save and Apply" button.

Figure 54. OV3600 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.

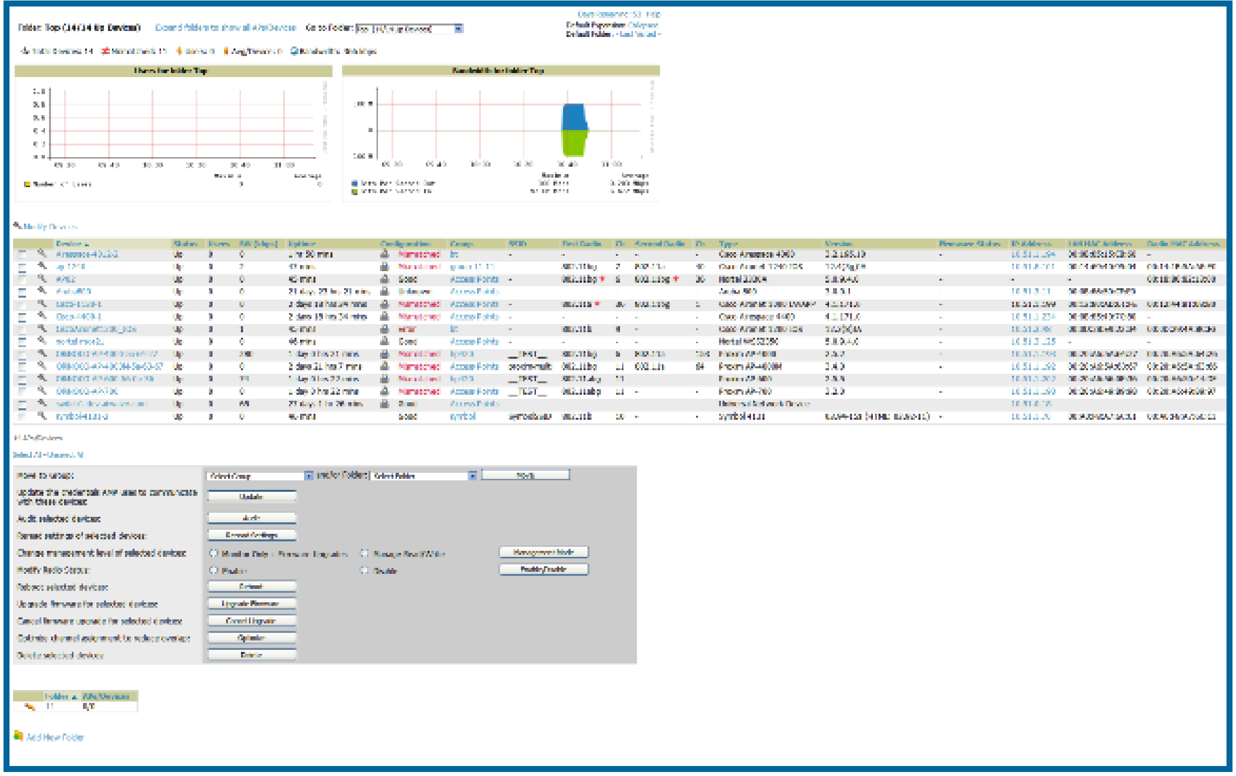
Current time:	December 20, 2007 2:45 pm PST
Start Date/Time:	

- OV3600 will display a Configuration Change screen confirming the changes that will be applied to the Group's settings.
- There are several action possibilities from within this confirmation page
  1. Apply Changes Now – will apply the changes immediately to access points within the group. If you wish to edit multiple groups you must use the Preview button.
  2. Schedule – will schedule the changes to be applied to this group in the future. Enter the desired change date in the "Start Date/Time field." OV3600 will take the timezone into account for the group if a timezone other than "OV3600 System Time" has been configured on the **Group→Basic** page.
  3. Cancel – will cancel the application of changes (immediately or scheduled). *Note: To completely nullify the change request, click "Revert*" *on one of the group pages after you have hit cancel*.
  4. Apply changes to multiple groups by selecting the appropriate group or groups and clicking Preview.

Modifying Multiple Devices

OV3600 provides a very powerful utility which modifies all or a subset of access points unrelated to OV3600's normal group construct. This utility provides the ability to simultaneously delete multiple devices, migrate multiple devices to another group and/or folder, update credentials and optimize channels. To modify multiple devices navigate to the **APs/Devices→List**, **APs/Devices→Up**, **APs/Devices→Down, APs/Devices→Mismatched** or **Groups→Monitor** page and click on the "Modify Devices" link above the list of APs.

Figure 55. Modifying Multiple Devices


Modify Devices
Move to Group:
Update the credentials AMP uses to communicate with these devices
Update
Audit selected devices
Audit
Revert settings of selected devices
Revert Settings
Change management level of selected devices
Monitor Only + Firmware Upgrades
Manage Read/Write
Management Mode
Modify Radio Status
Enable
Disable
Enable/Disable
Reboot selected devices
Reboot
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
Folder
APs/Devices
Add New Folder

- Select the devices you wish to modify and click on the corresponding button.
- You will be taken to a confirmation page that will allow 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 dropdown 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.
- Using the neighbor lists OV3600 is able to optimize channel selection for APs. Select the APs to optimize and OV3600 will minimize the channel interference while giving channel priority to the most heavily used APs.

Action	Description
Delete	*Removes the selected APs from OV3600. The deletes will be performed in the background and may take a minute to be removed from the list.*
Move to Group	Moves the selected APs to a new group or folder. If the AP is in managed mode when it is moved to a new group it will be reconfigured.
Optimize channel assignment to reduce overlap	OV3600 will use the APs neighbor table to determine the optimal channel for the selected APs.

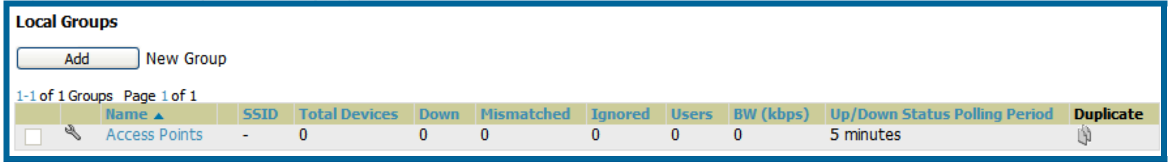
Action	Description
Update the credentials OV3600 uses to communicate with these devices.	Update changes the credentials OV3600 will use to communicate with the device. Update does NOT change the credentials on the AP.
Import settings	Imports settings from the selected device
Ignore selected devices	Ignores selected APs, preventing OV3600 from generating any alerts or including the AP in an up/down count. The device's history will be preserved but it will not be polled. Ignored devices can be seen and taken out of ignore status by navigating to the New Devices page and clicking the "View Ignored Devices" link at the bottom.
Modify Radio Status	Enables or disables the radios on the selected device. Does NOT apply Cisco IOS APs.
Change management level of selected devices	Places the selected APs into management or monitored mode. APs will start to be reconfigured when they are put into Management.
Audit selected devices	Audit will update a number of the AP specific settings OV3600 initially read off of the AP including channel, power, antenna settings and SSL certs. OV3600 recommends using this setting if APs have been updated outside of OV3600. Most settings on the APs/Devices Manage page will be set to the values currently read off of the devices.
Reboot selected devices	Reboots the selected devices. Caution should be used when rebooting devices since it can disrupt wireless users.
Cancel firmware update for selected devices	Cancel any firmware upgrades that are scheduled or in progress for the selected APs.
Upgrade Firmware for selected devices	Upgrade firmware for the selected devices. Please see the firmware upgrade help under APs/Devices→Manage page for detailed help on Firmware job options.
Audit selected devices	Fetches the current configuration from the device and compares it to OV3600s desired configuration. The audit action will cause the Configuration Status to get updated.

Using Global Groups for Group Configuration

To apply group configurations using OV3600's global groups feature, first navigate to the **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.

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 visibile to users of all roles, so they may not contain devices, which can be made visible only to certain roles.

Figure 56. "Groups→List" page



Local Groups

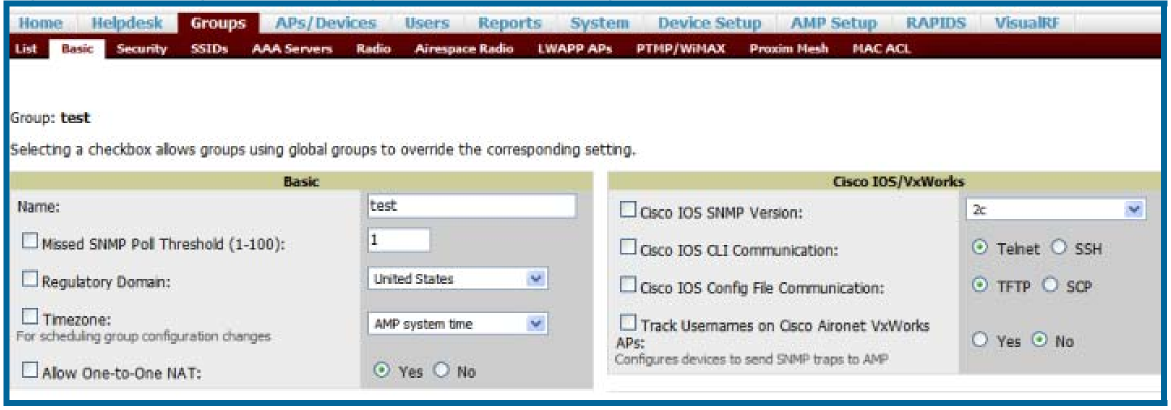
New Group

1-1 of 1 Groups Page 1 of 1

		Name ▲	SSID	Total Devices	Down	Mismatched	Ignored	Users	BW (kbps)	Up/Down Status Polling Period	Duplicate
□		Access Points	-	0	0	0	0	0	0	5 minutes	

To set a group as a global group, navigate to the **Groups→Basic** page of 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, Airespace Radio, LWAPP APs, PTMP/WiMAX, Proxim Mesh and MAC ACL tabs.

Figure 57. "Groups→Basic" page for a Global Group



Group: **test**

Selecting a checkbox allows groups using global groups to override the corresponding setting.

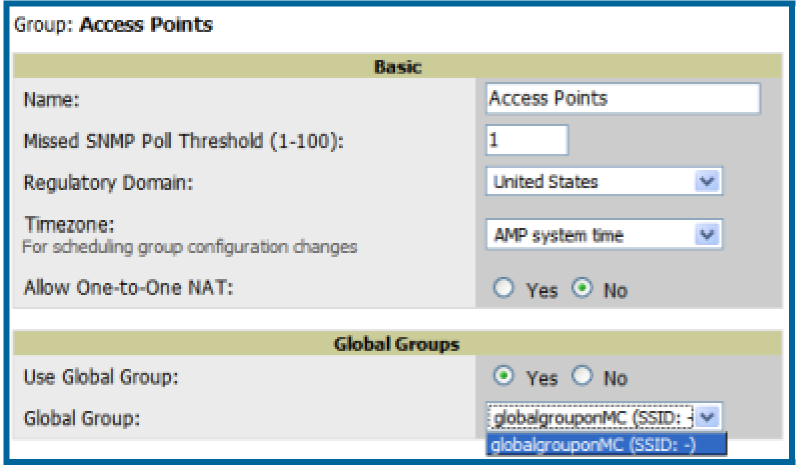
Basic	
Name:	test
□ Missed SNMP Poll Threshold (1-100):	1
□ Regulatory Domain:	United States
□ Timezone: For scheduling group configuration changes	AMP system time
□ Allow One-to-One NAT:	● Yes ○ No

Cisco IOS/VxWorks	
□ Cisco IOS SNMP Version:	2c
□ Cisco IOS CLI Communication:	● Telnet ○ SSH
□ Cisco IOS Config File Communication:	● TFTP ○ SCP
□ Track Usernames on Cisco Aironet VxWorks APs: Configures devices to send SNMP traps to AMP	○ Yes ● No

When a global group configuration is pushed to subscriber groups, 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). Global templates are also configurable as part of global groups; see the **Groups→Templates** section of this user guide 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** 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 dropdown menu. Then click "Save and Apply" to push the configuration from the global group to the subscriber group.

Figure 58. "Groups→Basic" page on a managed OV3600



Group: **Access Points**

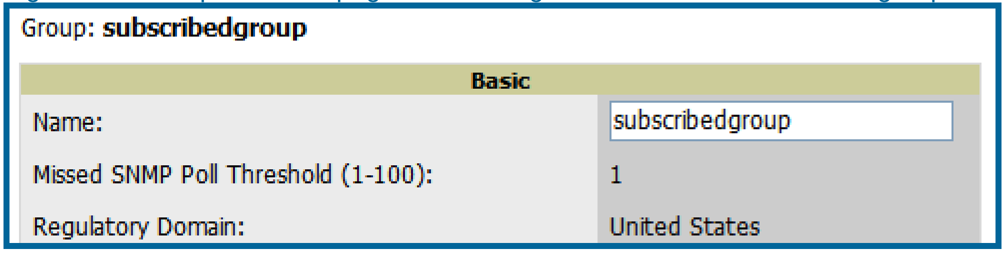
Basic	
Name:	Access Points
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	United States
Timezone: For scheduling group configuration changes	AMP system time
Allow One-to-One NAT:	○ Yes ● No

Global Groups	
Use Global Group:	● Yes ○ No
Global Group:	globalgrouponMC (SSID: -) globalgrouponMC (SSID: -)

Once the configuration is pushed, the unchecked fields from the global group 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 exOV3600le 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 only be altered on the global group.

Figure 59. "Groups→Basic" page on a managed OV3600 for a subscriber group



Group: **subscribedgroup**

Basic	
Name:	subscribedgroup
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	United States

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** page. The global groups feature can also be used with the Master Console. For more information about how this feature works, consult the Master Console section of this user guide.

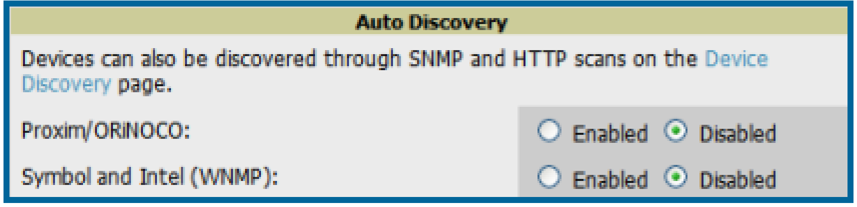
Discovery of Devices Overview

Once you have configured OV3600 on the network and defined at least one Group for APs, the next step is to discover all existing APs connected to your network and assign them to a configuration Group. OV3600 uses four methods to discover APs. OV3600 can discover APs via SNMP/HTTP scanning, Cisco Discovery Protocol (CDP), layer 2 methods (ORiNOCO and Intel/Symbol), and manual entry. OV3600's primary method for discovering APs on your network is to scan specified network segments using SNMP and/or HTTP.

Enabling AP Auto Discovery

- To enable automatic CDP (Cisco and Colubris), Proxim/ORiNOCO and Intel/Symbol (WNMP) scanning browse to the **OV3600 Setup→General** page and locate the Auto Discovery section.

Figure 60. "Setup→General" page (Auto Discovery)



Auto Discovery

Devices can also be discovered through SNMP and HTTP scans on the Device Discovery page.

Proxim/ORiNOCO: ○ Enabled ● Disabled

Symbol and Intel (WNMP): ○ Enabled ● Disabled

- Check the corresponding box for the appropriate Auto Discovery methods relating to your deployed access points. The ORiNOCO and Intel/Symbol methods send packets to the broadcast address and listen ever 30 seconds. The Cisco CDP uses the polling interval configured for each individual switch or router on the OV3600 **Setup→General** page.

- For CDP discovery OV3600 needs "read-only" access to a router or switch for all subnets that contain APs. As each router or switch is added to OV3600's database, OV3600 pings that device and initiates an SNMP connection with the specified community string to verify that the proper IP and community string have been provided.

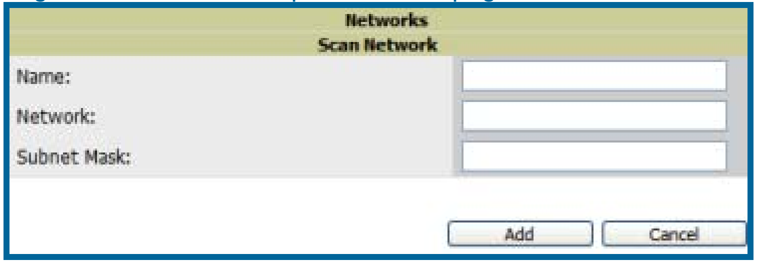
Setting	Default	Description
Proxim/ORiNOCO	Disabled	When enabled, OV3600 runs the OSU-NMS Protocol service to discover Proxim/ORiNOCO APs on the local subnet.
Intel/Symbol (WNMP)	Disabled	When enabled, OV3600 runs WNMP and the Intel IAPP service to discover Symbol and Intel access points on the local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

Defining Networks for SNMP/HTTP Scanning

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

- Browse to the **Device Setup→Discover** page and locate the "New Network" area.

Figure 61. “Device Setup→Discover” page "New Network” Area



Networks

Scan Network

Name:

Network:

Subnet Mask:

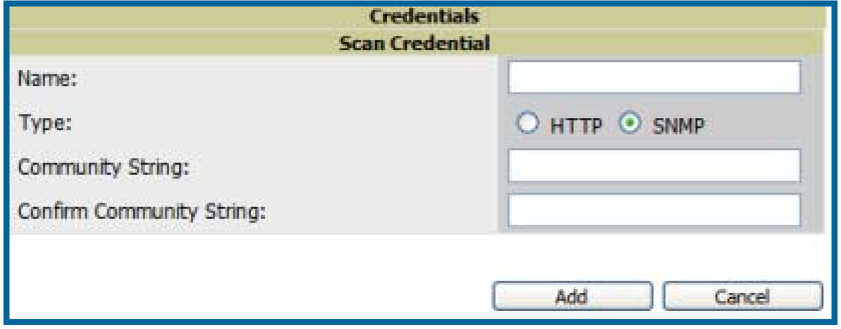
- Provide a name for the network to be scanned in the *Label* field (i.e., “Accounting Network”).
- Define the network range (or the first address on the network) to be scanned in the *Network* field (i.e., 10.52.0.0).
- Specify the *Subnet Mask* for the network to be scanned (i.e., 255.255.252.0). The largest subnet accepted by OV3600 is 255.255.0.0
- Click “Add.”
- Repeat this process to add as many networks as you would like to add to OV3600’s database.

Defining Credentials for Scanning

The next step is to define the credentials that will be used to scan the network. OV3600 only utilizes credentials defined for scans during discovery. New access points inherit credentials from the System Credentials configured on **Device Setup→Communications** page.

- Locate the “New Credentials” area on the **Device Setup→Discover** page.

Figure 62. “Device Setup→Discover” page “New Credentials” area



Credentials

Scan Credential

Name:

Type: ○ HTTP ● SNMP

Community String:

Confirm Community String:

- Specify the type of scan to be completed (SNMP or HTTP). *In most cases, SNMP scans should be used for discovery.*
- Provide a name for the credential in the *Label* field (i.e., “Default”). *NOTE: OV3600 automatically appends the type of scan (SNMP or HTTP) to the Label.*
- Define and confirm the community string to be used. *In this section, the community string used can be either “read-only” or “read/write” as OV3600 will only use it for discovering APs. To bring APs under management, OV3600 will use the credentials supplied in **Device Setup→SNMP** page.*

- Click “Add.”

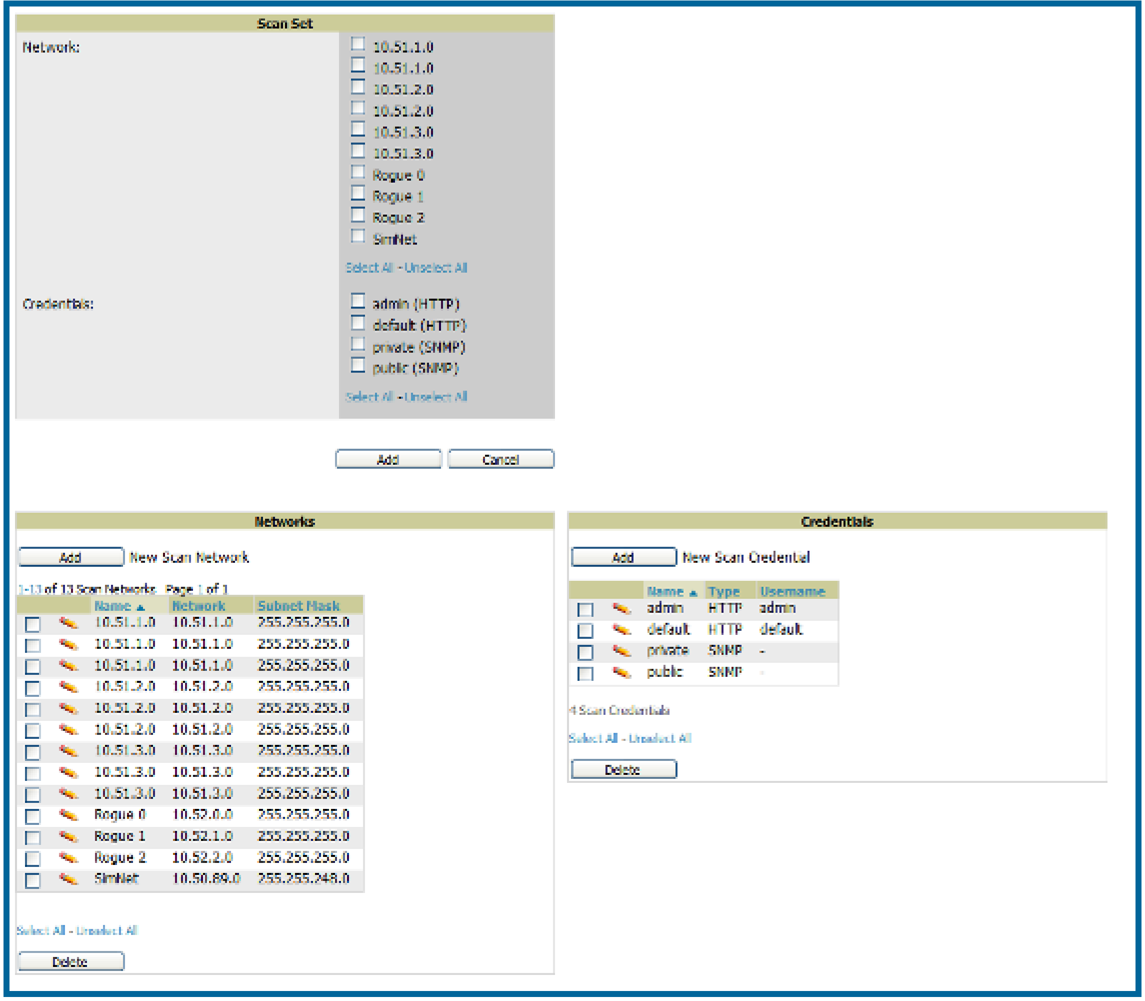
- Repeat this process to add as many credentials as you would like to OV3600’s database.

Defining a Scan

Once at least one network and one credential have been specified, you can define a network scan.

- Locate the “Define Scan” area of the **Device Setup→Discover** page.

Figure 63. “Device Setup→Discover” page “New Scan Set” area



Scan Set

Network:
□ 10.51.1.0
□ 10.51.1.0
□ 10.51.2.0
□ 10.51.2.0
□ 10.51.3.0
□ 10.51.3.0
□ Rogue 0
□ Rogue 1
□ Rogue 2
□ SimNet
Select All - Unselect All

Credentials:
□ admin (HTTP)
□ default (HTTP)
□ private (SNMP)
□ public (SNMP)
Select All - Unselect All

Add Cancel

Networks

Add New Scan Network

1-13 of 13 Scan Networks Page 1 of 1

		Name ▲	Network	Subnet Mask
□	✎	10.51.1.0	10.51.1.0	255.255.255.0
□	✎	10.51.1.0	10.51.1.0	255.255.255.0
□	✎	10.51.1.0	10.51.1.0	255.255.255.0
□	✎	10.51.2.0	10.51.2.0	255.255.255.0
□	✎	10.51.2.0	10.51.2.0	255.255.255.0
□	✎	10.51.2.0	10.51.2.0	255.255.255.0
□	✎	10.51.3.0	10.51.3.0	255.255.255.0
□	✎	10.51.3.0	10.51.3.0	255.255.255.0
□	✎	10.51.3.0	10.51.3.0	255.255.255.0
□	✎	Rogue 0	10.52.0.0	255.255.255.0
□	✎	Rogue 1	10.52.1.0	255.255.255.0
□	✎	Rogue 2	10.52.2.0	255.255.255.0
□	✎	SimNet	10.50.89.0	255.255.248.0

Select All - Unselect All

Delete

Credentials

Add New Scan Credential

		Name ▲	Type	Username
□	✎	admin	HTTP	admin
□	✎	default	HTTP	default
□	✎	private	SNMP	-
□	✎	public	SNMP	-

4 Scan Credentials

Select All - Unselect All

Delete

- Select the *Network(s)* to be scanned and the *Credentials* to be used. *You may select as many networks and Credentials as you would like. OV3600 will define a unique scan for each Network-Credential combination.*

- Click the “Add” button to define the selected scans.

- The newly defined scans will appear in a list at the top of the **Device Setup→Discover** page.

- To edit an existing scan, click the pencil icon next to the scan on the **Device Setup→Discover** page.

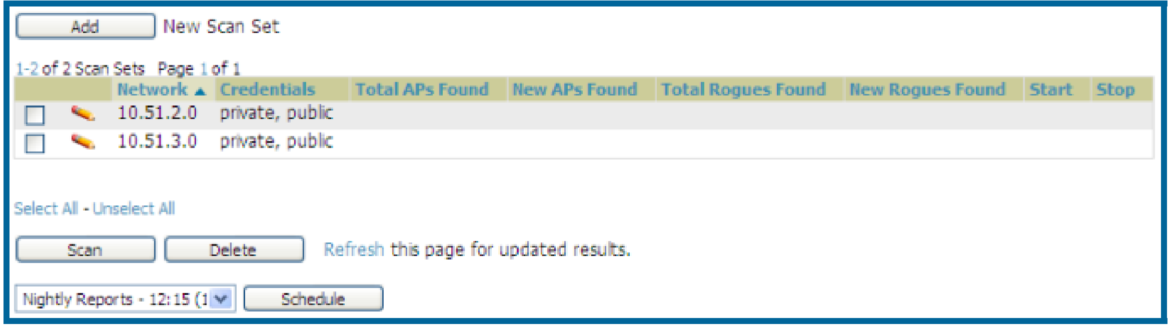
Note: Scheduling an HTTP scan to run daily on your network will help discover rogues. Some consumer access points, most D-Link, Linksys, NetGear models, do not support SNMP and will only be found, on the wired side, with an HTTP scan and will only be discovered if they have a valid IP. Proper credentials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

Executing a Scan

Once a scan has been defined on **OV3600 Setup→Discover** page, OV3600 can now execute the scan.

- Browse to the **Device Setup→Discover** page and locate the Discovery Execution area at the top of the page.

Figure 64. “Device Setup→Discover” page Discovery Execution area



New Scan Set

1-2 of 2 Scan Sets Page 1 of 1

		Network ▲	Credentials	Total APs Found	New APs Found	Total Rogues Found	New Rogues Found	Start	Stop
□	✎	10.51.2.0	private, public						
□	✎	10.51.3.0	private, public						

Select All - Unselect All

Refresh this page for updated results.

- Check the box next to the scan(s) that you would like to execute.
- Click “Scan” to execute the selected scans immediately.
- Click “Show Schedule Options” and enter the desired date and time to schedule a future scan.
- After several minutes have passed, click the “Refresh” button to refresh the screen and view the results of the scan:

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

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

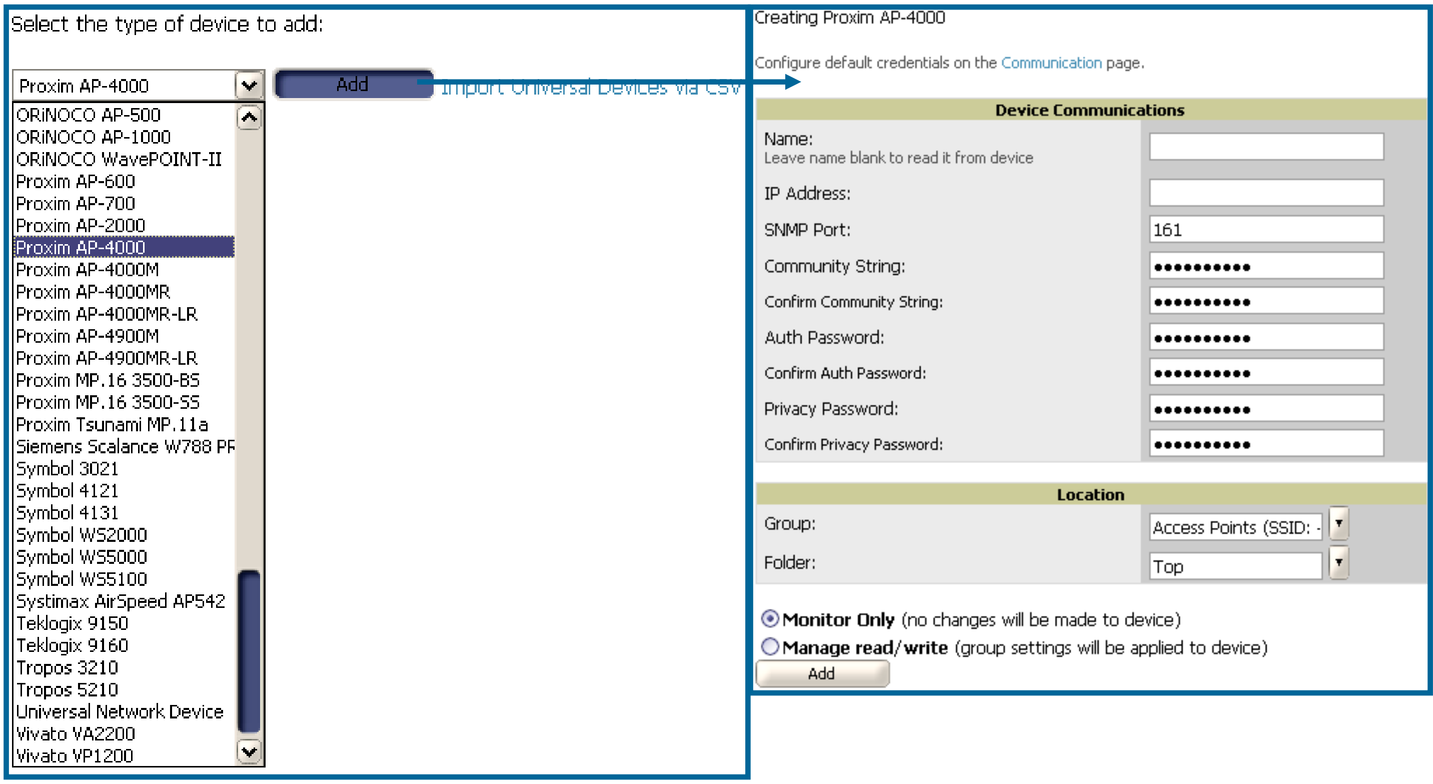
Manually Adding Devices

Although OV3600 has very robust discovery capabilities there are deployment situations which dictate manually adding devices to OV3600. Routers and switches need to be added manually to OV3600 by importing a CSV file (see below for more information). Access points can be added manually with a CSV file (see below) or on the **Device Setup→Add** page.

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

- Browse to the **Device Setup→Add** page and select the manufacturer and model.

Figure 65. “Device Setup→Add” page



Creating Proxim AP-4000

Configure default credentials on the Communication page.

Device Communications	
Name: Leave name blank to read it from device	
IP Address:	
SNMP Port:	161
Community String:	••••••••••
Confirm Community String:	••••••••••
Auth Password:	••••••••••
Confirm Auth Password:	••••••••••
Privacy Password:	••••••••••
Confirm Privacy Password:	••••••••••

Location	
Group:	Access Points (SSID: -
Folder:	Top

● **Monitor Only** (no changes will be made to device)

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

- Select the appropriate group and folder for the AP.

- Select either the “Monitor only” or “Management read/write” radio button.

- Click “Add” to finish creating the devices.

  NOTE: If “Manage read/write” is selected OV3600 will overwrite existing device settings with the Group settings. It is recommended that you place newly discovered devices in “Monitor read/only” mode to enable auditing of actual settings versus Group Policy.

Setting	Default	AP Type	Description
Name	None	All	User-configurable name for the AP (max. 20 characters)

Setting	Default	AP Type	Description
IP Address (Required)	None	All	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).
SNMP Port	161	All	The port OV3600 will use to communicate with the AP via SNMP.
Community String Confirm	Taken from the Device Setup →Communication Page	All Except Cisco VxWorks	Community string used to communicate with the AP. *Note: The community string should have RW (Read Write) capability*.
Username & Password	Taken from the Device Setup →Communication Page	Cisco VxWorks	This provides a read-write user account (SNMP, HTTP, and Telnet) within the Cisco Security System for access to existing APs. OV3600 will initially use this username password combination to control the Cisco AP. OV3600 will create a user-specified account with which to manage the AP if the User Creation Options is set to Create and user Specified User *(NOTE: New, "out-of-the-box" Cisco APs typically have SNMP disabled and a blank username & password combination for HTTP and telnet.)* Cisco supports multiple community strings per AP.
Telnet Username & Password	Taken from the Device Setup →Communication Page	Cisco IOS, Acton, HP 420, RoamAbout AP-3000	The Telnet username and password for existing Cisco IOS APs. OV3600 utilizes 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	The password which allows OV3600 to enter "enable" mode on the AP.
HTTP Username & Password	Taken from the Device Setup →Communication Page	Colubris Intel 2011b Symbol 4131	HTTP password used to initially manage the AP 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	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."***

Setting	Default	AP Type	Description
Telnet Port	23	Cisco IOS, Acton, HP 420, RoamAbout AP-3000	The port OV3600 utilizes to communicates with the AP via the telnet protocol.
HTTPS Port	443	Colubris	The port OV3600 uses to communicate with the AP via the HTTPS protocol.
Privacy Password	Taken from the Device Setup →Communication Page	Enterasys R2	The SNMPv3 privacy password.
Group	Default Group	All	Pull-down menu used to assign the AP to a Group.
Folder	Top	All	Pull-down menu used to assign the AP to a Folder.

Adding Access Points, Routers and Switches with a CSV File

Adding routers and switches into your OV3600 as managed devices allows OV3600 to:

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

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

NOTE: 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 utilizing the VPN on the AP will automatically provide this information to OV3600.

You can use a comma-separated values file to import lists of devices (access points, routers and switches) into OV3600. The list must contain the following columns:

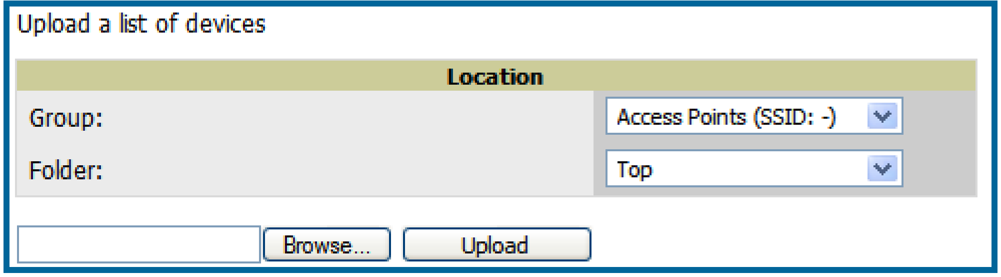
IP Address
SNMP Community String
Name
Type
Auth Password
SNMPv3 Auth Protocol
Privacy Password
SNMPv3 Username
Telnet Username
Telnet Password
Enable Password
SNMP Port

For exOV3600le:

IP Address,SNMP Community String,Name,Type,Auth Password,SNMPv3 Auth Protocol,Privacy Password,SNMPv3 Username,Telnet Username,Telnet Password,Enable Password,SNMP Port
10.34.64.163,private,switch1.exOV3600le.com,Router/Switch,nonradiance,md5,privacy,sv3user,telnetuser,telnetpwd,enable,161

To import a CSV file, navigate to the Device Setup→Add page and click the link to "Import Devices via CSV."

Figure 66. "Device Setup→Add (import from CSV)" page



Upload a list of devices

Location	
Group:	Access Points (SSID: -)
Folder:	Top

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

Adding Universal Devices

OV3600 is able to get basic monitoring information from any device that supports SNMP including switches, routers and unsupported access points. This allows monitoring of key elements of the wired network infrastructure, including upstream switches, RADIUS servers and other devices. While OV3600 can manage most leading brands and models of wireless infrastructure, UDS also enables basic monitoring of many of these less commonly used APs.

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

- Browse to the **Device Setup→Add** page and select the manufacturer and model.
- Select "Universal Network Device" from the dropdown and click "Add". Large numbers of Universal Network Devices can be added from a CSV file by clicking on the "Import Devices via CSV" link.
- Enter the name, IP address and read only SNMP community string for the device.
- Select the appropriate group and folder.
- 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 on the pencil icon next to an interface you can assign it to be unmonitored or to be monitored as interface 1 or 2. OV3600 will collect this information and display it on the **APs/Devices→Monitor** page. 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 see the "Configuring Groups" section. 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 will compare the device's current configuration settings with the Group configuration settings and automatically update the device's configuration to match the Group policy. If you place the device in "Monitor read only" mode, OV3600 will compare the current configuration with the policy and will display any discrepancies on the **APs/Devices→Audit** page but will not change the configuration of the device.

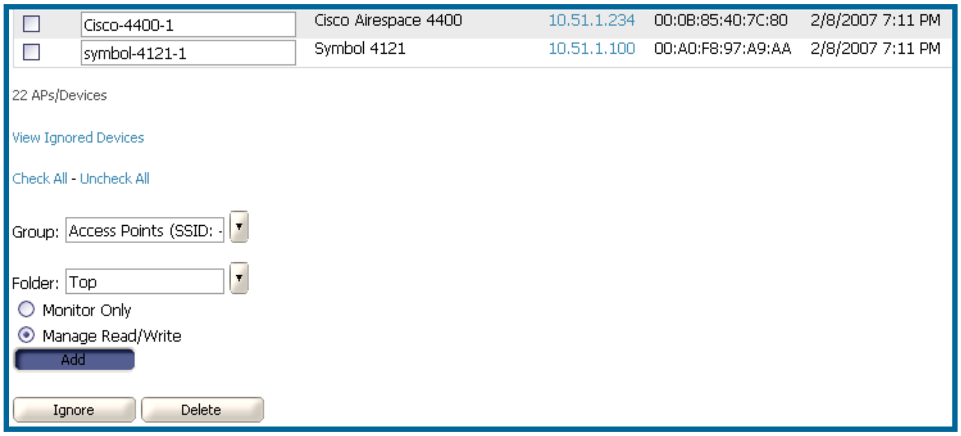
*It is recommended that you put devices in "**Monitor only**" mode when they are added to a newly established Group to avoid overwriting any important existing configuration settings. Once you have added several devices to the Group and verified that no unexpected or undesired configuration changes will 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

To add a newly discovered device to a Group:

- Browse to the **APs/Devices→New** page. The **APs/Devices→New** page displays all newly discovered devices, device manufacturer and model, MAC Address, IP Address, and the date/time of discovery.

Figure 67. "APs/Devices→New" page



□	Cisco-4400-1	Cisco Airespace 4400	10.51.1.234	00:0B:85:40:7C:80	2/8/2007 7:11 PM
□	symbol-4121-1	Symbol 4121	10.51.1.100	00:A0:F8:97:A9:AA	2/8/2007 7:11 PM

22 APs/Devices

View Ignored Devices

Check All - Uncheck All

Group: Access Points (SSID: -

Folder: Top

○ Monitor Only

● Manage Read/Write

- Select the device(s) to be added to a Group.

- Select the *Group* and folder to which the device will be added from the pull-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.

- Select either the "Monitor only" or the "Manage read/write" radio button and click the Add button. *NOTE: If you select "Manage Select Devices," OV3600 will automatically overwrite existing device settings with the specified Group settings. It is recommended* *that you place discovered devices in “Monitor” mode until you can confirm that all Group configuration settings are appropriate for that device.*

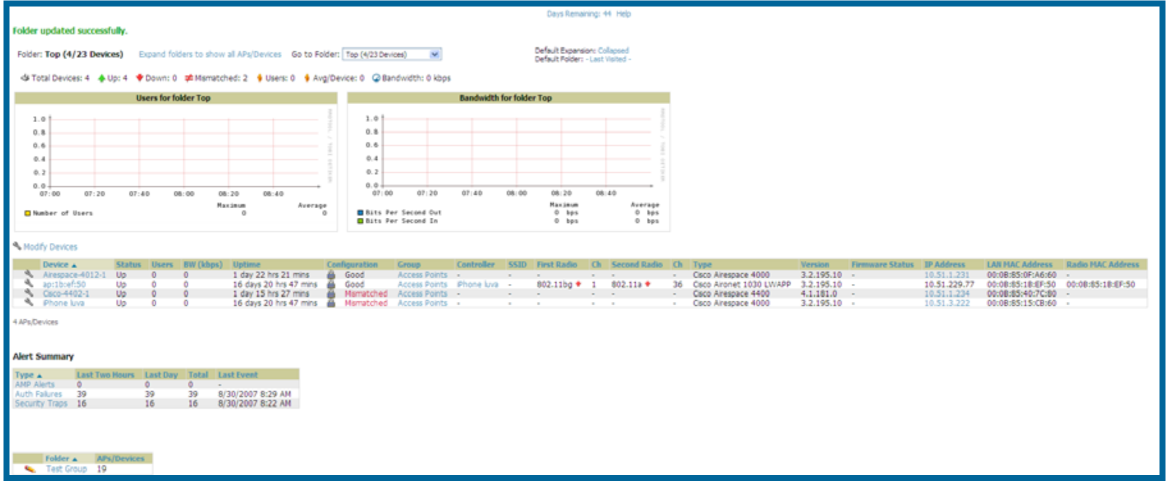
- If you do not wish to manage or monitor a discovered device, you may select the device(s) from the list and click either “Ignore Selected Devices” or “Delete Selected Devices.” *If you choose to “Ignore” the devices, they will not be displayed in the* ***APs/Devices→New*** *list if they are discovered in subsequent scans. You can view a list of all “Ignored” devices on the* ***APs/Devices→Ignored*** *page. If you choose to “Delete” the device, it will be listed on the* ***APs/Devices→New*** *list if discovered by OV3600 in a subsequent scan.*

Verifying that Devices have been Successfully Added to a Group

When you add a newly discovered device to a Group in either “Monitor” or “Manage” mode, you should verify that the process completed successfully:

- 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 68. “APs/Devices→List” page



Days Remaining: 44 Help

Folder updated successfully.

Folder: Top (4/23 Devices) Expand folders to show all APs/Devices Go to Folder: Top (4/23 Devices)

Default Expansion: Collapsed
Default Folder: - Last Visited -

Total Devices: 4 Up: 4 Down: 0 Mismatched: 2 Users: 0 Avg/Device: 0 Bandwidth: 0 kbps

Modify Devices

	Device ▲	Status	Users	BW (kbps)	Uptime	Configuration	Group	Controller	SSID	First Radio	Ch	Second Radio	Ch	Type	Version	Firmware Status	IP Address	LAN MAC Address	Radio MAC Address
	Airespace-4012-1	Up	0	0	1 day 22 hrs 21 mins	Good	Access Points	-	-	-	-	-	-	Cisco Airespace 4000	3.2.195.10	-	10.51.1.231	00:0B:85:0F:A6:60	-
	ap:1b:ef:50	Up	0	0	16 days 20 hrs 47 mins	Good	Access Points	iPhone luva	-	802.11bg	1	802.11a	36	Cisco Aironet 1030 LWAPP	3.2.195.10	-	10.51.229.77	00:0B:85:18:EF:50	00:0B:85:18:EF:50
	Cisco-4402-1	Up	0	0	1 day 15 hrs 27 mins	Mismatched	Access Points	-	-	-	-	-	-	Cisco Airespace 4400	4.1.181.0	-	10.51.1.234	00:0B:85:40:7C:80	-
	iPhone luva	Up	0	0	16 days 20 hrs 47 mins	Mismatched	Access Points	-	-	-	-	-	-	Cisco Airespace 4000	3.2.195.10	-	10.51.3.222	00:0B:85:15:CB:60	-

4 APs/Devices

Alert Summary

Type ▲	Last Two Hours	Last Day	Total	Last Event
AMP Alerts	0	0	0	-
Auth Failures	39	39	39	8/30/2007 8:29 AM
Security Traps	16	16	16	8/30/2007 8:22 AM

	Folder ▲	APs/Devices
	Test Group	19

- Verify that the devices you added are now appearing in the devices list with a Status of “Up.” *NOTE: Immediately after you have added the device to a Group, you will 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.*

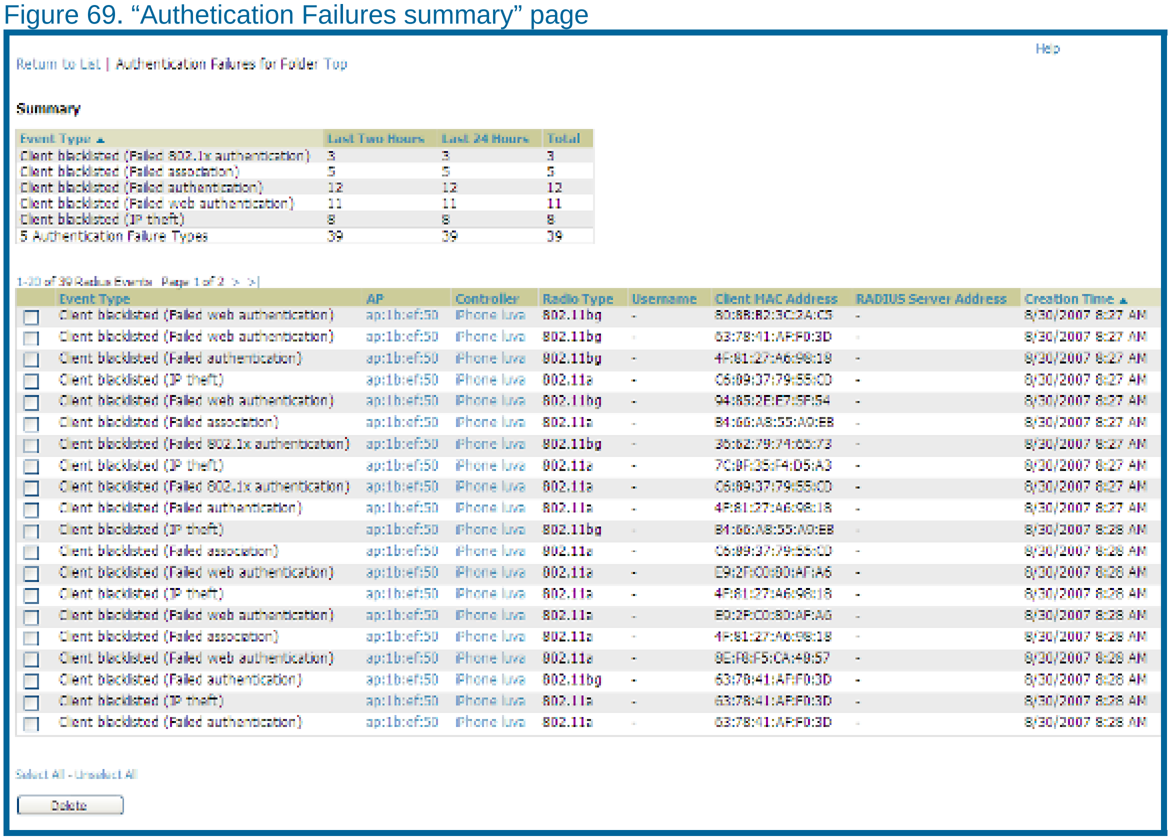
Navigate to the Alert Summary section of the **APs/Devices→List** page. This section displays OV3600 Alerts, Auth Failures, and Security Traps. The same section also appears on the **Groups→Monitoring page**, and is linked from a controller's monitoring page.

Clicking on the Auth Failures link takes you to a summary page of authentication failures. Authentication failures can be configured for Airespace devices on the **Group→Basic** page and for IOS devices by adding this line to the template:

snmp-server host <OV3600_ip> version 2c <community> aaa_server authenticate-fail

deauthenticate snmp syslog

Figure 69. "Authetication Failures summary" page



Return to List | Authentication Failures for Folder Top

Summary

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

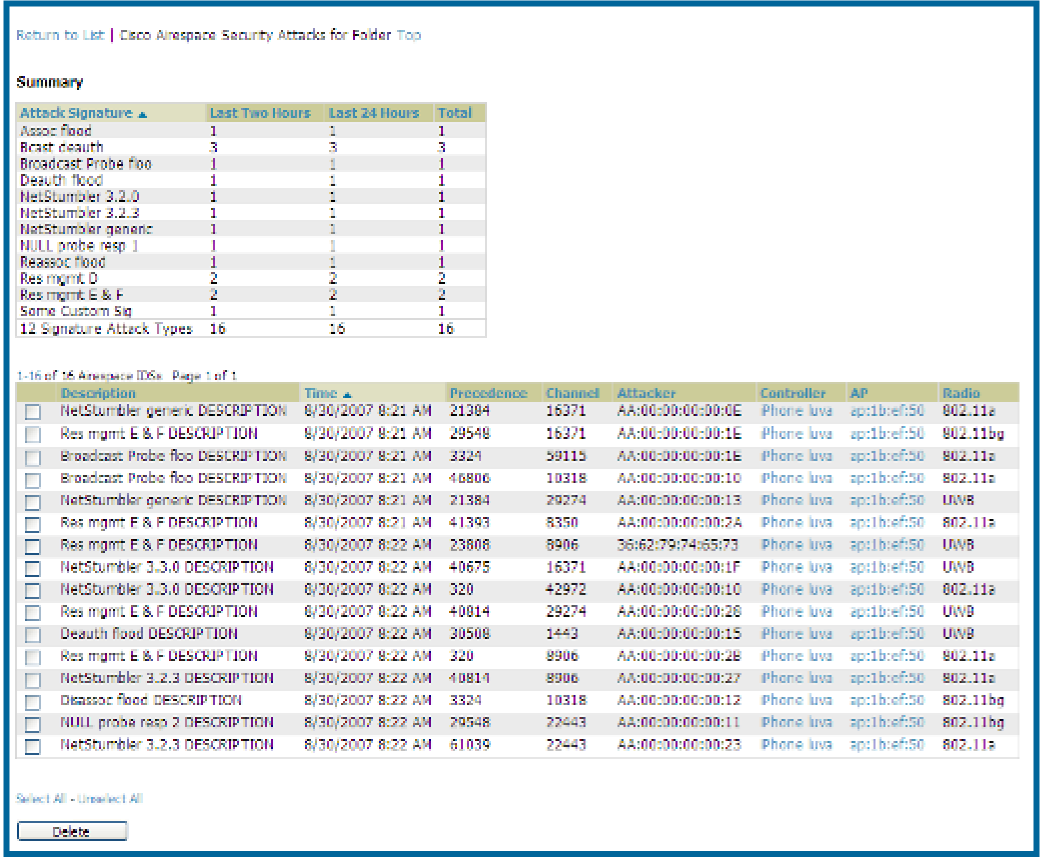
1-20 of 39 Radius Events Page 1 of 2 > >|

	Event Type	AP	Controller	Radio Type	Username	Client MAC Address	RADIUS Server Address	Creation Time ▲
□	Client blacklisted (Failed web authentication)	ap:1b:ef:50	iPhone luva	802.11bg	-	80:88:B2:3C:2A:C5	-	8/30/2007 8:27 AM
□	Client blacklisted (Failed web authentication)	ap:1b:ef:50	iPhone luva	802.11bg	-	63:78:41:AF:F0:3D	-	8/30/2007 8:27 AM
□	Client blacklisted (Failed authentication)	ap:1b:ef:50	iPhone luva	802.11bg	-	4F:81:27:A6:98:18	-	8/30/2007 8:27 AM
□	Client blacklisted (IP theft)	ap:1b:ef:50	iPhone luva	802.11a	-	C6:89:37:79:55:CD	-	8/30/2007 8:27 AM
□	Client blacklisted (Failed web authentication)	ap:1b:ef:50	iPhone luva	802.11bg	-	94:85:2E:E7:5F:54	-	8/30/2007 8:27 AM
□	Client blacklisted (Failed association)	ap:1b:ef:50	iPhone luva	802.11a	-	B4:66:A8:55:A0:EB	-	8/30/2007 8:27 AM
□	Client blacklisted (Failed 802.1x authentication)	ap:1b:ef:50	iPhone luva	802.11bg	-	36:62:79:74:65:73	-	8/30/2007 8:27 AM
□	Client blacklisted (IP theft)	ap:1b:ef:50	iPhone luva	802.11a	-	7C:8F:35:F4:D5:A3	-	8/30/2007 8:27 AM
□	Client blacklisted (Failed 802.1x authentication)	ap:1b:ef:50	iPhone luva	802.11a	-	C6:89:37:79:55:CD	-	8/30/2007 8:27 AM
□	Client blacklisted (Failed authentication)	ap:1b:ef:50	iPhone luva	802.11a	-	4F:81:27:A6:98:18	-	8/30/2007 8:27 AM
□	Client blacklisted (IP theft)	ap:1b:ef:50	iPhone luva	802.11bg	-	B4:66:A8:55:A0:EB	-	8/30/2007 8:28 AM
□	Client blacklisted (Failed association)	ap:1b:ef:50	iPhone luva	802.11a	-	C6:89:37:79:55:CD	-	8/30/2007 8:28 AM
□	Client blacklisted (Failed web authentication)	ap:1b:ef:50	iPhone luva	802.11a	-	E9:2F:C0:80:AF:A6	-	8/30/2007 8:28 AM
□	Client blacklisted (IP theft)	ap:1b:ef:50	iPhone luva	802.11a	-	4F:81:27:A6:98:18	-	8/30/2007 8:28 AM
□	Client blacklisted (Failed web authentication)	ap:1b:ef:50	iPhone luva	802.11a	-	E9:2F:C0:80:AF:A6	-	8/30/2007 8:28 AM
□	Client blacklisted (Failed association)	ap:1b:ef:50	iPhone luva	802.11a	-	4F:81:27:A6:98:18	-	8/30/2007 8:28 AM
□	Client blacklisted (Failed web authentication)	ap:1b:ef:50	iPhone luva	802.11a	-	8E:F8:F5:CA:40:57	-	8/30/2007 8:28 AM
□	Client blacklisted (Failed authentication)	ap:1b:ef:50	iPhone luva	802.11bg	-	63:78:41:AF:F0:3D	-	8/30/2007 8:28 AM
□	Client blacklisted (IP theft)	ap:1b:ef:50	iPhone luva	802.11a	-	63:78:41:AF:F0:3D	-	8/30/2007 8:28 AM
□	Client blacklisted (Failed authentication)	ap:1b:ef:50	iPhone luva	802.11a	-	63:78:41:AF:F0:3D	-	8/30/2007 8:28 AM

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

Clicking on the Security Traps link of the Alert Summary section takes you to the Cisco Airespace Security Attacks summary page. This page displays information from the Intrustion Detection System from the WCS. IDS traps do not need to be independently enabled in OV3600.

Figure 70. “Cisco Airespace Security Attacks” page



Return to List | Cisco Airespace Security Attacks for Folder Top

Summary

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

1-16 of 16 Airespace IDSs Page 1 of 1

	Description	Time ▲	Precedence	Channel	Attacker	Controller	AP	Radio
□	NetStumbler generic DESCRIPTION	8/30/2007 8:21 AM	21384	16371	AA:00:00:00:00:0E	Phone luva	ap:1b:ef:50	802.11a
□	Res mgmt E & F DESCRIPTION	8/30/2007 8:21 AM	29548	16371	AA:00:00:00:00:1E	Phone luva	ap:1b:ef:50	802.11bg
□	Broadcast Probe floo DESCRIPTION	8/30/2007 8:21 AM	3324	59115	AA:00:00:00:00:1E	Phone luva	ap:1b:ef:50	802.11a
□	Broadcast Probe floo DESCRIPTION	8/30/2007 8:21 AM	46806	10318	AA:00:00:00:00:10	Phone luva	ap:1b:ef:50	802.11a
□	NetStumbler generic DESCRIPTION	8/30/2007 8:21 AM	21384	29274	AA:00:00:00:00:13	Phone luva	ap:1b:ef:50	UWB
□	Res mgmt E & F DESCRIPTION	8/30/2007 8:21 AM	41393	8350	AA:00:00:00:00:2A	Phone luva	ap:1b:ef:50	802.11a
□	Res mgmt E & F DESCRIPTION	8/30/2007 8:22 AM	23808	8906	36:62:79:74:65:73	Phone luva	ap:1b:ef:50	UWB
□	NetStumbler 3.3.0 DESCRIPTION	8/30/2007 8:22 AM	40675	16371	AA:00:00:00:00:1F	Phone luva	ap:1b:ef:50	UWB
□	NetStumbler 3.3.0 DESCRIPTION	8/30/2007 8:22 AM	320	42972	AA:00:00:00:00:10	Phone luva	ap:1b:ef:50	802.11a
□	Res mgmt E & F DESCRIPTION	8/30/2007 8:22 AM	40814	29274	AA:00:00:00:00:28	Phone luva	ap:1b:ef:50	UWB
□	Deauth flood DESCRIPTION	8/30/2007 8:22 AM	30508	1443	AA:00:00:00:00:15	Phone luva	ap:1b:ef:50	UWB
□	Res mgmt E & F DESCRIPTION	8/30/2007 8:22 AM	320	8906	AA:00:00:00:00:2B	Phone luva	ap:1b:ef:50	802.11a
□	NetStumbler 3.2.3 DESCRIPTION	8/30/2007 8:22 AM	40814	8906	AA:00:00:00:00:27	Phone luva	ap:1b:ef:50	802.11a
□	Disassoc flood DESCRIPTION	8/30/2007 8:22 AM	3324	10318	AA:00:00:00:00:12	Phone luva	ap:1b:ef:50	802.11bg
□	NULL probe resp 2 DESCRIPTION	8/30/2007 8:22 AM	29548	22443	AA:00:00:00:00:11	Phone luva	ap:1b:ef:50	802.11bg
□	NetStumbler 3.2.3 DESCRIPTION	8/30/2007 8:22 AM	61039	22443	AA:00:00:00:00:23	Phone luva	ap:1b:ef:50	802.11a

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

Troubleshooting a Newly Discovered Device with "Down" Status

If the device *Status* on the **APs/Devices→List** page remains "Down" after it has been added to a Group, the most likely source of the problem is an error in the SNMP community string being used to manage the device. To troubleshoot this:

- Click on the *Name* of the device in the list of devices on the **APs/Devices→List** page. This will automatically direct you to the **APs/Device→Monitor** page for that device.

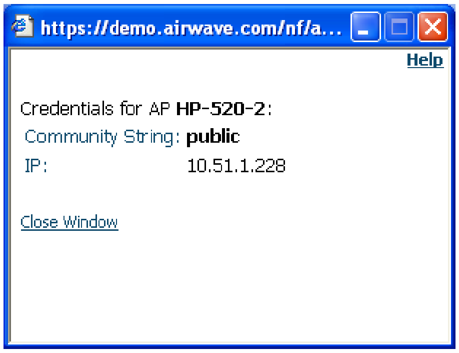
- Locate the *Status* section onscreen. If the *Status* is "Down," there will be an onscreen error message indicating the cause of the problem. Some of the common error messages are:

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.

- If the "SNMP Get Failed" message appears, click the **APs/Devices→Manage** tab to go to the management page for that device.

- Click the *View device credentials* link in the "Device Communications" area. This will display the credentials OV3600 is unsuccessfully using to communicate with the device. This link can be removed from the OV3600 for security reasons by setting a flag in the database. Only users with root access to the OV3600 command line can show or hide this link.

Figure 71. "View AP Credentials" Dialogue Box

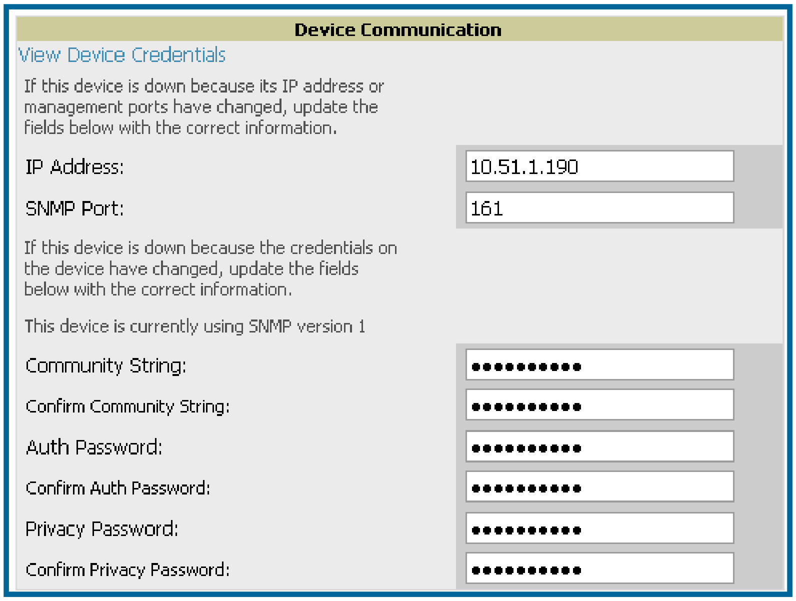


Credentials for AP **HP-520-2**:
Community String: **public**
IP: 10.51.1.228

NOTE: "View AP Credentials Dialogue Box" may appear slightly different depending on the particular manufacture and model.

- If the credentials are incorrect return to the “Device Communications” area on the **APs/Devices→Manage** page.

Figure 72. “APs/Devices→Manage” page Device Communication 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:	10.51.1.190
SNMP Port:	161

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

This device is currently using SNMP version 1

Community String:	●●●●●●●●●●●
Confirm Community String:	●●●●●●●●●●●
Auth Password:	●●●●●●●●●●●
Confirm Auth Password:	●●●●●●●●●●●
Privacy Password:	●●●●●●●●●●●
Confirm Privacy Password:	●●●●●●●●●●●

NOTE: “Device Communication” area may appear slightly different depending on the particular manufacture and model.

- Enter the appropriate *credentials*, and click “Apply.”

- 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. The first step is to replace the broken hardware. Once the new device is on the network, run a discovery scan in OV3600. 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”. 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. If the new device has the same IP as the broken device you will need to manually add it to OV3600 via the **Device Setup→Add** page before it will appear in the Replace Hardware dropdown menu.

Verifying the Device Configuration Status

When you have successfully added a newly discovered device to a Group in “Monitor” mode, the next step is to verify the device’s configuration status to determine whether any changes will be applied to that device when you convert it to “Managed read/write” mode.

- Browse to the **APs/Devices→List** page (see Figure 68. “APs/Devices→List” page above).

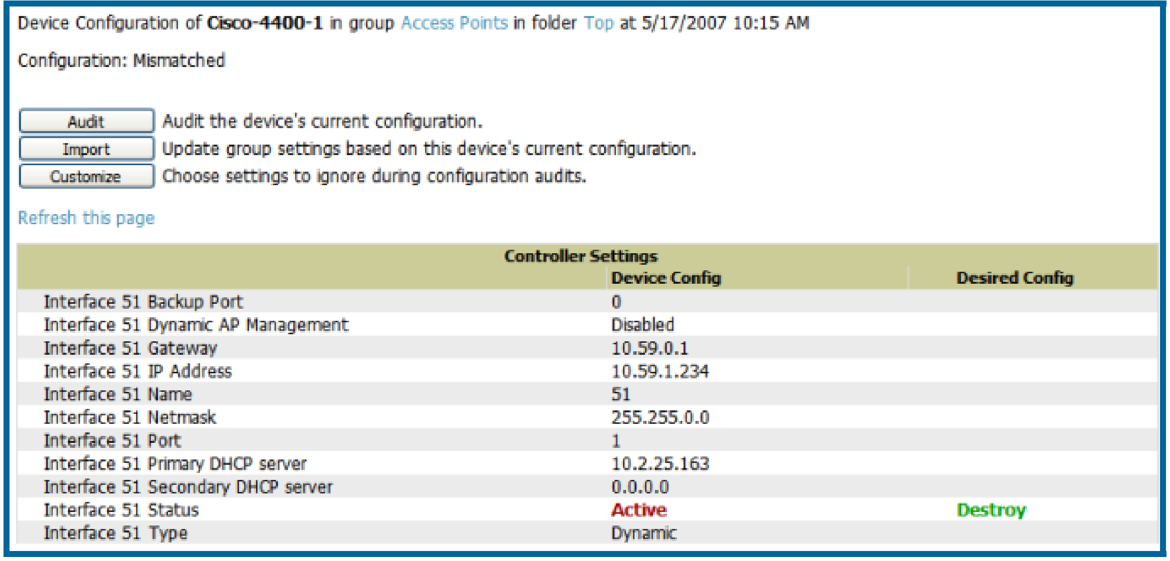
- Locate the device in the onscreen list and check the *Configuration* column.

- If the device is in “Monitor” mode, the 🔒 symbol will appear next to the *Configuration* column, indicating that the device is locked and will not be configured by OV3600.

- Verify the *Configuration* status of the device. A status of “Good” indicates that all of the device’s current settings match the Group policy settings and that no changes will be applied when the device is shifted to “Manage” mode. A status of “Mismatched” indicates that at least one of the device’s current configuration settings does not match the Group policy and will be changed when the device is shifted to “Manage” mode.

- If the device *Configuration* is “Mismatched,” click on the “Mismatched” link to go to the **APs/Devices→Audit** page. The **APs/Devices→Audit** page lists detailed information on all existing configuration parameters and settings for an individual device on the left side of the page. The Group configuration settings are displayed on the right side of the page. *If the device is moved from “Monitor” to “Manage” mode, the settings on the right side of the page will overwrite the settings on the left.*

Figure 73. “APs/Devices→Audit” page



Device Configuration of **Cisco-4400-1** in group Access Points in folder Top at 5/17/2007 10:15 AM

Configuration: Mismatched

Audit — Audit the device's current configuration.
Import — Update group settings based on this device's current configuration.
Customize — Choose settings to ignore during configuration audits.

Refresh this page

Controller Settings	Device Config	Desired Config
Interface 51 Backup Port	0	
Interface 51 Dynamic AP Management	Disabled	
Interface 51 Gateway	10.59.0.1	
Interface 51 IP Address	10.59.1.234	
Interface 51 Name	51	
Interface 51 Netmask	255.255.0.0	
Interface 51 Port	1	
Interface 51 Primary DHCP server	10.2.25.163	
Interface 51 Secondary DHCP server	0.0.0.0	
Interface 51 Status	Active	Destroy
Interface 51 Type	Dynamic	

- 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 manually enter shared secrets and security credentials that cannot be read from the device.
  - To ensure you have the current device configuration click “Audit”. Clicking “Audit” will cause OV3600 to reread the device configuration and 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 to the AP automatically. 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.

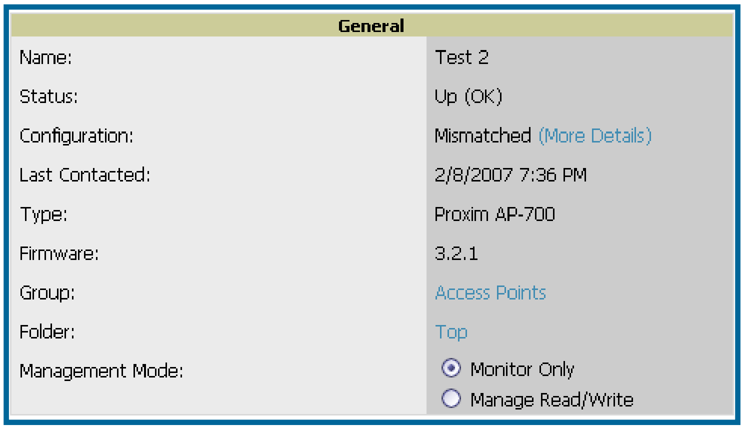
Moving a Device from “Monitor Only” to “Manage Read/Write” Mode

Once the device *Configuration* status is “Good” on the **APs/Devices→List** page or 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.

- Browse to the **APs/Devices→List** page and click the wrench icon next to the name of the AP to be shifted to “Manage Read/Write” mode. This will direct you to the **APs/Devices→Manage** page.

- Locate the “General” area.

Figure 74. “APs/Devices→Manage” page ‘General’ area



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

- Click “Manage Read/Write” on the *Management Mode* radio button to shift the device from “Monitor Only” to “Manage Read/Write” mode.

- Click “Apply.”

- OV3600 will present a confirmation screen reminding you of all configuration changes that will be applied to the device in “Manage” mode. Click “Confirm Edit” to apply the changes to the device immediately, “Schedule” to schedule the changes to occur during a specific maintenance window, or “Cancel” to return to the **APs/Devices→Manage** page. *NOTE: Some 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.*

- To move multiple devices into managed mode at once use the “Modify these devices link”. Please see the “Modifying Multiple devices” section of OV3600 for more information.

Configuring Individual Device Settings

Overview

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 exOV3600le, since devices within a Group are often contiguous with one another and have overlapping coverage areas, it would not make sense to configure RF channel settings at a Group level. Instead, channel settings are managed at an individual device level to avoid interference.

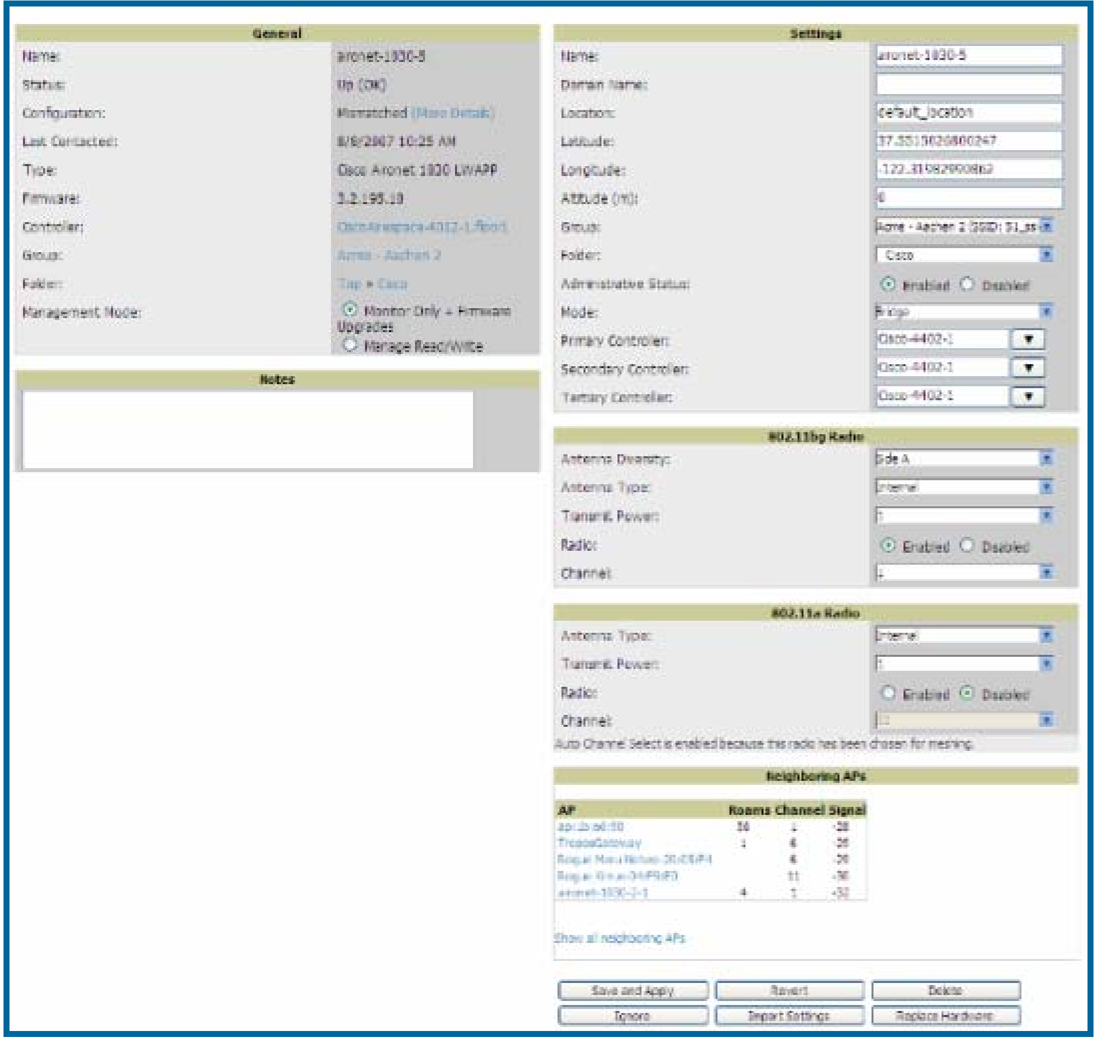
NOTE: Any changes made at an individual device level will automatically override Group level settings.

OV3600 automatically saves the last 10 device configs for reference and compliance purposes. Archived device configs are linked on the **AP→Audit** page and identified by name (which by default is the date and time it was created) and also by the date archived. Click the pencil icon next to the config name to change the name, add notes, or view the archived config. It is not possible to push archived configs to devices, but archived configs can be compared to the current config, the desired config, or to other archived configs using the dropdown menus on the **AP→Audit** page. Comparing two configs will highlight specific lines that are mismatched, and provide links to the OV3600 pages where the mismatched settings can be configured.

Configuring AP Settings

- Browse to the **APs/Devices→List** page and click the *Name* of the device. This will direct you to the **APs/Devices→Monitor** page.
- Click on the **APs/Devices→Manage** tab and locate the “Settings” area.

Figure 75. "APs/Devices→Manage” page



General

Name:	aironet-1030-5
Status:	Up (OK)
Configuration:	Mismatched (More Details)
Last Contacted:	8/6/2007 10:25 AM
Type:	Cisco Aironet 1030 LWAPP
Firmware:	3.2.195.10
Controller:	Cisco-Airespace-4012-1 [illegible]
Group:	Acme - Aachen 2
Folder:	Top > Cisco
Management Mode:	● Monitor Only + Firmware Upgrades ○ Manage Read/Write

Notes

Settings

Name:	aironet-1030-5
Domain Name:	
Location:	default_location
Latitude:	37.3515026800247
Longitude:	-122.3158299086[illegible]
Altitude (m):	6
Group:	Acme - Aachen 2 (SSID: 51_ss
Folder:	Cisco
Administrative Status:	● Enabled ○ Disabled
Mode:	Bridge
Primary Controller:	Cisco-4402-1
Secondary Controller:	Cisco-4402-1
Tertiary Controller:	Cisco-4402-1

802.11bg Radio

Antenna Diversity:	Side A
Antenna Type:	Internal
Transmit Power:	1
Radio:	● Enabled ○ Disabled
Channel:	1

802.11a Radio

Antenna Type:	Internal
Transmit Power:	1
Radio:	○ Enabled ● Disabled
Channel:	[illegible]

Auto Channel Select is enabled because this radio has been chosen for meshing.

Neighboring APs

AP	Roams	Channel	Signal
ap:1b:b6:50	16	1	-28
TroposGateway	1	6	-35
Rogue: [illegible]		6	-35
Rogue: [illegible]		11	-38
aironet-1030-1-1	4	1	-52

Show all neighboring APs

- If any changes are scheduled for this AP they will appear in a “Scheduled Changes” section at the top of the page above the rest of the fields. The linked name of the job will take you to the **System→Configuration Change Job Detail** page for the job.

- Locate the *General* section onscreen. The General section provides general information about the AP’s current status.

Message	Meaning
Name	The name currently set on the device.
Status	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 off of the device.
Configuration	The current configuration status of the AP. To update the status click “Audit” on the **APs/Devices→Audit** page.
Last Contacted	The last time OV3600 successfully contacted the AP.

Message	Meaning
Type	The type of AP.
Firmware	The version of firmware running on the AP.
Group	Link to the **Group→Monitoring** page for the AP.
Template	The name of the template currently configuring the AP. Also a link to the **Groups→Template** page. *Note: Only visible for APs that are being managed via templates.*
Folder	The name of the folder containing the AP. Also a link to the **APs/Devices→List** page for the folder.
Management Mode	The current management mode of the AP. No changes will be made to the AP when it is in Monitor Only mode. OV3600 will push configurations and make changes to an AP when it is in Manage Read/Write mode.
Notes	A free form text field.

- Review and provide the following information in the "Settings" area. Devices with dual radios will 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 will manage that device as if it were a single slot device. *NOTE: 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.*

Setting	Default	Device Type	Description
Name	None	All	User-configurable name for the device (max. 20 characters)
Domain	None	IOS	Field will be populated upon initial device discover or rereading settings. If option on **OV3600 Setup→Network** page is chosen will display fully-qualified domain names for IOS APs. Used in conjunction with "Domain" variable in IOS templates.
Location	Read from the device	All	The SNMP location set on the device.
Contact	Read from the device	All	The SNMP contact set on the device.
Latitude	None	All	Text field for entering the latitude of the device. The latitude is used with the Google earth integration.
Longitude	None	All	Text field for entering the longitude of the device. The longitude is used with the Google earth integration.
Group	Default Group	All	Pull-down menu that can be used to assign the device to another Group.
Folder	Top	All	Pull-down menu that can be used to assign the device to another Group.

Setting	Default	Device Type	Description
Mesh Role:	Mesh AP	Mesh Devices	Pull-down menu that 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 exOV3600le mounted on a light pole or in the ceiling. Select “Roaming” if the AP moves around. An exOV3600le would be an AP mounted in a police car or utility truck.
Bridge Role	Base Station	PTMP/WiMAX	Base Station units provide backhaul connections for satellite units, to which wireless users connect.
Mode of Operation	Bridge	PTMP/WiMAX	Units can operate in bridge or router mode.
Ethernet Interface Configuration	100 Mbps Full Duplex	PTMP/WiMAX	Bandwidth rates for uploading and downloading.
Dynamic Data Rate Selection	Enabled	PTMP/WiMAX	Allows subscribers to receive the maximum data rate possible.
Subscriber Station Class	G711 VoIP UGS	WiMAX Subscriber Stations	Defines the subscriber station class for the AP. Subscriber station classes are defined on the **Groups→WiMAX** page.
Uplink Modulation	bpsk-1-2	WiMAX Subscriber Stations	Dropdown menu that defines the uplink modulation type for the subscriber station.
Downlink Modulation	bpsk-1-2	WiMAX Subscriber Stations	Dropdown menu that defines the downlink modulation type for the subscriber station.
VLAN Mode	Inherit	WiMAX Subscriber Sations	Dropdown 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.

Setting	Default	Device Type	Description
Receive Antenna	Diversity	Cisco	Pull-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	Pull-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 it last received information on. 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 will be reduced by the number of decibels specified.

Setting	Default	Device Type	Description
Channel	6	All	Represents the AP's current RF channel setting (the number relates to the center frequency output by the AP's RF synthesizer.) *Contiguous APs should be set to different channels to minimize "crosstalk," which occurs when the signals from APs overlap and interfere with each other. This RF interference negatively influences WLAN performance.* *802.11b's 2.4-GHz range has a total bandwidth of 80-MHz, separated into 11 center channels. Of these channels, only 3 are non-overlapping (1, 6, and 11). In the United States, most organizations use only these non-overlapping channels.*
Neighboring APs	Blank	All	Represents top five contiguous access points calculated by summing the number of roams to and from the access point and the access point of focus. *Contiguous APs should be set to different channels to minimize "crosstalk," which occurs when the signals from APs overlap and interfere with each other. This RF interference negatively influences WLAN performance.*
Transmit Power Level	Highest power level supported by the radio in the regulatory domain (country)	Cisco, Colubris, Intel, Symbol, Proxim AP-600, AP-700, AP-2000 (802.11g)	Determines the power level of radio transmission. Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device. *You can increase the coverage RADIUS of the access point, by increasing the Transmit Power Level. However, while this increases the zone of coverage, it also makes it more likely that the AP will interfere with neighboring APs.* *Supported values are:* • Cisco (100mW, 50mW, 30mW, 20mW, 5mW, 1mW) • Intel/Symbol (Full or 50mW, 30mW, 15mW, 5mW, 1mW) • Colubris (High or 23 dBm, Med. or 17 dBm, Low or 13 dBm)
Distance Between APs	Large	Colubris	Determines how far a user can roam before roaming to another AP.
Notes (Optional)	Blank	All	Free form text field for entering fixed asset numbers or other device information. *This information is printed on the nightly inventory report.*

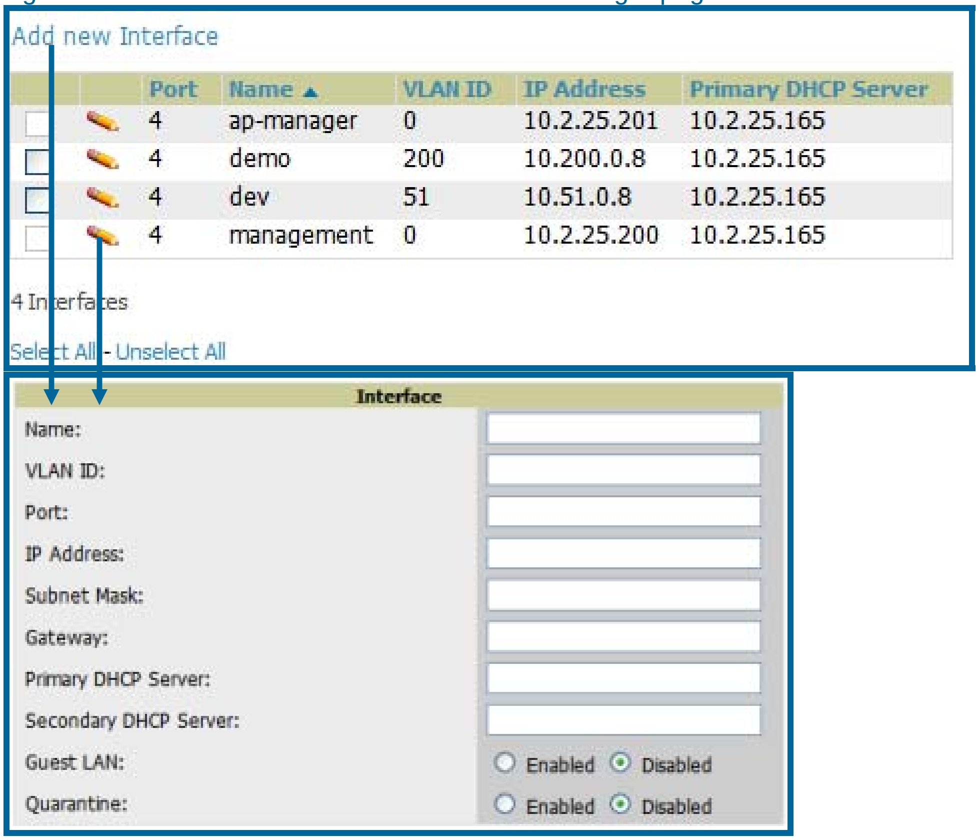
Setting	Default	Device Type	Description
Radio (Enable/Disable)	Enable	All	The Radio option allows you to disable the radio's ability to transmit or receive data while still maintaining Ethernet connectivity to the network. OV3600 will still monitor the Ethernet interface and ensure the AP stays online. *Customers typically use this option to temporarily disable wireless access in particular locations.* *NOTE: This setting can be scheduled at an AP-Level or Group-Level.*
DHCP	Yes	All (except Colubris)	If enabled, the AP will be assigned a new IP address via DHCP. If disabled, the AP will use a static IP address. *NOTE: For improved security and manageability, disable DHCP and use static IP addresses.*
LAN IP	None	All (except Colubris)	The IP Address of the AP's Ethernet interface. If One-to-One NAT is enabled, OV3600 will communicate with the AP on a different address (the IP Address defined in the "Device Communication" area). *NOTE: If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.*
BSID	00:00:00:00:00	WiMAX Base Station	Defines the BSID for the base station. This BSID should match the BSID on the **Groups→WiMAX** page if you want subscriber stations to associate with the base station. Subscriber stations use the BSID defined on the **Groups→WiMAX** page to determine which base stations to associate with.
Subnet Mask	None	All	Provides the IP subnet mask to identify the sub-network so the IP address can be recognized on the LAN *NOTE: If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.*
Gateway	None	All	The IP address of the default internet gateway. *NOTE: If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.*

- Locate the “IOS Template Options” area on the **APs/Devices→Manage** page. *Note: Only displayed for IOS APs in groups with Templates enabled.*

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 Airespace Controllers, navigate to the Interfaces section of the AP→Manage page. Click “Add new Interface” to add another controller interface, or click the pencil icon to edit an existing controller interface.

Figure 76. "Interface section of APs/Devices→Manage” page



Add new Interface

		Port	Name ▲	VLAN ID	IP Address	Primary DHCP Server
□	✎	4	ap-manager	0	10.2.25.201	10.2.25.165
□	✎	4	demo	200	10.200.0.8	10.2.25.165
□	✎	4	dev	51	10.51.0.8	10.2.25.165
□	✎	4	management	0	10.2.25.200	10.2.25.165

4 Interfaces

Select All - Unselect All

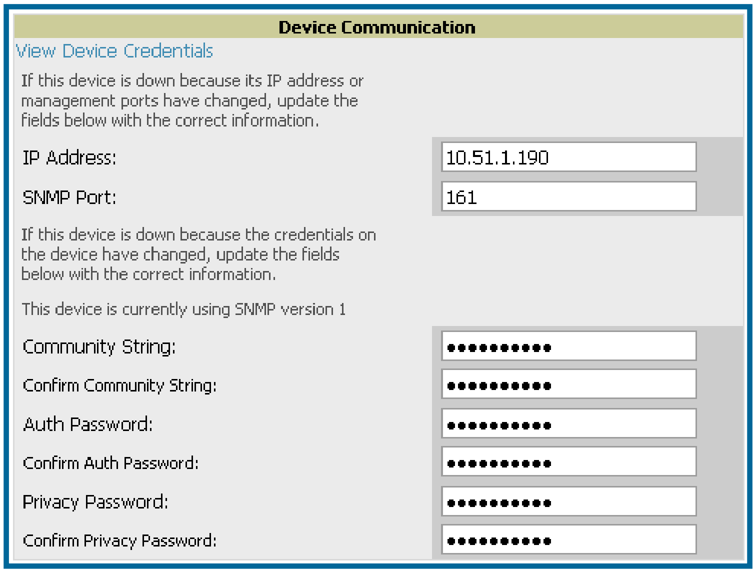
Interface	
Name:	
VLAN ID:	
Port:	
IP Address:	
Subnet Mask:	
Gateway:	
Primary DHCP Server:	
Secondary DHCP Server:	
Guest LAN:	○ Enabled ● Disabled
Quarantine:	○ Enabled ● Disabled

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 subnex mask for the controller.
Gateway	None	The controller’s gateway.
Primary and Secondary DHCP Servers	None	The DHCP servers for the controller.
Guest LAN	Disabled	Indicates a guest LAN.
Quarantine	Disabled	Enabled indicates it is a quarantine VLAN; used only for H-REAP-associated clients.

Configuring AP Communication Settings

- Locate the “Device Communication” area on the **APs/Devices→Manage** page.
- Specify the credentials to be used to manage the AP.

Figure 77. “APs/Devices→Manage” page “Device Communication” area



Device Communication

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

IP Address:	10.51.1.190
SNMP Port:	161

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

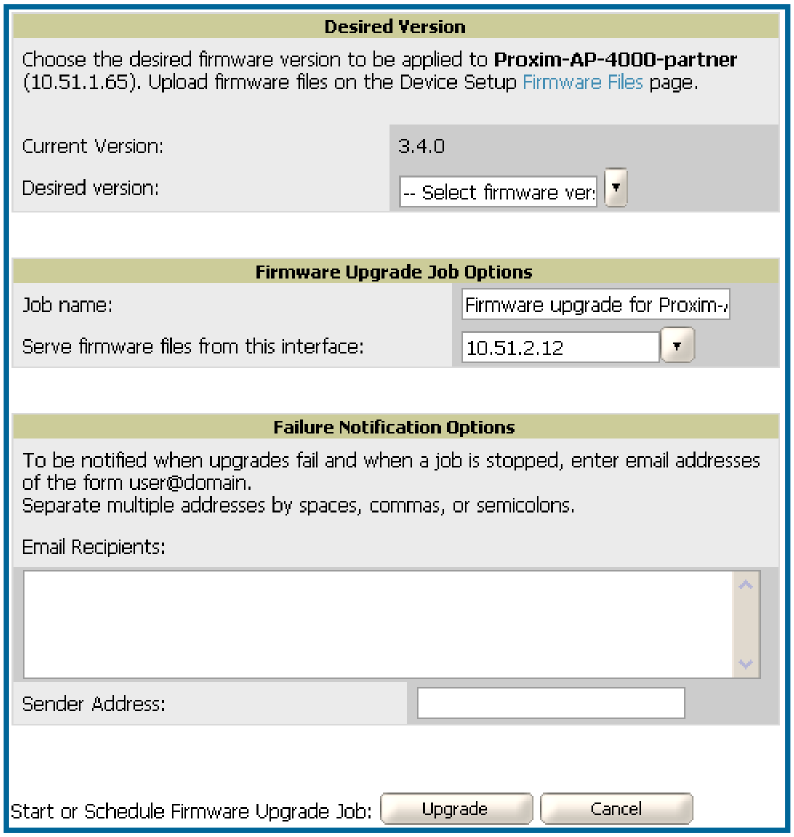
This device is currently using SNMP version 1

Community String:	●●●●●●●●●●
Confirm Community String:	●●●●●●●●●●
Auth Password:	●●●●●●●●●●
Confirm Auth Password:	●●●●●●●●●●
Privacy Password:	●●●●●●●●●●
Confirm Privacy Password:	●●●●●●●●●●

NOTE: “Device Communication” area may appear slightly different depending on the particular manufacture and model of the APs being used.

- Enter the appropriate *Auth Password* and *Privacy Passwords*.
- *The “View AP Credentials” link can be disabled in the database by the root user.*
- Click “Apply.” OV3600 will present 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. *NOTE: Some AP configuration changes may require the AP to be rebooted. Use the “Schedule” function to schedule these changes to occur at a time when WLAN users will not be affected.*
- Click “Upgrade Firmware” to upgrade the device’s firmware.
- Note that for Aruba/Alcatel-Lucent WLAN switch 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 Aruba/Alcatel-Lucent’s best practices for firmware upgrades and plan their upgrades using OV3600 accordingly.

Figure 78. “APs/Devices→Manage” Firmware Upgrades page



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:

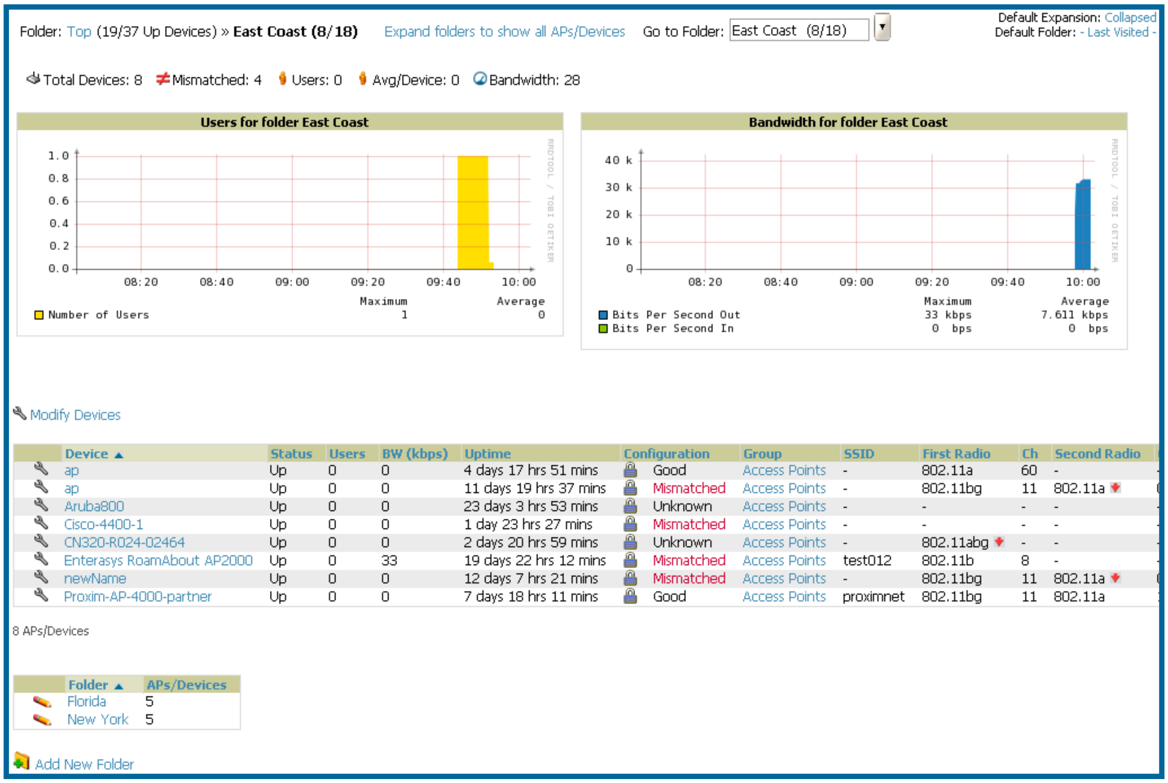
Setting	Default	Description
Desired Version	None	Drop down menu that specifies the firmware to be used in the upgrade. Firmware can be added to this drop down on the **Device Setup→Firmware Files** page.
Job Name	None	User defined name for the upgrade job. Use a meaningful and descriptive name.
Use “/safe” 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	A list of email addresses that should receive alert emails if a firmware upgrade failes.
Sender Address	None	The “From:” address in the alert email.

APs/Devices Pages

Folders (Optional)

The devices on the APs/Devices list pages (List, Up, Down, Mismatched) 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. Folders must be used if you want to limit the APs and devices viewable to OV3600 users.

Figure 79. “APs/Devices→Up” page East Coast folder



Folder: Top (19/37 Up Devices) » **East Coast (8/18)** Expand folders to show all APs/Devices Go to Folder: East Coast (8/18)

Default Expansion: Collapsed
Default Folder: - Last Visited -

Total Devices: 8 Mismatched: 4 Users: 0 Avg/Device: 0 Bandwidth: 28

Modify Devices

	Device ▲	Status	Users	BW (kbps)	Uptime	Configuration	Group	SSID	First Radio	Ch	Second Radio
	ap	Up	0	0	4 days 17 hrs 51 mins	Good	Access Points	-	802.11a	60	-
	ap	Up	0	0	11 days 19 hrs 37 mins	Mismatched	Access Points	-	802.11bg	11	802.11a
	Aruba800	Up	0	0	23 days 3 hrs 53 mins	Unknown	Access Points	-	-	-	-
	Cisco-4400-1	Up	0	0	1 day 23 hrs 27 mins	Mismatched	Access Points	-	-	-	-
	CN320-R024-02464	Up	0	0	2 days 20 hrs 59 mins	Unknown	Access Points	-	802.11abg	-	-
	Enterasys RoamAbout AP2000	Up	0	33	19 days 22 hrs 12 mins	Mismatched	Access Points	test012	802.11b	8	-
	newName	Up	0	0	12 days 7 hrs 21 mins	Mismatched	Access Points	-	802.11bg	11	802.11a
	Proxim-AP-4000-partner	Up	0	0	7 days 18 hrs 11 mins	Good	Access Points	proximnet	802.11bg	11	802.11a

8 APs/Devices

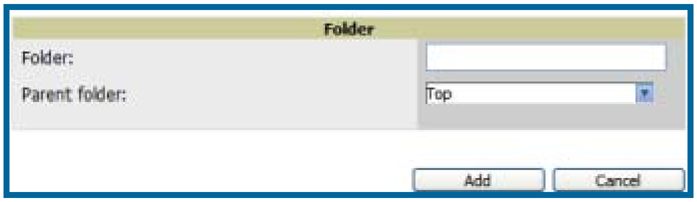
	Folder ▲	APs/Devices
	Florida	5
	New York	5

Add New Folder

In the figure above we see the **APs/Devices→Up** page for the East Cost folder. There are currently 8 up devices in the East Coast folder and 5 up devices in each of its sub folders. 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 on the Down link at the top of the page you will be taken to all of the down devices in the folder. If you want to see every down device click on the “Expand Folders to show all devices link”. When the folders are expanded you will see all of the devices on OV3600 that satisfy the criteria of the page. You will also see an additional column that lists the folder containing the AP. To add a folder click the “Add New Folder” link.

Figure 80. “Folder Creation” page



Folder

Folder:	
Parent folder:	Top

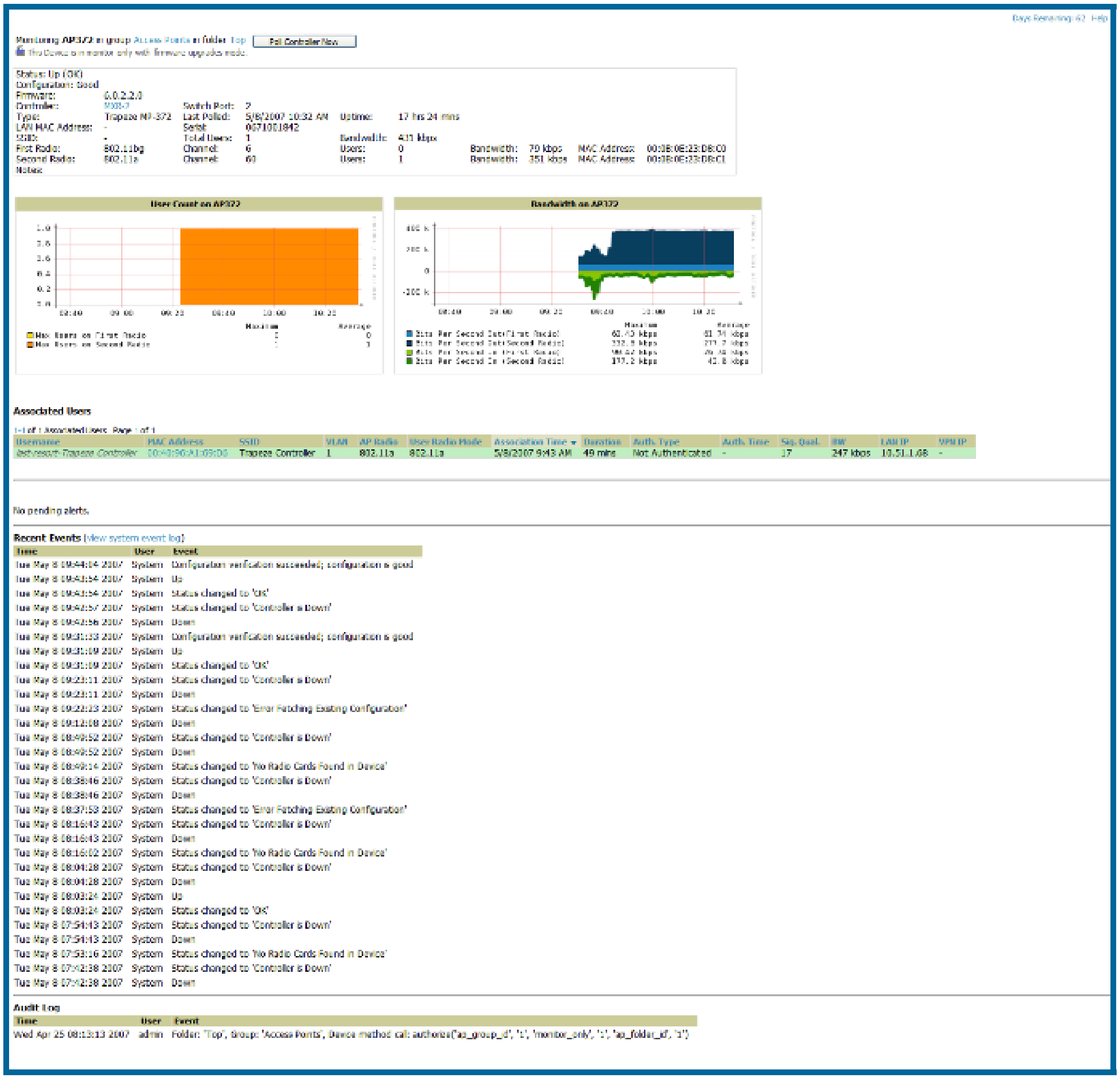
- Enter the name of the new folder
- Select the Parent folder.
- Click Add

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.

APs Monitoring

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

Figure 81. “APs/Devices→Monitor” page “Device Communication” area (note that some data on this page is displayed based on the device type)



Monitoring AP372 in group Access Points in folder Top

This Device is in monitor only with firmware upgrades mode.

Status: Up (OK)
Configuration: Good

Firmware:	6.0.2.2.0								
Controller:	MX8-7	Switch Port:	2						
Type:	Trapeze MP-372	Last Polled:	5/8/2007 10:32 AM	Uptime:	17 hrs 24 mins				
LAN MAC Address:	-	Serial:	0671001842						
SSID:	-	Total Users:	1	Bandwidth:	431 kbps				
First Radio:	802.11bg	Channel:	6	Users:	0	Bandwidth:	79 kbps	MAC Address:	00:0B:0E:23:D8:C0
Second Radio:	802.11a	Channel:	60	Users:	1	Bandwidth:	351 kbps	MAC Address:	00:0B:0E:23:D8:C1
Notes:									

User Count on AP372

	Maximum	Average
🟨 Max Users on First Radio	0	0
🟧 Max Users on Second Radio	1	1

Bandwidth on AP372

	Maximum	Average
🟦 Bits Per Second Out(First Radio)	61.43 kbps	61.34 kbps
■ Bits Per Second Out(Second Radio)	332.9 kbps	277.7 kbps
🟩 Bits Per Second In (First Radio)	98.42 kbps	26.48 kbps
🟩 Bits Per Second In (Second Radio)	177.2 kbps	42.8 kbps

Associated Users

1-1 of 1 Associated Users Page 1 of 1

Username	MAC Address	SSID	VLAN	AP Radio	User Radio Mode	Association Time ▾	Duration	Auth. Type	Auth. Time	Sig. Qual.	BW	LAN IP	VPN IP
dethesoutt-Trapeze Controller	00:40:96:A1:09:D0	Trapeze Controller	1	802.11a	802.11a	5/8/2007 9:43 AM	49 mins	Not Authenticated	-	17	247 kbps	10.51.1.68	-

No pending alerts.

Recent Events (view system event log)

Time	User	Event
Tue May 8 09:44:04 2007	System	Configuration verification succeeded; configuration is good
Tue May 8 09:43:54 2007	System	Up
Tue May 8 09:43:54 2007	System	Status changed to 'OK'
Tue May 8 09:42:57 2007	System	Status changed to 'Controller is Down'
Tue May 8 09:42:56 2007	System	Down
Tue May 8 09:31:33 2007	System	Configuration verification succeeded; configuration is good
Tue May 8 09:31:09 2007	System	Up
Tue May 8 09:31:09 2007	System	Status changed to 'OK'
Tue May 8 09:23:11 2007	System	Status changed to 'Controller is Down'
Tue May 8 09:23:11 2007	System	Down
Tue May 8 09:22:23 2007	System	Status changed to 'Error Fetching Existing Configuration'
Tue May 8 09:12:08 2007	System	Down
Tue May 8 08:49:52 2007	System	Status changed to 'Controller is Down'
Tue May 8 08:49:52 2007	System	Down
Tue May 8 08:49:14 2007	System	Status changed to 'No Radio Cards Found in Device'
Tue May 8 08:38:46 2007	System	Status changed to 'Controller is Down'
Tue May 8 08:38:46 2007	System	Down
Tue May 8 08:37:53 2007	System	Status changed to 'Error Fetching Existing Configuration'
Tue May 8 08:16:43 2007	System	Status changed to 'Controller is Down'
Tue May 8 08:16:43 2007	System	Down
Tue May 8 08:16:02 2007	System	Status changed to 'No Radio Cards Found in Device'
Tue May 8 08:04:28 2007	System	Status changed to 'Controller is Down'
Tue May 8 08:04:28 2007	System	Down
Tue May 8 08:03:24 2007	System	Up
Tue May 8 08:03:24 2007	System	Status changed to 'OK'
Tue May 8 07:54:43 2007	System	Status changed to 'Controller is Down'
Tue May 8 07:54:43 2007	System	Down
Tue May 8 07:53:16 2007	System	Status changed to 'No Radio Cards Found in Device'
Tue May 8 07:42:38 2007	System	Status changed to 'Controller is Down'
Tue May 8 07:42:38 2007	System	Down

Audit Log

Time	User	Event
Wed Apr 25 08:13:13 2007	admin	Folder: 'Top', Group: 'Access Points', Device method call: authorize('ap_group_id', '1', 'monitor_only', '1', 'ap_folder_id', '1')

The AP Monitoring Page has seven distinct sections: Text Status, Graph Statistics, QuickView (hidden by default), Associated Users, Alerts, Recent Events, and Audit Log.

- Locate the “General” area on the **APs/Devices→Monitor** page.

Field	Description
Poll Now/Poll Controller button	Polls the individual AP or the controller for a thin AP immediately; 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 (ok) 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

Field	Description
	blocked from connecting to the AP or the AP needs to be rebooted/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 will direct you to this specific AP's **APs/Devices→Audit** page where each mismatch will be highlighted.
*Portal **	Specifies the mesh AP acting as the wired connection to the network for this mesh AP.
*Mesh Mode **	Specifies whether the AP is a portal device or a mesh AP. The portal device is connected to the network over a wired connection. A mesh AP is a device downstream of the portal that uses wireless connections to reach the portal device.
*Hop Count **	The number of mesh links between this AP and the portal.
Type	The make and model of the access point.
Firmware	The firmware version running on the AP.
Last Polled	The most recent time OV3600 has polled the AP for information. The polling interval can be set on the Groups→Basic page.
Uptime	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	The MAC address of the Ethernet interface on the device.
Serial	The serial number of the device.
Radio Serial	The serial number of the radios in the device. *Note: This field is not available for all APs.*
Location	The SNMP location of the device.
Contact	The SNMP contact of the device.
IP	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.
SSID	The SSID of the primary radio.
Total Users	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	The Radio type of the first radio. (802.11a, 802.11b or 802.11g)
Second Radio	The Radio type of the second radio (802.11a, 802.11b or 802.11g.
Channel	The channel of the corresponding radio.
Users	The number of users associated to the corresponding radio at the time of the last polling.
Bridge Links	The number of bridge links for devices that are point-to-multi-point (see the **Groups→PTMP/WiMAX** page for more details).
*Mesh Links **	The total number of mesh links to the device including uplinks and downlinks.
Bandwidth	The amount of bandwidth being pushed through the corresponding radio interface or device at the time of the last polling.

Field	Description
MAC Address	The MAC address of the corresponding radio in the AP.
Last RAD Scan	The last time the device performed a wireless rogue scan and the number of devices discovered during the scan.
Notes	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.

** Note: These fields are only visible for Mesh APs.*

- Locate the "Statistics" link on the **APs/Devices→Monitor** page. This link launches the dot11counters graphs which includes:

  - 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

- 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.

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.

- Locate the "Associated Users" area on the **APs/Devices→Monitor** page. The "Associate Users" area lists details about the associated users. This information also appears on the **Users→All** page.

Field	Description
User	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.

Field	Description
MAC Address	Radio MAC address of the user associated to the AP. Also a link that redirects to the Users→Detail page.
Radio	The radio to which the user is associated.
Association Time	The first time OV3600 recorded the MAC address as being associated.
Duration	The length of time the MAC address has been associated.
Auth. Type	Type of authentication employed by the user, EAP, PPTP, RADIUS accounting, or not authenticated. EAP is only reported by Cisco VxWorks via SNMP traps. PPTP is supported by Colubris APs acting as VPNs. RADIUS accounting servers integrated with OV3600 will provide the RADIUS Accounting Auth type. All others will be considered not authenticated.
Auth. Time	How long ago the user authenticated.
Signal Quality	The average signal quality the user enjoyed.
BW	The average bandwidth consumed by the MAC address.
Location	The QuickView box allows users to view features including heatmap for a device and location history for a user.
LAN IP	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	The VPN IP of the user MAC. This information can be obtained from VPN servers that send RADIUS accounting packets to OV3600.

- Locate the “Pending Alerts” area on the **APs/Devices→Monitor** page. The “Pending Alerts” area will display all unacknowledged alerts for the AP.

- For Aruba/Alcatel-Lucent WLAN siwtches, 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.

- Locate the “Mesh Links” area on the **APs/Devices→Monitor** page. The “Mesh Links” section will display detailed information about all of the mesh links on the device.

- Locate the “View in Google Earth” area on the **APs/Devices→Monitor** page (this section will only be 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 on this button will open Google Earth and display the location of the AP. Google Earth will also display mesh and bridge links.

- The QuickView tool allows users at lower levels of administrative permissions (i.e. helpdesk staff) a window into OV3600’s VisualRF tool. By clicking on the location map on the **APs/Devices→Monitor** page you can see the heatmap for a device.

- QuickView runs faster than VisualRF because it has fewer features. It is geared toward resolving issues with single clients or single access points.

Field	Description
AP Name	The name of the AP that is linked with the currently viewed AP.
MAC Address	The radio MAC address of the AP that is linked with the currently viewed AP.

Field	Description
Link Time	The day and time when the link was initiated.
Duration	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	The RSSI observed between the two linked devices.
Hop Count	The number of hops between the device and its portal.

- 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.

Field	Description
Time	The day and time the event was recorded.
User	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	A short text description of the event.

- Locate the "Recent Events" area on the **APs/Devices→Monitor** page. The "Audit Log" area lists the most recent changes made to the AP.

Field	Description
Time	The day and time the event was recorded.
User	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	A text description of the change made to the device.

RAPIDS – Rogue Access Point Intrusion Detection System

Overview RAPIDS

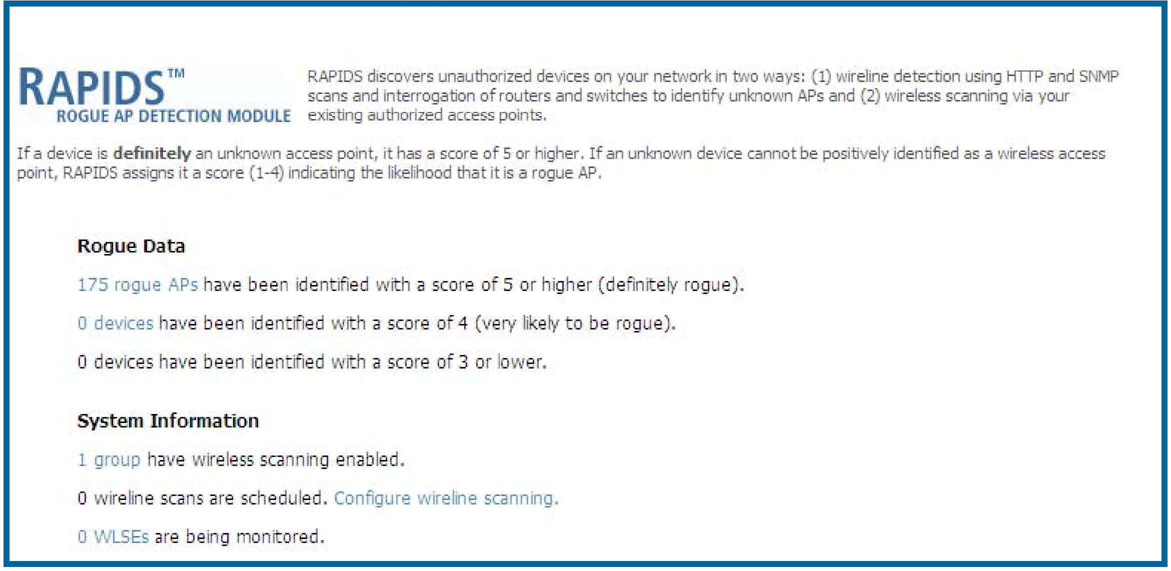
OV3600 provides the most comprehensive Rogue Access Point detection system in the industry. OV3600 enables organizations to leverage their existing wired and wireless infrastructure without requiring separate rogue scanning devices.

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

- Over the Air
  - Utilizing Enterprise APs (Intel, Symbol, Proxim, Avaya, and Colubris)
- On the Wire
  - Utilizing HTTP and SNMP Scanning
  - Interrogating Routers and Switches
  - Listening for OSU-NMS and WNMP messages
- Integration with External IDS systems
  - Cisco's WLSE (1100 and 1200 IOS). OV3600 fetches rogue information from the HTTP interface and gets new AP information from SOAP API.
  - AirMagnet Enterprise. AirMagnet Enterprise fetches a list of managed APs from OV3600.
  - AirDefense. AirDefense uses OV3600’s XML API to keep its list of managed devices up to date.
  - WildPackets OmniPeek. OmniPeek fetches a list of managed APs from OV3600.

The **RAPIDS→Overview** page provides a centralized view to all RAPIDS related services currently enabled on OV3600 plus pertinent statistics.

Figure 82. "RAPIDS →Overview" page



RAPIDS discovers unauthorized devices on your network in two ways: (1) wireline detection using HTTP and SNMP scans and interrogation of routers and switches to identify unknown APs and (2) wireless scanning via your existing authorized access points.

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

Rogue Data

175 rogue APs have been identified with a score of 5 or higher (definitely rogue).

0 devices have been identified with a score of 4 (very likely to be rogue).

0 devices have been identified with a score of 3 or lower.

System Information

1 group have wireless scanning enabled.

0 wireline scans are scheduled. Configure wireline scanning.

0 WLSEs are being monitored.

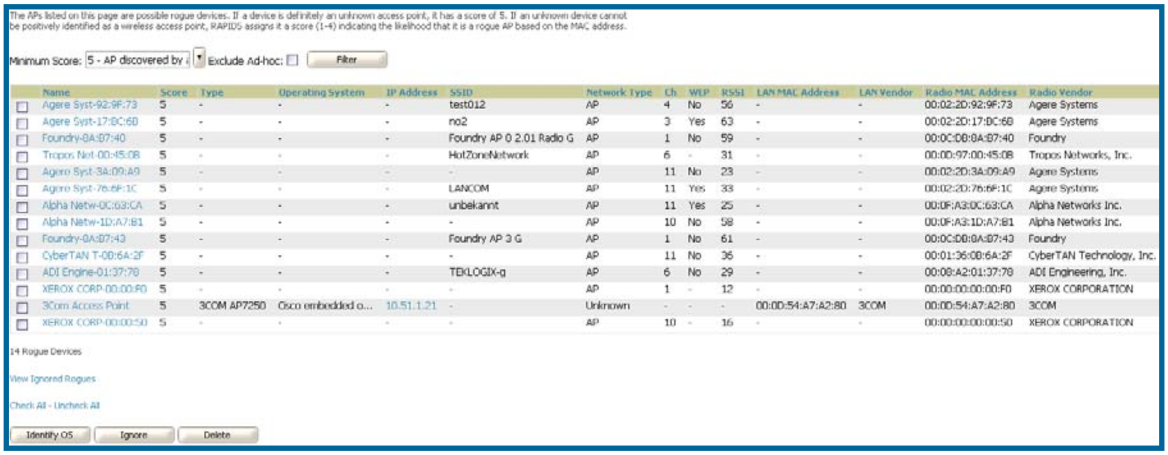
Variable	Description
# Rogue APs	Number of Access Points with a score of five, which means the AP was discovered over the air or matches an OV3600 HTTP or SNMP Rogue fingerprint. OV3600 has a very high level of certainty that these devices are rogue

Variable	Description
# Devices identified with a score of 7	Number of devices with a score of "7". These devices have been found on both the wired and the wireless networks. Any device with a score of 6 or more is definitely an unknown access point.
# Devices identified with a score of 6	Number of devices with a score of "6". These devices have been found on the wireless networks. Any device with a score of 6 or more is definitely an unknown access point.
# Devices identified with a score of 5	Number of devices with a score of "5". These devices have been discovered by a wireline rogue fingerprint.
# Devices identified with a score of 4	Number of devices with a score of "4". The devices have been discovered on the wired network by querying the Bridge Forwarding Tables on routers and switches. A Score of "4" means the OUI matches a block that belongs to a manufacturer which produces SOHO access points.
# Devices identified with a score of 3 or lower.	Number of devices with a score of "3". The devices have been discovered on the wired network by querying the Bridge Forwarding Tables on routers and switches. A Score of "3" means the OUI matches a block contains APs from vendors in the Enterprise and SOHO market.
# Routers and Switches	Number of Routers and switches participating in RAPIDS. OV3600 queries the Bridge Forwarding Table of each of these External devices and compares each downstream device's OUI against OV3600's Rogue OUI database. OV3600 scores the downstream device as to its likelihood of being a Rogue. Score 1: Any Device on the network Score 2: OUI belongs to a manufacturer that produces wireless (802.11) equipment. Score 3: OUI block contains access points (Enterprise and SOHO). Score 4: OUI block contains SOHO access points. Score 5: Discovered by a wireless scan or wireline rogue fingerprint.
# Groups	Number of Groups with wireless scanning enabled. This number is reflective of the full-time passive scanning supported by Proxim, Avaya, Colubris, and Symbol APs running 3.9.2. ***Groups → Radio page*** *"RAPIDS Scanning" radio button*
# Wireline Scans	Number of scheduled wireline scans. ***Device Setup → Discovery*** *– configure and schedule HTTP scans* ***System → Schedule*** *- view the schedule*
# WLSE	WLSEs monitored by OV3600. WLSE provides RF statistics including Rogue scanning information for 1100 and 1200 IOS access points. ***OV3600 Setup → WLSE***

RAPIDS → Rogue APs Page

The **RAPIDS→Rogue APs** page displays all rogue APs and all possible rogues. The device list is filtered by the minimum score selected in the dropdown menu.

Figure 83. “RAPIDS→Rogue APs” page



The APs listed on this page are possible rogue devices. If a device is definitely an unknown access point, it has a score of 5. If an unknown device cannot be positively identified as a wireless access point, RAPIDS assigns it a score (1-4) indicating the likelihood that it is a rogue AP based on the MAC address.

Minimum Score: 5 - AP discovered by ▾ Exclude Ad-hoc: □ Filter

	Name	Score	Type	Operating System	IP Address	SSID	Network Type	Ch	WEP	RSSI	LAN MAC Address	LAN Vendor	Radio MAC Address	Radio Vendor
□	Agere Syst-92:9F:73	5	-	-	-	test012	AP	4	No	56	-	-	00:02:2D:92:9F:73	Agere Systems
□	Agere Syst-17:0C:6B	5	-	-	-	no2	AP	3	Yes	63	-	-	00:02:2D:17:0C:6B	Agere Systems
□	Foundry-0A:07:40	5	-	-	-	Foundry AP 0 2.01 Radio G	AP	1	No	59	-	-	00:0C:DB:0A:07:40	Foundry
□	Tropos Net-00:45:0B	5	-	-	-	HotZoneNetwork	AP	6	-	31	-	-	00:0D:97:00:45:0B	Tropos Networks, Inc.
□	Agere Syst-3A:09:A9	5	-	-	-	-	AP	11	No	23	-	-	00:02:2D:3A:09:A9	Agere Systems
□	Agere Syst-76:6F:1C	5	-	-	-	LANCOM	AP	11	Yes	33	-	-	00:02:2D:76:6F:1C	Agere Systems
□	Alpha Netw-0C:63:CA	5	-	-	-	unbekannt	AP	11	Yes	25	-	-	00:0F:A3:0C:63:CA	Alpha Networks Inc.
□	Alpha Netw-1D:A7:B1	5	-	-	-	-	AP	10	No	58	-	-	00:0F:A3:1D:A7:B1	Alpha Networks Inc.
□	Foundry-0A:07:43	5	-	-	-	Foundry AP 3 G	AP	1	No	61	-	-	00:0C:DB:0A:07:43	Foundry
□	CyberTAN T-0B:6A:2F	5	-	-	-	-	AP	11	No	36	-	-	00:01:36:0B:6A:2F	CyberTAN Technology, Inc.
□	ADI Engine-01:37:78	5	-	-	-	TEKLOGIX-g	AP	6	No	29	-	-	00:08:A2:01:37:78	ADI Engineering, Inc.
□	XEROX CORP-00:00:F0	5	-	-	-	-	AP	1	-	12	-	-	00:00:00:00:00:F0	XEROX CORPORATION
□	3Com Access Point	5	3COM AP7250	Cisco embedded o...	10.51.1.21	-	Unknown	-	-	-	00:0D:54:A7:A2:80	3COM	00:0D:54:A7:A2:80	3COM
□	XEROX CORP-00:00:50	5	-	-	-	-	AP	10	-	16	-	-	00:00:00:00:00:50	XEROX CORPORATION

14 Rogue Devices

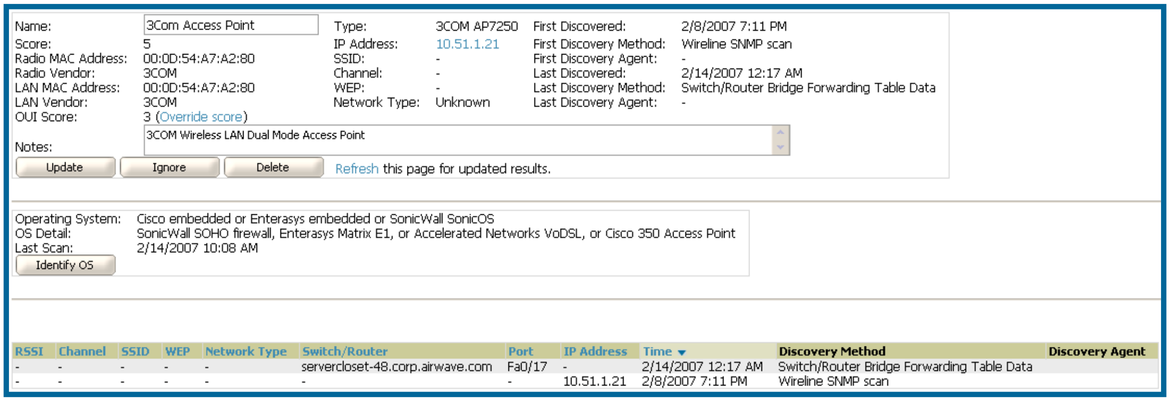
View Ignored Rogues

Check All - Uncheck All

Identify OS | Ignore | Delete

- Clicking on the device name launches the Rogue Detail page which provides additional Rogue information as well as historical view of all RAPIDS components which have discovered the device.
- Users with the role of “Admin” can see all rogues. Users with roles limited by folder can see a rogue if there is at least one discovering AP that they can also see. Discovery events from APs that are not visible to the user will not be clickable links, but they will still appear on the detail pages.

Figure 84. “RAPIDS→Rogue APs (Detail)” page



Name:	3Com Access Point	Type:	3COM AP7250	First Discovered:	2/8/2007 7:11 PM
Score:	5	IP Address:	10.51.1.21	First Discovery Method:	Wireline SNMP scan
Radio MAC Address:	00:0D:54:A7:A2:80	SSID:	-	First Discovery Agent:	-
Radio Vendor:	3COM	Channel:	-	Last Discovered:	2/14/2007 12:17 AM
LAN MAC Address:	00:0D:54:A7:A2:80	WEP:	-	Last Discovery Method:	Switch/Router Bridge Forwarding Table Data
LAN Vendor:	3COM	Network Type:	Unknown	Last Discovery Agent:	-
OUI Score:	3 (Override score)				
Notes:	3COM Wireless LAN Dual Mode Access Point				

Update | Ignore | Delete | Refresh this page for updated results.

Operating System: Cisco embedded or Enterasys embedded or SonicWall SonicOS
OS Detail: SonicWall SOHO firewall, Enterasys Matrix E1, or Accelerated Networks VoDSL, or Cisco 350 Access Point
Last Scan: 2/14/2007 10:08 AM
Identify OS

RSSI	Channel	SSID	WEP	Network Type	Switch/Router	Port	IP Address	Time ▾	Discovery Method	Discovery Agent
-	-	-	-	-	servercloset-48.corp.airwave.com	Fa0/17	-	2/14/2007 12:17 AM	Switch/Router Bridge Forwarding Table Data	
-	-	-	-	-	-	-	10.51.1.21	2/8/2007 7:11 PM	Wireline SNMP scan	

- Each Rogue device will typically have multiple discovery methods, all of which will be listed.

- As you work through the Rogue Devices use the Name and Notes fields to identify the AP and document its location. By utilizing these fields plus the multiple discovery agents you can triangulate where the Rogue is physically located in space and virtually located on the network. If you find the Rogue belongs to a neighboring business you can migrate it into an “ignored” state. Otherwise you want to extract the device from your building and delete the Rogue from the system.

- You can also use the global filtering options on the **RAPIDS→Setup** page to filter rogues according to signal strength, ad-hoc status, SSID.

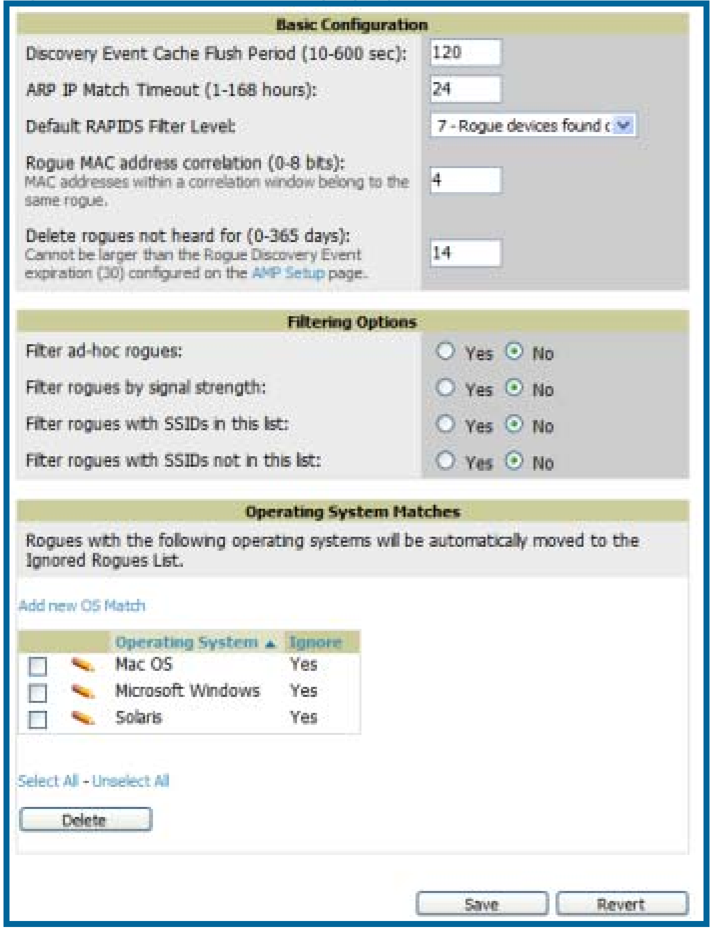
- The suggested workflow for RAPIDS is to first tackle devices ranked as 7 and connected to your wired network. Select all with an IP and OS fingerprint and navigate to the device detail page for remaining devices. Find the port and switch at which the device is located and shut down the port of follow wiring to the device. To mitigate the rogue remove it from the network and delete the rogue record. If you want to allow it on the network mark the device as “ignored” to elimiate future alerts.

Variable	Description
Name	User configurable name given to the rogue device.
Type	The model of the AP. Displayed if the AP is discovered using an http scan.
Discovery Method	APs can be discovered via a wireless AP scan, switch/router bridge forwarding table data or wireline HTTP scan.
Discovery Agent	The device that discovered the potential rogue.
Radio MAC Address	The radio MAC address of the rogue. Displayed if the AP is discovered via Wireless AP scans.
Radio Vendor	The owner of the OUI block of the Radio’s MAC address. Displayed if the device is discovered via Wireless AP scans.
SSID	The SSID of the rogue device. Displayed if the device is discovered via a wireless scan.
LAN MAC Address	The LAN MAC address of the device obtained from the bridge forwarding table of a router or switch.
LAN Vendor	The owner of the OUI block of the LAN MAC. The LAN vendor will not always be the same as the manufacturer of the device.
Channel	The channel used by the rogue device. Displayed only when the device is discovered by a wireless scan.
WEP	The encryption status of the AP. If yes then the AP is secured with WEP encryption.
Score	An index of the likelihood of a device being a rogue AP. The higher the score the more likely the device is an access point plugged into your network.
IP Address	The IP ddress of the device. OV3600 is able to get IP addresses by polling ARP data from routers and switches.
OUI Score	An index of the likelihood of a device being a rogue AP based on the first 6 digits of the LAN MAC.
Network Type	The type of network used by the rogue AP, either AP, Ad-Hoc or unknown. Displayed when the device is discovered by a wireless scan.
Operating System	OV3600’s best guess of the OS type of the rogue device based on a port scan performed by OV3600. OS detection helps weed out the false positives. It is rare for a rogue device to run Windows XP or Mac OS X.
OS Detail	Detailed information about the OS running on the rogue device.
Last Scan	The most recent operating system scan performed on the device.

Variable	Description
OS Detail	The probably OS based on the port scan performed by OV3600.
Notes	Free form text field.

RAPIDS→Setup Page

Figure 85. "RAPIDS→Setup" page



Basic Configuration

Discovery Event Cache Flush Period (10-600 sec):	120
ARP IP Match Timeout (1-168 hours):	24
Default RAPIDS Filter Level:	7 - Rogue devices found c
Rogue MAC address correlation (0-8 bits): MAC addresses within a correlation window belong to the same rogue.	4
Delete rogues not heard for (0-365 days): Cannot be larger than the Rogue Discovery Event expiration (30) configured on the AMP Setup page.	14

Filtering Options

Filter ad-hoc rogues:	○ Yes ● No
Filter rogues by signal strength:	○ Yes ● No
Filter rogues with SSIDs in this list:	○ Yes ● No
Filter rogues with SSIDs not in this list:	○ Yes ● No

Operating System Matches

Rogues with the following operating systems will be automatically moved to the Ignored Rogues List.

Add new OS Match

		Operating System ▲	Ignore
□		Mac OS	Yes
□		Microsoft Windows	Yes
□		Solaris	Yes

Select All - Unselect All

- On the **RAPIDS→Setup** page, locate the Basic Configuration section. This section allows you to set RAPIDS performance settings.

Setting	Default	Description
Discovery Event Cache Flush Period	300	Sets the length of time OV3600 will cache discovery event information before dumping it to the database.
ARP IP Match Time (1-168 hours)	24	Defines the size of the time window in which RAPIDS will correlate MAC addresses and IPs.
Default RAPIDS filter level	5	Defines the minimum rogue score to display on the **RAPIDS→Rogue APs** page. Rogues below the minimum score will not be reflected in the Rouges count in the OV3600 header.

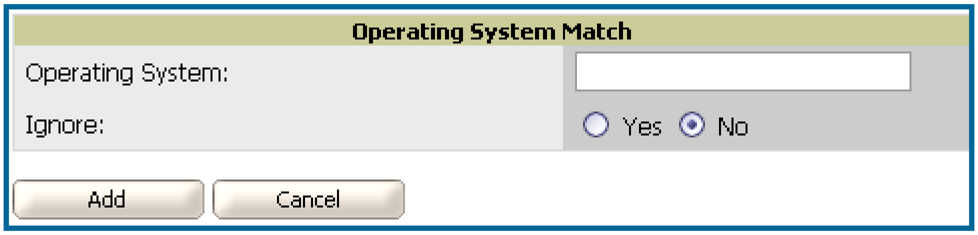
Setting	Default	Description
Rogue MAC address correlation	4	OV3600 will assume that MAC addresses of rogues that can be correlated to the same number of bits belong to the same rogue.
Delete rogues not heard for (0 – 365 days)	14	Rogues not heard for more than a certain number of days will be automatically deleted from OV3600. This setting cannot be larger than the Rogue Discovery Event expiration, which is configured on the **OV3600→Setup** page.

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

Setting	Default	Description
Filter ad-hoc rogues	No	Filter rogues according to ad-hoc status.
Filter rogues by signal strength	No	Filters rogues according to signal strength in dBm. Selecting "yes" will display a field for minimum signal strength. Rogues will not be recorded until they exceed the minium signal strength. It is important to pay attention to the use of a negative value as minimum signal strength. For exOV3600le, if "-85" is entered as the minimum signal strength a rogue with a value of -86 will be filtered, while a rogue with a score of -84 will be displayed.
Filter rogues with SSIDs in this list	No	Filters rogues according to select SSIDs. Selecting "yes" will display a text field to enter SSIDs (one per line). Rogues that have an SSID in the list *will* be filtered.
Filter rogue with SSIDs not in this list	No	Filters rogues according to select SSIDs. Selecting "yes" will display a text field to enter SSIDs (one per line). Rogues that have an SSID in the list *will not* be filtered.

- On the **RAPIDS→Setup** page, locate the Operating System Matches section. This section allows you to specify the Operating Systems that are considered safe. If Ignore is set to yes, any rogue device that returns the specified operating system will automatically be ignored.
- To enter additional operating systems to ignore click on the "Add new OS Match" link.

Figure 86. Adding an OS to Ignore.



Operating System Match

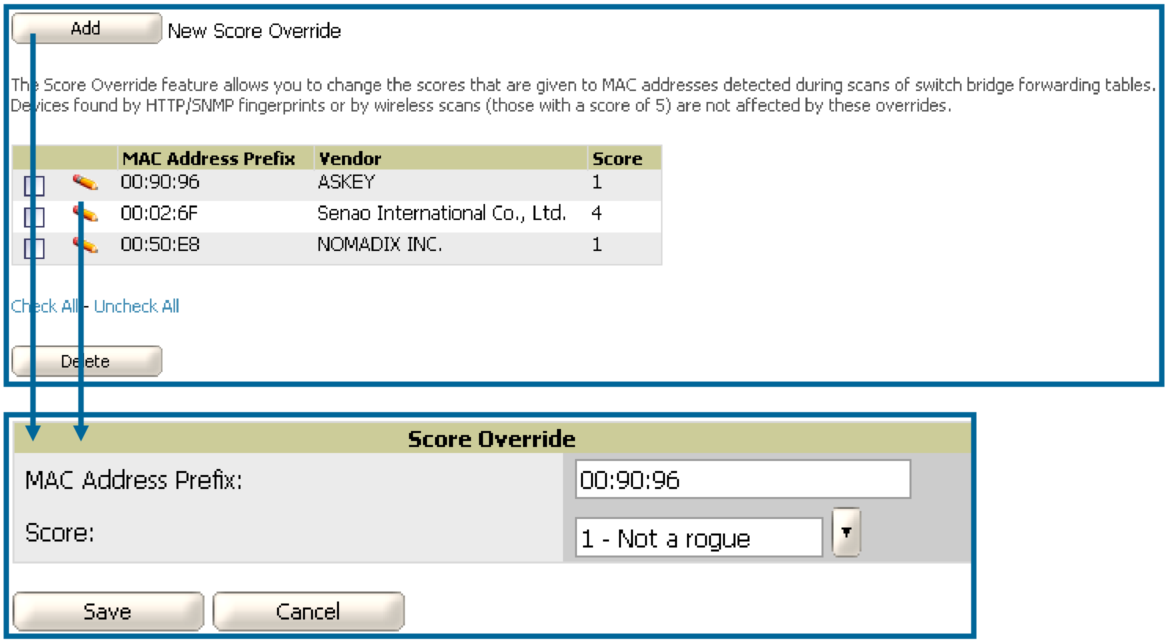
Operating System:	
Ignore:	○ Yes ● No

- Enter a substring to match. When “Yes” is selected any rogue device with an OS that matches the substring will be ignored. If “in” is entered into the Operating System field any OS name containing “in” will be ignored including wINdows, lINux and macINtosh. The substring match is not case sensitive. It is recommended you use the most specific string possible. Ideally cut and past the Operating System field from the details page of any rogue devices that you wish to ignore.

- Click Add to add the new OS Match

Rogue Score Override

The **RAPIDS→Score Override** page allows the user to override the score assigned to a MAC address prefix. If you have devices that you feel receive a high score than it should in your case you can adjust the score. Once a new score is assigned all devices with the specified MAC address prefix will receive the new score. Please note that rescoring a MAC Address Prefix poses a security risk. The block has received its score for a reason. Any rogues that fall within this block will receive the new score.



New Score Override

The Score Override feature allows you to change the scores that are given to MAC addresses detected during scans of switch bridge forwarding tables. Devices found by HTTP/SNMP fingerprints or by wireless scans (those with a score of 5) are not affected by these overrides.

		MAC Address Prefix	Vendor	Score
□	✎	00:90:96	ASKEY	1
□	✎	00:02:6F	Senao International Co., Ltd.	4
□	✎	00:50:E8	NOMADIX INC.	1

Check All - Uncheck All

Score Override

MAC Address Prefix: 00:90:96

Score: 1 - Not a rogue

Figure 87. "RAPIDS→Rogue APs (Detail)" page

- Clicking on the Edit or Add button will open the Score Override creation page. Enter in the 6-digit MAC prefix you wish to define a score for and select the desired score. Once the new score has been saved all detected devices with that prefix will receive the new score.

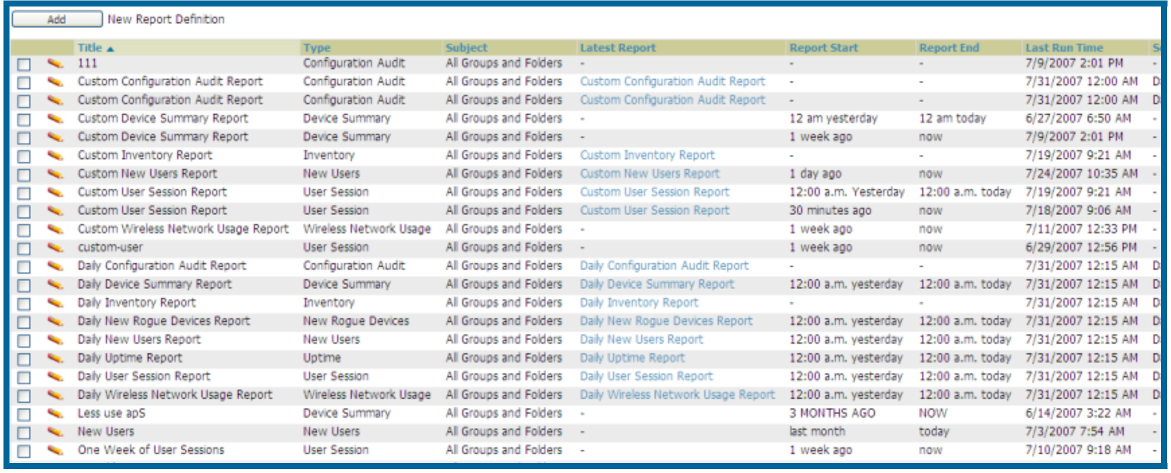
Reports

Overview

OV3600 has twelve report types: Wireless Network Usage, Inventory, Uptime, Device Summary, Capacity, New Rogue Devices, Configuration Audit, RAIDUS Authentication Issues, IDS Events, Memory and CPU Utilization, New User and User Session reports. OV3600 runs daily versions of all reports during predefined windows, minimizing downtime during nightly maintenance. All reports can be scheduled so that they can run in the background. AP Inventory and the Configuration Audit reports are the only reports that do not span a time period. They provide a detailed snapshot of the current state of the network. Users can create all other reports over a custom time period on the **Reports → Definitions** page. All reports can be emailed or exported to xml format for easy data manipulation via a spreadsheet.

Reports adhere to the access permissions defined for each OV3600 user. A user with the role “Admin” 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.

Figure 88. Reports→Definitions page



Add   New Report Definition

		Title ▲	Type	Subject	Latest Report	Report Start	Report End	Last Run Time	S
□	✎	111	Configuration Audit	All Groups and Folders	-	-	-	7/9/2007 2:01 PM	-
□	✎	Custom Configuration Audit Report	Configuration Audit	All Groups and Folders	Custom Configuration Audit Report	-	-	7/31/2007 12:00 AM	D
□	✎	Custom Configuration Audit Report	Configuration Audit	All Groups and Folders	Custom Configuration Audit Report	-	-	7/31/2007 12:00 AM	D
□	✎	Custom Device Summary Report	Device Summary	All Groups and Folders	-	12 am yesterday	12 am today	6/27/2007 6:50 AM	-
□	✎	Custom Device Summary Report	Device Summary	All Groups and Folders	-	1 week ago	now	7/9/2007 2:01 PM	-
□	✎	Custom Inventory Report	Inventory	All Groups and Folders	Custom Inventory Report	-	-	7/19/2007 9:21 AM	-
□	✎	Custom New Users Report	New Users	All Groups and Folders	Custom New Users Report	1 day ago	now	7/24/2007 10:35 AM	-
□	✎	Custom User Session Report	User Session	All Groups and Folders	Custom User Session Report	12:00 a.m. Yesterday	12:00 a.m. today	7/19/2007 9:21 AM	-
□	✎	Custom User Session Report	User Session	All Groups and Folders	Custom User Session Report	30 minutes ago	now	7/18/2007 9:06 AM	-
□	✎	Custom Wireless Network Usage Report	Wireless Network Usage	All Groups and Folders	-	1 week ago	now	7/11/2007 12:33 PM	-
□	✎	custom-user	User Session	All Groups and Folders	-	1 week ago	now	6/29/2007 12:56 PM	-
□	✎	Daily Configuration Audit Report	Configuration Audit	All Groups and Folders	Daily Configuration Audit Report	-	-	7/31/2007 12:15 AM	D
□	✎	Daily Device Summary Report	Device Summary	All Groups and Folders	Daily Device Summary Report	12:00 a.m. yesterday	12:00 a.m. today	7/31/2007 12:15 AM	D
□	✎	Daily Inventory Report	Inventory	All Groups and Folders	Daily Inventory Report	-	-	7/31/2007 12:15 AM	D
□	✎	Daily New Rogue Devices Report	New Rogue Devices	All Groups and Folders	Daily New Rogue Devices Report	12:00 a.m. yesterday	12:00 a.m. today	7/31/2007 12:15 AM	D
□	✎	Daily New Users Report	New Users	All Groups and Folders	Daily New Users Report	12:00 a.m. yesterday	12:00 a.m. today	7/31/2007 12:15 AM	D
□	✎	Daily Uptime Report	Uptime	All Groups and Folders	Daily Uptime Report	12:00 a.m. yesterday	12:00 a.m. today	7/31/2007 12:15 AM	D
□	✎	Daily User Session Report	User Session	All Groups and Folders	Daily User Session Report	12:00 a.m. yesterday	12:00 a.m. today	7/31/2007 12:15 AM	D
□	✎	Daily Wireless Network Usage Report	Wireless Network Usage	All Groups and Folders	Daily Wireless Network Usage Report	12:00 a.m. yesterday	12:00 a.m. today	7/31/2007 12:15 AM	D
□	✎	Less use apS	Device Summary	All Groups and Folders	-	3 MONTHS AGO	NOW	6/14/2007 3:22 AM	-
□	✎	New Users	New Users	All Groups and Folders	-	last month	today	7/3/2007 7:54 AM	-
□	✎	One Week of User Sessions	User Session	All Groups and Folders	-	1 week ago	now	7/10/2007 9:18 AM	-

Field	Description
Generation Time	The time OV3600 created the report.
Title	Title of the report.
Type	Type of the report. Either Wireless Network Usage, AP Inventory, AP Uptime, AP Summary or User Session.
Subject	The groups included in the report. When All Groups is selected on the Reports→Custom page Entire Network will appear as the subject on the Reports→List page.
Report Start	The beginning of the time period covered in the report.
Report End	The end of the time period covered in the report.

Viewing Reports

To view a report browse to the **Reports→Generated** page and click on the title of the report you wish to view. The reports are sorted by Generation Time. For quick access to reports there are links that may be bookmarked on the bottom of the **Reports→Generated** page. These bookmarks will display the most recently created report of the specified type. 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, where you wish to send the report.

Field	Description
Device	Name of the device.
Group	The Name of the device’s Group.
SNMP Uptime	The percentage of time the device was reachable via ICMP. OV3600 polls the device via SNMP at the rate specified on the **Groups→Basic** page.
ICMP Uptime	The percentage of time the device was reachable via ICMP. If the device is reachable via SNMP it is assumed to be reachable via ICMP. OV3600 only pings the device if SNMP fails and then it pings at the SNMP polling interval rate.
Time Since Last Boot	The uptime as reported by the device at the end of the time period covered by the report.
Average Uptime by Group	Average uptime of all the devices in the group.
Total Average Uptime	Average uptime of all the devices OV3600 is monitoring or managing.
Rank	The devices in each section of the device Summary report are ranked by the title field of each section.
Name	Name of the device.
Unique Users	Number of unique MAC address that have associated to the device in the report period.
Max Simult.	The largest number of simultaneous users observed during the report period.
Total Traffic	Total amount of Traffic pushed during the report period in megabytes.
Average Bandwidth	The average bandwidth in kilobits used on the device according to the device’s bandwidth counters. Almost all of this is user traffic. On some devices multicast data is counted as well.
Interval	The interval is based on the amount of time covered in the report as well as the age of the data in the report. Reports over recent time periods will have much smaller intervals and contain more information then a report of similar length 6 months ago.
Connected Users	Average number of connected users during the interval.
Type	The make and model of the access point.
Version	Firmware version of the access point.
LAN IP	The IP of the Ethernet interface on the device.
LAN/RADIO MAC Address	The MAC address of the radio and LAN interfaces.
Channel	The channel the device’s radio is using.

Field	Description
Uptime	The uptime as reported by the device when the device Inventory report is generated. This time is independent of OV3600.
SSID	Service Set Identifier (SSID) set on the device.
Serial	Serial number of the device. Only reported for certain Proxim and Colubris APs.
Radio Serial	Radio serial number. Only reported for certain Proxim and Colubris APs.
Notes	Any notes entered into the **APs/Devices→Manage** page.
Time Above x% of Capactiy	The amount of time the radio or interface spent broadcasting above the capacity threshold given in the report definition.
Capacity Combined	The combined bandwidth per second for both “in” and “out” paths summed together.
Usage While > Threshold (Combined, In and Out)	The average percent usage during the time that the usage is over the defined threshold (for bandwidth in, out, and combined).
Overall Usage (Combined, In,Out)	The average percent usage during the entire timespan of the report (for bandwidth in, out and combined).

- Click the Email This Report button to email the report to the address specified in the text box above the button

Exporting Reports

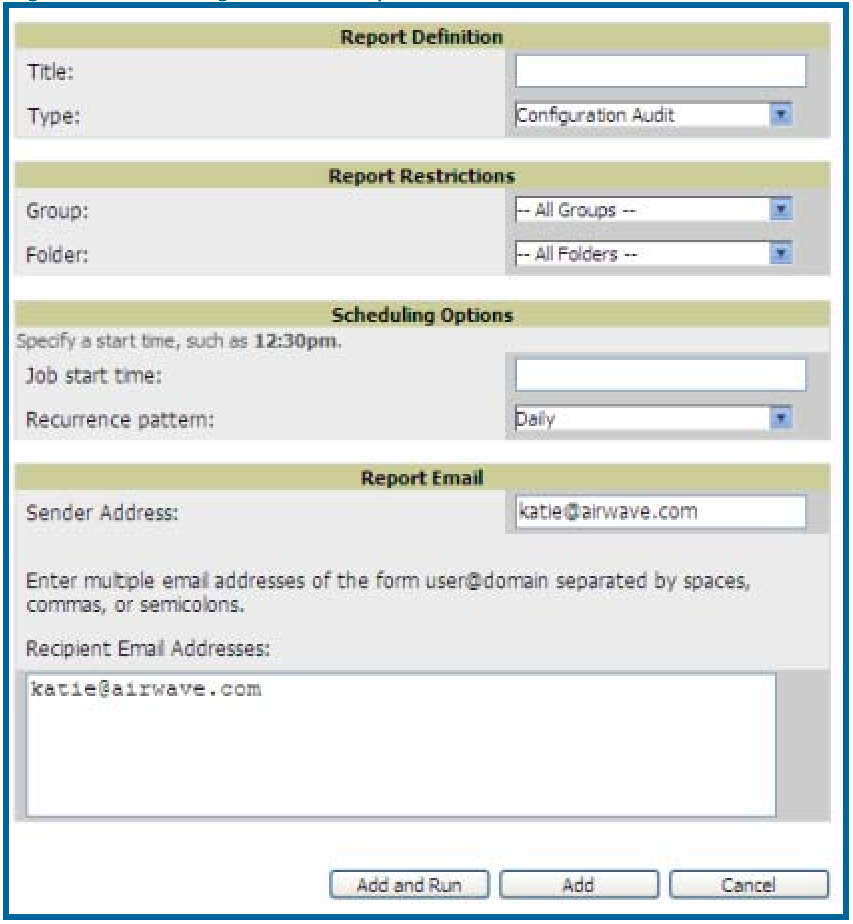
OV3600 allows users to export individual reports in xhtml form. These files may be read by an html browser or opened in Excel. To export the files

- Click on the “Link for XML (XHTML) Export” link.
- Save this file. To save it in Internet Explorer click File -->Save As. Save the file as a Web Page, HTML only file.
- Open the saved file with excel or a browser.

Creating Custom Reports

OV3600 allows users to create reports on any time period they wish. To create a custom report browse to the **Reports→Definition** page and click the “Add” button to add a new report definition, or click the pencil icon to edit an existing report definition.

Figure 89. Running a custom report.



Report Definition

Title:	
Type:	Configuration Audit

Report Restrictions

Group:	-- All Groups --
Folder:	-- All Folders --

Scheduling Options

Specify a start time, such as **12:30pm**.

Job start time:	
Recurrence pattern:	Daily

Report Email

Sender Address: katie@airwave.com

Enter multiple email addresses of the form user@domain separated by spaces, commas, or semicolons.

Recipient Email Addresses:

```
katie@airwave.com
```

- Enter a Report Title. It is recommended you use a title that is a meaningful and descriptive name for the report so it may be easily found on the **Reports→List** page.

- Choose the type of report you wish to create in the Report Type drop down menu.

- Specify the groups and folders that will 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 will appear, allowing you to choose which groups to include in the report.

  For some reports, like the user session report, “Report Start” and “Report End” fields will also appear. 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 5/5/2004 13:00 and an end date of 6/6/2004 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.

- Enter the job start time and select a recurrence pattern. Depending on the recurrence pattern selected you will get an additional dropdown menu. For exOV3600le, if you select a recurrence of “monthly” you will get an additional dropdown menu that allows you to pick which day of the month (day 1, day 2, etc.) the report should run.

- Enter the “Sender Address”. The sender address is what will appear in the “From” field of the report email.
- Specify the report recipients by entering an Email address or multiple addresses separated by commas in the text box.
- Click “Run” to generate the report immediately or click Schedule to schedule the report to run daily at the specified time.

Field	Description
Report Title	Name you wish to use to refer to the report.
Report Type	Drop-down menu that specifies which of the nine report types to create (see table below for more details).
Limit to Group	Drop-down menu that specifies which group to create the report for. Reports can be created for all groups or limited to one or more.
Limit to Folder	Drop-down menu that specifies which folder to create the report for. Reports can be created for all folders or limited to one or more.
Start Date/time	The report will start with data from this date.
End Date/Time	The report will contain data up to this date.
Email Address	The report will be mailed to this address when it finishes running. If left empty no email will be sent.

Report Type	Can by 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 maxium bandwidth capacity. Pulls data for AP radios or interfaces of universal devices (ifSpeed value).
Configuration Audit	No	Yes	Snapshot of the configuration of all monitored access points in OV3600.
Device Summary	Yes	Yes	Summarizes user and bandwidth stats and lists devices in OV3600.
Inventory	No	Yes	Audit of vendors, models and firmware versions of devices in OV3600.
New Rogue Devices	Yes	No	Shows new rogue devices by score, discovering AP, and MAC address vendor.
New Users	Yes	No	Summary list of new users, including username, MAC address, discovering AP, and association time.
RADIUS Authentication Issues	Yes	Yes	Summarizes RADIUS authentication issues by controller and by user, as well as a list of all issues.
User Session Report	Yes	Yes	Summarizes user data by radio mode, SSID and VLAN, as well as lists all sessions.
Wireless Network Usage	Yes	Yes	Summarizes bandwidth data and number of users.

IDS Events	Yes	Yes	Summarizes IDS events; can be limited to a summary of a certain number of events.
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.
Device Uptime	Yes	Yes	Summarizes device uptime within defined groups or folders.

- OV3600 utilizes 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 directly sending email to the specified recipient, use the following procedures to forward email to a “smarthost”.*

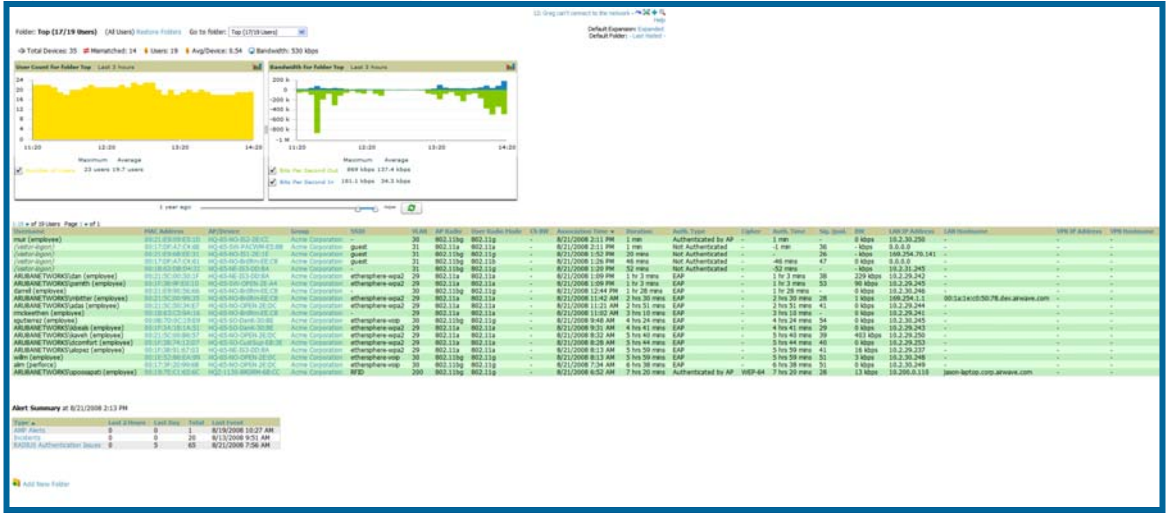
```
1. Add the following line to /etc/postfix/main.cf:
   relayhost = [mail.yourdomain.com]
   where mail.yourdomain.com is the IP address or hostname of
   your “smarthost”
2. Run service postfix restart
3. Send a test message to an email address
   Mail -v xxx@xxx.com
   Subject: test mail
   .
   CC: <press enter>
4. Check the mail log to ensure mail was sent
   tail -f /var/log/maillog
```

Users Page

Overview of the Users Page

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

Figure 90. “Users→Connected” Page



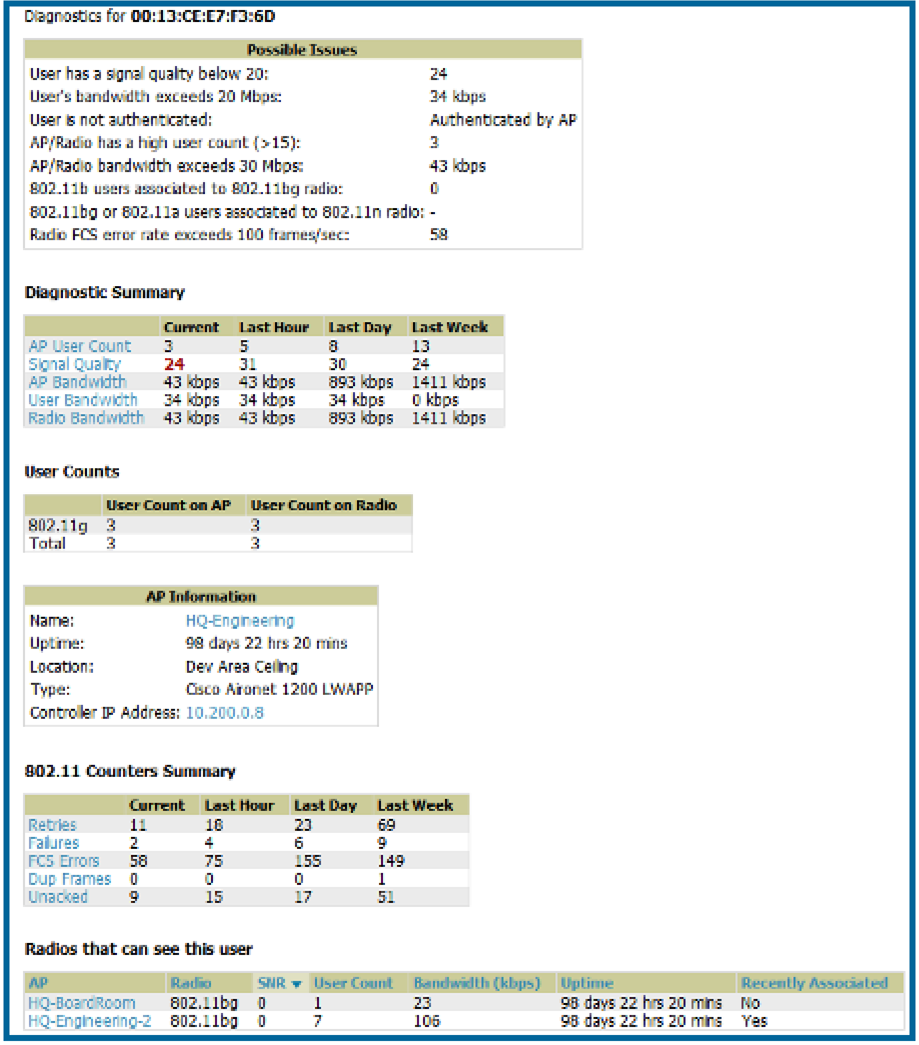
Field	Description
Username	Name of the User associated to the AP. OV3600 gathers this data in a variety of ways. It can be taken from RADIUS accounting data, traps from Cisco VxWorks APs and tables on Colubris APs.
MAC Address	Radio MAC address of the user associated to the AP. Also a link that redirects to the Users→Detail page.
AP/Device	The name of the AP the MAC address is associated to. Also a link that will take you to this AP’s Monitoring page.
Group	The group containing the AP that the user is associated with.
SSID	The SSID that the user is associated with.
VLAN	The VLAN assigned to the user.
AP Radio	The radio type of the radio that the user is associated with.
User Radio Mode	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	The first time OV3600 recorded the MAC address as being associated.
Duration	The length of time the MAC address has been associated.
Auth. Type	Type of authentication employed by the user, EAP, PPTP, RADIUS accounting, or not authenticated. EAP is only reported by Cisco VxWorks via SNMP traps. PPTP is supported by Colubris APs acting as VPNs. RADIUS accounting servers integrated with OV3600 will provide the RADIUS Accounting Auth type. All others will be considered not authenticated.

Field	Description
Cipher	Displays WEP with keys, WEP with 802.11x, WPA PSK (TKIP), WPA with 802.11x, WPA2 PSK (AES), or WPA2 with 802.11x (AES). This data is also displayed in the User Session report.
Auth. Time	How long ago the user authenticated.
Signal Quality	The average signal quality the user enjoyed.
BW	The average bandwidth consumed by the MAC address.
Location	The QuickView box allows users to view features including heatmap for a device and location history for a user.
LAN IP	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	The LAN hostname of the user MAC.
VPN IP	The VPN IP of the user MAC. This information can be obtained from VPN servers that send RADIUS accounting packets to OV3600.
VPN Hostname	The VPN hostname of the user MAC.

- The QuickView tool allows users at lower levels of administrative permissions (i.e. helpdesk staff) a window into OV3600's VisualRF tool. By clicking on the location map on the **User→Detail** page you can see the location history for a user.
- QuickView runs faster than VisualRF because it has fewer features. It is geared toward resolving issues with single clients or single access points.

Once you have clicked to a **Users→Detail** page from the **Users→Connected** list you can also view a diagnostics page for each user. The diagnostics page summarizes data for each user that can help to troubleshoot connectivity problems for the user on your network.

Figure 91. “Users→Diagnostics” page



Diagnostics for **00:13:CE:E7:F3:6D**

Possible Issues	
User has a signal quality below 20:	24
User's bandwidth exceeds 20 Mbps:	34 kbps
User is not authenticated:	Authenticated by AP
AP/Radio has a high user count (>15):	3
AP/Radio bandwidth exceeds 30 Mbps:	43 kbps
802.11b users associated to 802.11bg radio:	0
802.11bg or 802.11a users associated to 802.11n radio:	-
Radio FCS error rate exceeds 100 frames/sec:	58

Diagnostic Summary

	Current	Last Hour	Last Day	Last Week
AP User Count	3	5	8	13
Signal Quality	24	31	30	24
AP Bandwidth	43 kbps	43 kbps	893 kbps	1411 kbps
User Bandwidth	34 kbps	34 kbps	34 kbps	0 kbps
Radio Bandwidth	43 kbps	43 kbps	893 kbps	1411 kbps

User Counts

	User Count on AP	User Count on Radio
802.11g	3	3
Total	3	3

AP Information	
Name:	HQ-Engineering
Uptime:	98 days 22 hrs 20 mins
Location:	Dev Area Ceiling
Type:	Cisco Aironet 1200 LWAPP
Controller IP Address:	10.200.0.8

802.11 Counters Summary

	Current	Last Hour	Last Day	Last Week
Retries	11	18	23	69
Failures	2	4	6	9
FCS Errors	58	75	155	149
Dup Frames	0	0	0	1
Unacked	9	15	17	51

Radios that can see this user

AP	Radio	SNR ▼	User Count	Bandwidth (kbps)	Uptime	Recently Associated
HQ-BoardRoom	802.11bg	0	1	23	98 days 22 hrs 20 mins	No
HQ-Engineering-2	802.11bg	0	7	106	98 days 22 hrs 20 mins	Yes

- Navigate to the Diagnostics section of the **Users→Diagnostics** page. It displays common issues for wireless users in the left column, and the actual data for the user on your network is displayed on the right.
- Values on this page will be highlighted in red if they increase or drop by more than ten percent.

Field	Description
User has a signal quality below 20	A measure of the quality of signal the user enjoyed.
User’s bandwidth exceeds 20 Mbps	As reported by the device’s bandwidth counters.
User is not authenticated	User authentication protocols are defined in the device’s group.
AP/Radio has a user count of over 15	As reported by the device.

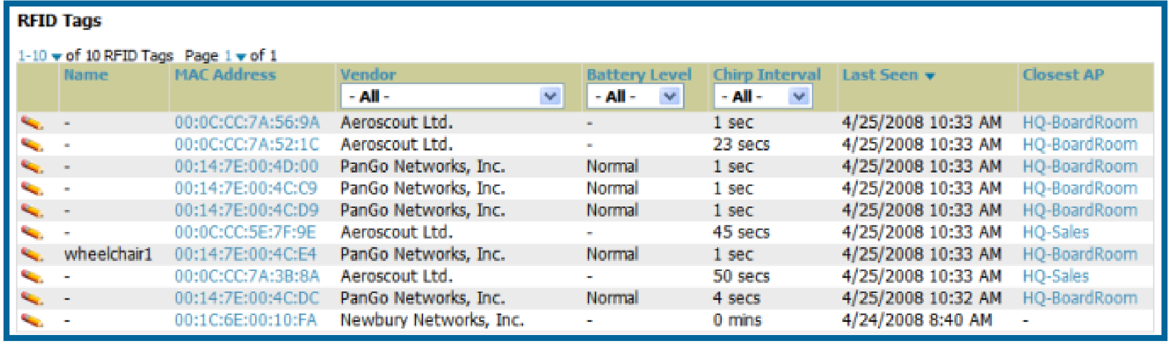
Field	Description
AP/Radio bandwidth exceeds 30 Mbps	As reported by the device's bandwidth counters.
802.11b users associated to 802.11 bg radio	As reported in the device's radio data.
802.11 bg or 802.11a radio users associated to n radio	As reported in the device's radio data.
Radio FCS error rate exceeds 100 frames/sec	This value is incremented when a Frame Check Sequence error is detected; it refers to additional checksum characters added when sending data to determine whether any data was lost in transit.

- Navigate to the Diagnostic Summary section of the **Users→Diagnostics** page. These sections summarize the user diagnostics data that has been collected currently and in the last hour, last day, and last week. Values are displayed in red when the data exceeds or misses the threshold defined in the "Possible Issues" box, i.e. when signal quality is below 20 or more than 15 users are associated to an AP or radio. Clicking on the blue link for any row in the table will display the information in graphical form.
- Users per radio are displayed in the User Counts box. This shows current data per radio and AP for the device to which the user is associated. Data is broken down by type (i.e., 802.11a).
- Basic information about the AP to which the users is associated is displayed in the AP Information box. This includes name, uptime, location, type and controller IP address (for thin APs).
- The 802.11 Counters Summary displays issues for the AP to which the user is associated. The summary of incidents is displayed according to incidents that are current and one hour, one day, and one week old. These counter summaries can offer some insight into interference and coverage for the access point. Clicking on the blue link for any row in the table will display the information in graphical form. The error counts will be driven up on networks with lots of activity, but identifying an unexpected spike in the counters can help to troubleshoot new problems.
- The Radios That Can See This User box shows radios on other access points that have reported the user, as well as basic information about those devices (such as uptime and user count). If the user has recently been associated to one of these radios the "Recently Associated" column will show "yes". Clicking on the blue link for any device in the table will take you to that AP's monitoring page.

Overview of the Users→Tags Page

The **Users→Tags** page.displays a list of wireless tags (Aeroscout, PanGo and Newbury) that are heard by thin APs and reported back to a controller that is monitored by OV3600. OV3600 displays the information it receives from the controller in a table on this page.

Figure 92. “Users→Tags page”



RFID Tags

1-10 ▾ of 10 RFID Tags Page 1 ▾ of 1

	Name	MAC Address	Vendor	Battery Level	Chirp Interval	Last Seen ▾	Closest AP
			- All -	- All -	- All -		
✎	-	00:0C:CC:7A:56:9A	Aeroscout Ltd.	-	1 sec	4/25/2008 10:33 AM	HQ-BoardRoom
✎	-	00:0C:CC:7A:52:1C	Aeroscout Ltd.	-	23 secs	4/25/2008 10:33 AM	HQ-BoardRoom
✎	-	00:14:7E:00:4D:00	PanGo Networks, Inc.	Normal	1 sec	4/25/2008 10:33 AM	HQ-BoardRoom
✎	-	00:14:7E:00:4C:C9	PanGo Networks, Inc.	Normal	1 sec	4/25/2008 10:33 AM	HQ-BoardRoom
✎	-	00:14:7E:00:4C:D9	PanGo Networks, Inc.	Normal	1 sec	4/25/2008 10:33 AM	HQ-BoardRoom
✎	-	00:0C:CC:5E:7F:9E	Aeroscout Ltd.	-	45 secs	4/25/2008 10:33 AM	HQ-Sales
✎	wheelchair1	00:14:7E:00:4C:E4	PanGo Networks, Inc.	Normal	1 sec	4/25/2008 10:33 AM	HQ-BoardRoom
✎	-	00:0C:CC:7A:3B:8A	Aeroscout Ltd.	-	50 secs	4/25/2008 10:33 AM	HQ-Sales
✎	-	00:14:7E:00:4C:DC	PanGo Networks, Inc.	Normal	4 secs	4/25/2008 10:32 AM	HQ-BoardRoom
✎	-	00:1C:6E:00:10:FA	Newbury Networks, Inc.	-	0 mins	4/24/2008 8:40 AM	-

Field	Description
Name	User-editable name associated with the tag.
MAC Address	MAC address of the AP that reported the tag.
Vendor	Vendor of the tag (Aeroscout, PanGo and Newbury) – display all or filter by type.
Battery Level	Filterable in dropdown menu at the top of the column; is not displayed for Aeroscout tags.
Chirp Interval	Filterable in dropdown menu at the top of the column.
Last Seen	Date and time the tag was last reported to OV3600.
Closest AP	The AP that last reported the tag to the controller (linked to the AP’s monitoring page in OV3600).

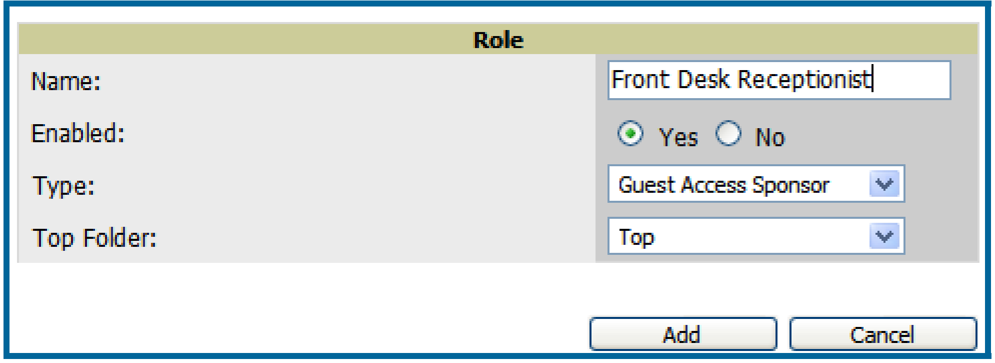
To edit the name of the tag, or to add notes to the tag’s record, click the pencil icon next to the entry in the list. You can then add or change the name and add notes like “maternity ward inventory” or “Chicago warehouse.”

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, consult the Alerts and Triggers section of this document.

Overview of the Users→Guest Users Page

OV3600 supports guest user provisioning for Aruba/Alcatel-Lucent WLAN switches and Airespace devices. This allows frontline staff, such as receptionists or help desk technicians, to grant wireless access to visitors or other temporary personnel. The first step in creating a guest access user is to define a role for the OV3600 users who will be responsible for this task, if those users are to have a role other than “Admin”. Navigate to the OV3600 Setup→Roles page and create a new role of type “Guest Access Sponsor”

Figure 92. “OV3600 Setup→Roles page”

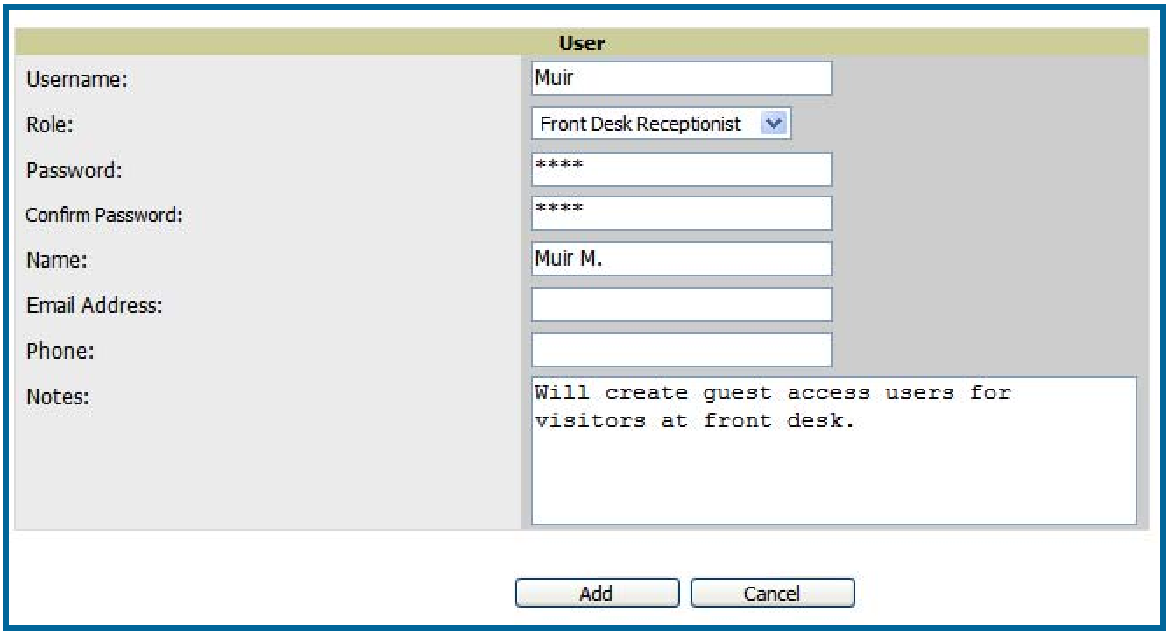


Role

Name:	Front Desk Receptionist
Enabled:	● Yes ○ No
Type:	Guest Access Sponsor
Top Folder:	Top

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 94. “OV3600 Setup→Users page”

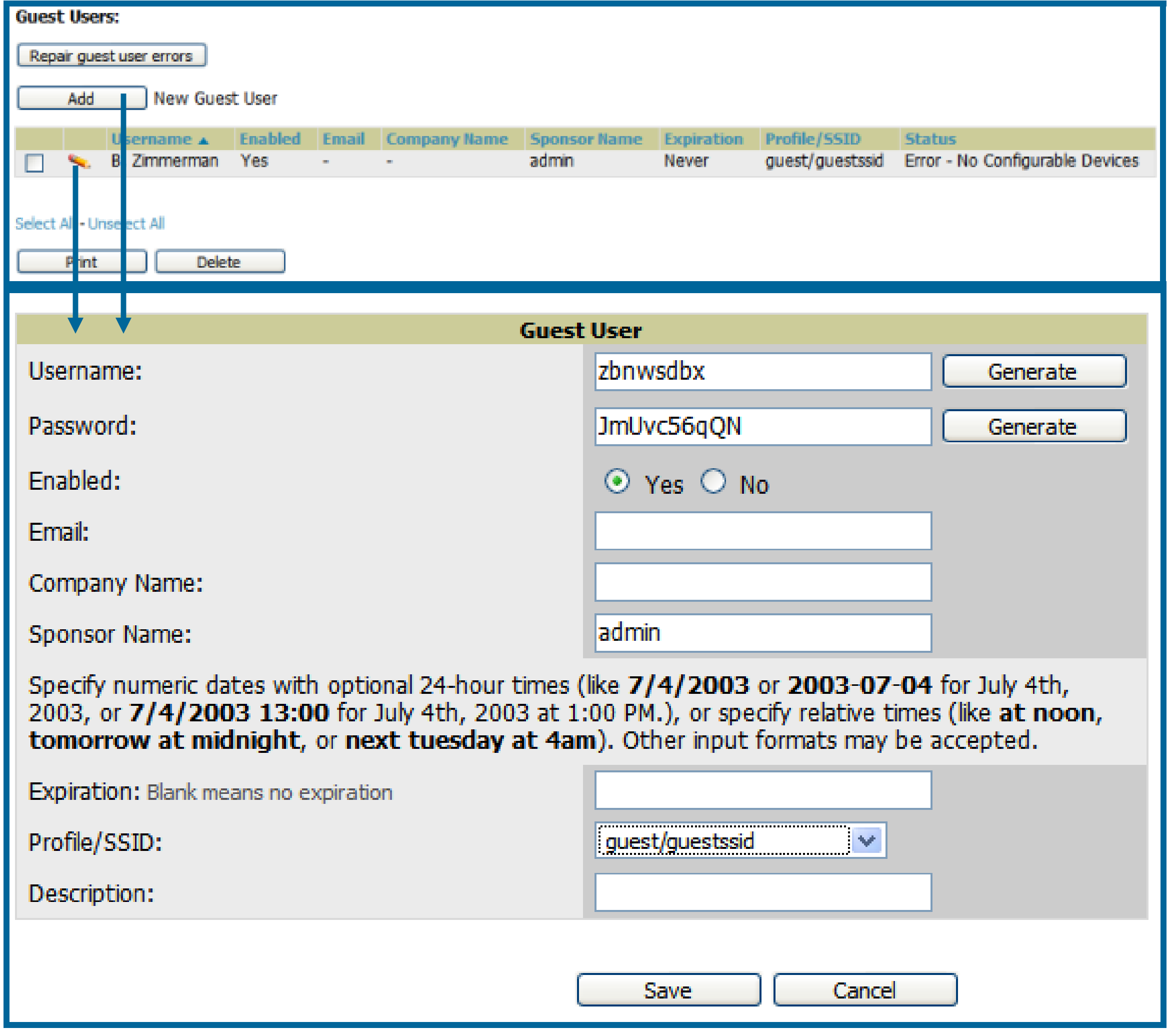


User

Username:	Muir
Role:	Front Desk Receptionist
Password:	****
Confirm Password:	****
Name:	Muir M.
Email Address:	
Phone:	
Notes:	Will create guest access users for visitors at front desk.

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. The next step in creating a guest access user is to navigate to the Users→Guest Users tab. From this tab, new guest users can be added or existing guest users can be edited. There is also a list of all guest users that shows data including the expiration date, the SSID (for Airespace) and other information.

Figure 95. “Users→Guest Users page”



Guest Users:

		Username ▲	Enabled	Email	Company Name	Sponsor Name	Expiration	Profile/SSID	Status
□		B Zimmerman	Yes	-	-	admin	Never	guest/guestssid	Error - No Configurable Devices

Guest User

Username:	zbnwsdbx
Password:	JmUvc56qQN
Enabled:	● Yes ○ No
Email:	
Company Name:	
Sponsor Name:	admin

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

Expiration: Blank means no expiration	
Profile/SSID:	guest/guestssid
Description:	

Field	Description
Repair Guest User Errors button	OV3600 will try to push the guest user again in an attempt to repair any errors in the Status column.
Add New Guest Users button	Add a new guest user to a controller via OV3600.
Username	Randomly generated on the guest user detail page.
Enabled	Status of guest user as active (enabled) or expired (disabled); configured on the guest user edit page.
Email	Optional, configured on the guest user edit page.
Company Name	Optional, configured on the guest user edit page.
Sponsor Name	Optional, configured on the guest user edit page.

Field	Description
Expiration	The date the guest user's access will expire; configured on the guest user add page.
Profile/SSID	Applies to Airespace only; the SSID the guest user can access.
Status	Reported by the controller; attempt to repair error messages with the "repair" button.
Print button (for checked users)	Sends the selected guest user's information to an external printer.
Delete button (for checked users)	Removes the selected guest user from OV3600 and from the controller.

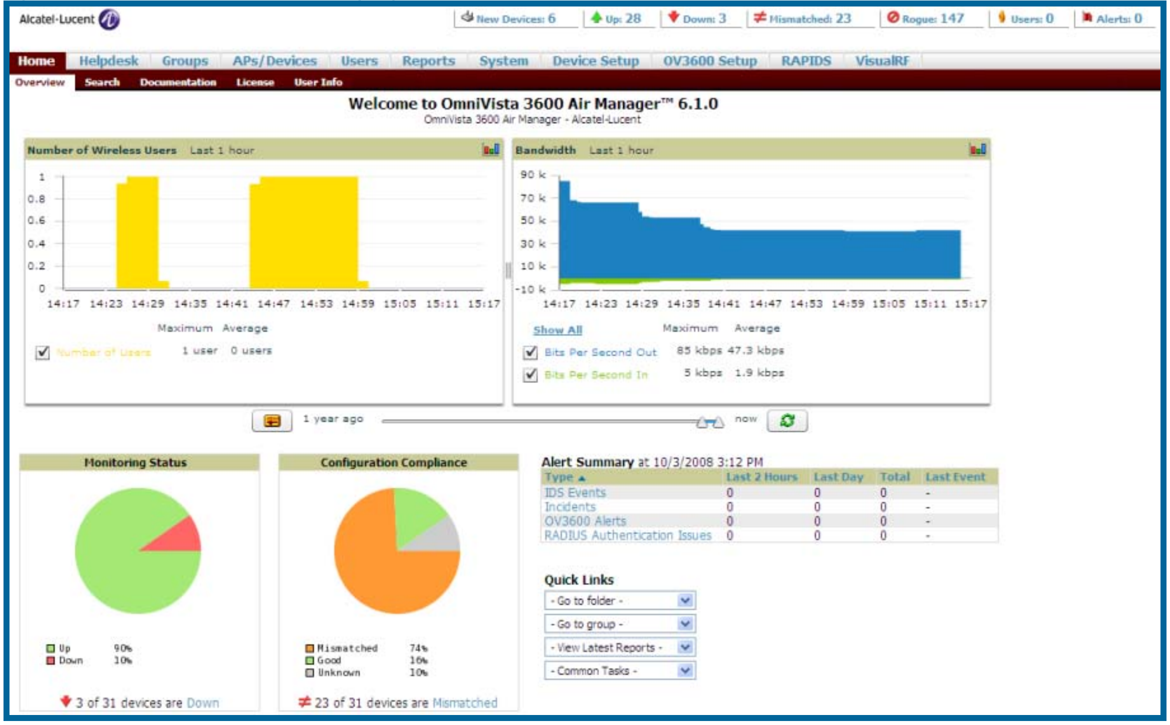
Guest users associated to the wireless network will appear on the same list as other wireless users, but will be identified as guest users in the SSID column. The User Detail page for a guest user also contain a box with the same guest information that appears for each user on the Users→Guest Users list.

Home Pages

Overview

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 on common links and shortcuts and view system information.

Figure 96. "Home→Overview" page



Welcome to OmniVista 3600 Air Manager™ 6.1.0

OmniVista 3600 Air Manager - Alcatel-Lucent

Alert Summary at 10/3/2008 3:12 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	-

Quick Links

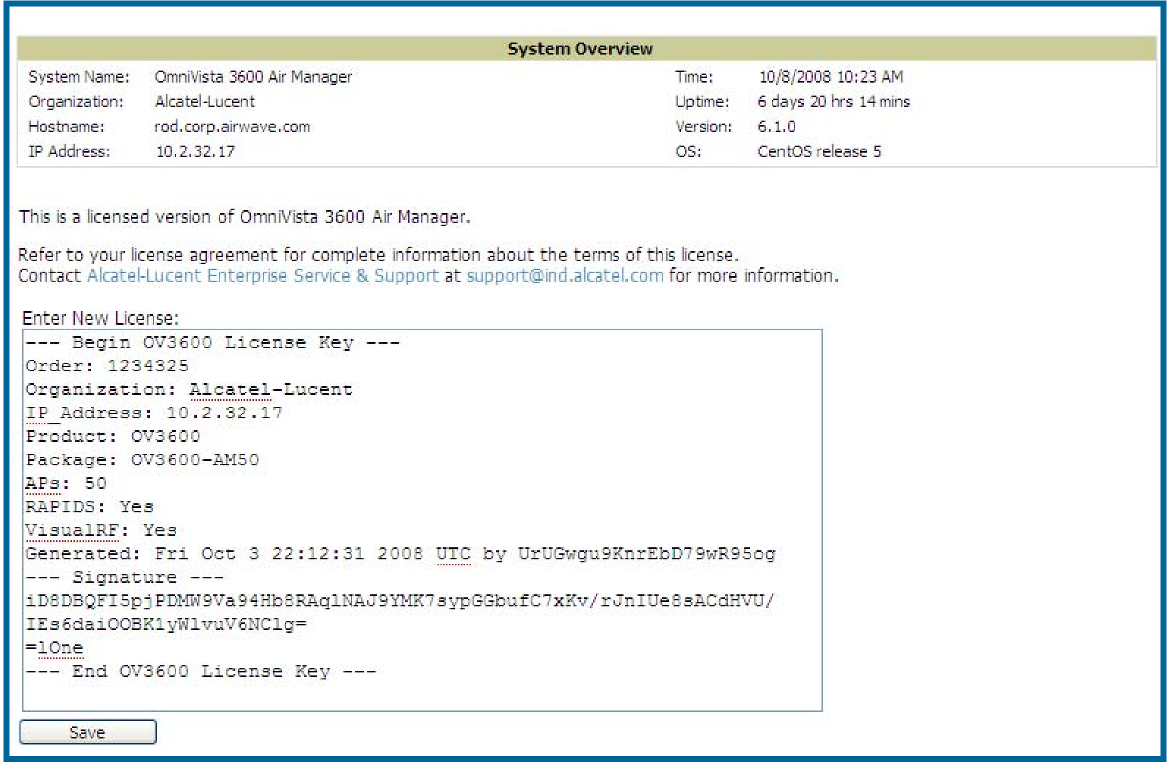
- Go to folder -

- Go to group -

- View Latest Reports -

- Common Tasks -

Figure 97. "Home→License" page



System Overview

System Name:	OmniVista 3600 Air Manager	Time:	10/8/2008 10:23 AM
Organization:	Alcatel-Lucent	Uptime:	6 days 20 hrs 14 mins
Hostname:	rod.corp.airwave.com	Version:	6.1.0
IP Address:	10.2.32.17	OS:	CentOS release 5

This is a licensed version of OmniVista 3600 Air Manager.

Refer to your license agreement for complete information about the terms of this license.
Contact Alcatel-Lucent Enterprise Service & Support at support@ind.alcatel.com for more information.

Enter New License:

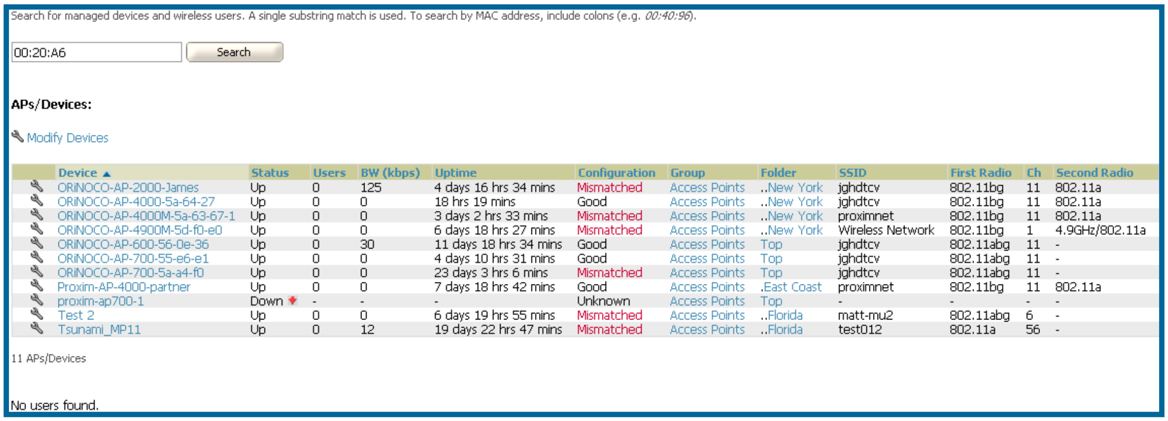
```
--- Begin OV3600 License Key ---
Order: 1234325
Organization: Alcatel-Lucent
IP_Address: 10.2.32.17
Product: OV3600
Package: OV3600-AM50
APs: 50
RAPIDS: Yes
VisualRF: Yes
Generated: Fri Oct 3 22:12:31 2008 UTC by UrUGwgu9KnrEbD79wR95og
--- Signature ---
iD8DBQFI5pjPDMW9Va94Hb8RAq1NAJ9YMK7sypGGbufC7xKv/rJnIUe8sACdHVU/
IEs6daiOOBK1yW1vuV6NC1g=
=1One
--- End OV3600 License Key ---
```

Field	Description
System Name	User-definable name for OV3600 (max. 20 characters).
Organization	The Organization listed on your license key.
Hostname	The DNS name assigned to OV3600.
IP Address	The static IP address assigned to OV3600.
Current Time	The current date and time set on OV3600.
Uptime	The amount of time since the operating system was last booted. Note: OV3600 processes get restarted daily as part of the nightly maintenance.
Software Version	The version number of OV3600 code currently running.
Operating system	The version of Linux installed on the server.
Latest Reports	Provides quick links to the most recently created report of the specified type.
Quick Links	Links to some common OV3600 tasks.
Search	Search for managed devices and wireless users. When searching for a MAC address colons are needed (e.g. 00:40:96).
Monitoring Status	Pie chart depicting the number of Up and Down APs.
Configuration Status	Pie chart depicting the number of mismatched APs.
Alert Summary	Summary of OV3600 Alerts, IDS Events, Incidents, RADIUS Authentication Issues.

Searching OV3600

The **Home→Search** page provides a simple way to find users and managed devices. Search performs partial string searches on a large number of fields including the notes, version, secondary version, radio serial number, device serial number, LAN MAC, radio MAC and apparent IP of all the APs as well as the client MAC, VPN user, User, LAN IP and VPN IP fields.

Figure 98. "Home→Search" page



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*).

00:20:A6

APs/Devices:

🔧 Modify Devices

	Device ▲	Status	Users	BW (kbps)	Uptime	Configuration	Group	Folder	SSID	First Radio	Ch	Second Radio
🔧	ORiNOCO-AP-2000-James	Up	0	125	4 days 16 hrs 34 mins	Mismatched	Access Points	..New York	jghdtcv	802.11bg	11	802.11a
🔧	ORiNOCO-AP-4000-5a-64-27	Up	0	0	18 hrs 19 mins	Good	Access Points	..New York	jghdtcv	802.11bg	11	802.11a
🔧	ORiNOCO-AP-4000M-5a-63-67-1	Up	0	0	3 days 2 hrs 33 mins	Mismatched	Access Points	..New York	proximnet	802.11bg	11	802.11a
🔧	ORiNOCO-AP-4900M-5d-f0-e0	Up	0	0	6 days 18 hrs 27 mins	Mismatched	Access Points	..New York	Wireless Network	802.11bg	1	4.9GHz/802.11a
🔧	ORiNOCO-AP-600-56-0e-36	Up	0	30	11 days 18 hrs 34 mins	Good	Access Points	Top	jghdtcv	802.11abg	11	-
🔧	ORiNOCO-AP-700-55-e6-e1	Up	0	0	4 days 10 hrs 31 mins	Good	Access Points	Top	jghdtcv	802.11abg	11	-
🔧	ORiNOCO-AP-700-5a-a4-f0	Up	0	0	23 days 3 hrs 6 mins	Mismatched	Access Points	Top	jghdtcv	802.11abg	11	-
🔧	Proxim-AP-4000-partner	Up	0	0	7 days 18 hrs 42 mins	Good	Access Points	.East Coast	proximnet	802.11bg	11	802.11a
🔧	proxim-ap700-1	Down ▼	-	-	-	Unknown	Access Points	Top	-	-	-	-
🔧	Test 2	Up	0	0	6 days 19 hrs 55 mins	Mismatched	Access Points	..Florida	matt-mu2	802.11abg	6	-
🔧	Tsunami_MP11	Up	0	12	19 days 22 hrs 47 mins	Mismatched	Access Points	..Florida	test012	802.11a	56	-

11 APs/Devices

No users found.

- Enter the text to search for. If you are searching for a MAC address be sure to put it in colon delimited format. Searching is case insensitive.
- Click search.

Home→Documentation Page

The Home→Documentation page provides easy access to all relevant OV3600 documentation. All of the documents on the Home Documentaiton page are hosted locally by OV3600 and can be viewed by any pdf viewer.

If you have any questions that are not answered by the documentation please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com.

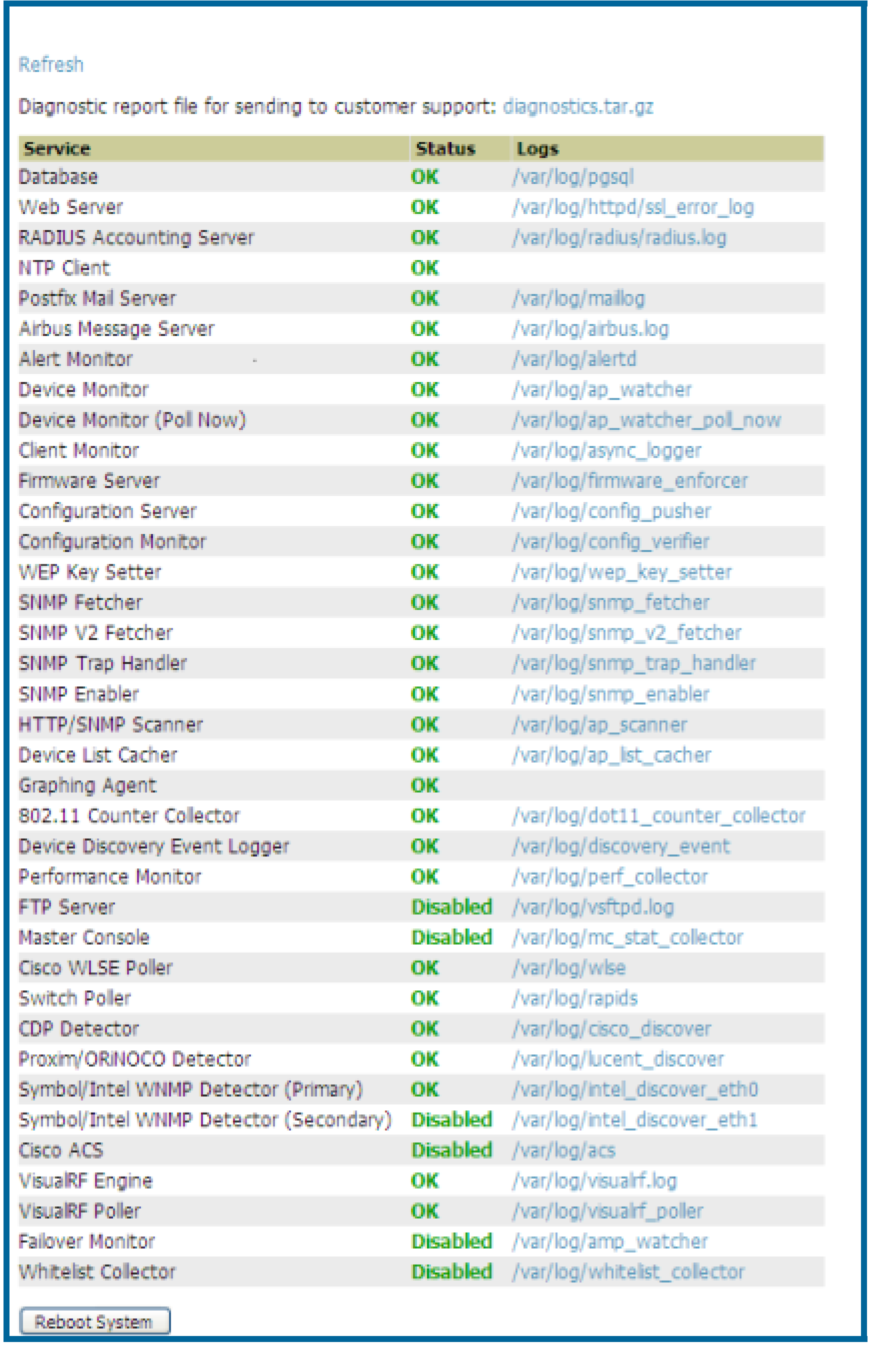
Home→User Info Page

The Home→User Info page displays information about the user logged in to OV3600 including the role, authentication type (local user or TACACS+) and access level. It also provides the user with the ability to change securely change their password without going through an OV3600 administrator. Users can also set preferences for the display of alerts in the OV3600 header – as well as the minimum alert severity to display – as well as the default number of records to appear in a list and the refresh rate for the console.

System Pages

The System Pages provide a centralized location for system wide OV3600 data and settings. The **System→Status Page** displays the status of all of OV3600 services. Services will either be OK, Disabled, or Down. OK and Disabled, displayed in green, are the expected states of the services. If any service is Down, displayed in red, please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com. The Reboot button provides a graceful way to restart your OV3600 remotely when it is needed.

Figure 101. "System→Status" page



Refresh

Diagnostic report file for sending to customer support: diagnostics.tar.gz

Service	Status	Logs
Database	OK	/var/log/pgsql
Web Server	OK	/var/log/httpd/ssl_error_log
RADIUS Accounting Server	OK	/var/log/radius/radius.log
NTP Client	OK	
Postfix Mail Server	OK	/var/log/maillog
Airbus Message Server	OK	/var/log/airbus.log
Alert Monitor	OK	/var/log/alertd
Device Monitor	OK	/var/log/ap_watcher
Device Monitor (Poll Now)	OK	/var/log/ap_watcher_poll_now
Client Monitor	OK	/var/log/async_logger
Firmware Server	OK	/var/log/firmware_enforcer
Configuration Server	OK	/var/log/config_pusher
Configuration Monitor	OK	/var/log/config_verifier
WEP Key Setter	OK	/var/log/wep_key_setter
SNMP Fetcher	OK	/var/log/snmp_fetcher
SNMP V2 Fetcher	OK	/var/log/snmp_v2_fetcher
SNMP Trap Handler	OK	/var/log/snmp_trap_handler
SNMP Enabler	OK	/var/log/snmp_enabler
HTTP/SNMP Scanner	OK	/var/log/ap_scanner
Device List Cacher	OK	/var/log/ap_list_cacher
Graphing Agent	OK	
802.11 Counter Collector	OK	/var/log/dot11_counter_collector
Device Discovery Event Logger	OK	/var/log/discovery_event
Performance Monitor	OK	/var/log/perf_collector
FTP Server	Disabled	/var/log/vsftpd.log
Master Console	Disabled	/var/log/mc_stat_collector
Cisco WLSE Poller	OK	/var/log/wlse
Switch Poller	OK	/var/log/rapids
CDP Detector	OK	/var/log/cisco_discover
Proxim/ORiNOCO Detector	OK	/var/log/lucent_discover
Symbol/Intel WNMP Detector (Primary)	OK	/var/log/intel_discover_eth0
Symbol/Intel WNMP Detector (Secondary)	Disabled	/var/log/intel_discover_eth1
Cisco ACS	Disabled	/var/log/acs
VisualRF Engine	OK	/var/log/visualrf.log
VisualRF Poller	OK	/var/log/visualrf_poller
Failover Monitor	Disabled	/var/log/amp_watcher
Whitelist Collector	Disabled	/var/log/whitelist_collector

- The link “diagnostics.tar.gz” will download a tar file that contains reports and logs that are helpful to support in troubleshooting and solving problems. Support may request that you submit this file along with other logs that are linked on this page. Logs that are contained in diagnostics.tar.gz include cron_stopped_maintenance, OV3600_events, OV3600_watcher, async_logger, ssl_error and pgsql.

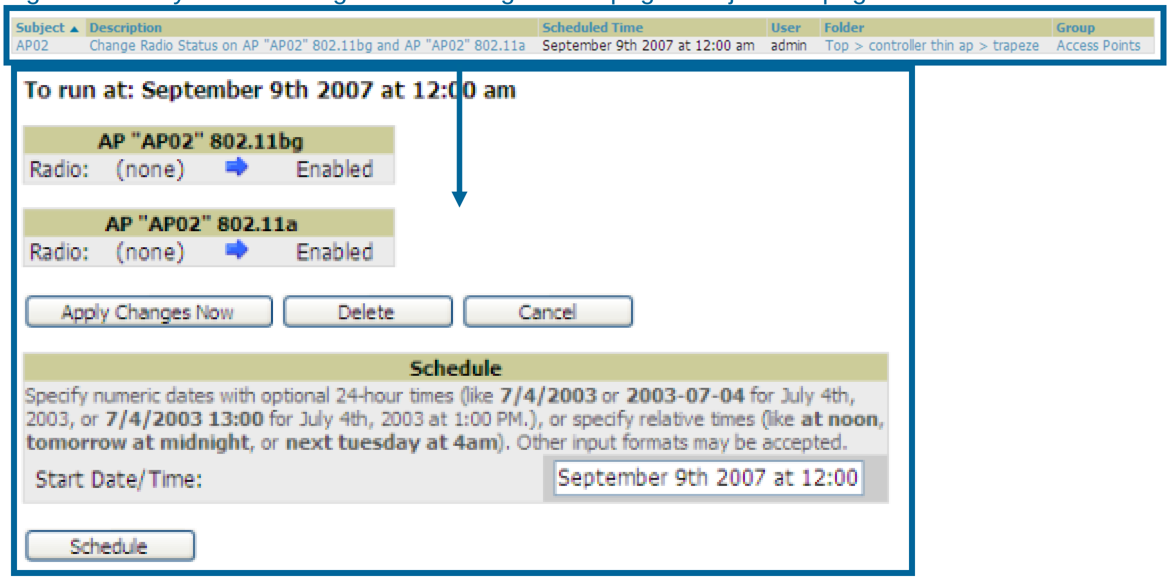
- A summary table of logs that appear on the **System→Status** page that are commonly used to diagnose OV3600 problems appears below. Additional logs are available via SSH access in the /var/log and /tmp directories; Support Engineers may request these logs for help in troubleshooting problems and will provide detailed instructions on how to retrieve them.

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 interface; please send this log to support whenever reporting an internal server error.
maillog	Useful for cases where emailed reports or alerts do not arrive at the intended recipient’s address.
radius	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.

Configuration Change Jobs

Schedule configuration change jobs are summarized on the **System→Configuration Change Jobs page**.

Figure 102. "System→Configuration Change Jobs" page and job edit page



Subject ▲	Description	Scheduled Time	User	Folder	Group
AP02	Change Radio Status on AP "AP02" 802.11bg and AP "AP02" 802.11a	September 9th 2007 at 12:00 am	admin	Top > controller thin ap > trapeze	Access Points

To run at: September 9th 2007 at 12:00 am

AP "AP02" 802.11bg			
Radio:	(none)	➡	Enabled

AP "AP02" 802.11a			
Radio:	(none)	➡	Enabled

Schedule

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

Start Date/Time: September 9th 2007 at 12:00

- 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.

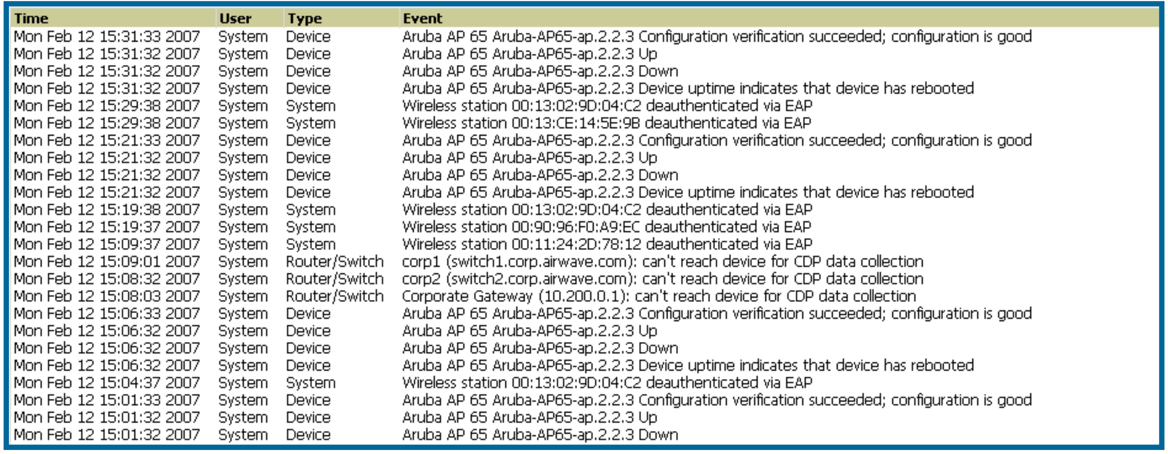
- Click the linked AP or group name under the “Subject” column to go to the monitoring page of the AP or group.

- Click the linked group and folder names under “Folder” or “Group” to go to the AP’s folder or group page.
- Scheduled configuration change jobs will also appear on the Manage page for an AP or the Monitoring page for a group.

Event Log

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 103. "System→Event Logs" page



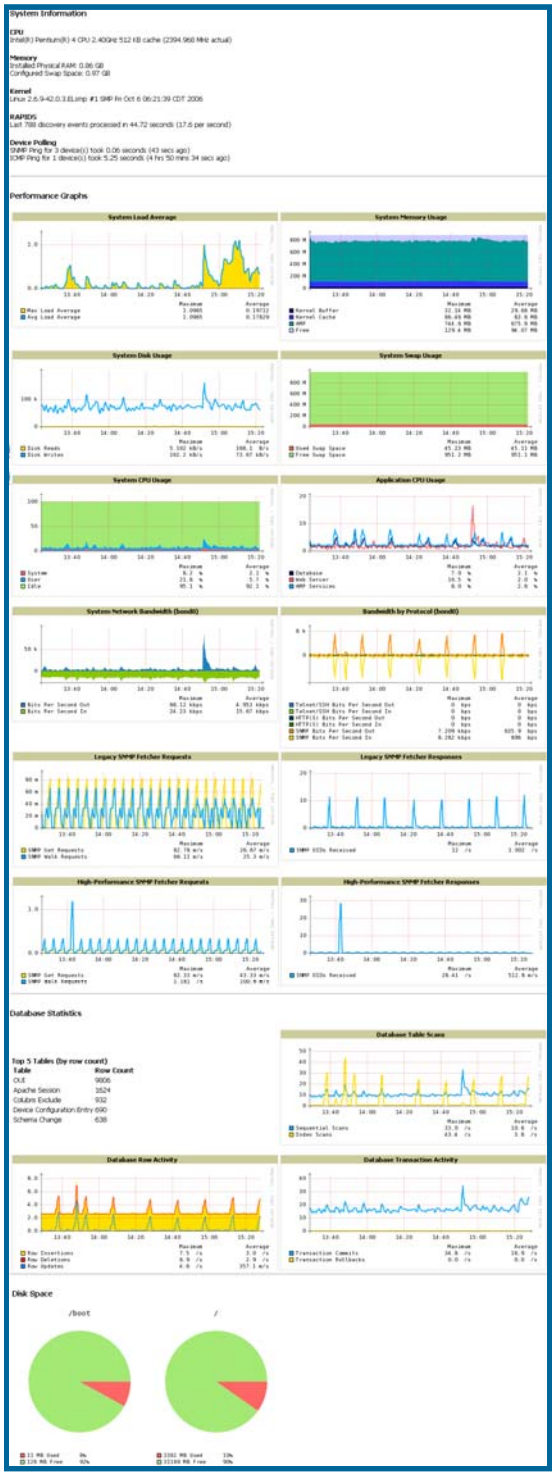
Time	User	Type	Event
Mon Feb 12 15:31:33 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good
Mon Feb 12 15:31:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Up
Mon Feb 12 15:31:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Down
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

Field	Description
Time	Date and time of the event.
User	The OV3600 user that triggered the event. When OV3600 itself is responsible for the event, System is displayed as the user.
Type	The Type of event recorded: 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.

Performance

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 useable polling period and track the health of OV3600 over time.

Figure 104. "OV3600 Setup→Performance" page



System Information

CPU
Intel(R) Pentium(R) 4 CPU 2.40GHz 512 KB cache (2394.960 MHz actual)

Memory
Installed Physical RAM: 0.86 GB
Configured Swap Space: 0.97 GB

Kernel
Linux 2.6.9-42.0.3.ELsmp #1 SMP Fri Oct 6 06:21:39 CDT 2006

RAPIDS
Last 788 discovery events processed in 44.72 seconds (17.6 per second)

Device Polling
SNMP Ping for 3 device(s) took 0.06 seconds (43 secs ago)
ICMP Ping for 1 device(s) took 5.25 seconds (4 hrs 50 mins 34 secs ago)

Performance Graphs

Database Statistics

Top 5 Tables (by row count)

Table	Row Count
OUI	9806
Apache Session	1624
Colubris Exclude	932
Device Configuration Entry	690
Schema Change	638

Disk Space

System Load Average
System Memory Usage
System Disk Usage
System Swap Usage
System CPU Usage
Application CPU Usage
System Network Bandwidth (bond0)
Bandwidth by Protocol (bond0)
Legacy SNMP Fetcher Requests
Legacy SNMP Fetcher Responses
High-Performance SNMP Fetcher Requests
High-Performance SNMP Fetcher Responses
Database Table Scans
Database Row Activity
Database Transaction Activity
/boot
/

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.
System Load Average	The System Load average is the number of jobs currently waiting to be processed. Load is a rough metric that will tell you how busy a server is. A typical OV3600 load is around 3. A constant load of 5 to 7 is cause for concern. A load above 10 is a serious issue and will probably result in an unusable OV3600. To lower the load average try increasing a few polling periods. Increasing the polling period for APs, routers/switches, WLSE, ACS, etc will decrease the amount of work OV3600 needs to perform and lower the load average. If you have a load that is consistently below 3 you might consider shortening your polling period and observing. *Note: If the load is less than one the y scale will be 1 to 1000 m standing for milli or 1/1000ths of 1.*
System Memory Usage	The amount of RAM that is currently used broken down by usage. It is normal for OV3600 to have very little free RAM. Linux automatically allocates all free ram as cache and buffer. If the kernel needs additional RAM for process it will dynamically take it from the cache and buffer.
System Disk Utilization	The amount of data read from the disk and written to the disk.
Swap Usage	The amount of Swap memory used by OV3600. Swap is used when the there is no more free physical RAM. A large performance penalty is paid when swap is used. If an OV3600 consistently uses swap you should consider installing additional RAM for the box.
System CPU Usage	The percentage of CPU that has been used by the user and the system as well as the amount that was idle.
Application CPU Usage	CPU usage broken down by application. OV3600 services includes all OV3600 processes except the database and the webserver.
System Network Bandwidth (Eth0)	All traffic in and out of Eth0 measured in bits per second.
Bandwidth by Protocol (Eth0)	Displays the amount of traffic used by Telnet, HTTPS and SNMP on Eth0.
Legacy SNMP Fetcher (SNMP Get/walk Requests)	The number of SNMP get and walk requests per second performed by the legacy (v1 and v3) SNMP fetcher.
Legacy SNMP Fetcher (SNMP OIDs Received)	The number of SNMP OIDs received per second performed by the legacy (v1 and v3) SNMP fetcher.
High Performance SNMP Fetcher (SNMP Get/walk Requests)	The number of SNMP get and walk requests per second performed by the high performance SNMP (v2c) fetcher.
High Performance SNMP Fetcher (SNMP OIDs Received)	The number of SNMP OIDs received per second performed by the high performance SNMP (v2c) fetcher.

Field	Description
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. It is recommended you decrease the length of time client data is stored on the **OV3600 Setup→General** page if a user/client table exceeds 250,000 rows.
Database Table Scans	The number of Database table scans performed by the database.
Database Row Activity	The number of insertions, deletions and updates performed to the database.
Database Tranaction 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 Setup→General** page or consider installing additional hard drive space.

There are several initial steps that can be taken to troubleshoot OV3600 performance problems, including slow page loads and timeout errors:

- Increasing the polling period settings on the **Groups→Basic** page.
- Increasing the polling period time for groups with routers and switches.
- Adding additional memory to the server. Please consult the sizing information in the latest edition of the OV3600 User Guide or contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com. for the latest recommendations.

Triggers & Alerts

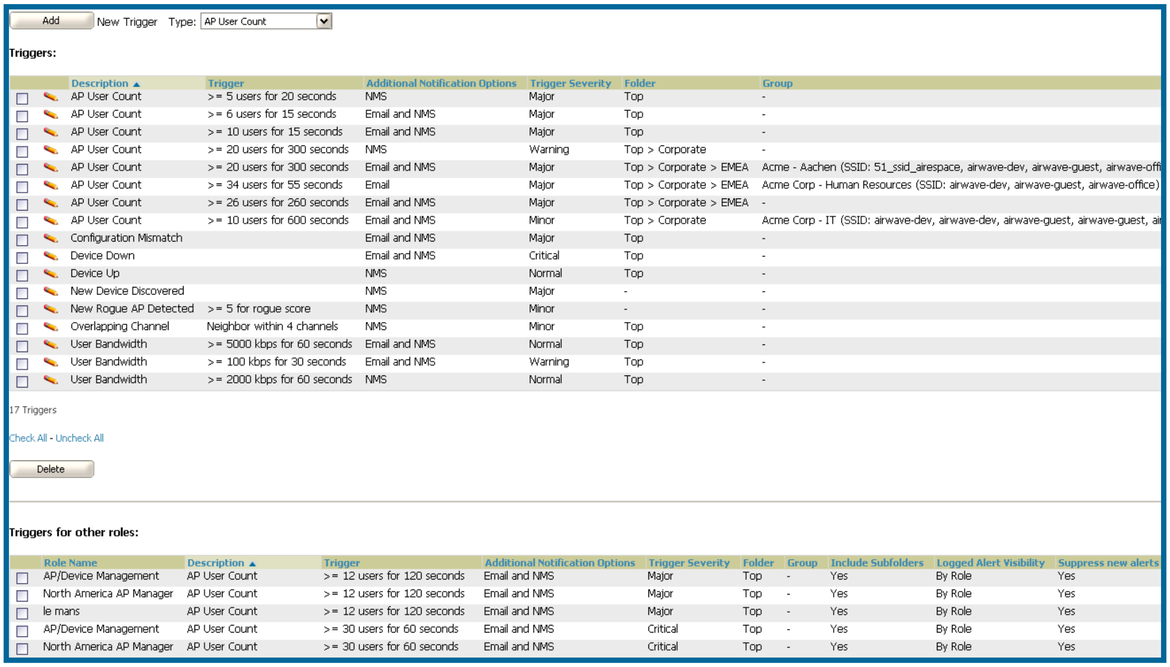
Overview Triggers & Alerts

OV3600 is designed to monitor key aspects of wireless LAN performance and to generate alerts when parameters are outside normal bounds, enabling problems to be addressed proactively before users are impacted. OV3600 provides two types of alerts: *normal alerts* that are triggered when a particular event occurs and *synthetic alerts* that are triggered when a condition persists for longer than a specified period. These synthetic alerts, enabled by OV3600's near real-time monitoring capabilities, help network administrators differentiate between minor, one-time events and sustained performance issues.

Setting Triggers

- To view defined system triggers, go to the **System→Triggers** page.

Figure 105. "System→Triggers" page



Add New Trigger Type: AP User Count

Triggers:

		Description ▲	Trigger	Additional Notification Options	Trigger Severity	Folder	Group
□	✎	AP User Count	>= 5 users for 20 seconds	NMS	Major	Top	-
□	✎	AP User Count	>= 6 users for 15 seconds	Email and NMS	Major	Top	-
□	✎	AP User Count	>= 10 users for 15 seconds	Email and NMS	Major	Top	-
□	✎	AP User Count	>= 20 users for 300 seconds	NMS	Warning	Top > Corporate	-
□	✎	AP User Count	>= 20 users for 300 seconds	Email and NMS	Major	Top > Corporate > EMEA	Acme - Aachen (SSID: 51_ssid_airespace, airwave-dev, airwave-guest, airwave-offi
□	✎	AP User Count	>= 34 users for 55 seconds	Email	Major	Top > Corporate > EMEA	Acme Corp - Human Resources (SSID: airwave-dev, airwave-guest, airwave-office)
□	✎	AP User Count	>= 26 users for 260 seconds	Email and NMS	Major	Top > Corporate > EMEA	-
□	✎	AP User Count	>= 10 users for 600 seconds	Email and NMS	Minor	Top > Corporate	Acme Corp - IT (SSID: airwave-dev, airwave-dev, airwave-guest, airwave-guest, ai
□	✎	Configuration Mismatch		Email and NMS	Major	Top	-
□	✎	Device Down		Email and NMS	Critical	Top	-
□	✎	Device Up		NMS	Normal	Top	-
□	✎	New Device Discovered		NMS	Major	-	-
□	✎	New Rogue AP Detected	>= 5 for rogue score	NMS	Minor	-	-
□	✎	Overlapping Channel	Neighbor within 4 channels	NMS	Minor	Top	-
□	✎	User Bandwidth	>= 5000 kbps for 60 seconds	Email and NMS	Normal	Top	-
□	✎	User Bandwidth	>= 100 kbps for 30 seconds	Email and NMS	Warning	Top	-
□	✎	User Bandwidth	>= 2000 kbps for 60 seconds	NMS	Normal	Top	-

17 Triggers

Check All - Uncheck All

Delete

Triggers for other roles:

	Role Name	Description ▲	Trigger	Additional Notification Options	Trigger Severity	Folder	Group	Include Subfolders	Logged Alert Visibility	Suppress new alerts
□	AP/Device Management	AP User Count	>= 12 users for 120 seconds	Email and NMS	Major	Top	-	Yes	By Role	Yes
□	North America AP Manager	AP User Count	>= 12 users for 120 seconds	Email and NMS	Major	Top	-	Yes	By Role	Yes
□	le mans	AP User Count	>= 12 users for 120 seconds	Email and NMS	Major	Top	-	Yes	By Role	Yes
□	AP/Device Management	AP User Count	>= 30 users for 60 seconds	Email and NMS	Critical	Top	-	Yes	By Role	Yes
□	North America AP Manager	AP User Count	>= 30 users for 60 seconds	Email and NMS	Critical	Top	-	Yes	By Role	Yes

- In OV3600, the triggers identified with an asterisk (*) below are automatically pre-configured. Other alerts are created using the *Create a New Trigger* pull-down menu.

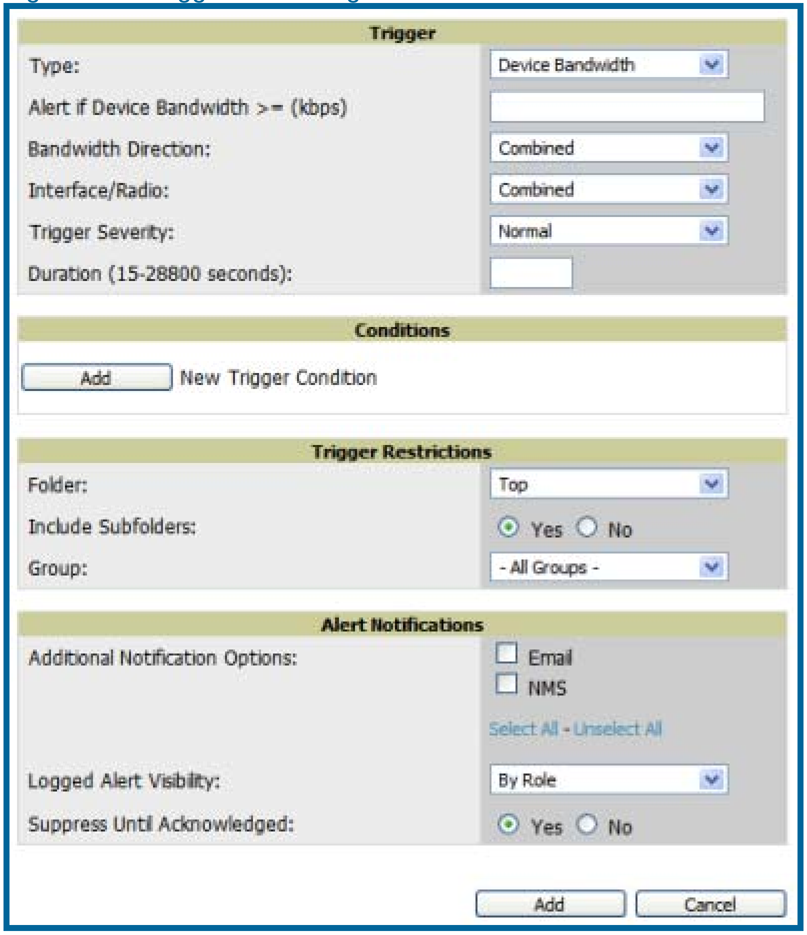
Trigger	Default	Description
Associated Users	None	A device (based on an inputed list of Mac addresses) has associated to the wireless network.
Configuration Mismatch	Yes	Actual configuration on the AP does not match the defined Group configuration policy.
*New Device Discovered**	Yes	OV3600 has discovered a new, manageable AP connected to the network (an AP that OV3600 can monitor and configure)
Device Down	None	An authorized, managed AP has failed to respond to OV3600's SNMP queries.

Trigger	Default	Description
Device Up	None	An authorized, previously down AP is now responding to SNMP queries.
Device IDS Events	None	The number of IDS events has exceeded a certain threshold, and/or lasted for more than a certain number of seconds.
802.11 QoS Counters	None	The rate of different paramenters including ACK Failures, Duplicated Frames and Transmitted Fragments. See dropdown Field menu in the conditions section of the trigger page for a complete list of parameters.
802.11 Frame Counters	None	The rate of different paramenters including ACK Failures, Retry Rate and Rx Fragment Rate. See dropdown Field menu in the conditions section of the trigger page for a complete list of parameters.
AP User Count	None	The number of user devices associated to an AP has exceeded a predefined threshold for more than a specified period, in seconds (i.e., "> 10 users associated for more than 60 seconds").
Device Bandwidth	None	The total bandwidth through the AP has exceeded a predefined threshold for more than a specified period, in seconds (i.e., "> 1500 kbps for more than 120 seconds"). You can also select bandwidth direction and interface/radio.
Device Resource	None	The CPU or memory utilization for a device has exceeded a defined a defined percentage for a specified period of time.
Disk Usage	None	Disk usage for the OV3600 server has met or surpassed a defined threshold.
New User		A new user has associated to a device within a defined set of groups or folders.
Total/Device/User RADIUS Authentication Issues	None	The threshold for the maximum number of failures before an alert is issued for a user, a device, or in total.
User Bandwidth	None	The sustained rate of bandwidth used by an individual user has exceeded a predefined threshold for more than a specified period, in seconds (i.e., "> 1500 kbps for more than 120 seconds").
Overlapping Channel	None	The neighboring AP is within a specified number of channels. *Note: This is calculated based on the AP with the most roams as reflected on the* ***APs/Devices→Manage*** *page Neighbors section.*
Failed Firmware Upgrade	None	An attempted firmware upgrade failed.
*New Rogue AP Detected**	None	A device has been discovered with the specified Rogue Score. Ad-hoc devices can be automatically excluded from this trigger by selecting the "Yes" button. See the RAPIDS section for more information on score definitions and discovery methods.
Radio Down	None	A device's radio is down.

Trigger	Default	Description
Inactive Tag	None	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.

- To create a new trigger, use the *Create a New Trigger* pull-down menu, highlight the type of trigger to be created, and click “Add”.

Figure 106. Trigger Detail Page



Trigger

Type:	Device Bandwidth
Alert if Device Bandwidth >= (kbps)	
Bandwidth Direction:	Combined
Interface/Radio:	Combined
Trigger Severity:	Normal
Duration (15-28800 seconds):	

Conditions

Add New Trigger Condition

Trigger Restrictions

Folder:	Top
Include Subfolders:	● Yes ○ No
Group:	- All Groups -

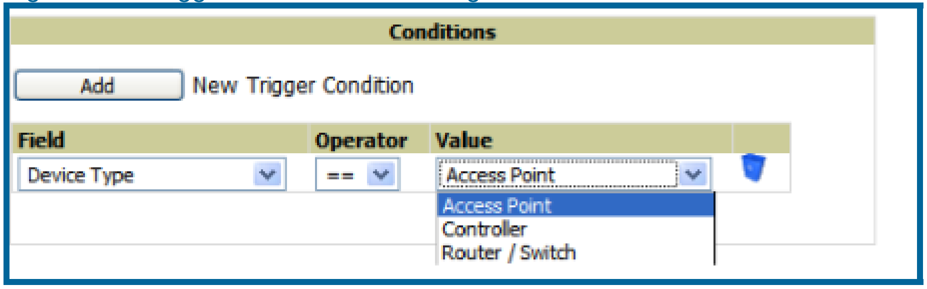
Alert Notifications

Additional Notification Options:	□ Email □ NMS Select All - Unselect All
Logged Alert Visibility:	By Role
Suppress Until Acknowledged:	● Yes ○ No

- OV3600 will automatically navigate to the Trigger Detail page, where you will specify the desired trigger threshold (i.e., “Alert if AP bandwidth is >= *1500* kbps for *60* seconds”) and Trigger Severity for the defined alert (Normal, Warning, Minor, Major, Critical). Triggers marked “Critical” will generate Severe Alerts. When Severe Alerts exist they appear at the right of the status bar as a bold, red component. Severe Alerts are visible for users based on the settings on the **Home→User Info** page. Other functionality mirrors that of regular alerts.

- In the Conditions section, use the dropdown menus to add conditions appropriate to the specific trigger by setting Fields, Operators and Values. For exOV3600le, for the device bandwidth trigger shown above, the conditions section allows the user to set the field as “Device Type”, the operator as “==” (equal) or “=!” (not equal), and the value as “Access Point”, “Controller”, “Router/Switch”, or “Universal Network Device.” The contents of the dropdown menu will vary from trigger to trigger, but the basic functionality and syntax is the same.

Figure 107. Trigger Condition Detail Page



- Specify the "Trigger Restrictions" for the defined alert:

Notification Option	Description
Folder	The trigger will only apply to APs/Devices in the specified folder or subfolders depending on the Include Subfolders option. *Note: If the trigger is restricted by folder and group , it will only apply to the intersection of the two. It will only apply to APs in the group and in the folder.*
Include Subfolders	Including subfolders will apply the trigger to all devices in the top folder and all of the devices in folders under the top folder.
Group	The trigger will only apply to APs/Devices in the specified group. *Note: If the trigger is restricted by folder and group , it will only apply to the intersection of the two. It will only apply to APs in the group and in the folder.*

- Specify the Alert Notifications for the defined alert:

Notification Option	Description
Notification Type	Checkboxes the action OV3600 should take when an alert is triggered. When the log checkbox is checked OV3600 will log the alert in OV3600's log files. When the NMS checkbox is checked OV3600 will send an SNMP trap to the NMS servers defined for the role.
Sender Address	The From field of alert emails will list this email address.
Recipient Email Addresses	The user, users or distribution lists that will receive any email alerts.
Logged Alert Visibility	Defines which users are able to view the alerts. When limited by role only users with the same role as the creator of the alert will be able to view it. When limited by triggering agent, any user who can view the device can view the alert.
Suppress new alerts until current alerts are acknowledged/deleted	Determines how often a trigger will fire. When No is selected a new alert will be created every time the trigger criteria are met. When Yes is selected an alert will only be received the first time the criteria is met. A new alert for the ap/device will not be created until the initial one is acknowledged.

NOTE: You may select more than one Notification Option for each alert by pressing the CTRL button and clicking the options with the mouse.

- Specify the *Severity Level* for the defined alert (Normal, Warning, Minor, Major, Critical) according to your business needs.

- Click “Add” to activate the trigger. The trigger will now appear on the **System→Triggers** page.

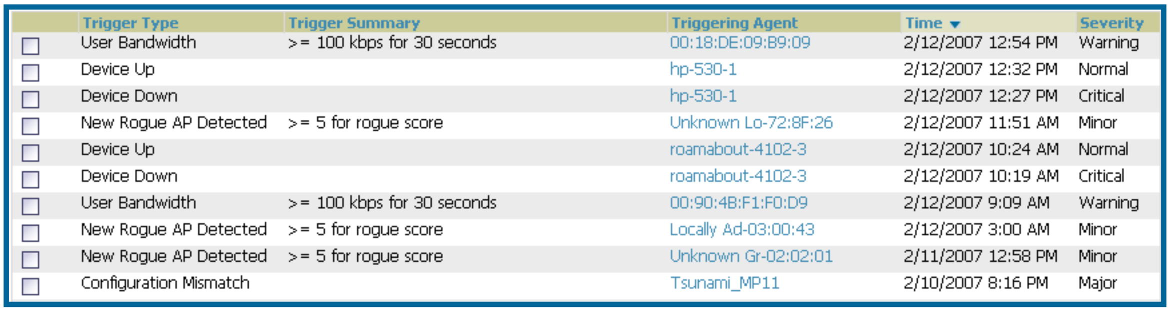
- OV3600 utilizes Postfix to deliver alerts and reports via email, because it provides a high level of security and locally queues email until delivery. *If OV3600 sits behind a firewall, which prevents it from directly sending email to the specified recipient, use the following procedures to forward email to a “smarthost”.*

```
1. Add the following line to /etc/postfix/main.cf:
   relayhost = [mail.yourdomain.com]
   where mail.yourdomain.com is the IP address or hostname of
   your “smarthost”
2. Run service postfix restart
3. Send a test message to an email address
   Mail -v xxx@xxx.com
   Subject: test mail
   .
   CC: <press enter>
4. Check the mail log to ensure mail was sent
   tail -f /var/log/maillog
```

Viewing Alerts

- When OV3600 generates a system alert, the *Alerts* counter in the Status Bar at the top of each page will increment. To view the active alerts, click on the Alerts or the Severe Alerts counter or navigate to the **System→Alerts** page.

Figure 108. “System→Alerts” page



	Trigger Type	Trigger Summary	Triggering Agent	Time ▼	Severity
□	User Bandwidth	>= 100 kbps for 30 seconds	00:18:DE:09:B9:09	2/12/2007 12:54 PM	Warning
□	Device Up		hp-530-1	2/12/2007 12:32 PM	Normal
□	Device Down		hp-530-1	2/12/2007 12:27 PM	Critical
□	New Rogue AP Detected	>= 5 for rogue score	Unknown Lo-72:8F:26	2/12/2007 11:51 AM	Minor
□	Device Up		roamabout-4102-3	2/12/2007 10:24 AM	Normal
□	Device Down		roamabout-4102-3	2/12/2007 10:19 AM	Critical
□	User Bandwidth	>= 100 kbps for 30 seconds	00:90:4B:F1:F0:D9	2/12/2007 9:09 AM	Warning
□	New Rogue AP Detected	>= 5 for rogue score	Locally Ad-03:00:43	2/12/2007 3:00 AM	Minor
□	New Rogue AP Detected	>= 5 for rogue score	Unknown Gr-02:02:01	2/11/2007 12:58 PM	Minor
□	Configuration Mismatch		Tsunami_MP11	2/10/2007 8:16 PM	Major

- For each new alert, the **System→Alerts** page displays:

Field	Description
Trigger Type	The type of trigger (see “Setting Triggers” above).
Trigger Summary	Additional summary information related to the trigger.
Triggering Agent	The name of the AP that generated the trigger. *Clicking on the AP name will bring you to the **APs/Devices→Manage** page for that AP.*
Time	The date and time the trigger was generated.

Field	Description
Severity	The severity code associated with that Trigger (see “Setting Triggers”).

- Once you have viewed an alert, you may:
  - Leave it in active alert status if it is unresolved. *The alert will remain on the New Alerts list until you “Acknowledge” or “Delete” it. If an alert already exists the trigger for that AP or User will not fire again until it has been acknowledged or deleted. If AP 7 exceeds a max bandwidth trigger that trigger will not fire again for AP 7 until the first alert is recognized.*
  - Move the alert to the Alert Log by selecting the alert and clicking the “Acknowledge” button at the bottom of the page (You may see all logged alerts by clicking the *View logged alerts* link at the top of the page. Click the *New Alerts* link to return to the list of new alerts only).
  - Delete the alert by selecting the alert from the list and clicking the “Delete” button at the bottom of the page.

Backups

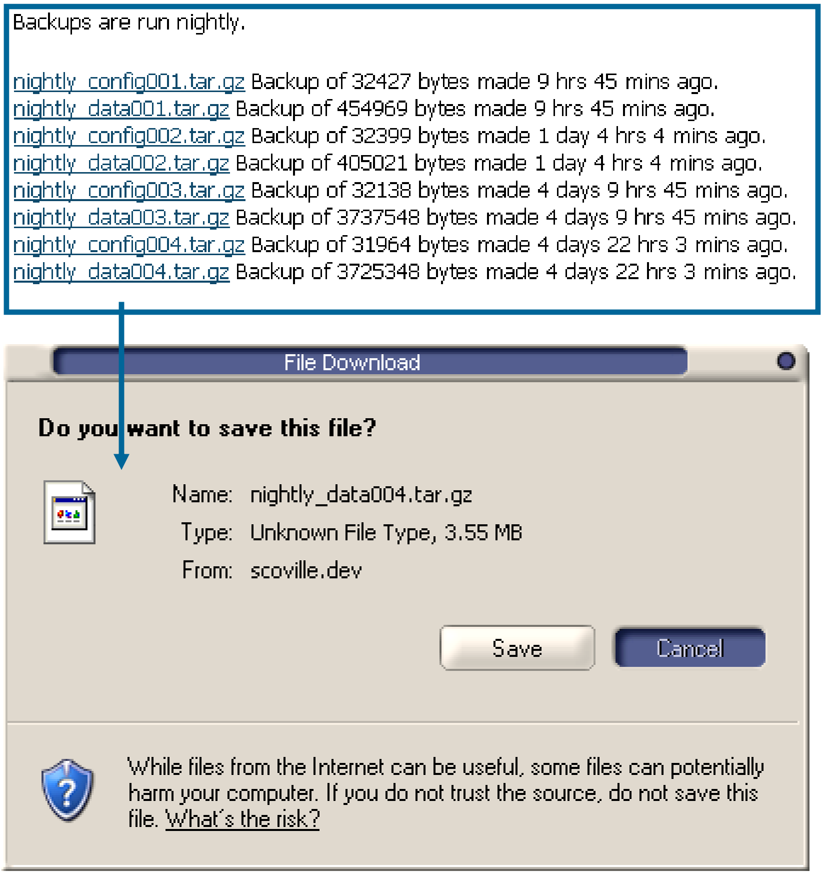
Overview of Backups

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. Although OV3600 only keeps the last four sets of archives, the archives can be manually or automatically downloaded off-site for more extensive backup strategies. OV3600 creates two backup files each night, a configuration backup and a data backup. The data backup contains all of the device and group information as well as all of the historical data. The configuration backup contains the OV3600 system files including IP address, NTP information, mail relay hosts and other OV3600 settings.

Viewing and Downloading Backups

- To view current backups, go to the **System→Backups** page.

Figure 109. "System→Backups" page



Backups are run nightly.

nightly_config001.tar.gz Backup of 32427 bytes made 9 hrs 45 mins ago.
nightly_data001.tar.gz Backup of 454969 bytes made 9 hrs 45 mins ago.
nightly_config002.tar.gz Backup of 32399 bytes made 1 day 4 hrs 4 mins ago.
nightly_data002.tar.gz Backup of 405021 bytes made 1 day 4 hrs 4 mins ago.
nightly_config003.tar.gz Backup of 32138 bytes made 4 days 9 hrs 45 mins ago.
nightly_data003.tar.gz Backup of 3737548 bytes made 4 days 9 hrs 45 mins ago.
nightly_config004.tar.gz Backup of 31964 bytes made 4 days 22 hrs 3 mins ago.
nightly_data004.tar.gz Backup of 3725348 bytes made 4 days 22 hrs 3 mins ago.

File Download

Do you want to save this file?

Name: nightly_data004.tar.gz
Type: Unknown File Type, 3.55 MB
From: scoville.dev

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

- To download a backup click the filename URL and the “File Download” popup will appear as above. It is recommended you regularly save both backup files to another machine or media.

- This process can easily be automated with a nightly script.

Backup on Demand

- To create an immediate backup use the following procedure:
    - Log into the OV3600 system as root
    - Change to the ‘scripts’ directory by typing ‘scripts’
    - Run the backup script by typing ‘/bin/sh ov3600_backup’

- This will create a backup of the system located in /alternative/databackup.tar.gz and /alternative/configbackup.tar.gz.
- For an OV3600 with 1000 APs it will take about 40 seconds to copy a backup. For an OV3600 with 2500 APs it will take about two minutes.

Restoring from a Backup

- To restore a backup file on a new machine use the following procedure:
    - 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.
    - Copy the nightly_data00[1-4].tar.gz file to the new OV3600. /tmp directory is an appropriate destination.

      A good open source Windows file transfer client that supports SFTP and SCP for is WinSCP which is available from http://winscp.sourceforge.net/eng/.

      WINSCP will allow you to transfer the nightly00[1-4].tar.gz file from your local PC to the new OV3600 using the secure copy protocol (SCP).

    - Log onto the new server as “root”
    - Change to the ‘scripts’ directory by typing ‘scripts’
    - 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

The Navigation Section displays tabs to all main UI 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.

Main Tab	Description	Sub-Menus
Home	The **Home** page provides basic OV3600 Failover information, including system name, hostname, IP address, current time, running time, software version, and watched OV3600 information.	• Overview • Watched 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).	• Status • Event Log • Backups • Performance
OV3600 Setup	**OV3600 Setup** page provides all information relating to the configuration of OV3600 itself and its connection to your network.	• General • Network • Users • TACACS+

Adding Watched OV3600s

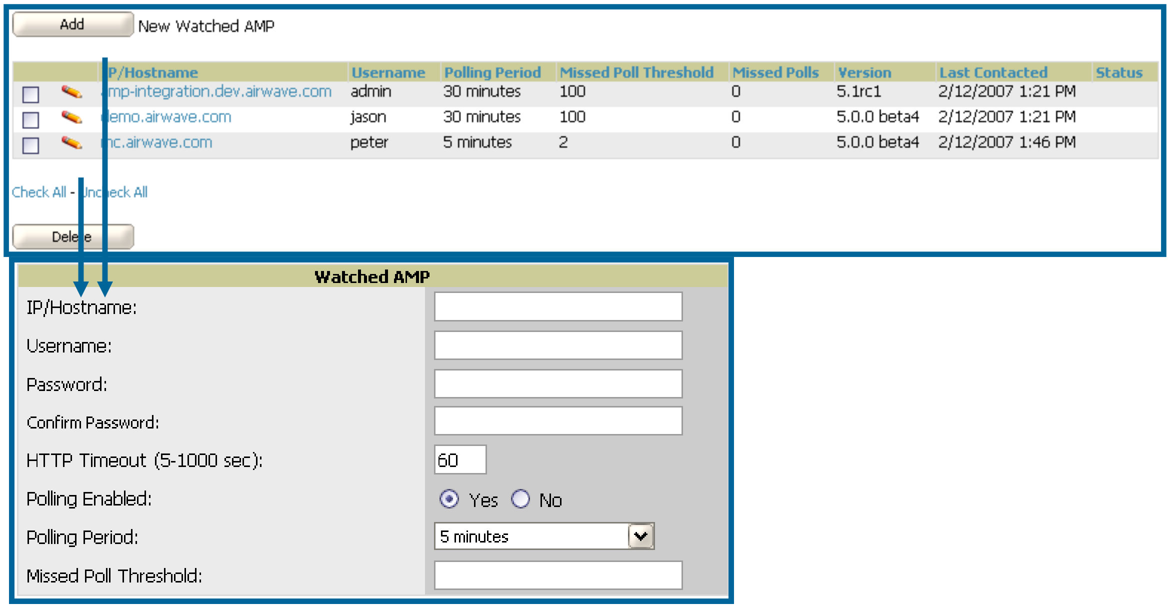
Navigate to the **Home→Watched OV3600s** page to begin backing up and monitoring OV3600s. Once an OV3600 has been added to the "Watched OV3600s" list, the Failover OV3600 will download the most recent backup and begin polling. The Failover OV3600 and the "Watched OV3600s" must be on the same version or else the watched OV3600s will be unable to restore properly. If any of the "watched" OV3600s are not on the same version of OV3600 you will need to upgrade. The Failover OV3600 will need HTTPS access (port 443) to the "watched" OV3600s to verify that the web interface 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's 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's 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's 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" Config file to the "Watched OV3600". Then run the restore script. More information about backups and restores can be found in the Backups section of the User Guide.

Figure 110. “Home→Watched OV3600s” page



		P/Hostname	Username	Polling Period	Missed Poll Threshold	Missed Polls	Version	Last Contacted	Status
□		mp-integration.dev.airwave.com	admin	30 minutes	100	0	5.1rc1	2/12/2007 1:21 PM	
□		emo.airwave.com	jason	30 minutes	100	0	5.0.0 beta4	2/12/2007 1:21 PM	
□		nc.airwave.com	peter	5 minutes	2	0	5.0.0 beta4	2/12/2007 1:46 PM	

Watched AMP

Watched AMP	
IP/Hostname:	
Username:	
Password:	
Confirm Password:	
HTTP Timeout (5-1000 sec):	60
Polling Enabled:	● Yes ○ No
Polling Period:	5 minutes
Missed Poll Threshold:	

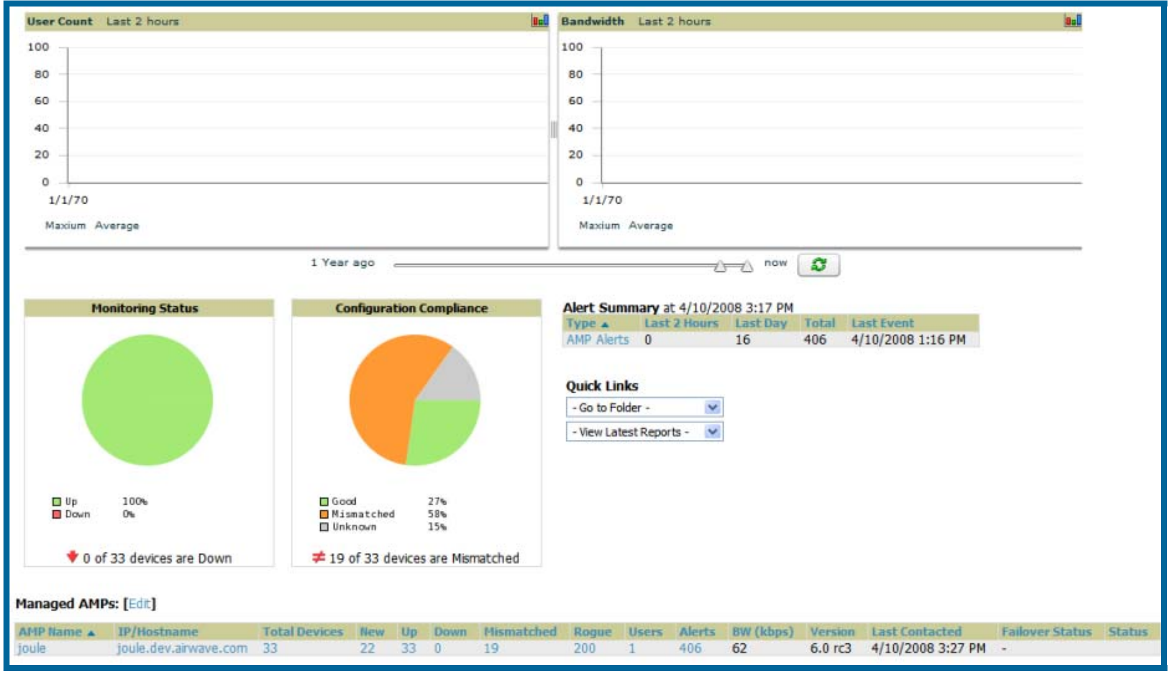
Setting	Default	Description
IP/Hostname	None	The IP address or Hostname of the watched OV3600. *Note: The Failover OV3600 needs HTTPS access to the “watched” OV3600s.*
Username	None	A username with management rights on the “watched” OV3600.
Password	None	The password for the username with management rights specified above.
HTTP Timeout (5-1 Sec)	60	The amount of time before OV3600 considers a polling attempt failed.
Polling Enabled	Yes	Enables or disables polling of the Watched OV3600. If a Watched OV3600 is going down for scheduled maintenance it is recommended to set the polling enabled flag to No.
Polling Period	5 minutes	The amount of time between polls of the Watched OV3600.
Missed Poll Threshold	None	The number of polls that can be missed before the failover OV3600 will begin actively monitoring the Watched OV3600s APs.

Master Console

The **Master Console (MC)** is used to monitor multiple OV3600s from one central location. The Master Console is designed for customers running multiple OV3600 servers. Once an OV3600 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 OV3600s; 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 OV3600s using the global groups feature.

There are two forms of Master Console, the standalone server and the OV3600 add-on. The license key determines if the Master console is enabled and the mode it should run. While running in add-on mode the OV3600 will function like a normal OV3600 but will have an extra MC tab that is used to access the master console. When in standalone mode the server will only poll other OV3600s and will not monitor any APs directly.

Figure 111. "Home→Overview" page



Alert Summary at 4/10/2008 3:17 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	16	406	4/10/2008 1:16 PM

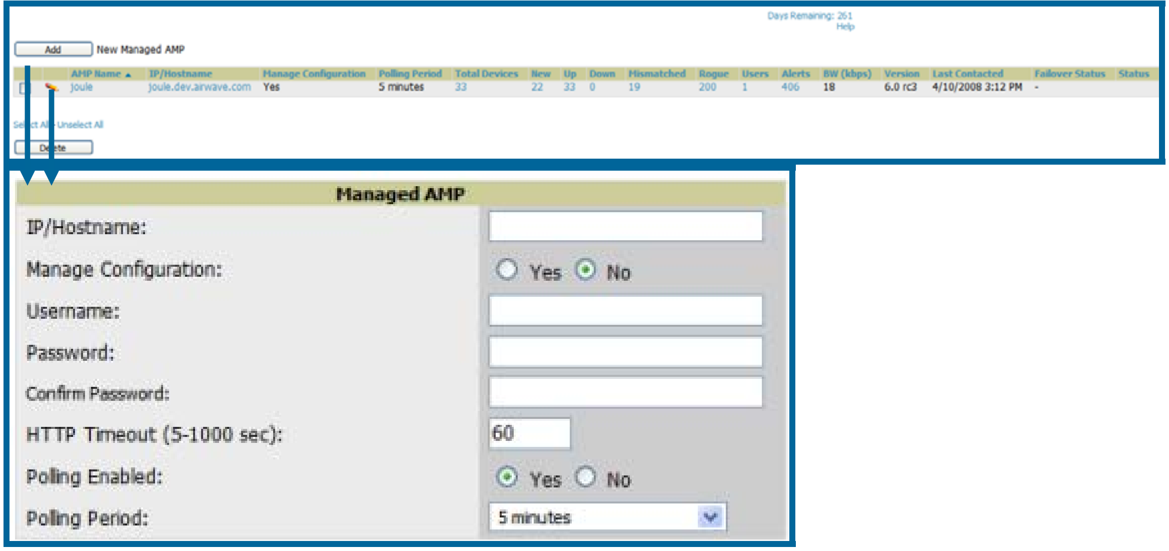
Managed AMPs: [Edit]

AMP Name ▲	IP/Hostname	Total Devices	New	Up	Down	Mismatched	Rogue	Users	Alerts	BW (kbps)	Version	Last Contacted	Failover Status	Status
joule	joule.dev.airwave.com	33	22	33	0	19	200	1	406	62	6.0 rc3	4/10/2008 3:27 PM	-	

- Much like the OV3600 **Home→Overview** page, the MC **Home→Overview** page provides summary statistics for the entire network at a glance.

- To add a managed OV3600 navigate to the **Home→Managed OV3600s** page and click on the add button.

Figure 112. "Master Console→Manage OV3600s" page



Days Remaining: 261
Help

New Managed AMP

		AMP Name ▲	IP/Hostname	Manage Configuration	Polling Period	Total Devices	New	Up	Down	Mismatched	Rogue	Users	Alerts	BW (kbps)	Version	Last Contacted	Failover Status	Status
□		joule	joule.dev.airwave.com	Yes	5 minutes	33	22	33	0	19	200	1	406	18	6.0 rc3	4/10/2008 3:12 PM	-	

Managed AMP

IP/Hostname:	
Manage Configuration:	○ Yes ● No
Username:	
Password:	
Confirm Password:	
HTTP Timeout (5-1000 sec):	60
Polling Enabled:	● Yes ○ No
Polling Period:	5 minutes

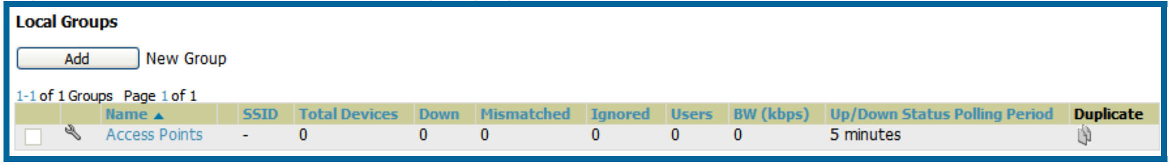
- Clicking on the IP/Hostname link will redirect your browser to the specified OV3600.

Field	Description
IP/Hostname	The IP or Hostname of the managed OV3600.
Manage Group Configuration	If yes is selected, group configurations can be pushed from the Master Console to the OV3600. This option is disabled ("No") by default.
Username	The usersname used by the Master Console to login to the managed OV3600s. The user needs to be an AP/Device Manager or OV3600 Administrator.
Password	The password used by the Master Console OV3600 to login to the managed OV3600.
Polling Period	Determines how frequently the Master Console will poll the managed OV3600s.
Total Devices	The number of Up and Down devices. The Total devices count does not include New devices.
New Devices	The number of devices that have been discovered by the managed OV3600 but not yet added to a group.
Up	The number of managed, authorized APs that are currently responding to the managed OV3600's requests.
Down	The number of managed, authorized APs that are **not** currently responding to the managed OV3600's SNMP requests.
Rogue	The number of unknown APs detected on the network by the managed OV3600 with a score of five. A score of five means the rogues were discovered via wireless or wireline fingerprint scanning techniques. *NOTE: A newly discovered AP is considered a "Rogue" if it is not a supported AP that OV3600 can manage and monitor. If the newly discovered AP is capable of being managed and monitored by OV3600 it will be classified as a "New" device rather than a "Rogue."*

Field	Description
Users	The number of wireless users currently associated to the wireless network via all APs managed by the managed OV3600.
Alerts	The number of non-acknowledged OV3600 alerts generated by user-configured triggers on the managed OV3600.
BW(kbps)	The total amount of bandwidth, in kbps, currently used by the managed OV3600.
Version	The version of OV3600 software currently running on the managed OV3600.
Last Contacted	The last time the managing OV3600 was able to connect to the managed OV3600.
Failover Status	Lists the status of Failover OV3600s. *Watching*: The failover server is monitoring healthy OV3600s. *Failed Over*: The monitored OV3600 failed to respond and the Failover OV3600 is currently monitoring APs.
Status	Description of any errors connecting to the managed OV3600. This is not a list of errors that have occurred on the managed OV3600.

To push configurations to managed groups using OV3600's 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).

Figure 113. "Master Console→Groups" page



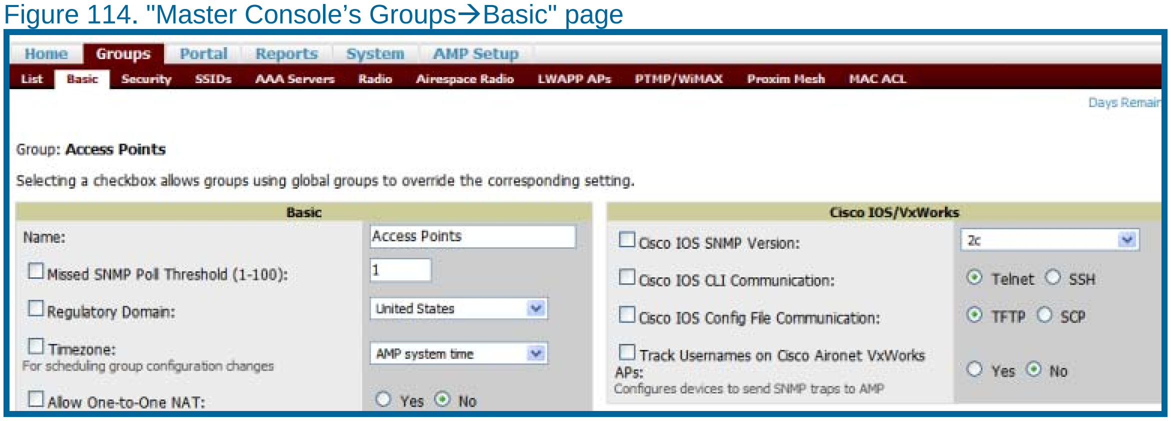
Local Groups

1-1 of 1 Groups Page 1 of 1

		Name ▲	SSID	Total Devices	Down	Mismatched	Ignored	Users	BW (kbps)	Up/Down Status Polling Period	Duplicate
□	🔧	Access Points	-	0	0	0	0	0	0	5 minutes	⧉

Clicking the name of an existing group on the Master Console loads the subtabs for Basic, Security, SSIDs, AAA Servers, Radio, Airespace Radio, LWAPP APs, PTMP/WiMAX, Proxim Mesh and MAC ACL pages. These subtabs contain the same fields as the group subtabs on a monitored OV3600, but each field also has a checkbox. The Master Console can also configure global templates that can be used in subscriber groups. The process is the same as described in the Groups→Templates section of the user guide, except that there is no process by which templates can be fetched from devices in the subscriber group on managed OV3600s. Instead, the template must be copied and pasted into the Master Console global group.

Figure 114. "Master Console's Groups→Basic" page



Group: **Access Points**

Selecting a checkbox allows groups using global groups to override the corresponding setting.

Basic	
Name:	Access Points
□ Missed SNMP Poll Threshold (1-100):	1
□ Regulatory Domain:	United States
□ Timezone: For scheduling group configuration changes	AMP system time
□ Allow One-to-One NAT:	○ Yes ● No

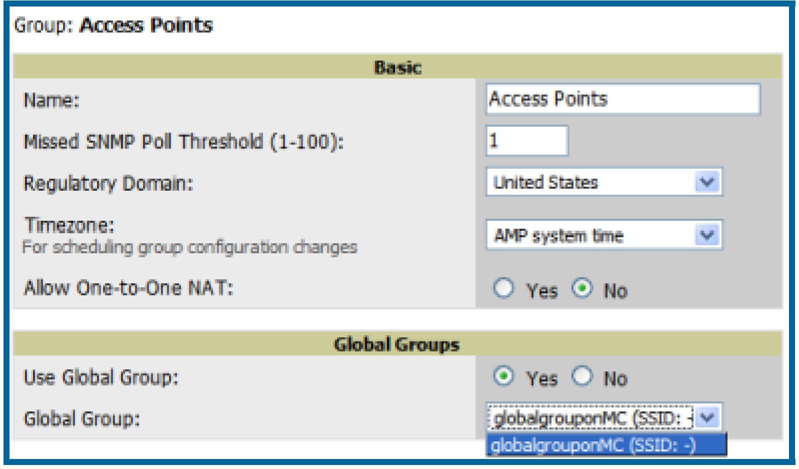
Cisco IOS/VxWorks	
□ Cisco IOS SNMP Version:	2c
□ Cisco IOS CLI Communication:	● Telnet ○ SSH
□ Cisco IOS Config File Communication:	● TFTP ○ SCP
□ Track Usernames on Cisco Aironet VxWorks APs: Configures devices to send SNMP traps to AMP	○ Yes ● No

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 dropdown menu. Then click "Save and Apply" for the configuration from the global group to be pushed to the subscriber group on the managed OV3600.

Figure 115. "Groups→Basic" page on a managed OV3600



Group: **Access Points**

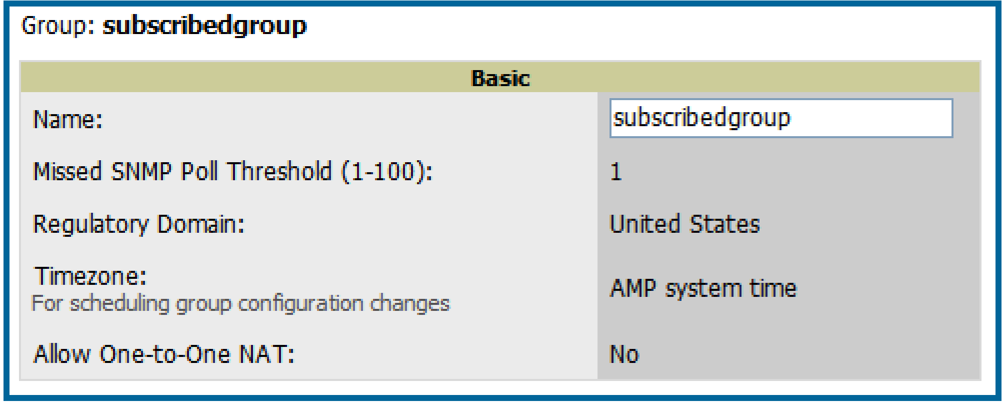
Basic	
Name:	Access Points
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	United States
Timezone: For scheduling group configuration changes	AMP system time
Allow One-to-One NAT:	○ Yes ● No

Global Groups	
Use Global Group:	● Yes ○ No
Global Group:	globalgrouponMC (SSID: - globalgrouponMC (SSID: -)

Once the configuration is pushed, the non-overriden 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 exOV3600le below, the field “Name” was overridden with the checkbox in the global group on the Master Console, so it can be configured for each subscriber group on the managed OV3600. The other four fields in the Basic section were not overridden, so they are static fields that will be the same for each subscriber group. These fields can only be altered on the global group on the Master Console.

Figure 116. "Groups→Basic" page on a managed OV3600 for a subscriber group



Group: **subscribedgroup**

Basic	
Name:	subscribedgroup
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	United States
Timezone: For scheduling group configuration changes	AMP system time
Allow One-to-One NAT:	No

The global groups feature can also be used without the Master Console. For more information about how this feature works, consult the Groups section of this user guide.

Package Management

Yum

It is recommended you run Yum to ensure your packages are up to date so 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 will verify OV3600 is running the most recently released RPMs and upgrade any out-of-date packages. Yum will go to the internet and download and install new versions of any installed RPMs. It is important to keep OV3600's 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.

To run Yum on a CentOS 4 machine use the steps below; for a CentOS 5 machine, yum-cron is also required:

- Before Yum is run for the first time you will need to install the GPG key. The GPG key is used to validate the authenticity all packages downloaded by Yum. To install the GPG key type 'rpm --import /usr/share/doc/fedora-release-3/RPM-GPG-KEY-fedora'.

- To manually run Yum 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.

- To configure Yum to run nightly type 'chkconfig yum on' and press enter. The chkconfig command tells yum to run nightly at 4:02 AM when the yum service is running but chkconfig does not start yum. Type 'service yum start' and press enter to start Yum or restart the server and Yum will start automatically.

In some instances, running Yum may cause a problem with OV3600. If that happens, a good first step is to SSH into the OV3600 server as root as issue the following command:

```
# root; make
```

If that does not resolve the issue, please contact Alcatel-Lucent Enterprise Service and Support at support@ind.alcatel.com. for further assistance.

NOTE: Yum or Up2date are not supported on Red Hat 8 or 9. Running Yum on RH8 or RH9 will cause serious problems.

Appendix A – WLSE Configuration

Overview

WLSE functions as an integral part of Cisco's 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.

SWAN Component	Requirements
WDS	• WDS Name • Primary and backup IP for WDS devices (IOS AP or WLSM) • WDS Credentials • APs within WDS Group *Note – WDS can be either a WLSM or an IOS AP. WLSM (WDS) can control up to 250 access points. AP (WDS) can control up to 30 access points.*
WLSE	• IP Address • Login
ACS	• IP Address • Login
APs	• APs within WDS Group

Helpful Cisco Links
Ciscoworks WLSE
http://www.cisco.com/en/US/products/sw/cscowork/ps3915/

WLSE Release Notes
http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_release_notes_list.html

WLSE Release Notes
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/

Initial WLSE Configuration

Use the following instructions to configure a WLSE.

Add ACS Server

- Navigate to the **Devices→Discover→AAA Server** page
- Select "New" from the pull down list
- Enter "Server Name", "Server Port" (default 2002), "Username", "Password", and "Secret"
- Click the "Save" button.

Enable Rogue Alerts

- Navigate to the **Faults→Network Wide Settings→Rogue AP Detection** page
- Select the "Enable" toggle
- Click the "Apply" button.

Configure WLSE to communicate with APs

- Navigate to the **Device→Discover** page
- Configure SNMP Information (Additional Information)
- Configure HTTP Information (Additional Information)
- Configure Telnet/SSH Credentials (Additional Information)
- HTTP ports for IOS access points (Additional Information)
- WLCCP Credentials (Additional Information)
- AAA Information (Additional Information)

Discover Devices

There are three methods to discover access points within WLSE: (1) CDP, (2) Import from a File, and (3) Import from CiscWorks.

- Navigate to the **Device→Managed Devices→Discovery Wizard** page
- Import Devices from File (Additional Information)
- Import Devices from Cisco Works (Additional Information)

CDP - (Additional Information)

Manage Devices

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

Note: OV3600 will be 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 APsl.

- Navigate to **Device→Discover→Advanced Options**
- Select method to bring APs into management "Auto" or specify via filter (Additional Information)

Inventory Report

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

- Navigate to **Devices→Inventory→Run Inventory**
- "Run Inventory" executes immediately between WLSE polling cycles. (Additional Information)

Defining Access

OV3600 requires System Admin access to WLSE.

- Navigate to **Administration→User Admin→**
- Configure "Role" and "User"

Grouping

It is much easier to generate reports or faults if APs are grouped in WLSE.

- Navigate to **Devices→Group Management**
- Configure "Role" and "User"

Configure IOS APs for WDS Participation

IOS APs (1100, 1200) can function in three roles within SWAN: (1) Primary WDS, (2) Backup WDS, and (3) WDS Member

WDS Participation

- Login to the AP
- Navigate to the **Wireless Services→AP** page
- Click "Enable" participation in SWAN Infrastructure
- Click "Specified Discovery" and enter the IP address of the Primary WDS device (AP or WLSM)
- Enter the "Username" and "Password" for the WLSE server

Primary or Secondary WDS (Optional)

- Navigate to the **Wireless Services→WDS→General Setup** page
- If the AP is Primary or Backup WDS then select "Use the AP as Wireless Domain Services"
    - Select Priority
        - "200" for Primary
        - "100" for Secondary
    - Configure Wireless Network Manager
        - Configure IP of WLSE
- If the AP is Member Only leave all options unchecked
- Navigate to the **Security→ Server Manager** page
- Enter the "IP" and "Shared Secret" for ACS Server
- Click the "Apply" button
- Navigate to the **Wireless Services→WDS→Server Group** page
- Enter the WDS Group of AP
- Select the ACS server in the Priority 1 pull down
- Click the "Apply" button

Configure ACS for WDS Authentication

ACS authenticates all components of the WDS and must be configured first.

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

Appendix B – Security Integration

Bluesocket Integration (Optional)

Requirements

- Bluesocket version 2.1 or higher
- OV3600 version 1.8 or higher
- Completion of **OV3600 Setup→RADIUS Accounting** section on OV3600

Bluesocket Configuration

1. Login into the Bluesocket Server via HTTP with proper user credentials.
2. Navigate to *Users→External Accounting Servers*.

3. Select “External RADIUS Accounting” from the *Create* pull-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 you need to ensure that the accounting records are forwarding to OV3600 upon authentication.
12. Navigate to *Users→External Authentication Servers*.
13. Modify the LDAP server.
14. Ensure under the Accounting server matches the server entered in step 5.
15. Click the “Save button”
16. To verify and view the log files on the Bluesocket server, proceed to *Status→Log*.
17. To verify and view the log files on OV3600, proceed to SYSTEM→Event Log.

ReefEdge Integration (Optional)

Requirements

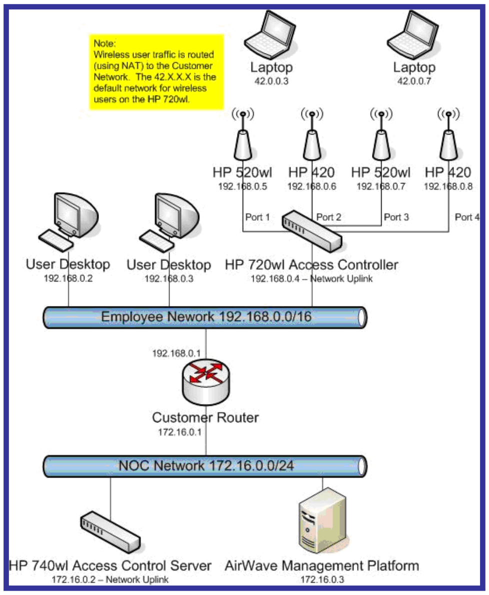
- ReefEdge version 3.0.3 or higher
- OV3600 version 1.5 or higher
- Completion of OV3600 **Setup→RADIUS Accounting** section on OV3600

ReefEdge Configuration

1. Login into the ReefEdge ConnectServer via HTTP with the proper user credentials
2. Navigate to *Connect System→Accounting*

3. Click “Enable RADIUS Accounting”
4. Enter the *Primary Server IP Address* or DNS entry for OV3600 server,
5. Enter *Primary Server Port Number* 1813
6. Enter the *Shared Secret* (matching OV3600’s shared secret)
7. To verify and view the log files on the Connect Server proceed to *Monitor→System Log*.
8. To verify and view the log files on OV3600, proceed to **System→Event Log**.

HP ProCurve 700wl Series Secure Access Controllers Integration (Optional)


Note:
Wireless user traffic is routed (using NAT) to the Customer Network. The 42.X.X.X is the default network for wireless users on the HP 720wl.
Laptop
42.0.0.3
Laptop
42.0.0.7
HP 520wl
192.168.0.5
HP 420
192.168.0.6
HP 520wl
192.168.0.7
HP 420
192.168.0.8
Port 1
Port 2
Port 3
Port 4
User Desktop
192.168.0.2
User Desktop
192.168.0.3
HP 720wl Access Controller
192.168.0.4 – Network Uplink
Employee Nework 192.168.0.0/16
192.168.0.1
Customer Router
172.16.0.1
NOC Network 172.16.0.0/24
HP 740wl Access Control Server
172.16.0.2 – Network Uplink
AirWave Management Platform
172.16.0.3

Requirements

- HP 700 version 4.1.1.33 or higher
- OV3600 version 3.0.4 or higher
- Completion of the **OV3600 Setup→RADIUS Accounting** section on OV3600

ExOV3600le Network Configuration

In this exOV3600le the APs are connected to the Access Controller. The Access Controller will route wireless user traffic to the Employee Network, while bridging AP management traffic. I assume each AP will have a static IP address.

HP ProCurve 700wl Series Configuration – Allow OV3600 to manage APs through Control

1. Login 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 Point 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 – Send Client Authentication Information to OV3600

1. Login to the Access Control Server via HTTP with proper credentials
2. Navigate to *Rights → Authentication Policies*
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 & Confirm* (matching OV3600’s shared secret)
11. Enter *Reauthentication Field* – “Session Timeout”
12. Enter *Timeout* – “5”
13. Select “*Enable RADIUS Accounting RFC-2866*” check box
14. Enter *Port* – “1813” for RFC-2866
15. To verify and view the log files on OV3600, proceed to **SYSTEM→Event Log**.

Appendix C – Access Point Notes

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: Cisco changed the procedure for resetting the AP configuration beginning with software version 11.07. The procedure below will help you determine which software version your AP(s) is currently running and which procedure to use to reset the AP.*

Connecting to the AP

1. Connect the COM 1 or COM 2 port on your computer to the RS-232 port on the AP, using a straight-through cable with 9-pin-male to 9-pin-female connectors.

2. Open a terminal-emulation program on your computer.

    Note: The instructions below assume that you are using Microsoft HyperTeminal; 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, and use the pull-down menu to select the port the cable is connected to, 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.

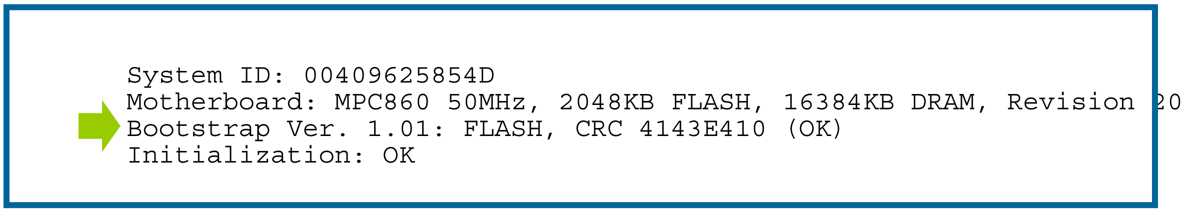
Determining the Boot-Block Version

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*:

Figure 117. SOV3600le Screen Shot



```
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.

   Note: The :resetall command is valid for only 2 minutes after the AP reboots. If you do not enter and confirm the :resetall command during that 2 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 timestOV3600s debug datetime msec
service timestOV3600s log datetime msec
service password-encryption
hostname %hostname%
enable secret 5 $1$ceH2$/1BN2DQpOoBAz/KI2opH7/
ip subnet-zero
ip domain name alcatellucent.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.

Appendix D - Cisco Clean Access Integration (Perfigo)

Requirements

- Clean Access Software 3.5 or higher
- OV3600 version 3.4.0 or higher
- Completion of the **OV3600 SETUP→RADIUS Accounting** section on OV3600

Add OV3600 as RADIUS Accounting Server

1. Login to the clean machine server and Navigate to *User Management → Accounting → Server Config*
   - Select “Enable RADIUS Accounting”
   - Input OV3600 Hostname or IP Address
   - Timeout (sec) – leave default “30”
   - Ensure Server Port is set for “1813”
   - Input Shared Secret matching OV3600’s shared secret
2. Select “Update” button to save

Configure Data in Accounting Packets

3. Navigate to *User Management → Accounting → Shared Events*
4. 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.

Appendix E – HP Insight install instructions for OV3600 servers

Following are instructions for installing HP/Compaq Insight Manager on the OV3600:

Step 1: SCP 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

Step 2: Type 'rpm -i hpasm-7.8.0-88.rhel4.i386.rpm'

Step 3: Type 'hpasm activate'

Take the default values. You will need the SNMP RW and RO strings at this point.

Step 4: Type ‘ rpm –i --nopre hpsmh-2.1.9-178.linux.i386.rpm ' <- - The ‘nopre’ is required to keep the rpm from erroring out on CentOS vs. RedHat. This rpm MUST be run after the hpasm rpm since the pre-install scripts in the hpsmh rpm aren’t being run.

Step 5: Type 'perl /usr/local/hp/hpSMHSetup.pl'

This will configure the web server.
Add Group -> Administrator with name '0'
IP Binding enable (type 1)
Next page enter the Ip address and mask of the server

Step 6: Type /etc/init.d/hpasm reconfigure

When going through this menu this time, select 'y' to use existing snmpd.conf.

Step 7: Type 'vi /etc/snmp/snmpd.conf'

Change these two lines:
rwcommunity xxxstringxxx 127.0.0.1
rocommunity xxxstringxxx 127.0.0.1

to read:

rwcommunity xxxstringxxx
rwcommunity xxxstringxxx

Step 8: Type 'service snmpd restart'

Step 9: type 'user add xxusernamexx'

Step 10: type 'passwd xxusernamexx' and put in a password for the user.

Step 11: type 'vi /etc/passwd '

Scroll to the bottom of the list and change the new users UID and GroupID to 0 (4th and 5th column).

Step 12: Connect to the server using https://xxx.xxx.xxx.xxx:2381 and the username and password that you created in steps 9 and 10.

Appendix F – Configuring Templates for Symbol APs

Symbol controllers (5100 and 2000) can be configured in OV3600 using templates. A sOV3600le running-config template is provided below for reference. A template can be fetched from a "model" device using the procedure described earlier in the section on configuring templates for Cisco IOS devices. Certain parameters like hostname and location are turned into variables with the "%" tags so that device-specific values can be read off of the individual manage pages and inserted.

There is an option on the Group→Templates to reboot the device after pushing a configuration. Certain settings have now been variabilized, including ap-license and adoption-preference-id. The readio preamble has now been templatized as well. OV3600 supports Symbol 5100 firmware upgrades for 3.x to 3.x.

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

set server 8 secondary 0.0.0.0
set port 8 secondary 1812
```

```
/
// Hotspot Whitelist configuration
network
wlan
hotspot
white-list
clear rule all
// Hotspot Whitelist 1 configuration
// Hotspot Whitelist 2 configuration
// Hotspot Whitelist 3 configuration
// Hotspot Whitelist 4 configuration
// Hotspot Whitelist 5 configuration
// Hotspot Whitelist 6 configuration
// Hotspot Whitelist 7 configuration
// Hotspot Whitelist 8 configuration
/
/
network
dhcp
// network->dhcp menu
set firmwareupgrade 1
set configupgrade 1
set interface s2
set dhcpvendorclassid
/
Save
```

An example 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%
```

Appendix G – Installing OV3600 on VMware ESX (3i version 3.5)

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 Configuaration

3) Name your virtual machine (OmniVista 3600 Air Manager) and then click ‘Next’

4) Select an available datastore with sufficent space for the number of APs your OV3600 will manage (see OmniVista 3600 Air Manager User Guide page 6, ‘Choosing the right server hardware’ for information and a table outlining suggested disk space for typical wireless network setups), then 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 minumum of 2 virtual processors (or more information, see page 6, ‘Choosing the right server hardware’ for a table listing OV3600 processor requirements), then click ‘Next’

7) Enter ‘3072’ as the minimum virtual RAM (more virtual RAM may be required, please see page 6, ‘Choosing the right server hardware’ for a table listing RAM requirements for OV3600 and Visual RF), click ‘Next’

8) Accept VMware’s default virtual network adapter and click ‘Next’

9) Allocate a virual disk large enough to contain the OV3600 operating system, application and data files (see page 6, ‘Choosing the right server hardware’ lists 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 typically be done in one of three ways:

1) By burning an OV3600 ISO to CD , inserting the CD into a physical drive on a VMware server, then configuring the OV3600 virtual machine to boot from the CD

2) Copying the OV3600 ISO to the VMware server’s datastore, or to a networked filesystem available to the VMware server, then configuring the OV3600 virtual machine to boot from the ISO file

3) Using either a local physical CD or an OV3600 ISO file from the VMware Infrastructure Client, then creating a virtual CD on the virtual OV3600 to point to and boot from that device

Overall, option #2 is probably the most efficent method to install OV3600. In addition, after booting the OV3600 virtual machine with either a physical CD or a ISO image file, the install process is identical to the steps outlined in the OmniVista 3600 Air Manager Quick Start Guide.

OV3600 Post-Install 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, follow 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’ (note that 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, ‘/tmp/vmware-toolsdistrib/vmware-install.pl’

6. During the text-based VMware Tools install, select all default options

7. Reboot the virtual machine once the VMware Tools install is complete

Appendix H – Third-Party Copyright Information

OmniVista 3600 Air Manager contains some software provided by third parties (both commercial and open-source licenses).

Copyright Notices

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Google Earth and the Google Earth icon are the property of Google.

Packages

Net::IP:

Copyright (c) 1999 - 2002 RIPE NCC

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appear in all copies and that
both that copyright notice and this permission notice appear in
supporting documentation, and that the name of the author not be
used in advertising or publicity pertaining to distribution of the
software without specific, written prior permission.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS; IN NO EVENT SHALL AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Net-SNMP:

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appears in all copies and
that both that copyright notice and this permission notice appear in
supporting documentation, and that the name of CMU and The Regents of
the University of California not be used in advertising or publicity

pertaining to distribution of the software without specific written
permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL
WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR
THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER
RESULTING
FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF
CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the
   names of its contributors may be used to endorse or promote
   products derived from this software without specific prior written
   permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or
   promote products derived from this software without specific prior
   written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the
   names of its contributors may be used to endorse or promote
   products derived from this software without specific prior written
   permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2004, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ‘‘AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may

be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ‘‘AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Copyright (C) 1995, 1996 Systemics Ltd (http://www.systemics.com/)
All rights reserved.

This library and applications are FREE FOR COMMERCIAL AND NON-COMMERCIAL USE as long as the following conditions are adhered to.

Copyright remains with Systemics Ltd, and as such any Copyright notices in the code are not to be removed. If this code is used in a product, Systemics should be given attribution as the author of the parts used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this
   software must display the following acknowledgement:
   This product includes software developed by Systemics Ltd
   (http://www.systemics.com/)

THIS SOFTWARE IS PROVIDED BY SYSTEMICS LTD ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Perl-Net-IP:

Copyright (c) 1999 - 2002 RIPE NCC

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of the author not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS; IN NO EVENT SHALL AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Berkeley DB 1.85:

Copyright (c) 1987, 1988, 1990, 1991, 1992, 1993, 1994, 1996, 1997, 1998 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN

CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SWFObject v. 1.5:

Flash Player detection and embed - http://blog.deconcept.com/swfobject/
SWFObject is (c) 2007 Geoff Stearns and is released under the MIT License

mod_auth_tacacs - TACACS+ authentication module:

Copyright (c) 1998-1999 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.