OmniVista 3600 Air Manager
Version 7.6

Alcatel·Lucent

Alcatel-Lucent Configuration Guide

Legal Notice

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

Contents

Chapter 1

Alcatel-Lucent Configuration in OV3600

Introduction

AOS-W is the operating system, software suite, and application engine that operates Alcatel-Lucent mobility switches and centralizes control over the entire mobile environment. The AOS-W wizards, command-line interface (CLI), and the AOS-W WebUI are the primary means used to configure and deploy AOS-W. For a complete description of AOS-W, refer to the *Alcatel-Lucent AOS-W User Guide* for your release.

The Alcatel-Lucent Configuration feature in OV3600consolidates AOS-W configuration and pushes global Alcatel-Lucent configurations from one utility. This chapter introduces the components and initial setup of Alcatel-Lucent Configuration with the following topics:

- "Requirements, Restrictions, and AOS-W Support in OV3600" on page 1
- "Additional Concepts and Components" on page 10
- "Setting Up Initial Alcatel-Lucent Configuration" on page 13

> OV3600 supports Alcatel-Lucent *AP Groups* which should not be confused with standard OV3600 *Device Groups*. This document provides information about the configuration and use of Alcatel-Lucent AP Groups, and describes how Alcatel-Lucent *AP Groups* interoperate with standard OV3600 Device Groups.

Requirements, Restrictions, and AOS-W Support in OV3600

Requirements

Alcatel-Lucent Configuration has the following requirements in OV3600:

- OV3600 6.3 or a later OV3600 version must be installed and operational on the network.
- Alcatel-Lucent switches on the network must have AOS-W installed and operational.
- For access to all monitoring features, you must provide Telnet/SSH credentials for a user with minimum access level of read only. In order to perform configuration, the credentials must be for a root level user. In either case, the enable password must be provided.

Restrictions

Alcatel-Lucent Configuration has the following *restrictions* in OV3600:

- At present, Alcatel-Lucent Configuration in OV3600 does not support every AOS-W network component. For example, OV3600 supports only **IP Mobility** and **VLANs** in the **Advanced Services** section.
- AOS-W Configuration is not supported in either Global Groups or the Master Console. Appropriate options will be available in the Subscriber Groups containing the switch(es).

AOS-W Support in OV3600

OV3600 provides three options for configuring OV3600 devices:

- Template-based configuration for devices with firmware versions before AOS-W 3.3.2.10
- Global GUI config for organizations who have near-identical deployments on all of their switches
- Group-level GUI config for organizations who have two or more configuration strategies
- Configuration changes are pushed to the switch via SSH with no reboot required.

OV3600 only supports configuration of the settings which a master switch would push to the standby / local switches (global features). OV3600 supports all master, master-standby, and master-local deployments. OV3600 supports all settings for Profiles, Alcatel-Lucent AP Groups, Servers and Roles are supported, as is the AOS-W WLAN Wizard. **Switch IP addresses, VLANs, and interfaces are not supported, nor are Advanced Services, with the exception of VPN and IP Mobility.**

Other features of Alcatel-Lucent Configuration in OV3600 include the following:

- OV3600 understands AOS-W license dependencies.
- OV3600 supports a variety of Alcatel-Lucent firmware versions, so profiles / fields which are not supported by an older version will not be configured on switches running that version.
- You can provision thin APs from the **AP/Devices > Manage** page. You can move APs into Alcatel-Lucent AP Groups from the **Modify Devices** option on the **APs/Devices > List** page.
- You can configure AP names as **AP Overrides**.
- Values for specific fields may be overwritten for individual switches on the switch's **APs/Devices > Manage** page.

Changes to dependency between the OV3600 group and folders help customers who want to use the folder structure to manage configuration; however, users will be able to see (but not access) group and folder paths for which they do not have permissions.

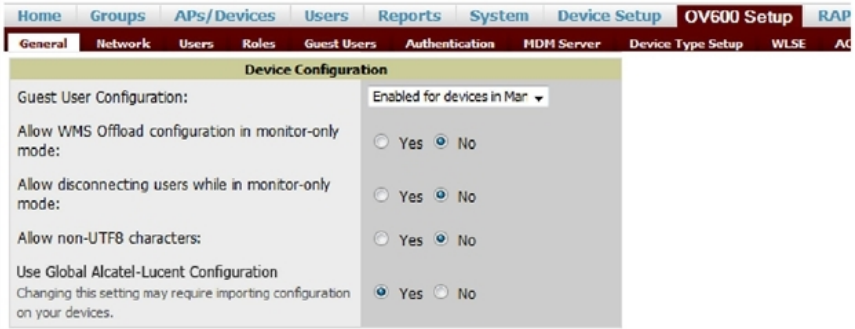
For more detailed information about this feature, as well as steps to transition from template-based configuration to web-based configuration, refer to additional chapters in this user guide. For known issues and details on the AOS-W version supported by each release, refer to the OV3600 Release Notes.

Overview of Alcatel-Lucent Configuration in OV3600

This section describes the pages in OV3600 that support Alcatel-Lucent Configuration.

OV3600 can be configured on **OV3600 Setup** > **General** > **Device Configuration** to configure Alcatel-Lucent devices globally (in the **Device Setup** > **Alcatel-Lucent Configuration** page) or by Device Group (in the **Groups** > **Alcatel-Lucent Config** page). By default, global Alcatel-Lucent Configuration is enabled.

Figure 1 ***OV3600 Setup* > *General*** *Setting for Global or Group Configuration*



Device Configuration

Guest User Configuration: Enabled for devices in Mar ▾

Allow WMS Offload configuration in monitor-only mode: ○ Yes ● No

Allow disconnecting users while in monitor-only mode: ○ Yes ● No

Allow non-UTF8 characters: ○ Yes ● No

Use Global Alcatel-Lucent Configuration
Changing this setting may require importing configuration on your devices. ● Yes ○ No

OV3600 supports Alcatel-Lucent Configuration with the following pages:

- "Device Setup > Alcatel-Lucent Configuration Page" on page 3—Deploys and maintains *global*Alcatel-Lucent Configuration in OV3600. You can limit the view to a folder.
- "Groups > Alcatel-Lucent Config Page With Global Configuration Enabled" on page 3—the way this page displays depends on whether global or group configuration is enabled in OV3600 Setup > General > Device Configuration:
  - If global configuration is enabled, the **Groups** > **Alcatel-Lucent Config** page manages Alcatel-Lucent AP group and other switch-wide settings defined on the **Device Setup** > **Alcatel-Lucent Configuration** page.

- If global configuration is disabled, the **Groups > Alcatel-Lucent Config** page resembles the **Device Setup > Alcatel-Lucent Configuration** tree navigation (the same sections listed in the previous bullet are available), but the **Groups > Alcatel-Lucent Config** pages do not display the **Folder** as a column in the list tables or as a field in the individual profiles.

- "Groups > Alcatel-Lucent Config when Global Configuration is Disabled" on page 4— this page modifies or reboots all devices when Global Alcatel-Lucent Configuration is enabled.
- "APs/Devices > Manage Page" on page 9—supports device-level settings and changes in OV3600.
- "APs/Devices > Monitor Page" on page 9—supports device-level monitoring in OV3600.
- "APs/Devices > Audit Page" on page 10—supports device level configuration importing in OV3600.
- "Groups > Basic Page" on page 10—For device groups containing Alcatel-Lucent devices, basic information such as the group's name, regulatory domain, the use of Global Groups, SNMP Polling periods, and turning on the Alcatel-Lucent GUI Config are managed here.

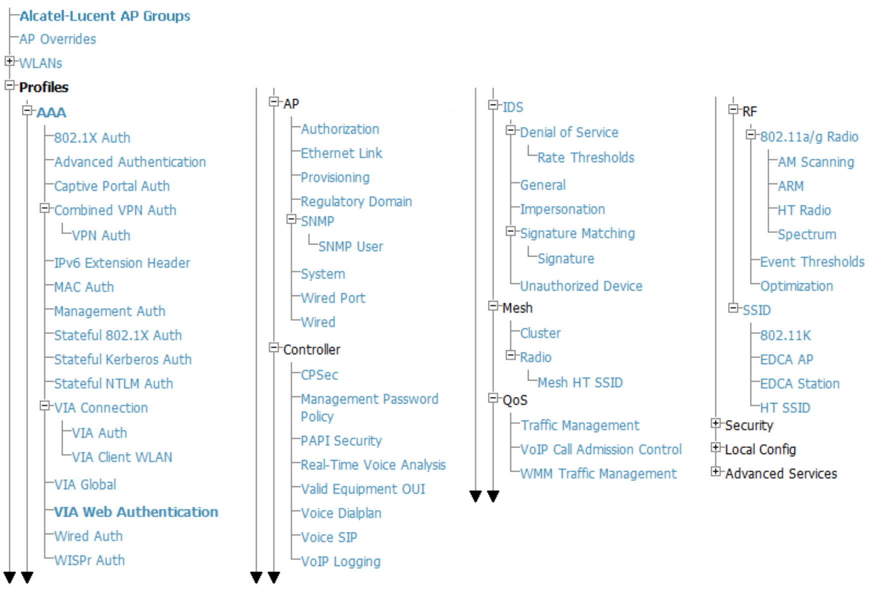
Device Setup > Alcatel-Lucent Configuration Page

NOTE

This page is not available if **Use Global Alcatel-Lucent Configuration** is disabled in **OV3600 Setup > General**.

The **Device Setup > Alcatel-Lucent Configuration** page displays the expandable navigation pane shown in Figure 2, allowing you to monitor and configure Alcatel-Lucent AP Groups, AP Overrides, WLANs, Profiles, Security, Local Config, and Advanced Services. Each of these sections is summarized in "Alcatel-Lucent Configuration Sections in the Tree View" on page 4.

Figure 2 ***Device Setup > Alcatel-Lucent Configuration*** *Navigation Illustration*



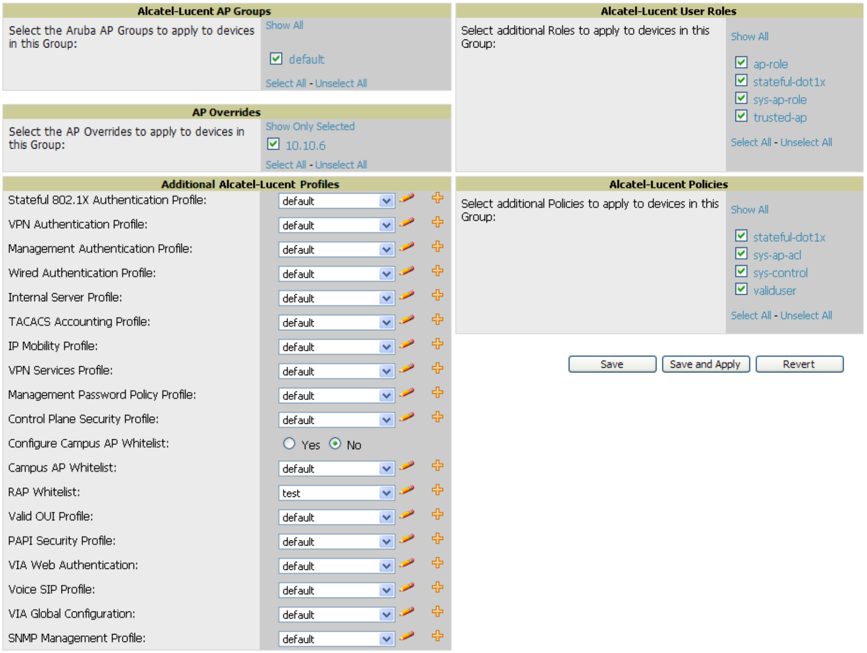
Groups > Alcatel-Lucent Config Page With Global Configuration Enabled

When **Use Global Alcatel-Lucent Configuration** is enabled in **OV3600 Setup > General,** focused submenu page displays and edits all configured Alcatel-Lucent AP groups, with the following factors:

- Alcatel-Lucent AP Groups must be defined from the **Device Setup > Alcatel-Lucent Configuration** page before they are visible on the **Groups > Alcatel-Lucent Config** page.
- Use this page to select the Alcatel-Lucent AP Groups that you push to switches.
- Use this page to associate a device group to one or more Alcatel-Lucent AP Groups.

- From this page, you can select other profiles that are defined on the switch, like an internal server.

Figure 3 ***Groups > Alcatel-Lucent Config*** *Page Illustration (Partial Display)*



Alcatel-Lucent AP Groups

Select the Aruba AP Groups to apply to devices in this Group:

☑ default

AP Overrides

Select the AP Overrides to apply to devices in this Group:

☑ 10.10.6

Additional Alcatel-Lucent Profiles

Stateful 802.1X Authentication Profile:	default
VPN Authentication Profile:	default
Management Authentication Profile:	default
Wired Authentication Profile:	default
Internal Server Profile:	default
TACACS Accounting Profile:	default
IP Mobility Profile:	default
VPN Services Profile:	default
Management Password Policy Profile:	default
Control Plane Security Profile:	default
Configure Campus AP Whitelist:	○ Yes ● No
Campus AP Whitelist:	default
RAP Whitelist:	test
Valid OUI Profile:	default
PAPI Security Profile:	default
VIA Web Authentication:	default
Voice SIP Profile:	default
VIA Global Configuration:	default
SNMP Management Profile:	default

Alcatel-Lucent User Roles

Select additional Roles to apply to devices in this Group:

☑ ap-role
☑ stateful-dot1x
☑ sys-ap-role
☑ trusted-ap

Alcatel-Lucent Policies

Select additional Policies to apply to devices in this Group:

☑ stateful-dot1x
☑ sys-ap-acl
☑ sys-control
☑ validuser

Show All
Select All - Unselect All
Show Only Selected
Select All - Unselect All
Show All
Select All - Unselect All
Show All
Select All - Unselect All
Save
Save and Apply
Revert

Groups > Alcatel-Lucent Config when Global Configuration is Disabled

If **Use Global Alcatel-Lucent Configuration** in **OV3600 Setup** > **General** is set to **No**, the **Groups** > **Alcatel-Lucent Config** page can be used to manage two or more distinctive configuration strategies using the same tree navigation as the **Device Setup** > **Alcatel-Lucent Configuration** page. Each of the sections is explained in "Alcatel-Lucent Configuration Sections in the Tree View" on page 4.

Alcatel-Lucent Configuration Sections in the Tree View

Whether you are using global or group configuration, the Alcatel-Lucent Configuration tree view page supports several sections, as follows:

- "Alcatel-Lucent AP Groups Section" on page 5
- "AP Overrides Section" on page 5
- "WLANs Section" on page 6
- "Profiles Section" on page 7
- "Security Section" on page 7
- "Local Config Section" on page 8
- "Advanced Services Section" on page 8

NOTE

Only Alcatel-Lucent AP Groups, AP Overrides, and WLANs contain custom-created items in the navigation pane.

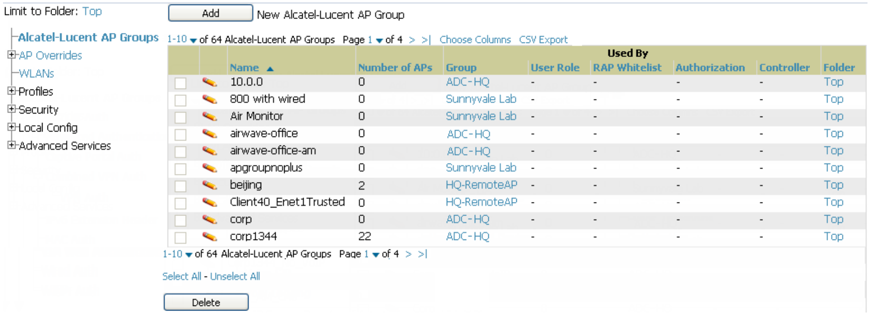
For the remainder of this document, the navigation **Alcatel-Lucent Configuration** > refers to the tree view in **Device Setup** or **Groups** tabs, depending on whether global or group configuration is enabled.

Alcatel-Lucent AP Groups Section

An Alcatel-Lucent AP Group is a collection of configuration profiles that define specific settings on Alcatel-Lucent switches and the devices that they govern. An Alcatel-Lucent AP Group references multiple configuration profiles, and in turn links to multiple WLANs.

Navigate to the **Alcatel-Lucent Configuration** > **Alcatel-Lucent AP Groups** page. The figure below illustrates one example of this page.

Figure 4 ***Alcatel-Lucent Configuration > Alcatel-Lucent AP Groups*** *Navigation*



					Used By				
		Name ▲	Number of APs	Group	User Role	RAP Whitelist	Authorization	Controller	Folder
□	✎	10.0.0	0	ADC-HQ	-	-	-	-	Top
□	✎	800 with wired	0	Sunnyvale Lab	-	-	-	-	Top
□	✎	Air Monitor	0	Sunnyvale Lab	-	-	-	-	Top
□	✎	airwave-office	0	ADC-HQ	-	-	-	-	Top
□	✎	airwave-office-am	0	ADC-HQ	-	-	-	-	Top
□	✎	apgroupnoplus	0	Sunnyvale Lab	-	-	-	-	Top
□	✎	beijing	2	HQ-RemoteAP	-	-	-	-	Top
□	✎	Client40_Enet1Trusted	0	HQ-RemoteAP	-	-	-	-	Top
□	✎	corp	0	ADC-HQ	-	-	-	-	Top
□	✎	corp1344	22	ADC-HQ	-	-	-	-	Top

1-10 of 64 Alcatel-Lucent AP Groups Page 1 of 4 > >|
Select All - Unselect All
Delete

Alcatel-Lucent AP Groups are not to be confused with conventional OV3600 device groups. OV3600 supports both group types, and both are viewable on the ***Groups > List*** *page when so configured.*

Alcatel-Lucent AP Groups have the following characteristics:

- Any Alcatel-Lucent switch can support multiple Alcatel-Lucent AP Groups.
- Alcatel-Lucent AP Groups are assigned to folders, and folders define visibility. Using conventional OV3600 folders to define visibility, Alcatel-Lucent AP Groups can provide visibility to some or many components while blocking visibility to other users for more sensitive components, such as SSIDs. Navigate to the **Users** pages to define folder visibility, and refer to "Visibility in Alcatel-Lucent Configuration" on page 25.
- You can import a switch configuration file from AOS-W for Alcatel-Lucent AP Group deployment in OV3600.

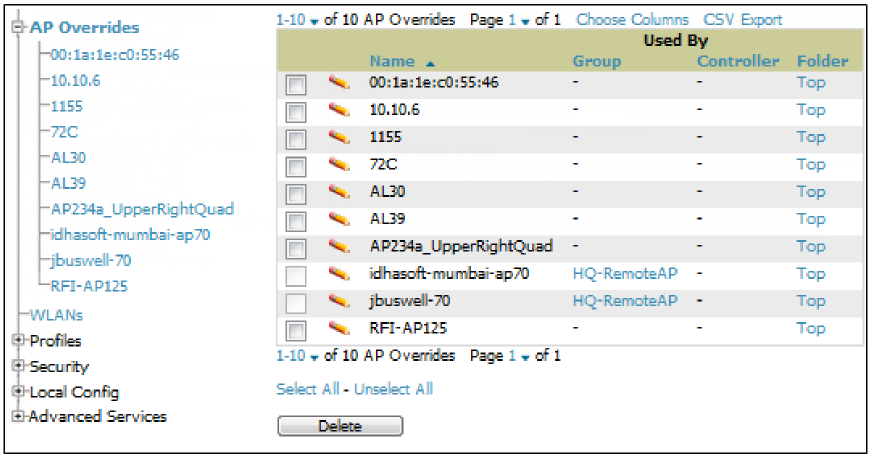
For additional information, refer to the following sections in this document:

- "Setting Up Initial Alcatel-Lucent Configuration" on page 13
- "Alcatel-Lucent AP Groups Procedures and Guidelines" on page 19

AP Overrides Section

The second major component of Alcatel-Lucent Configuration is the **AP Overrides** page, appearing immediately below Alcatel-Lucent **AP Groups** in the Navigation Pane. Figure 5 illustrates this location and access:

Figure 5 ***Alcatel-Lucent Configuration*** > ***AP Overrides*** *Navigation*



			Used By	
	Name ▲	Group	Controller	Folder
□	00:1a:1e:c0:55:46	-	-	Top
□	10.10.6	-	-	Top
□	1155	-	-	Top
□	72C	-	-	Top
□	AL30	-	-	Top
□	AL39	-	-	Top
□	AP234a_UpperRightQuad	-	-	Top
□	idhasoft-mumbai-ap70	HQ-RemoteAP	-	Top
□	jbuswell-70	HQ-RemoteAP	-	Top
□	RFI-AP125	-	-	Top

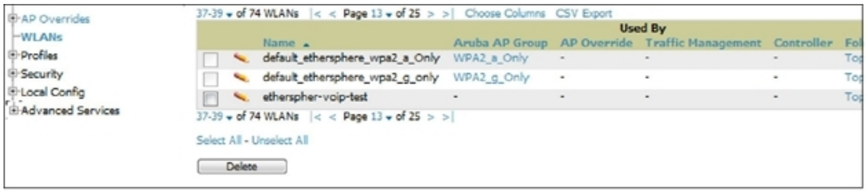
AP Overrides operate as follows in Alcatel-Lucent Configuration:

- Custom-created AP Overrides appear in the Alcatel-Lucent Configuration navigation pane, as illustrated in Figure 5.
- Alcatel-Lucent switch and AP devices operate in Alcatel-Lucent AP Groups that define shared parameters for all devices in those groups. The **Alcatel-Lucent Configuration** > **Alcatel-Lucent AP Groups** page displays all current Alcatel-Lucent AP groups.
- **AP Override** allows you to change some parameters for any specific device without having to create an Alcatel-Lucent AP group per AP.
- The name of any **AP Override** should be the same as the name of the device to which it applies. This establishes the basis of all linking to that device.
- Once you have created an **AP Override** for a device in a group, you specify the **WLANs** to be included and excluded.
- For additional information about how to configure and use AP Overrides, refer to "AP Overrides" on page 34.

WLANs Section

Access WLANs with **Alcatel-Lucent Configuration** > **WLANs**, illustrated in Figure 6.

Figure 6 ***Alcatel-Lucent Configuration > WLANs*** *Navigation*


AP Overrides
WLANs
Profiles
Security
Local Config
Advanced Services
37-39 of 74 WLANs |< < Page 13 of 25 > >| Choose Columns CSV Export
Select All - Unselect All
Delete

			Used By			
	Name ▲	Aruba AP Group	AP Override	Traffic Management	Controller	Fol
□	default_ethersphere_wpa2_a_Only	WPA2_a_Only	-	-	-	To
□	default_ethersphere_wpa2_g_only	WPA2_g_Only	-	-	-	To
□	ethersphe-voip-test	-	-	-	-	To

The following concepts govern the use of WLANs in Alcatel-Lucent Configuration:

- WLANs are the same as virtual AP configuration profiles.
- WLAN profiles contain several diverse settings including SSIDs, referenced Alcatel-Lucent AP Groups, Traffic Management profiles, and device folders.

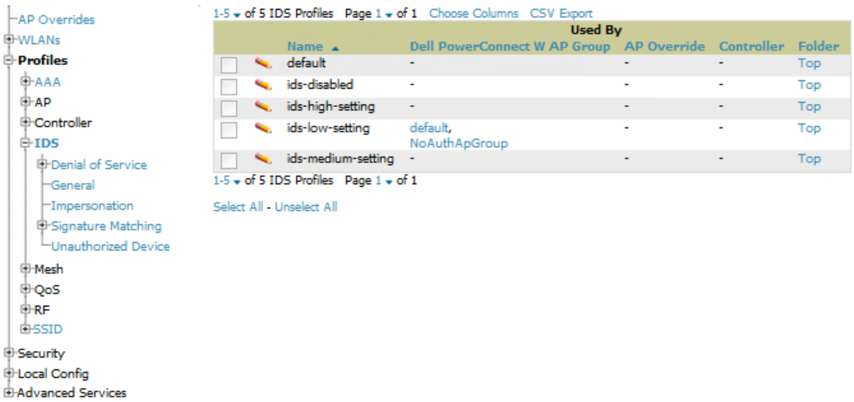
This document describes WLAN configuration in the following sections:

- "Setting Up Initial Alcatel-Lucent Configuration" on page 13
- "General WLAN Guidelines" on page 20
- "WLANs" on page 38

Profiles Section

Profiles provide a way to organize and deploy groups of configurations for Alcatel-Lucent AP Groups, WLANs, and other profiles. Profiles are assigned to folders; this establishes visibility to Alcatel-Lucent AP Groups and WLAN settings. Access **Profiles** with **Alcatel-Lucent Configuration** > **Profiles**, illustrated in Figure 7.

Figure 7 ***Alcatel-Lucent Configuration > Profiles*** *Navigation*



1-5 of 5 IDS Profiles   Page 1 of 1   Choose Columns   CSV Export

			Used By			
		Name ▲	Dell PowerConnect W AP Group	AP Override	Controller	Folder
□	✎	default	-	-	-	Top
□	✎	ids-disabled	-	-	-	Top
□	✎	ids-high-setting	-	-	-	Top
□	✎	ids-low-setting	default, NoAuthApGroup	-	-	Top
□	✎	ids-medium-setting	-	-	-	Top

1-5 of 5 IDS Profiles   Page 1 of 1

Select All - Unselect All

Profiles are organized by type. Custom-named profiles do not appear in the navigation pane as do custom-named Alcatel-Lucent AP Groups, WLANs, and AP Overrides.

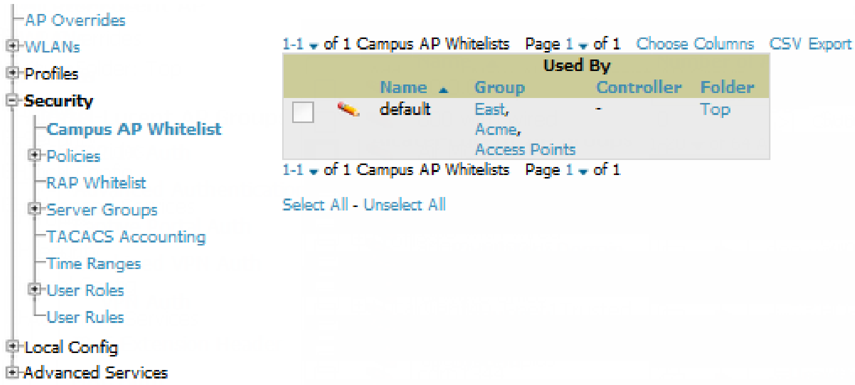
For additional information about profile procedures and guidelines, refer to the following sections in this document:

- "Setting Up Initial Alcatel-Lucent Configuration" on page 13
- "General Profiles Guidelines" on page 20
- "Profiles" on page 43

Security Section

The **Security** section displays, adds, edits, or deletes security profiles in multiple categories, including user roles, policies, rules, and servers such as RADIUS, TACACS+, and LDAP servers. Navigate to Security with the **Alcatel-Lucent Configuration** > **Security** path, illustrated in Figure 8.

Figure 8 ***Alcatel-Lucent Configuration > Security*** *Navigation*



1-1 of 1 Campus AP Whitelists   Page 1 of 1   Choose Columns   CSV Export

			Used By		
		Name ▲	Group	Controller	Folder
□	✎	default	East, Acme, Access Points	-	Top

1-1 of 1 Campus AP Whitelists   Page 1 of 1

Select All - Unselect All

The following general guidelines apply to **Security** profiles in Alcatel-Lucent configuration:

- Roles can have multiple policies; each policy can have numerous roles.
- Server groups are comprised of servers and rules. Security rules apply in Alcatel-Lucent Configuration in the same way as deployed in AOS-W.

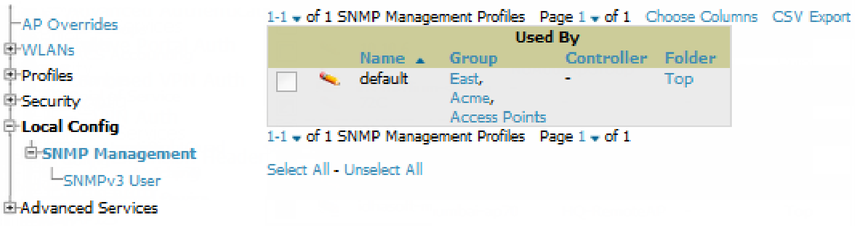
For additional information about Security, refer to "Security" on page 44 in the Appendix.

Local Config Section

The Local Config section is used for local configuration of Alcatel-Lucent switches. Locally configured settings are not pushed to local switches by master switches.

SNMP trap settings for switches are managed locally.

Figure 9 ***Alcatel-Lucent Configuration > Local Config Navigation***



1-1 of 1 SNMP Management Profiles Page 1 of 1

			Used By		
		Name ▲	Group	Controller	Folder
□	✎	default	East, Acme, Access Points	-	Top

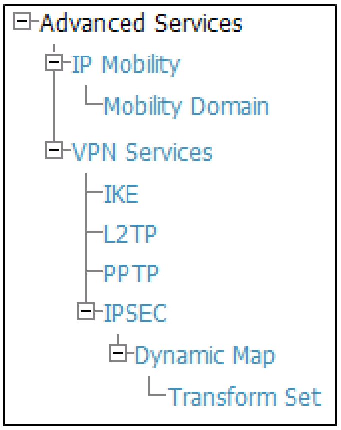
1-1 of 1 SNMP Management Profiles Page 1 of 1

For complete details on the Local Config section, refer to "Local Config of SNMP Management" on page 66.

Advanced Services Section

Navigate to Advanced Services with the **Alcatel-Lucent Configuration** > **Advanced Services** path. The **Advanced Services** section includes IP Mobility and VPN Services. Figure 10 illustrates this navigation and the components.

Figure 10 ***Alcatel-Lucent Configuration > Advanced Services** Navigation*

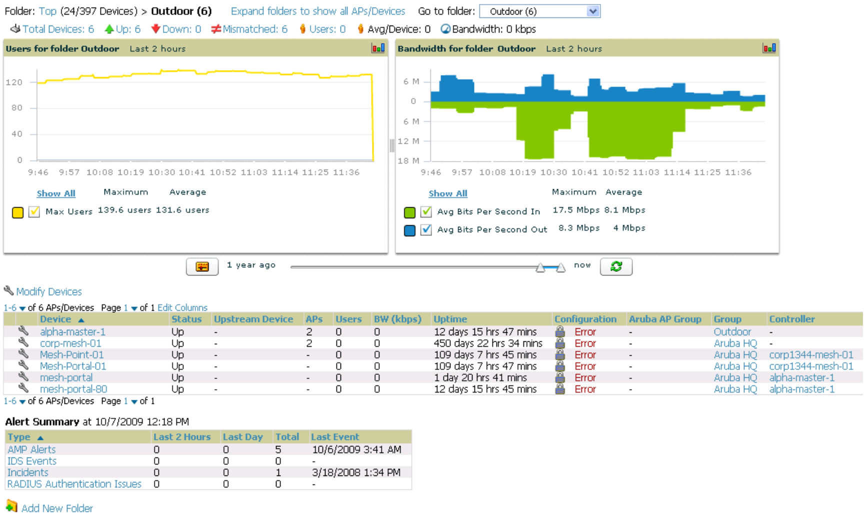


For additional information about IP Mobility and VPN Services, refer to "Advanced Services" on page 68.

APs/Devices > List Page

This page supports devices in all of OV3600. This page supports switch reboot, switch re-provisioning, and changing Alcatel-Lucent AP groups. Select **Modify Devices** to configure thin AP settings.

Figure 11 *APs/Devices List* Page Illustration (Partial Display)



Folder: Top (24/397 Devices) > **Outdoor (6)** Expand folders to show all APs/Devices Go to folder: Outdoor (6)

Total Devices: 6 Up: 6 Down: 0 Mismatched: 6 Users: 0 Avg/Device: 0 Bandwidth: 0 kbps

		Maximum	Average
🟨	☑ Max Users	139.6 users	131.6 users

		Maximum	Average
🟩	☑ Avg Bits Per Second In	17.5 Mbps	8.1 Mbps
🟦	☑ Avg Bits Per Second Out	8.3 Mbps	4 Mbps

Modify Devices

1-6 of 6 APs/Devices Page 1 of 1 Edit Columns

Device ▲	Status	Upstream Device	APs	Users	BW (kbps)	Uptime	Configuration	Aruba AP Group	Group	Controller
alpha-master-1	Up	-	2	0	0	12 days 15 hrs 47 mins	Error	-	Outdoor	-
corp-mesh-01	Up	-	2	0	0	450 days 22 hrs 34 mins	Error	-	Aruba HQ	-
Mesh-Point-01	Up	-	-	0	0	109 days 7 hrs 45 mins	Error	-	Aruba HQ	corp1344-mesh-01
Mesh-Portal-01	Up	-	-	0	0	109 days 7 hrs 47 mins	Error	-	Aruba HQ	corp1344-mesh-01
mesh-portal	Up	-	-	0	0	1 day 20 hrs 41 mins	Error	-	Aruba HQ	alpha-master-1
mesh-portal-80	Up	-	-	0	0	12 days 15 hrs 45 mins	Error	-	Aruba HQ	alpha-master-1

1-6 of 6 APs/Devices Page 1 of 1

Alert Summary at 10/7/2009 12:18 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	5	10/6/2009 3:41 AM
IDS Events	0	0	0	-
Incidents	0	0	1	3/18/2008 1:34 PM
RADIUS Authentication Issues	0	0	0	-

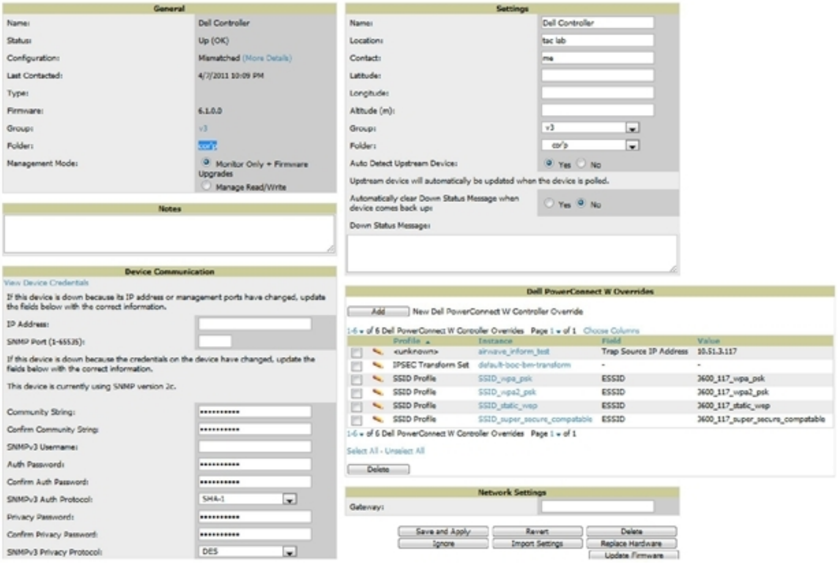
Add New Folder

APs/Devices > Manage Page

This page configures device-level settings, including **Manage** mode that enables pushing configurations to switches. For additional information, refer to "Pushing Device Configurations to Switches" on page 21.

You can create switch overrides for entire profiles or a specific profile setting per profile. This allows you to avoid creating new profiles or Alcatel-Lucent AP Groups that differ by one more settings. Switch overrides can be added from the switch's **APs/Devices** > **Manage** page. Figure 12 illustrates an **APs/Devices** > **Manage** page with switch overrides.

Figure 12 *APs/Devices* > *Manage* Page Illustration (Partial Display)



General

Name:	Dell Controller
Status:	Up (OK)
Configuration:	Mismatched (More Details)
Last Contacted:	4/7/2011 10:09 PM
Type:	
Firmware:	6.1.0.0
Group:	v3
Folder:	corp
Management Mode:	● Monitor Only + Firmware Upgrades ○ Manage Read/Write

Notes

Device Communication

View Device Credentials

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

IP Address:	
SNMP Port (1-65535):	

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

This device is currently using SNMP version 2c.

Community String:	•••••••••••
Confirm Community String:	•••••••••••
SNMPv3 Username:	
Auth Password:	•••••••••••
Confirm Auth Password:	•••••••••••
SNMPv3 Auth Protocol:	SHA-1
Privacy Password:	•••••••••••
Confirm Privacy Password:	•••••••••••
SNMPv3 Privacy Protocol:	DES

Settings

Name:	Dell Controller
Location:	tac lab
Contact:	me
Latitude:	
Longitude:	
Altitude (m):	
Group:	v3
Folder:	corp
Auto Detect Upstream Device:	● Yes ○ No

Upstream device will automatically be updated when the device is polled.

Automatically clear Down Status Message when device comes back up:	○ Yes ● No

Down Status Message:

Dell PowerConnect W Overrides

Add New Dell PowerConnect W Controller Override

1-6 of 6 Dell PowerConnect W Controller Overrides Page 1 of 1 Choose Columns

	Profile ▲	Instance	Field	Value
☐	<unknown>	airwave_inform_test	Trap Source IP Address	10.51.3.117
☐	IPSEC Transform Set	default-boc-bm-transform	-	-
☐	SSID Profile	SSID_wpa_psk	ESSID	3600_117_wpa_psk
☐	SSID Profile	SSID_wpa2_psk	ESSID	3600_117_wpa2_psk
☐	SSID Profile	SSID_static_wep	ESSID	3600_117_static_wep
☐	SSID Profile	SSID_super_secure_compatable	ESSID	3600_117_super_secure_compatable

1-6 of 6 Dell PowerConnect W Controller Overrides Page 1 of 1

Select All - Unselect All

Delete

Network Settings

Gateway:	

APs/Devices > Monitor Page

Used in conjunction with the **Manage** page, the **Monitor** page enables review of device-level settings. This page is large and often contains a great amount of information, including the following sections:

- Status information
- Switch’s License link

- Radio Statistics of some Alcatel-Lucent thin APs
- User and Bandwidth interactive graphs
- CPU Utilization and Memory Utilization interactive graphs
- APs Managed by this Switch list (when viewing a switch)
- Alert Summary
- Recent Events
- Audit Log

For additional information, refer to "Pushing Device Configurations to Switches" on page 21.

APs/Devices > Audit Page

The **APs/Devices** > **Audit** page is used to view the configuration status of a device. You can also perform the following tasks:

- Audit a device's current configuration
- Update group settings based on the device's current configuration using the **Import** button
- Customize settings to include/ignore during configuration audits
- View any mismatches

Groups > Basic Page

The **Groups** > **Basic** page deploys the following aspects of Alcatel-Lucent Configuration:

- Use this page to control which device settings appear on the **Groups** pages.
- If you want to configure your switches using templates instead, you should disable Alcatel-Lucent GUI configuration from the **Groups** > **Basic** page and use template-based configuration. See the Templates chapter of the *OmniVista 3600 Air Manager 7.6 User Guide* in **Home** > **Documentation** for more information on templates.

Additional Concepts and Components

Alcatel-Lucent Configuration emphasizes the following components and network management concepts.

- "Global Configuration and Scope" on page 10
- "Referenced Profile Setup" on page 11
- "Save, Save and Apply, and Revert Buttons" on page 12
- "Additional Concepts and Benefits" on page 12

Global Configuration and Scope

Alcatel-Lucent Configuration supports AOS-W as follows:

- OV3600 supports global configuration from both a master-local switch deployment and an all-master switch deployment:
  - In a master-local switch deployment, AOS-W is the agent that pushes global configurations from master switches to local switches. OV3600 supports this AOS-W functionality.
  - In an all-master-switch scenario, every master switch operates independent of other master switches. OV3600 provides the ability to push configuration to all master switches in this scenario.
- Alcatel-Lucent Configuration supports AOS-W profiles, Alcatel-Lucent AP Profiles, Servers, and User Roles.

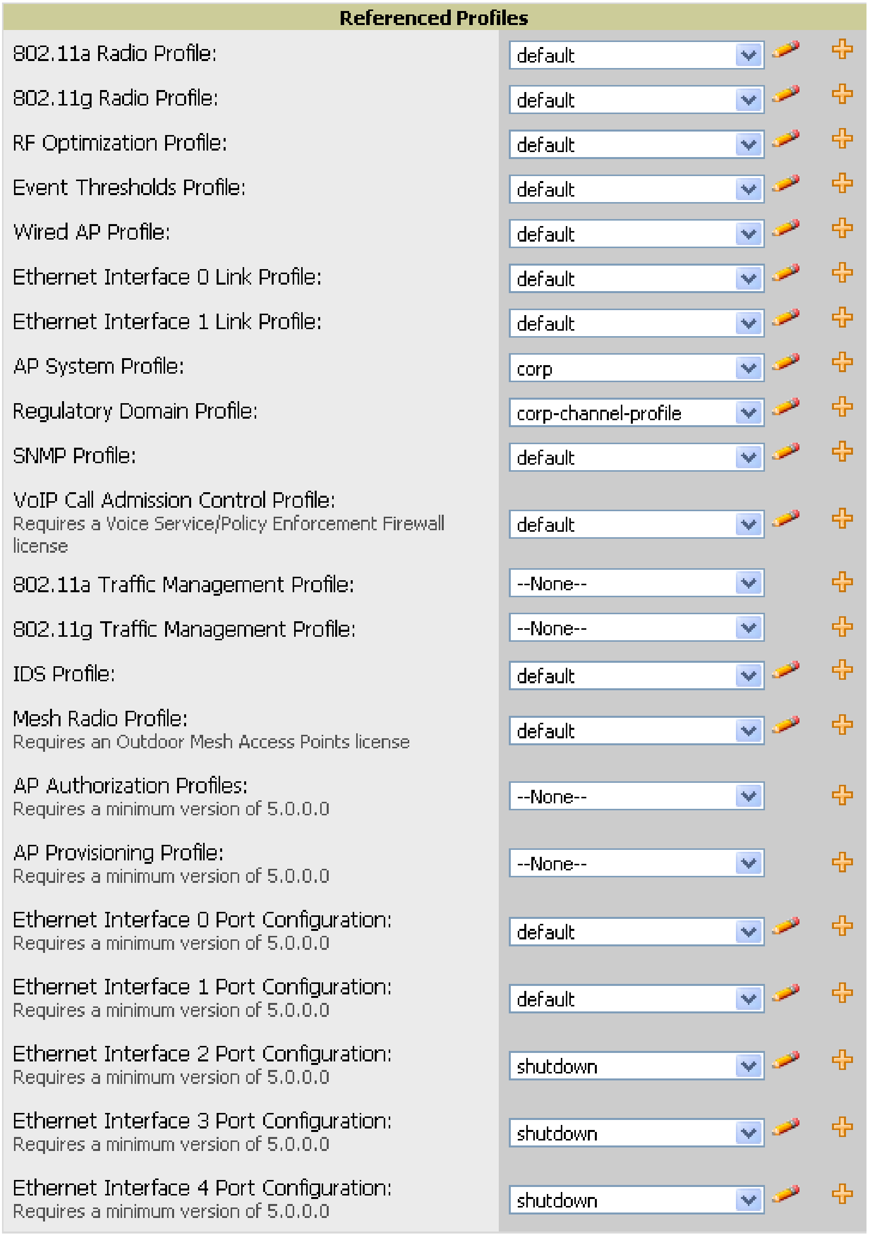
For additional information about these and additional functions, refer to "General Switch Procedures and Guidelines" on page 21.

Referenced Profile Setup

OV3600 allows you to add or reconfigure many configuration profiles while guiding you through a larger configuration sequence for an Alcatel-Lucent AP Group or WLAN. Consider the following example:

- When you create a new Alcatel-Lucent AP Group from the **Device Setup** > **Alcatel-Lucent Configuration** page, the **Referenced Profile** section appears as shown in Figure 13:

Figure 13 *Referenced Profile Configuration for an Alcatel-Lucent AP Group*



Referenced Profiles	
802.11a Radio Profile:	default
802.11g Radio Profile:	default
RF Optimization Profile:	default
Event Thresholds Profile:	default
Wired AP Profile:	default
Ethernet Interface 0 Link Profile:	default
Ethernet Interface 1 Link Profile:	default
AP System Profile:	corp
Regulatory Domain Profile:	corp-channel-profile
SNMP Profile:	default
VoIP Call Admission Control Profile: Requires a Voice Service/Policy Enforcement Firewall license	default
802.11a Traffic Management Profile:	--None--
802.11g Traffic Management Profile:	--None--
IDS Profile:	default
Mesh Radio Profile: Requires an Outdoor Mesh Access Points license	default
AP Authorization Profiles: Requires a minimum version of 5.0.0.0	--None--
AP Provisioning Profile: Requires a minimum version of 5.0.0.0	--None--
Ethernet Interface 0 Port Configuration: Requires a minimum version of 5.0.0.0	default
Ethernet Interface 1 Port Configuration: Requires a minimum version of 5.0.0.0	default
Ethernet Interface 2 Port Configuration: Requires a minimum version of 5.0.0.0	shutdown
Ethernet Interface 3 Port Configuration: Requires a minimum version of 5.0.0.0	shutdown
Ethernet Interface 4 Port Configuration: Requires a minimum version of 5.0.0.0	shutdown

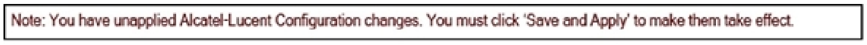
- Click the **Add** icon (the plus symbol) on the right to add a referenced profile. After you **Save** or **Save and Apply** that profile, OV3600 automatically returns you to the original Alcatel-Lucent AP Group configuration page.
- This embedded configuration is also supported on the **Additional Alcatel-Lucent Profiles** section of the **Groups > Alcatel-Lucent Config** page.

Save, Save and Apply, and Revert Buttons

Several **Add** or **Detail** pages in Alcatel-Lucent Configuration include the **Save**, **Save and Apply**, and **Revert** buttons. These buttons function as follows:

- **Save** —This button saves a configuration but does not apply it, allowing you to return to complete or apply the configuration at a later time. If you use this button, you may see the following alert on other Alcatel-Lucent Configuration pages. You can apply the configuration when all changes are complete at a later time.

Figure 14 *Unapplied Alcatel-Lucent Configuration Changes Message*



Note: You have unapplied Alcatel-Lucent Configuration changes. You must click 'Save and Apply' to make them take effect.

- **Save and Apply** —This button saves and applies the configuration with reference to Manage and Monitor modes. For example, you must click **Save and Apply** for a configuration profile to propagate to all switches in **Manage** mode. If you have switches in **Monitor Only** mode, OV3600 audits them, comparing their current configuration with the new desired configuration. For additional information and instructions about using **Manage** and **Monitor Only** modes, refer to "Pushing Device Configurations to Switches" on page 21.
- **Revert**—This button cancels out of a new configuration or reverts back to the last saved configuration.

Additional Concepts and Benefits

Scheduling Configuration Changes

You can schedule deployment of Alcatel-Lucent Configuration to minimize impact on network performance.

For example, configuration changes can be accumulated over time by using **Save and Apply** for devices in **Monitor Only** mode, then pushing all configuration changes at one time by putting devices in **Manage** mode. Refer to "Pushing Device Configurations to Switches" on page 21.

If your switches are already in Manage mode, you can also schedule the application of a single set of changes when clicking **Save and Apply**; just enter the date/time under **Scheduling Options** and click **Schedule**.

OV3600 pushes configuration settings that are defined in the GUI to the Alcatel-Lucent switches as a set of CLI commands using Secure Shell (SSH). No switch reboot is required.

Auditing and Reviewing Configurations

OV3600 supports auditing or reviewing in these ways:

1. You can review the AOS-W running configuration file. This is configuration information that OV3600 reads from the device. In template-based configuration, you can review the running configuration file when working on a related template.
2. You can use the **APs/Devices** > **Audit** page for device-specific auditing.
3. Once you audit your switch, you can click **Import** from the **APs/Devices** > **Audit** page to import the switch's current settings into its OV3600 Group's desired settings.

Licensing and Dependencies in Alcatel-Lucent Configuration

You can review your current licensing status with the **Licenses** link on the **APs/Devices** > **Monitor** page.

OV3600 requires that you have a policy enforcement firewall license always installed on all Alcatel-Lucentswitches. If you push a policy to a switch without this license, a **Good** configuration will not result, and the switch will show as **Mismatched** on OV3600 pages that reflect device configuration status.

Alcatel-Lucent Configuration includes several settings or functions that are dependent on special licenses. The user interface conveys that a special license is required for any such setting, function, or profile. OV3600 does not push such configurations when a license related to those configurations is unavailable. For details on the licenses required by a specific version of AOS-W, refer to the *Alcatel-Lucent AOS-W User Guide* for that release.

Setting Up Initial Alcatel-Lucent Configuration

This section describes how to deploy an initial setup of Alcatel-Lucent Configuration.

NOTE

Alcatel-Lucent Configuration is enabled by default in OV3600.

Prerequisites

- Complete the OV3600 upgrade to OV3600 6.4 or later. Upon upgrade to OV3600 Version 6.4 or later, global Alcatel-Lucent Configuration is enabled by default in groups with devices in monitor-only mode and AOS-W firmware of 3.3.2.10 or greater.
- Back up your AOS-Wswitch configuration file. Information about backing OV3600 is available in the *OmniVista 3600 Air Manager 7.6 User Guide* in the Performing Daily Operations in OV3600 chapter.

Procedure

Perform the following steps to deploy Alcatel-Lucent Configuration when at least one Alcatel-Lucent AP Group currently exists on at least one Alcatel-Lucent switch on the network:

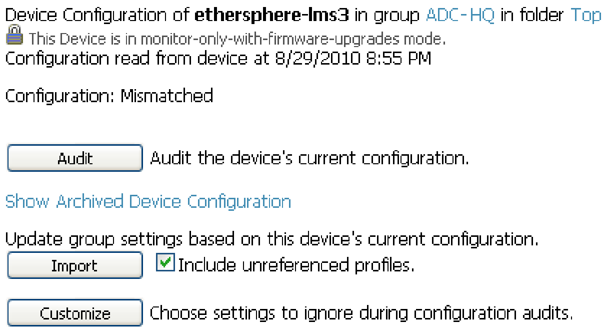
1. Determine whether you are using global or group configuration, and set **OV3600 Setup** > **General** > **Device Configuration** > **Use Global Alcatel-Lucent Configuration** accordingly.
2. On the **Groups > Basic** page, enable device preferences for Alcatel-Lucent devices. This configuration defines optional group display options. This step is not critical to setup, and default settings will support groups appropriate for Alcatel-Lucent Configuration. One important setting on this page is the **Alcatel-Lucent GUI Config** option. Ensure that setting is **Yes**, which is the default setting.
3. Authorize Alcatel-Lucent switches into the device group in **Monitor Only** mode.

CAUTION

When authorizing the first switch onto a device group, you must add the device in monitor-only mode. Otherwise, OV3600 removes the configuration of the switch before you have a chance to import the configuration, and this would remove critical network configuration and status.

4. Navigate to the **AP/s/Devices** > **Audit** page for the first switch to prepare for importing an existing Alcatel-Lucent switch configuration file. Figure 15 illustrates the information available on this page if the device is mismatched.

Figure 15 ***APs/Devices > Audit*** *Page Illustration*


Device Configuration of **ethersphere-lms3** in group ADC-HQ in folder Top
This Device is in monitor-only-with-firmware-upgrades mode.
Configuration read from device at 8/29/2010 8:55 PM

Configuration: Mismatched

Audit the device's current configuration.

Update group settings based on this device's current configuration.

☑ Include unreferenced profiles.

Choose settings to ignore during configuration audits.

If the page reports a device mismatch, the page will display an **Import** button that allows you to import the Alcatel-Lucent switch settings from anAlcatel-Lucent switch that has already been configured. To import the complete configuration from the switch (including any unreferenced profiles) select the **Include unreferenced**

profiles checkbox. If you deselect the checkbox, OV3600 will delete the unreferenced profiles/AP Groups on the switch when that configuration is pushed later, and they will not be imported.

In Global Configuration:

Importing this configuration creates all the Profiles and Alcatel-Lucent AP Groups on the **Device Setup** > **Alcatel-Lucent Configuration** page. This action also adds and selects the Alcatel-Lucent AP Groups that appear on the **Groups** > **Alcatel-Lucent Config** page.

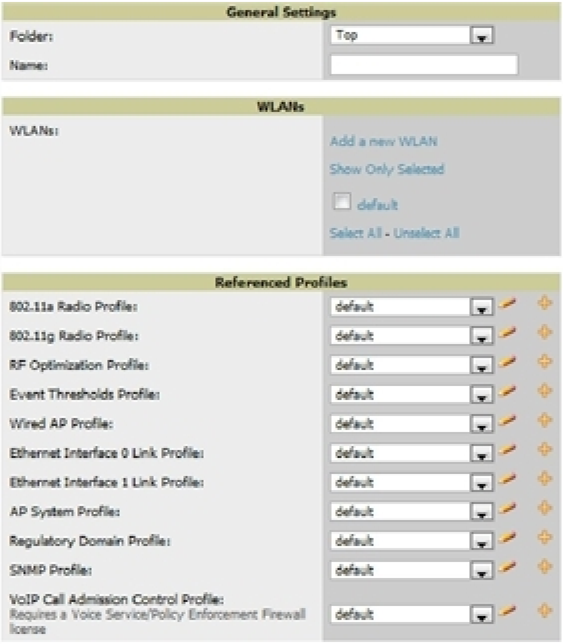
The folder for all the Profiles and Alcatel-Lucent AP Groups is set to the top folder of the OV3600 user who imports the configuration. This folder is **Top** in the case of managing administrators with read/write privileges.

In Group Configuration:

Importing this configuration creates Profiles and Alcatel-Lucent AP Groups in the switch's **Groups** > **Alcatel-Lucent Config** page.

5. After configuration file import is complete, refresh the page to verify the results of the import and add or edit as required.
6. Navigate to the **Alcatel-Lucent Configuration** page.
   - This page displays a list of APs authorized on the OV3600 that are using the Alcatel-Lucent AP Group.
   - The **User Role** is the Alcatel-Lucent User Role used in firewall settings. For additional information, refer to "Security > User Roles" on page 45.
   - *Global Configuration only:* The **Folder** column cites the visibility level to devices in each Alcatel-Lucent AP Group. For additional information, refer to "Visibility in Alcatel-Lucent Configuration" on page 25.
7. Add or modify **Alcatel-Lucent AP Groups** as required.
   a. Navigate to the **Alcatel-Lucent Configuration > Alcatel-Lucent AP Groups** page.
   b. Click **Add** from the **Alcatel-Lucent AP Groups** page to create a new Alcatel-Lucent AP Group. To edit an AP Group, click the pencil icon next to the group. The **Details** page for the AP Group appears. This page allows you to select the profiles to apply to the AP Group, and to select one or more WLANs that support that AP Group. Figure 16 illustrates this page.

Figure 16 ***Alcatel-Lucent Configuration > Alcatel-Lucent AP Groups > Add/Edit*** *Details Page (Partial View)*



General Settings

Folder:	Top
Name:	

WLANs

WLANs:

Add a new WLAN

Show Only Selected

□ default

Select All - Unselect All

Referenced Profiles

802.11a Radio Profile:	default
802.11g Radio Profile:	default
RF Optimization Profile:	default
Event Thresholds Profile:	default
Wired AP Profile:	default
Ethernet Interface 0 Link Profile:	default
Ethernet Interface 1 Link Profile:	default
AP System Profile:	default
Regulatory Domain Profile:	default
SNMP Profile:	default
VoIP Call Admission Control Profile: Requires a Voice Service/Policy Enforcement Firewall license	default

For additional information about configuring Alcatel-Lucent AP Groups, see "Alcatel-Lucent AP Groups Procedures and Guidelines" on page 19.

8. Add or edit WLANs in Alcatel-Lucent Configuration as required.
   a. Navigate to the **Alcatel-Lucent Configuration** > **WLANs** page. This page can display all WLANs currently configured, or can display only selected WLANs.
   b. Click **Add** to create a new WLAN, or click the pencil icon to edit an existing WLAN.

   You can add or edit WLANs in one of two ways, as follows:

   - **Basic**—This display is essentially the same as the AOS-W Wizard View on the Alcatel-Lucent switch. This page does not require in-depth knowledge of the profiles that define the Alcatel-Lucent AP Group.
   - **Advanced**—This display allows you to select individual profiles that define the WLAN and associated Alcatel-Lucent AP Group. This page requires in-depth knowledge of all profiles and their respective settings.

   The following sections of this configuration guide provides additional information and illustrations for configuring WLANs:

   - "General WLAN Guidelines" on page 20
   - "WLANs" on page 38 for details on all WLAN settings

9. Add or edit Alcatel-Lucent Configuration Profiles as required.
   a. Navigate to **Alcatel-Lucent Configuration** > **Profiles** section of the navigation pane.
   b. Select the type of profile in the navigation pane to configure: **AAA**, **AP**, **Switch**, **IDS**, **Mesh**, **QoS**, **RF**, or **SSID**.
   c. Click **Add** from any of these specific profile pages to create a new profile, or click the pencil icon to edit an existing profile.

   Most profiles in OV3600 are similar to the **All Profiles** display in the Alcatel-Lucent switch WebUI. The primary difference in OV3600 is that **AAA** and **SSID** profiles are not listed under the **WLAN** column, but under **Profiles**.

   d. Save changes to each element as you proceed through profile and WLAN configuration.

   All other settings supported on Alcatel-Lucent switches can be defined on the **Alcatel-Lucent Configuration** page. The following section in this document provides additional information about configuring profiles:

   - "General Profiles Guidelines" on page 20

10. Provision multiple Alcatel-Lucent AP Groups on one or more switches by putting the switches into an OV3600 group and configuring that group to use the selected Alcatel-Lucent AP Groups. With global configuration enabled, configure such Alcatel-Lucent AP Groups settings on the **Group** > **Alcatel-Lucent Config** page. With group configuration, use the Alcatel-Lucent AP Groups. The following section of this document provides additional information:

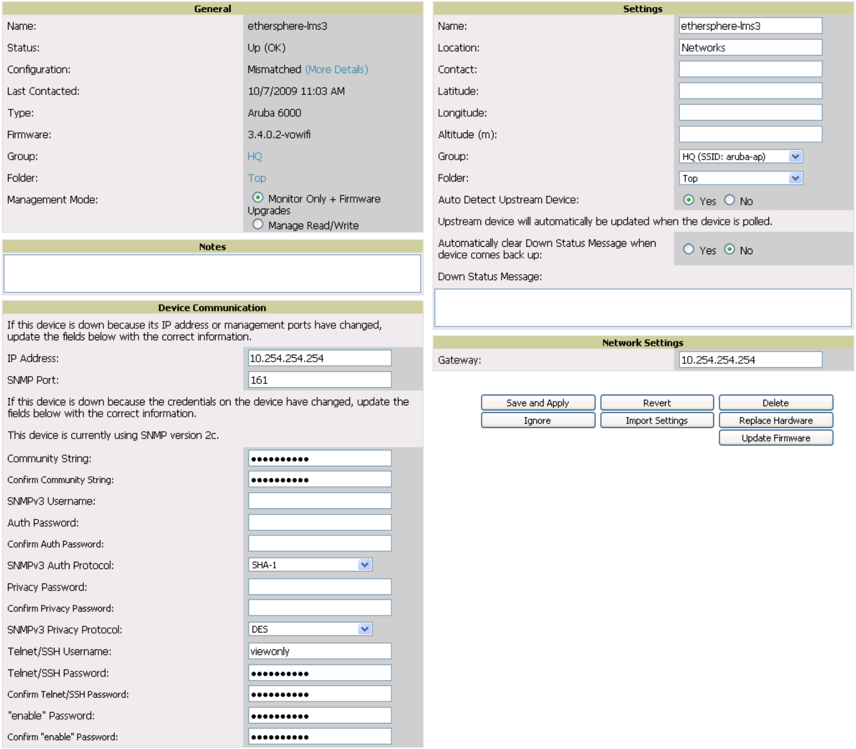
    - "Alcatel-Lucent AP Groups Procedures and Guidelines" on page 19

11. As required, add or edit AP devices. The following section of this document has additional information:

    - "Selecting Alcatel-Lucent AP Groups" on page 19

12. Each AP can be assigned to a single Alcatel-Lucent AP Group. Make sure to choose an AP Group that has been configured on that switch using that switch'sOV3600 Group. Use the **APs/Devices** > **List, Modify Devices** field and the **APs/Devices** > **Manage** page. You can create or edit settings such as the AP name, syslocation, and syscontact on the **APs/Devices** > **Manage** page. For additional information, refer to "Supporting APs with Alcatel-Lucent Configuration" on page 21.

Figure 17 ***APs/Devices > Manage** Page Illustration (Partial Display)*



General	
Name:	ethersphere-lms3
Status:	Up (OK)
Configuration:	Mismatched (More Details)
Last Contacted:	10/7/2009 11:03 AM
Type:	Aruba 6000
Firmware:	3.4.0.2-vowifi
Group:	HQ
Folder:	Top
Management Mode:	● Monitor Only + Firmware Upgrades ○ Manage Read/Write

Notes

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:	10.254.254.254
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 2c.

Community String:	••••••••••
Confirm Community String:	••••••••••
SNMPv3 Username:	
Auth Password:	
Confirm Auth Password:	
SNMPv3 Auth Protocol:	SHA-1
Privacy Password:	
Confirm Privacy Password:	
SNMPv3 Privacy Protocol:	DES
Telnet/SSH Username:	viewonly
Telnet/SSH Password:	••••••••••
Confirm Telnet/SSH Password:	••••••••••
"enable" Password:	••••••••••
Confirm "enable" Password:	••••••••••

Settings	
Name:	ethersphere-lms3
Location:	Networks
Contact:	
Latitude:	
Longitude:	
Altitude (m):	
Group:	HQ (SSID: aruba-ap)
Folder:	Top
Auto Detect Upstream Device:	● Yes ○ No

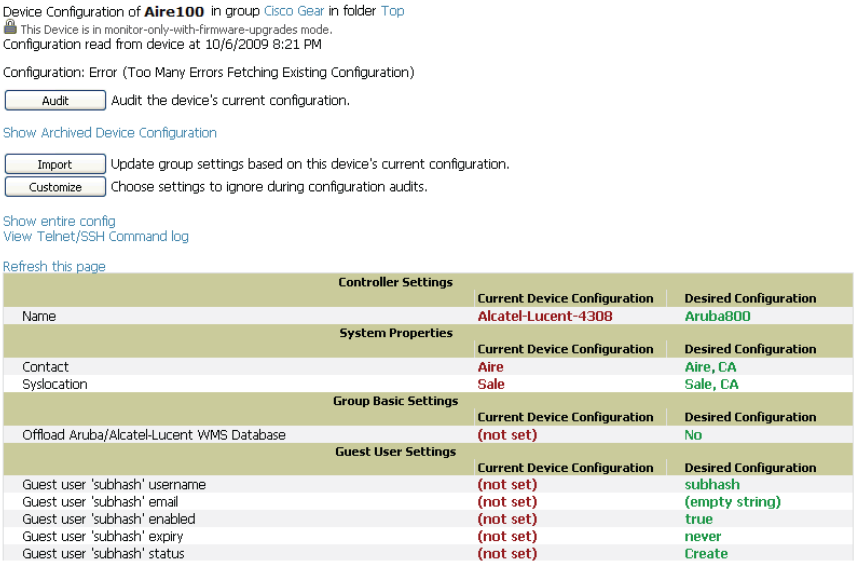
Upstream device will automatically be updated when the device is polled.

Automatically clear Down Status Message when device comes back up:	○ Yes ● No
Down Status Message:	

Network Settings	
Gateway:	10.254.254.254

13. Navigate to the **APs/Devices > Audit** page for the switch to view mismatched settings. This page provides links to display additional and current configurations. You can display all mismatched devices by navigating to the **APs/Devices > Mismatched** page.

Figure 18 ***APs/Devices > Audit** Page Illustration (Partial Display)*



Device Configuration of **Aire100** in group Cisco Gear in folder Top
This Device is in monitor-only-with-firmware-upgrades mode.
Configuration read from device at 10/6/2009 8:21 PM

Configuration: Error (Too Many Errors Fetching Existing Configuration)

Audit the device's current configuration.

Show Archived Device Configuration

Update group settings based on this device's current configuration.

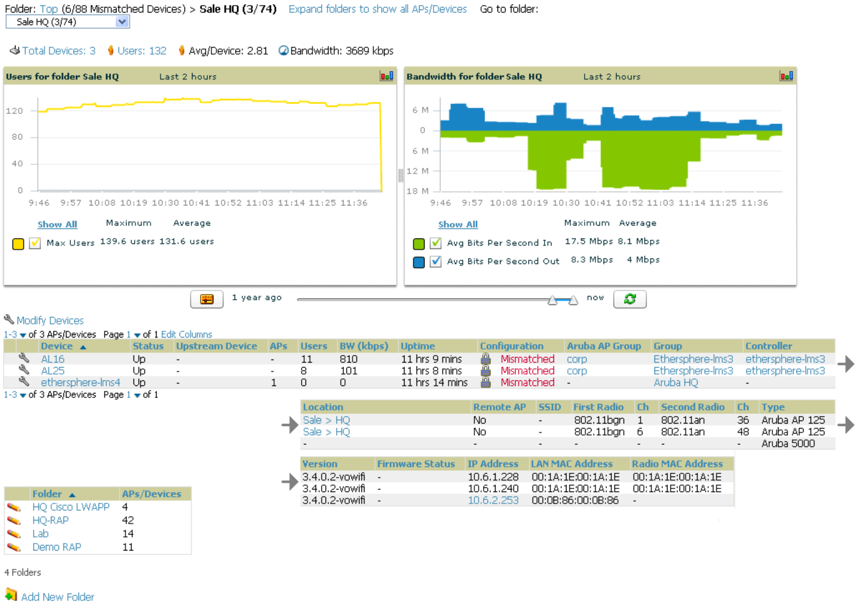
Choose settings to ignore during configuration audits.

Show entire config
View Telnet/SSH Command log

Refresh this page

	Controller Settings	
	Current Device Configuration	**Desired Configuration**
Name	Alcatel-Lucent-4308	Aruba800
	System Properties	
	Current Device Configuration	**Desired Configuration**
Contact	Aire	Aire, CA
Syslocation	Sale	Sale, CA
	Group Basic Settings	
	Current Device Configuration	**Desired Configuration**
Offload Aruba/Alcatel-Lucent WMS Database	(not set)	No
	Guest User Settings	
	Current Device Configuration	**Desired Configuration**
Guest user 'subhash' username	(not set)	subhash
Guest user 'subhash' email	(not set)	(empty string)
Guest user 'subhash' enabled	(not set)	true
Guest user 'subhash' expiry	(not set)	never
Guest user 'subhash' status	(not set)	Create

Figure 19 ***APs/Devices > Mismatched** Page Illustration*



Folder: Top (6/88 Mismatched Devices) > **Sale HQ (3/74)** Expand folders to show all APs/Devices Go to folder: Sale HQ (3/74)

Total Devices: 3 Users: 132 Avg/Device: 2.81 Bandwidth: 3689 kbps

Show All	Maximum	Average
🟨 ☑ Max Users	139.6 users	131.6 users

Show All	Maximum	Average
🟩 ☑ Avg Bits Per Second In	17.5 Mbps	8.1 Mbps
🟦 ☑ Avg Bits Per Second Out	8.3 Mbps	4 Mbps

Modify Devices

1-3 of 3 APs/Devices Page 1 of 1 Edit Columns

Device ▲	Status	Upstream Device	APs	Users	BW (kbps)	Uptime	Configuration	Aruba AP Group	Group	Controller
AL16	Up	-	-	11	810	11 hrs 9 mins	Mismatched	corp	Ethersphere-lms3	ethersphere-lms3
AL25	Up	-	-	8	101	11 hrs 8 mins	Mismatched	corp	Ethersphere-lms3	ethersphere-lms3
ethersphere-lms4	Up	-	1	0	0	11 hrs 14 mins	Mismatched	-	Aruba HQ	-

1-3 of 3 APs/Devices Page 1 of 1

Location	Remote AP	SSID	First Radio	Ch	Second Radio	Ch	Type
Sale > HQ	No	-	802.11bgn	1	802.11an	36	Aruba AP 125
Sale > HQ	No	-	802.11bgn	6	802.11an	48	Aruba AP 125
-	-	-	-	-	-	-	Aruba 5000

Version	Firmware Status	IP Address	LAN MAC Address	Radio MAC Address
3.4.0.2-vowifi	-	10.6.1.228	00:1A:1E:00:1A:1E	00:1A:1E:00:1A:1E
3.4.0.2-vowifi	-	10.6.1.240	00:1A:1E:00:1A:1E	00:1A:1E:00:1A:1E
3.4.0.2-vowifi	-	10.6.2.253	00:0B:86:00:0B:86	-

Folder ▲	APs/Devices
HQ Cisco LWAPP	4
HQ-RAP	42
Lab	14
Demo RAP	11

4 Folders

Add New Folder

After initial AOS-W deployment with the Alcatel-Lucent Configuration feature, you can make additional configurations or continue with maintenance tasks, such as the following examples:

- Once Alcatel-Lucent Configuration is deployed in OV3600, you can perform debugging with Telnet/SSH. Review the `telnet_cmds` file in the `/var/log` folder from the command line interface, or access this file from the **System** > **Status** page. For additional information, refer to the *Alcatel-Lucent OmniVista 3600 7.6 User Guide*.
- To resolve communication issues, review the credentials on the **APs/Devices** > **Manage** page.
- Mismatches can occur when importing profiles because OV3600 deletes orphaned profiles, even if following a new import.

Additional Capabilities

OV3600 supports many additional AOS-W configurations and settings. Refer to these additional resources for more information in **Home** > **Documentation**:

- *Alcatel-Lucent AOS-W User Guide*
- *Alcatel-Lucent OmniVista 3600 7.6 User Guide*
- *Alcatel-Lucent OmniVista 3600 7.6 Best Practices Guide*

Chapter 2

Alcatel-Lucent Configuration in Daily Operations

This section presents common tasks or concepts after initial setup of Alcatel-Lucent Configuration is complete, as described in the section "Setting Up Initial Alcatel-Lucent Configuration" on page 13. This chapter emphasizes frequent procedures as follows:

- "Alcatel-Lucent AP Groups Procedures and Guidelines" on page 19
- "General WLAN Guidelines" on page 20
- "General Switch Procedures and Guidelines" on page 21
- "Supporting APs with Alcatel-Lucent Configuration" on page 21
- "Visibility in Alcatel-Lucent Configuration" on page 25
- "Using OV3600 to Deploy Alcatel-Lucent APs" on page 23

NOTE

For a complete reference on all Configuration pages, field descriptions, and certain additional procedures that are more specialized, refer to "Alcatel-Lucent Configuration Reference" on page 29.

Alcatel-Lucent AP Groups Procedures and Guidelines

Guidelines and Pages for Alcatel-Lucent AP Groups

The fields and default settings for Alcatel-Lucent AP Groups are described in "Alcatel-Lucent AP Groups" on page 30. The following guidelines govern the configuration and use of Alcatel-Lucent AP Groups across OV3600:

- Alcatel-Lucent AP Groups function with standard OV3600 groups that contain them. Add Alcatel-Lucent AP Groups to standard OV3600 groups. Additional procedures in this document explain their interoperability.
- APs can belong to a switch's OV3600 group or to an OV3600 group by themselves.
- All configurations of Alcatel-Lucent AP Groups must be pushed to Alcatel-Lucent switches to become active on the network.
- Additional dynamics between master, standby master, and local switches still apply. In this case, refer to "Using Master, Standby Master, and Local Switches" on page 21.

The following *pages* in OV3600 govern the configuration and use of Alcatel-Lucent AP Groups or standard device groups across OV3600:

- The **Alcatel-Lucent Configuration** navigation pane displays standard AOS-W components and your custom-configured Alcatel-Lucent AP Groups, WLANs, and AP Overrides.
- You define or modify Alcatel-Lucent AP Groups on the **Alcatel-Lucent Configuration** page. Click **Alcatel-Lucent AP Groups** from the navigation pane.
- With Global configuration enabled, select **Alcatel-Lucent AP Groups** to associate with OV3600 Groups with the **Groups > Alcatel-Lucent Config** page.
- You modify devices in Alcatel-Lucent AP Groups with the **APs/Devices > List** page, clicking **Modify Devices**. This is the page where you assign devices to a given group and Alcatel-Lucent AP Group.

Selecting Alcatel-Lucent AP Groups

To select Alcatel-Lucent AP Groups, navigate to the **Alcatel-Lucent Configuration** > **Alcatel-Lucent AP Groups** page. This page is central to defining Alcatel-Lucent AP Groups, viewing the OV3600 groups with which an AP Group is associated, changing or deleting AP Groups, and assigning AP devices to an AP Group.

Configuring Alcatel-Lucent AP Groups

Perform the following steps to display, add, edit, or delete AP Groups in **Alcatel-Lucent Configuration.**

1. Browse to the **Alcatel-Lucent Configuration** page, and click the **AP Groups** heading in the navigation pane on the left. The **Groups Summary** page appears and displays all current Alcatel-Lucent AP Groups.
2. To add a new group, click the **Add AP Group** button. To edit an existing group, click the **pencil** icon next to the group name. The **Details** page appears with current or default configurations. The settings on this page are described in "Alcatel-Lucent AP Groups Procedures and Guidelines" on page 19.
3. Click **Add** or **Save** to finish creating or editing the Alcatel-Lucent AP Group. Click **Cancel** to exit this screen and to cancel the AP Group configurations.
4. New AP groups appear in the **AP Groups** section of the Alcatel-Lucent Configuration navigation pane, and clicking the group name takes you to the **Details** page for that group.
5. When this and other procedures are completed, push the configuration to the Alcatel-Lucent switches by clicking **Save and Apply**. The principles of Monitor and Manage mode still apply. For additional information, refer to "Pushing Device Configurations to Switches" on page 21.

Once Alcatel-Lucent AP groups are defined, ensure that all desired WLANs are referenced in Alcatel-Lucent AP Groups, as required. Repeat the above procedure to revise WLANs as required. You can add or edit AP devices in Alcatel-Lucent AP Groups, and you can configure AP Override settings that allow for custom AP configuration within the larger group in which it operates.

General WLAN Guidelines

Guidelines and Pages for WLANs in Alcatel-Lucent Configuration

- The **Alcatel-Lucent Configuration** navigation pane displays custom-configured WLANs and Alcatel-Lucent AP Groups. You define or modify WLANs on the **Alcatel-Lucent Configuration** page. Click **WLANs** from the navigation pane.
- You can create or edit any profile in an WLAN as you define or modify that WLAN. If you digress to profile setup from a different page, OV3600 returns you to your place on the **WLAN** setup page once you are done with profile setup.
- All configurations must be pushed to Alcatel-Lucent switches to become active on the network.

General Profiles Guidelines

AOS-W elements can be added or edited after an AOS-W configuration file is imported to OV3600 and pushed to switches with the steps described in "Setting Up Initial Alcatel-Lucent Configuration" on page 13.

Profiles in Alcatel-Lucent configuration entail the following concepts or dynamics:

- Profiles define nearly all parameters for Alcatel-Lucent AP Groups and WLANs, and Alcatel-Lucent Configuration supports many diverse profile types.
- Some profiles provide configurations for additional profiles that reference them. When this is the case, this document describes the interrelationship of such profiles to each other.
- Profiles can be configured in standalone fashion using the procedures in this chapter, then applied elsewhere as desired. Otherwise, you can define referenced profiles as you progress through Alcatel-Lucent AP Group or WLAN setup. In the latter case, OV3600 takes you to profile setup on separate pages, then returns to the Alcatel-Lucent AP Group or WLAN setup.

For complete Profiles inventory and field descriptions, refer to "Profiles" on page 43.

General Switch Procedures and Guidelines

Using Master, Standby Master, and Local Switches

OV3600 implements the following general approaches to switches:

- Master Switch—This switch maintains and pushes all global configurations. OV3600 pushes configurations only to a master switch.
- Standby Switch—The master switch synchronizes with the standby master switch, which remains ready to govern global configurations for all switches should the active master switch fail.
- Local Switch—Master switches push local configurations to local switches. Local switches retain settings such as the interfaces and global VLANs.

OV3600 is aware of differences in what is pushed to master switches and local switches, and automatically pushes all configurations to the appropriate switches. Thin AP provisioning is pushed to the switch to which a thin AP is connected.

You can determine additional details about what is specific to each switch by reviewing information on the **Groups > Alcatel-Lucent Config** page, and the **Groups > Monitor** page for any specific AP that lists its master and standby master switch.

Pushing Device Configurations to Switches

When you add or edit device configurations, you can push device configurations to switch as follows:

- Make device changes on the **Alcatel-Lucent Configuration** page and click **Save and Apply**.
- If global configuration is enabled, also make devices changes on the **Groups > Alcatel-Lucent Config** page and click **Save and Apply**.

A device must be in **Manage** mode to push configurations in this way.

NOTE

If you click **Save and Apply** when a device is in **Monitor** mode, this initiates a verification process in which OV3600 advises you of the latest mismatches. Mismatches are viewable from the **APs/Devices > Mismatched** page. Additional **Audit** and **Group** pages list mismatched statuses for devices.

Normally, devices are in Monitor mode. It may be advisable in some circumstances to accumulate several configuration changes in Monitor mode prior to pushing an entire set of changes to switches. Follow these general steps when implementing configuration changes for devices in Monitor mode:

1. Make all device changes using the **Alcatel-Lucent Configuration** pages. Click **Save and Apply** as you complete device-level changes. This builds an inventory of pending configuration changes that have not been pushed to the switch and APs.
2. Review the entire set of newly mismatched devices on the **APs/Devices > Mismatched** page.
3. For each mismatched device, navigate to the **APs/Devices > Audit** page to audit recent configuration changes as desired.
4. Once all mismatched device configurations are verified to be correct from the **APs/Devices > Audit** page, use the **Modify Devices** link on the **Groups > Monitor** page to place these devices into **Manage** mode. This instructs OV3600 to push the device configurations to the switch.
5. As desired, return devices to **Monitor** mode until the next set of configuration changes is ready to push to switches.

Supporting APs with Alcatel-Lucent Configuration

AP Overrides Guidelines

The **AP Override** component of Alcatel-Lucent Configuration operates with the following principles:

- AP devices function within groups that define operational parameters for groups of APs. This is standard across all of OV3600.
- **AP Overrides** allows you to change some parameters of any given AP without having to remove that AP from the configuration group in which it operates.
- The name of any **AP Override** that you create should be the same as the name of the AP device to which it applies. This establishes the basis of all linking to that AP device.
- Once you have created an **AP Override**, you select the **WLANs** in which it applies.
- Once you have created the AP Override, you can go one step further with the **Exclude WLANs** option of **AP Override**, which allows you to exclude certain SSIDs from the **AP override**. For example, if you have a set of WLANs with several SSIDs available, the **Exclude WLANs** option allows you to specify which SSIDs to exclude from the **AP Override**.
- You can also exclude mesh clusters from the **AP Override**.

In summary, the **AP Override** feature prevents you from having to create a new AP group for customized APs that otherwise share parameters with other APs in a group. **AP Override** allows you to have less total AP groups than you might otherwise require.

Changing Adaptive Radio Management (ARM) Settings

You can adjust ARM settings for the radios of a particular Alcatel-Lucent AP Group. To do so, refer to the following topics that describe ARM in relation to Alcatel-Lucent AP groups and device-level radio settings:

- "Configuring Alcatel-Lucent AP Groups" on page 20
- "Alcatel-Lucent AP Groups Procedures and Guidelines" on page 19
- "Profiles" on page 43

Changing SSID and Encryption Settings

You can adjust SSID and Encryption parameters for devices by adjusting the profiles that define these settings, then applying those profiles to Alcatel-Lucent AP Groups and WLANs that support them. To do so, refer to the following topics that describe relevant steps and configuration pages:

- "Configuring Alcatel-Lucent AP Groups" on page 20
- "Guidelines and Pages for WLANs in Alcatel-Lucent Configuration" on page 20
- "Profiles" on page 43

Changing the Alcatel-Lucent AP Group for an AP Device

You can change the Alcatel-Lucent AP Group to which an AP device is associated. Perform the following steps to change the AP Group for an AP device:

1. As required, review the Alcatel-Lucent AP Groups currently configured in OV3600. Navigate to the **Alcatel-Lucent Configuration** page, and click **Alcatel-Lucent AP Groups** from the navigation pane. This page displays and allows editing for all AP Groups that are currently configured in OV3600.
2. Navigate to the **APs/Devices > List** page to view all devices currently seen by OV3600.
3. If necessary, add the device to OV3600 using the **APs/Devices** > **New** page.

   To discover additional devices, ensure that the switch is set to perform a thin AP poll period.
4. On the **APs/Devices** > **List** page, you can specify the **Group** and **Folder** to which a device belongs. Click **Modify Devices** to change more than one device, or click the **Wrench** icon associated with any specific device to make changes. The **APs/Devices** > **Manage** page appears.
5. In the **Settings** section of the **APs/Devices** > **Manage** page, select the new Alcatel-Lucent AP Group to assign to the device. Change or adjust any additional settings as desired.

6. Click **Save and Apply** to retain these settings and to propagate them throughout OV3600, or click one of the alternate buttons as follows for an alternative change:
   - Click **Revert** to cancel out of all changes on this page.
   - Click **Delete** to remove this device from OV3600.
   - Click **Ignore** to keep the device in OV3600 but to ignore it.
   - Click **Import Settings** to define device settings from previously created configurations.
   - Click **Replace Hardware** to replace the AP device with a new AP device.
   - Click **Update Firmware** to update the Firmware that operates this device.
7. Push this configuration change to the AP switch that is to support this AP device. For additional information, refer to "Pushing Device Configurations to Switches" on page 21.

Using OV3600 to Deploy Alcatel-Lucent APs

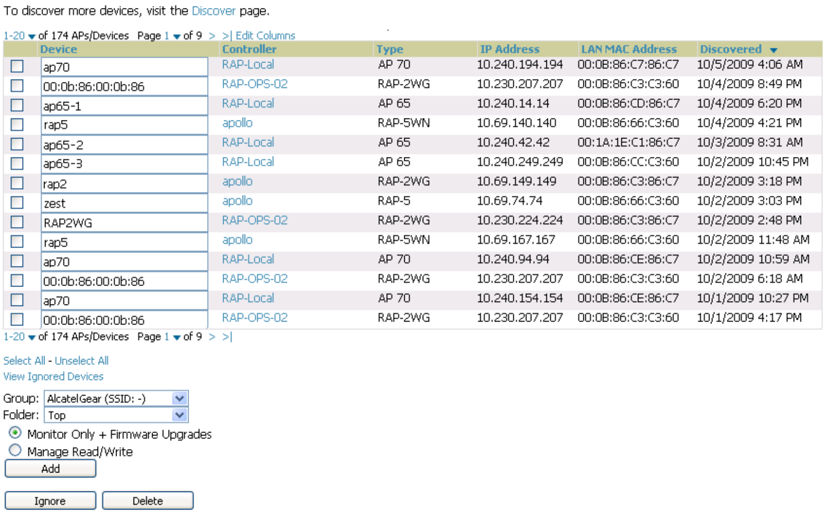
In addition to migrating Alcatel-Lucent access points (APs) from AOS-W-oriented administration to OV3600 administration, you can use OV3600 to deploy Alcatel-Lucent APs for the first time without separate AOS-W configuration. Be aware of the following dynamics in this scenario:

- OV3600 can manage all wireless network management functions, including:
  - the first-time provisioning of Alcatel-Lucent APs
  - managing Alcatel-Lucent switches with OV3600
- In this scenario, when a new Alcatel-Lucent AP boots up, OV3600 may discover the AP before you have a chance to configure and launch it through AOS-W configuration on the Alcatel-Lucent switch. In this case, the AP appears in OV3600 with a device name based on the MAC address.
- When you provision the AP through the Alcatel-Lucent switch and then rename the AP, the new AP name is *not* updated in OV3600.

An efficient and robust approach to update an Alcatel-Lucent AP device name is to deploy Alcatel-Lucent APs in OV3600 with the following steps:

1. Define communication settings for Alcatel-Lucent APs pending discovery in the **Device Setup > Communication** page. This assigns communication settings to multiple devices at the time of discovery, and prevents having to define such settings manually for each device after discovery.
2. Discover new Alcatel-Lucent APs with OV3600. You can do so with the **Device Setup > Discover** page.
3. Click **New Devices** In the **Status** section at the top of any OV3600 page, or navigate to the **APs/Devices > New** page.

Figure 20 *New Devices*



To discover more devices, visit the Discover page.

1-20 ▾ of 174 APs/Devices Page 1 ▾ of 9 > >| Edit Columns

	Device	Controller	Type	IP Address	LAN MAC Address	Discovered ▾
☐	ap70	RAP-Local	AP 70	10.240.194.194	00:0B:86:C7:86:C7	10/5/2009 4:06 AM
☐	00:0b:86:00:0b:86	RAP-OPS-02	RAP-2WG	10.230.207.207	00:0B:86:C3:C3:60	10/4/2009 8:49 PM
☐	ap65-1	RAP-Local	AP 65	10.240.14.14	00:0B:86:CD:86:C7	10/4/2009 6:20 PM
☐	rap5	apollo	RAP-5WN	10.69.140.140	00:0B:86:66:C3:60	10/4/2009 4:21 PM
☐	ap65-2	RAP-Local	AP 65	10.240.42.42	00:1A:1E:C1:86:C7	10/3/2009 8:31 AM
☐	ap65-3	RAP-Local	AP 65	10.240.249.249	00:0B:86:CC:C3:60	10/2/2009 10:45 PM
☐	rap2	apollo	RAP-2WG	10.69.149.149	00:0B:86:C3:86:C7	10/2/2009 3:18 PM
☐	zest	apollo	RAP-5	10.69.74.74	00:0B:86:66:C3:60	10/2/2009 3:03 PM
☐	RAP2WG	RAP-OPS-02	RAP-2WG	10.230.224.224	00:0B:86:C3:86:C7	10/2/2009 2:48 PM
☐	rap5	apollo	RAP-5WN	10.69.167.167	00:0B:86:66:C3:60	10/2/2009 11:48 AM
☐	ap70	RAP-Local	AP 70	10.240.94.94	00:0B:86:CE:86:C7	10/2/2009 10:59 AM
☐	00:0b:86:00:0b:86	RAP-OPS-02	RAP-2WG	10.230.207.207	00:0B:86:C3:C3:60	10/2/2009 6:18 AM
☐	ap70	RAP-Local	AP 70	10.240.154.154	00:0B:86:CE:86:C7	10/1/2009 10:27 PM
☐	00:0b:86:00:0b:86	RAP-OPS-02	RAP-2WG	10.230.207.207	00:0B:86:C3:C3:60	10/1/2009 4:17 PM

1-20 ▾ of 174 APs/Devices Page 1 ▾ of 9 > >|

Select All - Unselect All

View Ignored Devices

Group: AlcatelGear (SSID: -)

Folder: Top

● Monitor Only + Firmware Upgrades

○ Manage Read/Write

4. Select (check) the box next to any AP you want to provision.
5. Rename all new APs. Type in the new device name in the **Device** column.
6. Scroll to the bottom of the page and put APs in the appropriate OV3600 group and folder. Set the devices to **Manage Read/Write** mode.
7. Click **Add**. Wait approximately five to 10 minutes. You can observe that the APs have been renamed not only in OV3600 but also on the Alcatel-Lucent AP Group and Alcatel-Lucent switch with the `show ap database aosw` command.
8. To set the appropriate Alcatel-Lucent AP Group, select the **AP/Devices** or **Groups** page and locate your APs.
9. Click **Modify Devices**.
10. Select the APs you want to re-group.
11. In the field that states **Move to Alcatel-Lucent AP Group** below the list of the devices, select the appropriate group and click **Move**.

NOTE

If the list of Alcatel-Lucent AP Groups are not there, ensure you either create these AP groups manually on the **Device Setup >** Alcatel-Lucent **Configuration** page, wherein you merely need the device names and not the settings, or import the configuration from one of your switches to learn the groups.

12. Wait another 5 to 10 minutes to observe the changes on OV3600. The changes should be observable within one or two minutes on the switch.

Using General OV3600Device Groups and Folders

OV3600 only allows any given AP to belong to one OV3600 device group at a time. Supporting one AP in two or more OV3600 device groups would create at least two possible issues including the following:

- Data collection for such an AP device would have two or more sources and two or more related processes.
- A multi-group AP would be counted several times and that would change the value calculations for OV3600 graphs.

As a result, some users may wish to evaluate how they deploy the group or folder for any given AP.

NOTE

Alcatel-Lucent APs can also belong to Alcatel-Lucent AP Groups, but each AP is still limited to one general OV3600 device group.

You can organize and manage any group of APs by type and by location. Use groups and folders with either of the following two approaches:

- Organize AP device groups by device type, and device folders by device location.

  In this setup, similar devices are in the same device group, and operate from a similar configuration or template. Once this is established, create and maintain device folders by location.
- Organize AP device groups by location, and device folders by type.

  In this setup, you can organize all devices according to location in the device groups, but for viewing, you organize the device hierarchy by folders and type.

Be aware of the following additional factors:

- Configuration audits are done at the OV3600 group level.
- OV3600 folders support multiple sublevels.

Therefore, unless there is a compelling reason to use the folders-by-device-type approach, Alcatel-Lucent generally recommends the first approach where you use groups for AP type and folders strictly for AP location.

Visibility in Alcatel-Lucent Configuration

Visibility Overview

Alcatel-Lucent Configuration supports device configuration and user information in the following ways;

- User roles
- AP/Device access level
- Folders (in *global* configuration)

Additional factors for visibility are as follows:

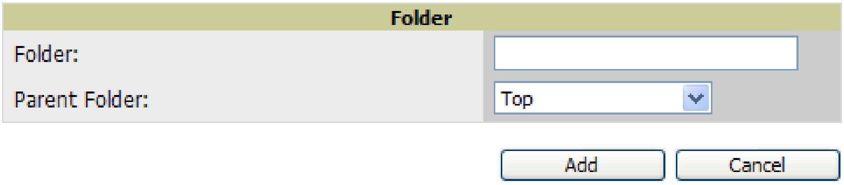
- Administrative and Management users in OV3600 can view the **Alcatel-Lucent Configuration** page and the **APs/Devices > Manage** pages.
  - Administrative users are enabled to view all configurations.
  - Management users have access to all profiles and Alcatel-Lucent AP groups for their respective folders.
- The **Device Setup > Alcatel-Lucent Configuration** page has a limit to folder drop-down options for customers that manage different accounts and different types of users.
- Alcatel-Lucent Configuration entails specific user role and security profiles that define some components of visibility, as follows:
  - "Security > User Roles" on page 45
  - "Security > Policies" on page 51
- OV3600 continues to support the standard operation of folders, users, and user roles as described in the *OmniVista 3600 Air Manager 7.6 User Guide*.

Defining Visibility for Alcatel-Lucent Configuration

Perform these steps to define or adjust visibility for users to manage and support Alcatel-Lucent Configuration:

1. As required, create a new OV3600 device folder with management access.
   a. Navigate to the **APs/Device > List** page, scroll to the bottom of the page. (An alternate page supporting new folders is **Users > Connected** page.)
   b. Click the **Add New Folder** link. The **Folder** detail page appears, as illustrated in Figure 21:

Figure 21 ***APs/Devices > Add New Folder > Folders*** *Page Illustration*



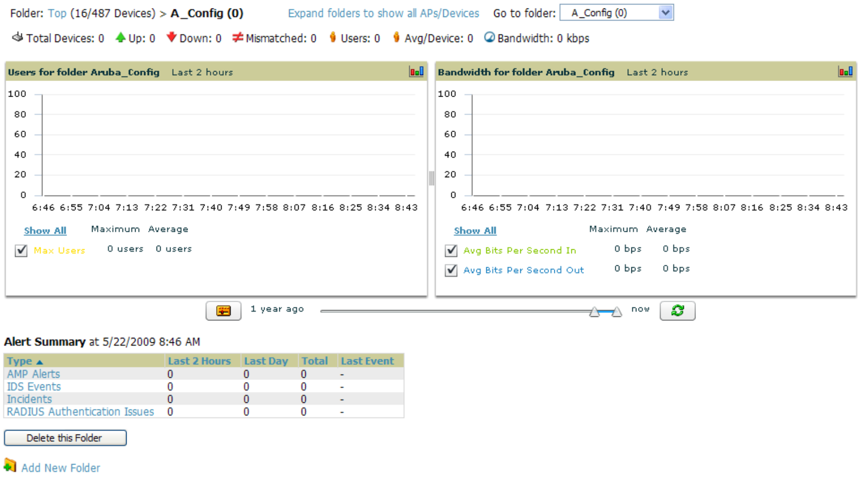
Folder

Folder:

Parent Folder: Top

c. Click **Add**. The **APs/Devices** > **List** page reappears. You can view your new folder by selecting it from the **Go to folder** drop-down list at the top right of this page. Figure 22 illustrates an unpopulated device page for an example folder.

Figure 22 ***APs/Devices > List*** *Page With No Devices*



Folder: Top (16/487 Devices) > **A_Config (0)** Expand folders to show all APs/Devices Go to folder: A_Config (0)

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

Users for folder Aruba_Config Last 2 hours

Show All	Maximum	Average
☑ Max Users	0 users	0 users

Bandwidth for folder Aruba_Config Last 2 hours

Show All	Maximum	Average
☑ Avg Bits Per Second In	0 bps	0 bps
☑ Avg Bits Per Second Out	0 bps	0 bps

Alert Summary at 5/22/2009 8:46 AM

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

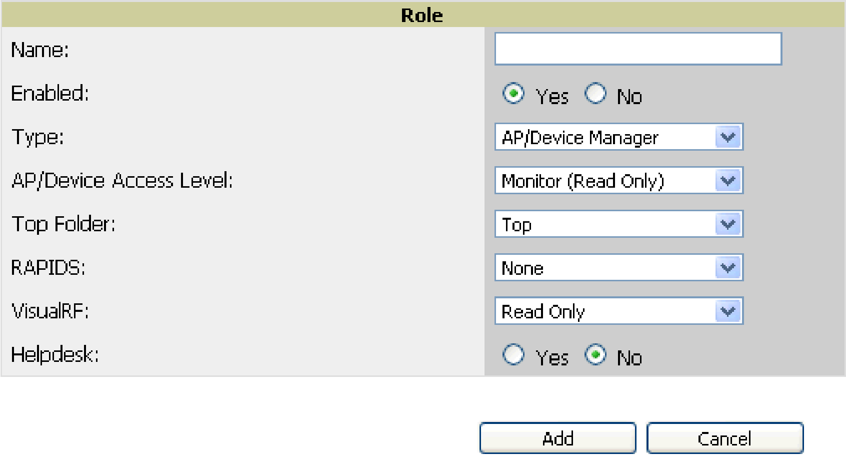
2. Add Alcatel-Lucent switch devices to that folder as required. Use the **Device Setup** > **Add** page following instructions available in the *OmniVista 3600 Air Manager 7.6 User Guide*.

3. As required, create or edit a user role that is to have rights and manage privileges required to support their function in Alcatel-Lucent Configuration.

   a. At least one user must have administrative privileges, but several additional users may be required with less rights and visibility to support Alcatel-Lucent Configuration without access to the most sensitive information, such as SSIDs or other security related data.

   b. Navigate to the **OV3600 Setup** > **Roles** page, and click **Add New Role** to create a new role with appropriate rights, or click the **pencil** (manage) icon next to an existing role to adjust rights as required. The Role page appears, illustrated in Figure 23.

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



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

c. As per standard OV3600 configuration, complete the settings on this page. The most important fields with regard to Alcatel-Lucent Configuration, device visibility and user rights are as follows:

- **Type**—Specify the type of user. Important consideration should be given to whether the user is an administrative user with universal access, or an AP/Device manager to specialize in device administration, or additional users with differing rights and access.
- **AP/Device Access Level**—Define the access level that this user is to have in support of Alcatel-Lucent switches, devices, and general Alcatel-Lucent Configuration operations.
- **Top Folder**—Specify the folder created earlier in this procedure, or specify the Top folder for an administrative user.

d. Click **Add** to complete the role creation, or click **Save** to retain changes to an existing role. The **OV3600 Setup** page now displays the new or revised role.

4. As required, add or edit one or more users to manage and support Alcatel-Lucent Configuration. This step creates or edits users to have rights appropriate to Alcatel-Lucent Configuration. This user inherits visibility to Alcatel-Lucent switches and Alcatel-Lucent Configuration data based on the role and device folder created earlier in this procedure.

   a. Navigate to the **OV3600 Setup > User** page.

   b. Click **Add New User**, or click the **pencil** (manage) icon next to an existing user to edit that user.

   c. Select the user role created with the prior step, and complete the remainder of this page as per standard OV3600 configuration. Refer to the *OmniVista 3600 Air Manager 7.6 User Guide* as required.

5. Observe visibility created or edited with this procedure.

   The user, role, and device folder created with this procedure are now available to configure, manage, and support Alcatel-Lucent Configuration and associated devices according to the visibility defined in this procedure. Any component of this setup can be adjusted or revised by referring to the steps and OV3600 pages in this procedure.

6. Add or discover devices for the device folder defined during step 1 of this procedure. Information about devices is available in the *OmniVista 3600 Air Manager 7.6 User Guide*.

7. Continue to other elements of Alcatel-Lucent Configuration described in the Reference section of this document.

Introduction

This section describes the pages, field-level settings, and interdependencies of Alcatel-Lucent Configuration profiles. Additional information is available as follows:

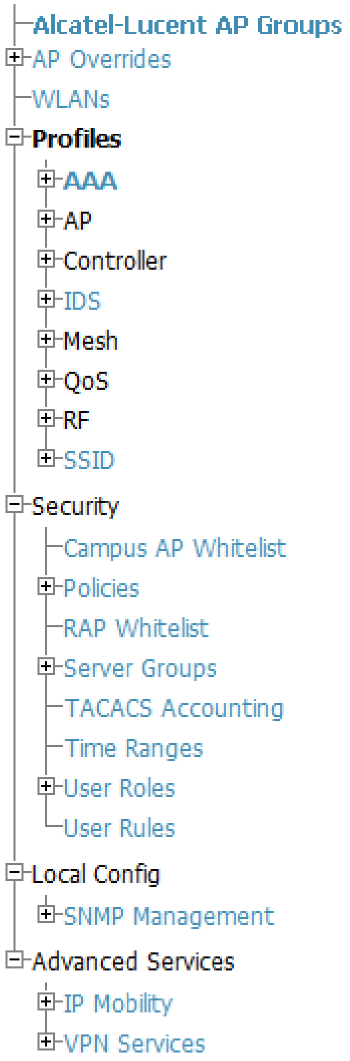
- Alcatel-Lucent Configuration components are summarized in "Additional Concepts and Components" on page 10.
- For procedures that use several of these components, refer to earlier chapters in this document.
- For architectural information about AOS-W, refer to the *Alcatel-Lucent AOS-W User Guide*.

NOTE

The default values of profile parameters or functions may differ slightly between AOS-W releases.

Access all pages and field descriptions in this appendix from the **Device Setup > Alcatel-Lucent Configuration** page, illustrated in Figure 24. The one exception is the additional **Groups** > **Alcatel-Lucent Config** page that you access from the standard OV3600 navigation menu.

Figure 24 *Alcatel-Lucent Configuration Components*



This section describes Alcatel-Lucent Configuration components with the following organization and topics:

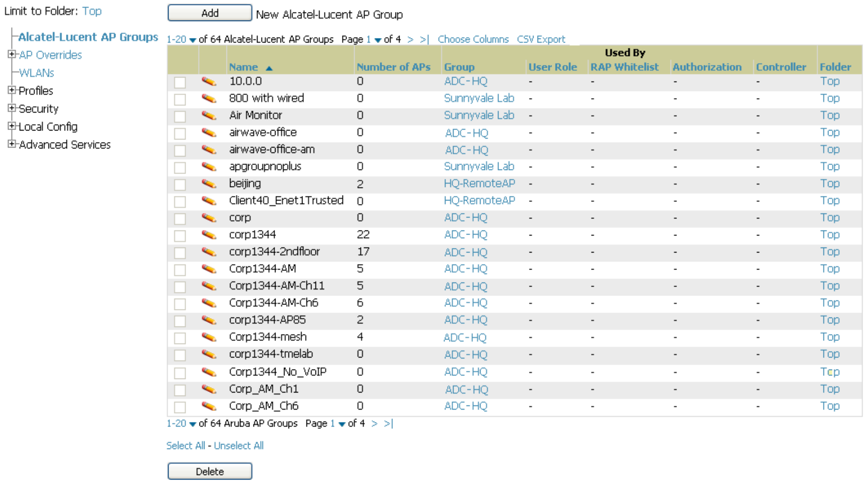
- "Alcatel-Lucent AP Groups" on page 30
- "AP Overrides" on page 34
- "WLANs" on page 38
- "Profiles" on page 43
- "Security" on page 44
- "Local Config of SNMP Management" on page 66
- "Advanced Services" on page 68
- "Groups > Alcatel-Lucent Config Page" on page 80

Alcatel-Lucent AP Groups

Alcatel-Lucent AP Groups appear at the top of the Alcatel-Lucent Configuration navigation pane. This section describes the configuration pages and fields of Alcatel-Lucent AP Groups.

About Alcatel-Lucent AP Groups

The **Alcatel-Lucent AP Groups** page displays all configured Alcatel-Lucent AP Groups and enables you to add or edit Alcatel-Lucent AP Groups. For additional information about using this page, refer to "Alcatel-Lucent AP Groups Procedures and Guidelines" on page 19.



				Used By					
		Name ▲	Number of APs	Group	User Role	RAP Whitelist	Authorization	Controller	Folder
□	✎	10.0.0	0	ADC-HQ	-	-	-	-	Top
□	✎	800 with wired	0	Sunnyvale Lab	-	-	-	-	Top
□	✎	Air Monitor	0	Sunnyvale Lab	-	-	-	-	Top
□	✎	airwave-office	0	ADC-HQ	-	-	-	-	Top
□	✎	airwave-office-am	0	ADC-HQ	-	-	-	-	Top
□	✎	apgroupnoplus	0	Sunnyvale Lab	-	-	-	-	Top
□	✎	beijing	2	HQ-RemoteAP	-	-	-	-	Top
□	✎	Client40_Enet1Trusted	0	HQ-RemoteAP	-	-	-	-	Top
□	✎	corp	0	ADC-HQ	-	-	-	-	Top
□	✎	corp1344	22	ADC-HQ	-	-	-	-	Top
□	✎	corp1344-2ndfloor	17	ADC-HQ	-	-	-	-	Top
□	✎	Corp1344-AM	5	ADC-HQ	-	-	-	-	Top
□	✎	Corp1344-AM-Ch11	5	ADC-HQ	-	-	-	-	Top
□	✎	Corp1344-AM-Ch6	6	ADC-HQ	-	-	-	-	Top
□	✎	corp1344-AP85	2	ADC-HQ	-	-	-	-	Top
□	✎	Corp1344-mesh	4	ADC-HQ	-	-	-	-	Top
□	✎	corp1344-tmelab	0	ADC-HQ	-	-	-	-	Top
□	✎	Corp1344_No_VoIP	0	ADC-HQ	-	-	-	-	Top
□	✎	Corp_AM_Ch1	0	ADC-HQ	-	-	-	-	Top
□	✎	Corp_AM_Ch6	0	ADC-HQ	-	-	-	-	Top

1-20 ▾ of 64 Aruba AP Groups Page 1 ▾ of 4 > >|
Select All - Unselect All
Delete

The **Alcatel-Lucent AP Groups** page displays the following information for every group currently configured:

Table 1: *Alcatel-Lucent Configuration > Alcatel-Lucent AP Groups Page*

Column	Description
Name	Displays the name of the Alcatel-Lucent AP Group. Select the pencil icon next to any group to edit.
(Used by) Group	Displays the Alcatel-Lucent device groups that define this Alcatel-Lucent AP Group. Select the name of any group in this column to display the detailed **Groups > Alcatel-Lucent Config page.** The device groups in this column receive the profile configurations from the associated Alcatel-Lucent AP Group. Any Alcatel-Lucent AP Group profiles can define device groups.

Column	Description
(Used by) Number of AP	Displays the number of APs in this Alcatel-Lucent AP Group. A detailed list of each AP by name can be displayed by navigating to the **Groups > List** page and selecting that group.
(Used By) User Role	Displays the user role or roles that support the respective Alcatel-Lucent AP Group, when defined.
Folder	Displays the folder that is associated with this Alcatel-Lucent AP Group, when defined. A **Top** viewable folder for the role is able to view all devices and groups contained by the top folder. The top folder and its subfolders must contain all the devices in any groups it can view. Clicking any folder name takes you to the **APs/Devices > List** page for folder inventory and configuration.

Select **Add** to create a new Alcatel-Lucent AP Group, or click the pencil icon next to an existing Alcatel-Lucent AP Group to edit that group. The **Add/Edit Alcatel-Lucent AP Group** page contains the following fields, describes in Table 2.

Table 2: *Alcatel-Lucent Configuration > Alcatel-Lucent AP Groups Details, Settings and Default Values*

Field	Default	Description
General Settings		
Folder	Top	Displays the folder with which the AP Group is associated. The drop-down menu displays all folders available for association with the AP Group. Folders provide a way to organize the visibility of device parameters that is separate from the configuration groups of devices. Using folders, you can view basic statistics about device, and define which users have visibility to which device parameters.
Name	Default	Enter the name of the AP Group.
WLANs		
Add a new WLAN		Select this link to create a new WLAN to support Alcatel-Lucent Configuration. Once created, that new WLAN will appear with others on this page.
Show only selected/Show All		To set the WLANs that appear on this page, select (check) the desired WLANs, then click **Show Only Selected**.
WLANs	None selecte-d	Displays the WLANs currently present in Alcatel-Lucent Configuration with checkboxes. You may select as few or as many WLANS as desired for which this AP Group is active. To configure additional WLANs that appear in this section, click **Add a new WLAN** or navigate to the **WLANs** section in the navigation pane on the left.
Referenced Profiles		
802.11a Radio Profile	5_am	Defines AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Select the **pencil** icon next to this field to edit or create additional profile settings in the **RF > 802.11a/g Radio** page of Alcatel-Lucent Configuration.
802.11g Radio Profile	2.4_am	Defines AP radio settings for the 2.4 GHz frequency band, including the

Field	Default	Description
		Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Each 802.11a and 802.11b radio profile includes a reference to an Adaptive Radio Management (ARM) profile. If you would like the ARM feature to select dynamically the best channel and transmission power for the radio, verify that the 802.11a/802.11g radio profile references an active and enabled ARM profile. If you want to manually select a channel for each AP group, create separate 802.11a and 802.11g profiles for each AP group and assign a different transmission channel for each profile. The drop-down menu displays these options: ● **default** ● **nchannel too high** ● **nchannel too low** Select the **pencil** icon next to this field to edit profile settings in the **RF > 802.11a/g Radio** page.
RF Optimization Profile	default	Enables or disables load balancing based on a user-defined number of clients or degree of AP utilization on an AP. Use this profile to detect coverage holes, radio interference and STA association failures and configure Received signal strength indication (RSSI) metrics. Select the pencil icon next to this field to display the **Profiles > RF** section and edit these settings as desired.
Event Thresholds Profile	default	Defines error event conditions, based on a customizable percentage of low-speed frames, non-unicast frames, or fragmented, retry or error frames. The drop-down menu displays these options: ● **default** ● all additional RF profiles currently configured in Alcatel-Lucent Configuration Select the pencil icon next to this field to display the **Profiles > RF > Events Threshold** section and edit these settings as desired.
Wired AP Profile	default	Controls whether 802.11 frames are tunneled to the switch using Generic Routing Encapsulation (GRE) tunnels, bridged into the local Ethernet LAN (for remote APs), or are configured for combination of the two (split-mode). This profile also configures the switching mode characteristics for the port, and sets the port as either trusted or untrusted. Select the pencil icon next to this field to display the **Profiles > AP > Wired** page and adjust these settings as desired.
Ethernet Interface 0 Link Profile	default	Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 0. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link. Select the pencil icon next to this field to display the **Profiles > AP > Ethernet Link** details page and adjust these settings as desired.
Ethernet Interface 1 Link Profile	default	Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 1. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link. Select the pencil icon next to this field to display the **Profiles > AP > Ethernet Link** details page and adjust these settings as desired.
AP System Profile	default	Defines administrative options for the switch, including the IP addresses of the local, backup, and master switches, Real-Time Locating Systems (RTLS) server values, and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps.

Field	Default	Description
		This field is a drop-down menu with the following options: ● **Non-integer RTLS Server Station Message Frequency** ● **Too-high RTLS Server Port** ● **Too-low AeroScout RTLS Server Port** ● **Too-low RTLS Server Port** Select the **pencil** icon next to this field to display the **Profiles > AP > System** details page and adjust these settings as desired.
Regulatory Domain Profile	default	Defines an AP's country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios. Select the pencil icon next to this field to display the **Profiles > AP > Regulatory Domain** page and adjust these settings as desired.
SNMP Profile	default	Selects the SNMP profile to associate with this AP group. The drop-down menu lists all SNMP profiles currently enabled in OV3600. Select the pencil icon next to this field to display the **Profiles > AP > SNMP** page and adjust these settings as desired.
VoIP Call Admission Control Profile	default	Voice Call Admission Control limits the number of active voice calls per AP by load-balancing or ignoring excess call requests. This profile enables active load balancing and call admission controls, and sets limits for the numbers of simultaneous Session Initiated Protocol (SIP), SpectraLink Voice Priority (SVP), Cisco Skinny Client Control Protocol (SCCP), Vocera or New Office Environment (NOE) calls that can be handled by a single radio. Select the pencil icon next to this field to display the **Profiles > AP > Regulatory Domain** page and adjust these settings as desired.
802.11g Traffic Management Profile	default	Specify the minimum percentage of available bandwidth to be allocated to a specific SSID when there is congestion on the wireless network, and sets the interval between bandwidth usage reports. This setting pertains specifically to 802.11g.
802.11a Traffic Management Profile	default	Specify the minimum percentage of available bandwidth to be allocated to a specific SSID when there is congestion on the wireless network, and sets the interval between bandwidth usage reports. This setting pertains specifically to 802.11a.
IDS Profile	default	Selects the IDS profile to be associated with the new AP Group. The drop-down menu contains these options: ● **ids-disabled** ● **ids-high-setting** ● **ids -low-setting** ● **ids-medium-setting** The IDS profiles configure the AP's Intrusion Detection System features, which detect and disable rogue APs and other devices that can potentially disrupt network operations. An AP is considered to be a rogue AP if it is both unauthorized and plugged into the wired side of the network. An AP is considered to be an interfering AP if it is seen in the RF environment but is not connected to the wired network. Select the pencil icon next to this field to display the **Profiles > IDS** page and adjust these settings as desired.
Mesh Radio Profile	default	Determines many of the settings used by mesh nodes to establish mesh links and the path to the mesh portal, including the maximum number of children a mesh node can accept, and transmit rates for the 802.11a and 802.11g radios.

Field	Default	Description
Mesh Cluster Profiles		
Add New Mesh Cluster Profile		Select to display a new **Mesh Cluster Profile** section to this page. This section has two fields, as follows: ● **Mesh Cluster Profile**–Drop-down menu displays all supported profiles. Select one from the menu. ● **Priority (1-16)**–Type in the priority number for this profile. The priority may be any integer between 1 and 16. Complete these fields, click the **Add** button, and the profile displays as an option in the **Mesh Cluster Profile** section, which may be selected for the AP Group to be added or edited.

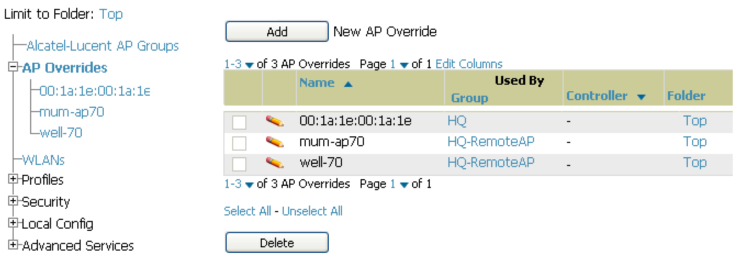
Select **Add** to complete the creation or click **Save** to complete the editing of the Alcatel-Lucent AP Group. This group now appears in the navigation pane of the Alcatel-Lucent Configuration page.

AP Overrides

The **AP Overrides** component of Alcatel-Lucent Configuration allows you to define device-specific settings for an AP device without having to remove that device from an existing Alcatel-Lucent AP Group or create a new Alcatel-Lucent AP Group specifically for that device. The **AP Overrides** page is for custom AP devices that otherwise comply with most settings in the Alcatel-Lucent AP Group in which it is managed.

The **AP Overrides** page displays all AP overrides that are currently configured. These overrides also appear in the navigation pane at left. The name of any override matches the AP device name.

Figure 25 *AP Overrides Page Illustration*



		Name ▲	Used By Group	Controller ▼	Folder
□	✎	00:1a:1e:00:1a:1e	HQ	-	Top
□	✎	mum-ap70	HQ-RemoteAP	-	Top
□	✎	well-70	HQ-RemoteAP	-	Top

Table 3 describes the fields on this page.

Table 3: *AP Overrides Fields and Descriptions*

Field	Description
Name	Displays the name of the AP Overrides profile. This name matches the name of the specific AP device that it defines.
Used By (Group)	Displays the name of and link to the Alcatel-Lucent AP Group in which this AP Override applies. Additional details about the Alcatel-Lucent AP Group appear on the **Groups > Alcatel-Lucent Config** page when you click the name of the group.
Folder	Displays the folder associated with the AP Overrides profile. The folder establishes the visibility of this profile to users.

Select **Add** on the **AP Overrides** page to create a new AP Override, or click the pencil icon next to an existing override to edit that override. Table 4 describes the fields on the **AP Overrides** > **Add/Edit Details** page.

Table 4: *AP Overrides Add or Edit Page Fields*

Field	Default	Description
Name	Blank	Name of the AP Override. Use the name of the AP device to which it applies.
Folder	Top	Displays the folder with which the WLAN is associated. The drop-down menu displays all folders available for association with the WLAN.
WLANs		
WLANs		This section lists the WLANs currently defined in Alcatel-Lucent Configuration by default. You can display selected WLANs or all WLANs. Select one or more WLANs for which AP Override is to apply.
Excluded WLANs		
Excluded WLANs		This section displays WLANs currently defined in Alcatel-Lucent Configuration by default. This section can display selected WLANs or all WLANs. Use this section to specify which WLANs are *not* to support **AP Override**.
Referenced Profiles		
802.11a Radio Profile	5_am	Defines AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Select the **pencil** icon next to this field to edit or create additional profile settings in the **RF > 802.11a/g Radio** page.
802.11g Radio Profile	2.4_am	Defines AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Each 802.11a and 802.11b radio profile includes a reference to an Adaptive Radio Management (ARM) profile. If you would like the ARM feature to select dynamically the best channel and transmission power for the radio, verify that the 802.11a/802.11g radio profile references an active and enabled ARM profile. If you want to manually select a channel for each AP group, create separate 802.11a and 802.11g profiles for each AP group and assign a different transmission channel for each profile. The drop-down menu displays these options: ● **default** ● **nchannel too high** ● **nchannel too low** Select the **pencil** icon next to this field to edit or create additional profile settings in the **RF > 802.11a/g Radio** page of **Alcatel-Lucent Configuration.**
RF Optimization Profile	default	Enables or disables load balancing based on a user-defined number of clients or degree of AP utilization on an AP. Use this profile to detect coverage holes, radio interference and STA association failures and configure Received signal strength indication (RSSI) metrics. Select the pencil icon next to this field to display the **Profiles > RF** section and edit these settings as desired.

Field	Default	Description
Event Thresholds Profile	default	Defines error event conditions, based on a customizable percentage of low-speed frames, non-unicast frames, or fragmented, retry or error frames. The drop-down menu displays these options: - **default** - all additional RF profiles currently configured in Alcatel-Lucent Configuration Select the pencil icon next to this field to display the **Profiles > RF > Events Threshold** section and edit these settings as desired.
Wired AP Profile	default	Controls whether 802.11 frames are tunneled to the switch using Generic Routing Encapsulation (GRE) tunnels, bridged into the local Ethernet LAN (for remote APs), or a configured for combination of the two (split-mode). This profile also configures the switching mode characteristics for the port, and sets the port as either trusted or untrusted. Select the pencil icon next to this field to display the **Profiles > AP > Wired** page and adjust these settings as desired.
Ethernet Interface 0 Link Profile	default	Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 0. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link. Select the pencil icon next to this field to display the **Profiles > AP > Ethernet Link** details page and adjust these settings as desired.
Ethernet Interface 1 Link Profile	default	Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 1. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link. Select the pencil icon next to this field to display the **Profiles > AP > Ethernet Link** details page and adjust these settings as desired.
AP System Profile	default	Defines administrative options for the switch, including the IP addresses of the local, backup, and master switches, Real-time Locating Systems (RTLS) server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps. This field is a drop-down menu with the following options: - Non-integer RTLS Server Station Message Frequency - Too-high RTLS Server Port - Too-low AeroScout RTLS Server Port - Too-low RTLS Server Port Select the pencil icon next to this field to display the **Profiles > AP > System** details page and adjust these settings as desired.
Regulatory Domain Profile	default	Defines an AP's country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios. Select the pencil icon next to this field to display the **Profiles > AP > Regulatory Domain** page and adjust these settings as desired.
SNMP Profile	default	Selects the SNMP profile to associate with this AP group. The drop-down menu lists all SNMP profiles currently enabled in OV3600. Select the pencil icon next to this field to display the **Profiles > AP > SNMP** page and adjust these settings as desired.
VoIP Call Admission Control Profile	default	Voice Call Admission Control limits the number of active voice calls per AP by load-balancing or ignoring excess call requests. This profile enables active load balancing and call admission controls, and sets limits

Field	Default	Description
		for the numbers of simultaneous Session Initiated Protocol (SIP), SpectraLink Voice Priority (SVP), Cisco Skinny Client Control Protocol (SCCP), Vocera or New Office Environment (NOE) calls that can be handled by a single radio. Select the pencil icon next to this field to display the **Profiles > AP > Regulatory Domain** page and adjust these settings as desired.
802.11g Traffic Management Profile	default	Specify the minimum percentage of available bandwidth to be allocated to a specific SSID when there is congestion on the wireless network, and sets the interval between bandwidth usage reports. This setting pertains specifically to 802.11g.
802.11a Traffic Management Profile	default	Specify the minimum percentage of available bandwidth to be allocated to a specific SSID when there is congestion on the wireless network, and sets the interval between bandwidth usage reports. This setting pertains specifically to 802.11a.
IDS Profile	default	Selects the IDS profile to be associated with the new AP Group. The drop-down menu contains these options: ● **ids-disabled** ● **ids-high-setting** ● **ids -low-setting (the default)** ● **ids-medium-setting** The IDS profiles configure the AP's Intrusion Detection System features, which detect and disable rogue APs and other devices that can potentially disrupt network operations. An AP is considered to be a rogue AP if it is both unauthorized and plugged into the wired side of the network. An AP is considered to be an interfering AP if it is seen in the RF environment but is not connected to the wired network. Select the pencil icon next to this field to display the **Profiles > IDS** page and adjust these settings as desired.
Mesh Radio Profile	default	Determines many of the settings used by mesh nodes to establish mesh links and the path to the mesh portal, including the maximum number of children a mesh node can accept, and transmit rates for the 802.11a and 802.11g radios.
AP Authorization Profile		Selects the AP Authorization profile to be associated with the new AP Group. This profile requires a Remote Access Points license.
AP Provisioning Profile		Selects the AP Provisioning profile to be associated with the new AP Group.
Ethernet Interface 0-4 Port Configuration		Selects the Ethernet port configuration to be associated with the new AP Group. This profile allows you to configure all AP wired port profiles and their status. The drop-down menu contains these options: ● default ● NoWiredAuthPort ● shutdown
Mesh Cluster Profiles		
Add New Mesh Cluster Profile	Hidden by default until the **Add** button	Clicking this **Add** button displays a new **Mesh Cluster Profile** field. The drop-down menu displays all supported profiles. Select one from the menu. Complete this field, click the **Add** button, and the profile displays as an

Field	Default	Description
	is clicked	option in the **Mesh Cluster Profile** section, which may be selected for the AP Group to be added or edited.
Excluded Mesh Cluster Profiles		
Excluded Mesh Cluster Profiles		If required, select one or more Mesh Cluster profiles from this field. This field can display all Mesh Cluster profiles or can display only selected Mesh Cluster profiles.

Select **Add** to complete the creation of the new AP Overrides profile, or click **Save** to preserve changes to an existing AP Overrides profile. The **AP Overrides** page and the Alcatel-Lucent Configuration navigation pane display the name of the AP Overrides profile.

WLANs

Overview of WLANs Configuration

You have a wide variety of options for authentication, encryption, access management, and user rights when you configure a WLAN. However, you must configure the following basic elements:

- An SSID that uniquely identifies the WLAN
- Layer-2 authentication to protect against unauthorized access to the WLAN
- Layer-2 encryption to ensure the privacy and confidentiality of the data transmitted to and from the network
- A user role and virtual local area network (VLAN) for the authenticated client

  Refer to the *OmniVista 3600 Air Manager 7.6 User Guide* for additional information.

Use the following guidelines when configuring and using WLANs in Alcatel-Lucent Configuration:

- The **Device Setup** > **Alcatel-Lucent Configuration** navigation pane displays custom-configured WLANs and Alcatel-Lucent AP Groups. All other components of the navigation pane are standard across all deployments of Alcatel-Lucent Configuration.
- You define or modify WLANs on the **Device Setup** > **Alcatel-Lucent Configuration** page. Select **WLANs** from the navigation pane.
- You can create or edit any profile in an WLAN as you define or modify that WLAN. If you digress to profile setup from a different page, OV3600 returns you to the **WLAN** setup page once you are done with profile setup.

WLANs

The **WLANs** page displays all configured WLANs in Alcatel-Lucent Configuration and enables you to add or edit WLANs. For additional information about using this page, refer to "General WLAN Guidelines" on page 20.

The **Alcatel-Lucent Configuration** > **WLANs** page contains additional information as described in Table 5:

Table 5: *Alcatel-Lucent Configuration > WLANs Page Fields and Descriptions*

Field	Description
Name	Lists the name of the WLAN.
SSID	Lists the SSID currently defined for the WLAN.

Field	Description
Alcatel-Lucent AP Group	Lists the Alcatel-Lucent AP Group or Groups that use the associated WLAN.
AP Override	Lists any AP Override configurations for specific APs on the WLAN and in the respective Alcatel-Lucent AP Groups.
Traffic Management	Lists Traffic Management profiles that are currently configured and deployed on the WLAN.
Folder	Lists the folder for the WLAN.

You can create new WLANs from this page by clicking the **Add** button. You can edit an existing WLAN by clicking the pencil icon for that WLAN.

You have two pages by which to create or edit WLANs: the **Basic** page and the **Advanced** page. The remainder of this section describes these two pages.

WLANs > Basic

From the **Alcatel-Lucent Configuration** > **WLANs** page, click **Add** to create a new WLAN, or click the pencil icon to edit an existing WLAN, then click **Basic**. This page provides a streamlined way to create or edit a WLAN. Table 6 describes the fields for this page.

Table 6: *WLANs > Basic Page Fields and Descriptions*

Field	Default	Description
Name	Blank	Enter the name of the WLAN.
Folder	Top	Displays the folder with which the WLAN is associated. The drop-down menu displays all folders available for association with the WLAN.
SSID		Select the SSID profile that defines encryption, EDCA or high-throughput SSID parameters. Access these SSID profiles by clicking **Profiles > SSID** in the navigation pane at left.
Radio Type		Define whether the supported radio type on the WLAN is 802.11a, 802.11g, or all.
Enable 802.11n	Yes	Define whether the WLAN is to support 802.11n.
VLAN	1	Select the VLAN ID number to be supported on this WLAN.
Intended Use	Internal	Define whether this WLAN is **Internal** to the enterprise or to support **Guest** users.
Encryption	opensystem	Select one or more encryption types, as desired, to be supported by this WLAN.
Use Captive Portal	No	Select whether this WLAN will use captive portal authentication. Captive portal authentication directs clients to a special web page that typically requires them to enter a username and password before accessing the network.
Authenticated User Role	logon	For the captive portal authentication profile, you specify the previously-created auth-guest user role as the default user role for authenticated captive portal clients and the authentication server group (Internal). Refer to "Security > User Roles" on page 45.

Select **Add** to create the WLAN, or click **Save** to finish reconfiguring an existing WLAN. The WLAN appears on the **WLANs** page in the Alcatel-Lucent Configuration navigation pane.

The alternate way to create or edit WLANs is from the **Advanced** page. Refer to "WLANs > Advanced" on page 40.

WLANs > Advanced

From the **Alcatel-Lucent Configuration** > **WLANs** page, click **Add** to create a new WLAN, or click the pencil icon to edit an existing WLAN, then click **Advanced**. The **Advanced** page allows you to configure many more sophisticated settings when creating or editing WLANs. Table 7 describes the fields for this page.

Table 7: *WLANs > Advanced Page Fields*

Field	Default	Description
General Settings		
Folder	Top	Displays the folder with which the WLAN is associated. The drop-down menu displays all folders available for association with the WLAN.
Name	Blank	Name of the WLAN.
Referenced Profiles		
SSID Profile		Select the SSID profile that defines encryption, EDCA or high-throughput SSID parameters. Access these SSID profiles by clicking **Profiles > SSID** in the navigation pane at left.
AAA Profile		Select the AAA profile that defines RADIUS, TACACS+, or other AAA server configurations for this WLAN. Access these SSID profiles by clicking **Profiles > AAA** in the navigation pane at left
802.11k Profile		Manages settings for the 802.11k protocol. The 802.11k protocol allows APs and clients to dynamically query their radio environment and take appropriate connection actions. For example, in a 802.11k network if the AP with the strongest signal reaches its CAC (Call Admission Control) limits for voice calls, then on-hook voice clients may connect to an under utilized AP with a weaker signal. You can configure the following options in 802.11k profile: ● Enable or disable 802.11K support on the AP ● Forceful disassociation of on-hook voice clients ● Measurement mode for beacon reports. For more details, see the Configuring 802.11k Protocol topic in the *Alcatel-Lucent AOS-W User Guide*.
WMM Traffic Management Profile		Manages settings for the bandwidth management profile for Wi-Fi Multimedia (WMM).
Other Settings		
Virtual AP Enable	Yes	Enable this setting to allow virtual AP configurations to be deployed on this WLAN. This profile defines your WLAN by enabling or disabling the bandsteering, fast roaming, and DoS prevention features. It defines radio band, forwarding mode and blacklisting parameters, and includes references an AAA Profile, an EDCA Parameters AP Profile and a High-throughput SSID profile

Field	Default	Description
Allowed Band	All	Select whether this WLAN is to support 802.11a, 802.11g, or both.
VLAN		Enter the VLAN or range of VLANs to be supported with this WLAN.
Forward Mode	Tunnel	Define whether this WLAN is to support tunnel, bridge, or split-mode IP forwarding.
Deny Time Range	None	Define the time range restrictions for the roles in this WLAN, if any.
Mobile IP	Yes	Enable or disable mobile IP functions. This setting specifies whether the switch is the home agent for a client. When enabled, this setting detects when a mobile client has moved to a foreign network and determines the home agent for a roaming client.
HA Discovery on Association	No	Enable or disable HA discovery on Association. In normal circumstances a switch performs an HA discovery only when it is aware of the client's IP address which it learns through the ARP or any L3 packet from the client. This limitation of learning the client's IP and then performing the HA discovery is not effective when the client performs an inter switch move silently (does not send any data packet when in power save mode). This behavior is commonly seen with various handheld devices, Wi-Fi phones, etc. This delays HA discovery and eventually resulting in loss of downstream traffic if any meant for the mobile client. With HA discovery on association, a switch can perform a HA discovery as soon as the client is associated. By default, this feature is disabled. You can enable this on virtual APs with devices in power-save mode and requiring mobility. This option will also poll for all potential HAs.
DoS Prevention	No	Enable or disable DoS prevention functions, as defined in virtual AP profiles.
Station Blacklisting	Yes	Enable or disable DoS prevention functions, as defined in virtual AP profiles. The blacklisting option can be used to prevent access to clients that are attempting to breach the security. When a client is blacklisted in the Alcatel-Lucent system, the client is not allowed to associate with any AP in the network for a specified amount of time. If a client is connected to the network when it is blacklisted, a de-authentication message is sent to force the client to disconnect. While blacklisted, the client cannot associate with another SSID in the network.
Blacklist Time	3600	If station blacklisting is enabled, specify the time in seconds for which blacklisting is enabled. When a client is blacklisted in the Alcatel-Lucent system, the client is not allowed to associate with any AP in the network for a specified amount of time.
Authentication Failure Blacklist Time	3600	You can configure a maximum authentication failure threshold in seconds for each of the following authentication methods: ● 802.1x ● MAC ● Captive portal ● VPN When a client exceeds the configured threshold for one of the above methods, the client is automatically blacklisted by the switch, an event is logged, and an SNMP trap is sent. By default, the maximum authentication failure threshold is set to 0 for the above authentication methods, which means that there is no limit to the number of times a client can attempt to authenticate. With 802.1x authentication, you can also configure blacklisting of clients

Field	Default	Description
		who fail machine authentication. **NOTE:** This requires that the External Services Interface (ESI) license be installed in the switch. **NOTE:** When clients are blacklisted because they exceed the authentication failure threshold, they are blacklisted indefinitely by default. You can configure the duration of the blacklisting.
Fast Roaming	No	Fast roaming is a component of virtual AP profiles in which client devices are allowed to roam from one access point to another without requiring reauthentication by the main RADIUS server.
Strict Compliance	No	Define whether clients should have strict adherence to settings on this page for network access.
VLAN Mobility	No	Define whether clients in the WLAN and VLAN should have mobility or roaming privileges.
Remote AP Operation	Standard	Define the rights for remote APs in this WLAN. Options are as follows: ● standard ● persistent ● backup ● always Remote APs connect to a switch using Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec). AP control and 802.11 data traffic are carried through this tunnel. Secure Remote Access Point Service extends the corporate office to the remote site. Remote users can use the same features as corporate office users. Secure Remote Access Point Service can also be used to secure control traffic between an AP and the switch in a corporate environment. In this case, both the AP and switch are in the company's private address space.
Drop Broadcast and Multicast	No	Specify whether the WLAN should drop broadcast and multicast mesh network advertising on the WLAN.
Convert Broadcast ARP Requests to Unicast	No	Specify whether ARP table information should be distributed in broadcast (default) or unicast fashion.
Deny Inter User Traffic	No	If enabled, this setting disables traffic between all untrusted users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic. Requires a minimum version of 6.1.0.0.
Band Steering	No	Enable or disable band steering on the WLAN. Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5GHz band than on the 2.4GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40MHz or 20MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.
Steering Mode	Prefer-5ghz	Band steering supports three different band steering modes. ● **Force-5GHz**: When the AP is configured in **force-5GHz** band steering mode, the AP will try to force 5GHz-capable APs to use that radio band. ● **Prefer-5GHz** (Default): If you configure the AP to use **prefer-5GHz**

Field	Default	Description
		band steering mode, the AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. ● **Balance-bands**: In this band steering mode, the AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5GHz band has more channels than the 2.4 GHz band, and that the 5GHz channels operate in 40MHz while the 2.5GHz band operates in 20MHz. **NOTE:** Steering modes do not take effect until the band steering feature has been enabled. The band steering feature in AOS-W versions 3.3.2-5.0 does not support multiple band-steering modes. The band-steering feature in these versions of AOS-W functions the same way as the default **prefer-5GHz** steering mode available in AOS-W 6.0 and later.
Dynamic Multicast Optimization (DMO)	No	If enabled, DMO techniques will be used to reliably transmit video data.
Dynamic Multicast Optimization (DMO) Threshold (2-255)	6	Maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops.
Preserve Client VLAN	No	Whether to preserve the client VLAN. Requires version between 3.4.4.3 and 5.0.0.0, or version 6.1.0.0 and above.
Disable conversion of IPv6 multicast Router Advertisements to unicast	No	Enable or disable converting advertised IPv6 multicast routers to unicast to reduce unnecessary traffic. Firmware version 6.1.2.0 is required.

Select **Add** to create the WLAN, or click **Save** to finish reconfiguring an existing WLAN. The WLAN appears on the **WLANs** page in the Alcatel-Lucent Configuration navigation pane.

Profiles

Understanding Alcatel-Lucent Configuration Profiles

In AOS-W, related configuration parameters are grouped into a profile that you can apply as needed to an AP group or to individual APs. This section lists each category of AP profiles that you can configure and then apply to an AP group or to an individual AP. Note that some profiles reference other profiles. For example, a virtual AP profile references SSID and AAA profiles, while an AAA profile can reference an 802.1x authentication profile and server group.

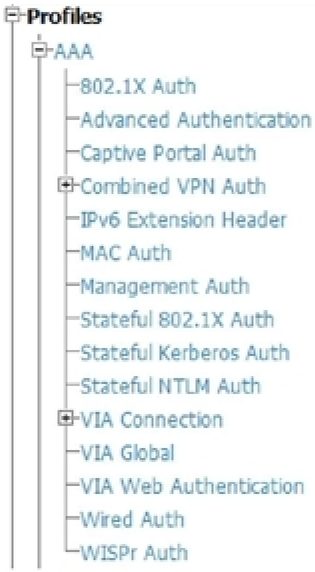
You can apply profiles to an AP or AP group.

Browse to the **Device Setup > Alcatel-Lucent Configuration** page, and click the **Profiles** heading in the navigation pane on the left. Expand the **Profiles** menu by clicking the plus sign (**+**) next to it. The following profile options appear:

- 802.1X Auth
- Advanced Authentication
- Captive Portal Auth
- IPv6 Extension Header
- MAC Auth

- Management Auth
- Stateful 802.1X Auth
- Stateful Kerberos Auth
- Stateful NTLM Auth
- VIA Connection
- VIA Global
- VIA Web Authentication
- Wired Auth
- WISPr Auth

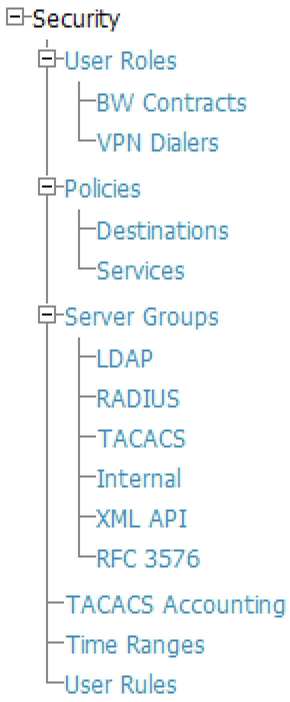
Figure 26 *Profiles*



Security

Alcatel-Lucen Configuration supports user roles, policies, server groups, and additional security parameters with profiles that are listed in the **Security** portion of the navigation pane on the **Alcatel-Lucent Configuration** page, as illustrated in Figure 27:

Figure 27 *Security Components in Alcatel-Lucent Configuration*



This section describes the profiles, pages, parameters and default settings for all **Security** components in **Alcatel-Lucent Configuration**, as follows:

- "Security > User Roles" on page 45
  - "Security > User Roles > BW Contracts" on page 48
  - "Security > User Roles > VPN Dialers" on page 49
- "Security > Policies" on page 51
  - "Security > Policies > Destinations" on page 53
  - "Security > Policies > Services" on page 54
- "Security > Server Groups" on page 55
  - "Security > Server Groups > LDAP" on page 58
  - "Security > Server Groups > RADIUS" on page 59
  - "Security > Server Groups > TACACS" on page 60
  - "Security > Server Groups > Internal" on page 61
  - "Security > Server Groups > XML API" on page 62
  - "Security > Server Groups > RFC 3576" on page 62
- "Security > TACACS Accounting" on page 64
- "Security > Time Ranges" on page 64
- "Security > User Rules" on page 65

Security > User Roles

A client is assigned a user role by one of several methods. A user role assigned by one method may take precedence over a user role assigned by a different method. The methods of assigning user roles are, from lowest to highest precedence:

1. The initial user role for unauthenticated clients is configured in the AAA profile for a virtual AP.
2. The user role can be derived from user attributes upon the client's association with an AP (this is known as a user-derived role). You can configure rules that assign a user role to clients that match a certain set of criteria. For example, you can configure a rule to assign the role VoIP-Phone to any client that has a MAC address that starts with bytes xx:yy:zz. User-derivation rules are executed before client authentication.
3. The user role can be the default user role configured for an authentication method, such as 802.1x or VPN. For each authentication method, you can configure a default role for clients who are successfully authenticated using that method.
4. The user role can be derived from attributes returned by the authentication server and certain client attributes (this is known as a server-derived role). If the client is authenticated via an authentication server, the user role for the client can be based on one or more attributes returned by the server during authentication, or on client attributes such as SSID (even if the attribute is not returned by the server). Server-derivation rules are executed after client authentication.
5. The user role can be derived from Alcatel-Lucent Vendor-Specific Attributes (VSA) for RADIUS server authentication. A role derived from an Alcatel-Lucent VSA takes precedence over any other user roles.

In the Alcatel-Lucent user-centric network, the user role of a wireless client determines its privileges, including the priority that every type of traffic to or from the client receives in the wireless network. Thus, QoS for voice applications is configured when you configure firewall roles and policies.

In an Alcatel-Lucent system, you can configure roles for clients that use mostly data traffic, such as laptop computers, and roles for clients that use mostly voice traffic, such as VoIP phones. Although there are different ways for a client to derive a user role, in most cases the clients using data traffic will be assigned a role after they are authenticated through a method such as 802.1x, VPN, or captive portal. The user role for VoIP phones can be derived from the OUI of their MAC addresses or the SSID to which they associate. This user role will typically be configured to have access allowed only for the voice protocol being used (for example, SIP or SVP).

NOTE

You must install the Policy Enforcement Firewall license in the switch.

This page displays the current user roles in Alcatel-Lucent Configuration and where they are used. This page contains the columns described in Table 8:

Table 8: *Security > User Roles Page Contents*

Column	Description
Name	Name of the user role.
AAA	Displays the AAA profile or profiles that are referenced by the user role.
Captive Portal Profile	Displays the Captive Portal Auth profiles, if any, that are referenced by the user role.
802.1X Auth	Displays the 802.1X Auth profiles that are referenced by the user role.
Stateful 802.1X Auth	Displays the Stateful 802.1X Auth profiles that are referenced by the user role.
VPN Auth	Displays the VPN Auth profiles that are referenced by the user role.
Folder	Displays the folder that is associated with this User Role. A Top viewable folder for the role is able to view all devices and groups contained by the top folder. The top folder and its subfolders must contain all of the devices in any of the groups it can view. Clicking any folder name takes you to the **APs/Devices > List** page for folder inventory and configuration.

The **Security** > **User Roles** > **Add New User Role** page contains the following fields, as described in Table 9:

Table 9: *Security > User Roles > Add New User Role Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the User Role is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the user role.
Other Settings		
Captive Portal Profile	None	(Optional) Select the Captive Portal Auth profile, if any, that is to be referenced by the user role. Select the add icon to create a new profile, or click the pencil icon to edit an existing profile.
Downstream Bandwidth Contract	None	(Optional) You can assign a bandwidth contract to provide an upper limit to upstream or downstream bandwidth utilized by clients in this role. You can select the Per User option to apply the bandwidth contracts on a per-user basis instead of to all clients in the role. Refer to "Security > User Roles > BW Contracts" on page 48.
Downstream Contract Applies Per User	No	If you selected a DS BW contract in the prior field, this gray field becomes active. Select **Yes** or **No**.
Upstream Bandwidth Contract	None	(Optional) You can assign a bandwidth contract to provide an upper limit to upstream or downstream bandwidth utilized by clients in this role. You can select the Per User option to apply the bandwidth contracts on a per-user basis instead of to all clients in the role. Refer to "Security > User Roles > BW Contracts" on page 48.
Upstream Contract Applies Per User	No	If you selected an US BW contract in the prior field, this gray field becomes active. Select **Yes** or **No**.
Maximum Number of Datapath Sessions Allowed	None	Use this field to configure a maximum number of sessions per user in this role. You can configure any value between 0-65535.
Reauthentication Interval Time	0	(Optional) Set the time, in minutes, after which the client is required to re-authenticate. Enter a value between 0-4096. 0 disables reauthentication.
VLAN To Be Assigned		(Optional) By default, a client is assigned a VLAN on the basis of the ingress VLAN for the client to the switch. Use this field to override this assignment and configure the VLAN ID that is to be assigned to the user role.
VPN Dialer Profile	None	(Optional) Use this field to assign a VPN dialer to a user role. Select a dialer from the drop-down list and assign it to the user role. This dialer will be available for download when a client logs in using captive portal and is assigned this role. For additional VPN information, refer to "Security > User Roles > VPN Dialers" on page 49.
VIA Connection Profile	None	Use this field to assign a VIA connection to a user role.

Field	Default	Description
Policies		
Add New Policy		Select this button to add a new policy to the user role. The following two columns appear: - Policy - Alcatel-Lucent AP Group
Policy	allow-diskservices	Select the policy to apply to this user role. Once any policy is selected, you can edit the policy by clicking the pencil icon. You can create a new policy by clicking the add icon. Refer to "Security > Policies" on page 51.
Alcatel-Lucent AP Group	None	Select the Alcatel-Lucent AP group in which this policy and user role will apply. Refer to "Alcatel-Lucent AP Groups Procedures and Guidelines" on page 19.

Select **Add** to complete the configuration of the **User Role**, or click **Save** to complete the editing of an existing role. The new role appears on the **Security > User Roles** page.

Security > User Roles > BW Contracts

You can manage bandwidth utilization by assigning maximum bandwidth rates, or bandwidth contracts, to user roles. You can configure bandwidth contracts, in kilobits per second (Kbps) or megabits per second (Mbps), for the following types of traffic:

- from the client to the switch (upstream traffic)
- from the switch to the client (downstream traffic)

You can assign different bandwidth contracts to upstream and downstream traffic for the same user role. You can also assign a bandwidth contract for only upstream or only downstream traffic for a user role; if there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.

By default, all users that belong to the same role share a configured bandwidth rate for upstream or downstream traffic. You can optionally apply a bandwidth contract on a per-user basis; each user who belongs to the role is allowed the configured bandwidth rate. For example, if clients are connected to the switch through a DSL line, you may want to restrict the upstream bandwidth rate allowed for each user to 128 Kbps. Or, you can limit the total downstream bandwidth used by all users in the guest role in Mbps.

The **Details** page for **Security** > **User Roles** > **Add New Bandwidth Contract** contains the following fields, as described in Table 10:

Table 10: *Security > User Roles > Add New BW Contract Page Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the Bandwidth Contract is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Units	kbits	Configure bandwidth contracts, in kilobits per second (Kbps) or megabits per

Field	Default	Description
		second (Mbps), for the following types of traffic: ● from the client to the switch (upstream traffic) ● from the switch to the client (downstream traffic)
Bandwidth		Specify whether this bandwidth contract is upstream or downstream by typing one of the following terms in lower case: ● **upstream** ● **downstream** Select **Add** to finish the new BW Contract and to return to the **BW Contract** page. The new contact appears below the **Add New BW Contract** button.

Select **Add** to complete the configuration of the **BW Contract** profile, or click **Save** to complete the editing of an existing profile. The new BW contract appears on the **Security** > **User Roles** page.

Security > User Roles > VPN Dialers

The VPN dialer can be downloaded using Captive Portal. For the user role assigned through Captive Portal, configure the dialer by the name used to identify the dialer. For example, if the captive portal client is assigned the guest role after logging on through captive portal and the dialer is called mydialer, configure mydialer as the dialer to be used in the guest role.

Select a dialer from the drop-down list and assign it to the user role. This dialer will be available for download when a client logs in using captive portal and is assigned this role.

The **Security** > **User Roles** > **Add New VPN Dialer** page contains the following fields, as described in Table 11:

Table 11: *Security > User Roles > Add VPN Dialer Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the VPN Dialer is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Enable PPTP	No	Enable PPTP with this setting as desired. Point-to-Point Tunneling Protocol (PPTP) is an alternative to L2TP/IPSec. Like L2TP/IPSec, PPTP provides a logical transport mechanism to send PPP frames as well as tunneling or encapsulation so that the PPP frames can be sent across an IP network. PPTP relies on the PPP connection process to perform user authentication and protocol configuration. With PPTP, data encryption begins after PPP authentication and connection process is completed. PPTP connections use Microsoft Point-to-Point Encryption (MPPE), which uses the Rivest-Shamir-Aldeman (RSA) RC-4 encryption algorithm. PPTP connections require user-level authentication through a PPP-based authentication protocol (MSCHAPv2) is the currently-supported method).
Enable L2TP	Yes	Enable L2TP with this setting as desired. The combination of Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec) is a highly secure technology that enables VPN

Field	Default	Description
		connections across public networks such as the Internet. L2TP/IPSec provides both a logical transport mechanism on which to transmit PPP frames as well as tunneling or encapsulation so that the PPP frames can be sent across an IP network. L2TP/IPSec relies on the PPP connection process to perform user authentication and protocol configuration. With L2TP/IPSec, the user authentication process is encrypted using the Data Encryption Standard (DES) or Triple DES (3DES) algorithm. L2TP/IPSec requires two levels of authentication: ● Computer-level authentication with a preshared key to create the IPSec security associations (SAs) to protect the L2TP-encapsulated data. ● User-level authentication through a PPP-based authentication protocol using passwords, SecureID, digital certificates, or smart cards after successful creation of the SAs.
Send traffic to the direct network in clear	No	Use this setting if no encryption is to be used and packets passing between the wireless client and switch are to be in clear text.
Disable wireless devices when client is wired	No	Use this setting to disable wireless clients when a wired device is known to be on the VPN.
Enable SecurID New and Next Pin Mode	No	Use this setting to enable or disable SecurID PIN modes. The SecurID authentication scheme authenticates the user on a RSA ACE/Server. When challenged, the user has to enter a password that is a combination of two numbers: a personal identification number (PIN), supplied by RSA, combined with a token code, which is the number displayed on the RSA SecurID authenticator. New PIN mode is applied in cases where the authentication process requires additional verification of the PIN. In this case, the user is required to use a new PIN. The new PIN is derived from one of the following two sources, depending on the configuration of the RSA ACE/Server: ● The user is prompted to select and enter a new PIN. ● The server supplies the user with a new PIN. The user is then required to re-authenticate with the new PIN. The use of the New PIN mode is optional and can be enabled or disabled.
PPP Authentication Modes	CHAP MSCHAP MSCHAPv2 PAP	Use this section to select the authentication modes to be supported for PPP in the VPN. The following options are available: ● CHAP ● Cache SecurID Token ● MSCHAP ● MSCHAPv2 ● PAP
IKE Lifetime (300-85400 secs)	28800	Specify the Internet Key Exchange (IKE) Lifetime in seconds. When this period of time expires, the IKE SA is replaced by a new SA or is terminated. The IKE SA specifies values for the IKE exchange: the authentication method used, the encryption and hash algorithms, the Diffie-Hellman group used, the lifetime of the IKE SA in seconds, and the shared secret key values for the encryption algorithms. The IKE SA in each peer is bi-directional.
IKE Encryption	168-bit 3DES-CBC	Select the Internet Key Exchange (IKE) encryption method from the following two options:

Field	Default	Description
		- 168-bit 3DES-CBC - 56-bit DES-CBC
IKE Diffie-Hellman Group	1024-bit (1)	Select the IPSEC Mode Group that matches the Diffie Hellman Group configured for the IPSEC policy. The two options are as follows: - 1024-bit - 768-bit The IKE policy selections, along with the preshared key, need to be reflected in the VPN configuration. Set the VPN configuration on clients to match the choices made above. In case the Alcatel-Lucent dialer is used, these configuration need to be made on the dialer prior to downloading the dialer onto the local client.
IKE Hash Algorithm	SHA	Set the IKE Hash Algorithm to either SHA or MD5, to match the IKE policy for IPSEC.
IKE Authentication	Pre-Shared	IKE Phase 1 authentication can be done with either an IKE preshared key or digital certificates. This establishes how the client is authenticated with the internal database on the switch. The options are **Pre-Shared Keys** or **RSA Signatures**.
IPSEC Lifetime	7200	Define the IPSEC lifetime in seconds, after which a new IPSEC key is required.
IPSEC Diffie Hellman Group	1024-bit (1)	Select the IPSEC Mode Group that matches the Diffie Hellman Group configured for the IKE policy. The two options are as follows: - 1024-bit - 768-bit The IPSEC policy selections, along with the preshared key, need to be reflected in the VPN configuration. Set the VPN configuration on clients to match the choices made above. In case the Alcatel-Lucent dialer is used, these configuration need to be made on the dialer prior to downloading the dialer onto the local client.
IPSEC Encryption	168-bit 3DES	Specify the type of IPSEC encryption to support for the VPN. Options are as follows: - Encapsulating Security Payload (ESP) with 168-bit 3DES - ESP with 56-bit DES
IPSEC Hash Algorithm	SHA	Set the IKE Hash Algorithm to either SHA or MD5, to match the IKE policy for IKE Hash Algorithm.

Select **Add** to finish the new **VPN Dialers** profile, or click **Save** to complete the editing of an existing profile. You return to the **VPN Dialers** page. The new profile appears below the **Add New VPN Dialer** button.

Security > Policies

The **Security** > **Policies** page displays all currently configured policies, to include the policy name, type, and cites the groups, user roles, and folders to which the security policy applies. To create a new policy, click the **Add New Policy** button. To edit an existing policy, click the pencil icon.

The **Security** > **Policies** > **Add New Policy** page contains the following fields, as described in Table 12:

Table 12: *Security > Policies > Add New Policy Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the policy is associated. The drop-down menu displays all folders available for association with the policy.
Name	Blank	Enter the name of the policy.
Rules		
IPv6	No	Select whether to use the IPv6 protocol. If you select No, OV3600 displays options for the IPv4 protocol instead. **NOTE:** As of AOS 6.0, you can mix IPv4 and IPv6 rules on one policy.
Source Traffic Match	any	The traffic source, which can be one of the following: - **alias**: After choosing this option, specify the network resource from the **Source Alias** drop-down menu that appears. Select the pencil icon to edit, or the plus icon to add a new alias. - **any**: match any traffic (wildcard) - **host**: This refers to traffic from a specific host. When this option is chosen, you must configure the source IP address of the host. For example, 2002:d81f:f9f0:1000:c7e:5d61:585c:3ab - **localip**: (IPv4 only) specify the local IP address to match traffic - **network**: This refers to a traffic that has a source IP from a subnet of IP addresses. When this option is chosen, you must configure the source address and network mask of the subnet. For example, 2002:ac10:fe:: ffff:ffff:ffff::. - **user**: This refers to traffic from the wireless client.
Destination Traffic Match	any	The traffic destination, which can be any of the same types as the Source Traffic Match options.
Service Type	any	Type of traffic, which can be one of the following: - **any**: This option specifies that this rule applies to any type of traffic. - **tcp**: Using this option, configure a range of TCP port(s) to match for the rule to be applied. - **udp**: Using this option, configure a range of UDP port(s) to match for the rule to be applied. - **service**: Selecting this option creates a new field called **Service** underneath **Service Type** with a drop-down list of pre-defined services (common protocols such as HTTPS, HTTP, and others) as the protocol to match for the rule to be applied. Select the pencil icon to edit the Netservice Profile (refer to "Security > Policies > Services" on page 54), or the plus sign to create a new Netservice profile. - **protocol**: Using this option, specify a different layer 4 protocol (other than TCP/UDP) by configuring the IP protocol value. - **icmpv6**: Use this option to configure ICMPv6. Requires IPv6 enabled.
Action	permit	Action if rule is applied, which can be one of the following: **reject**: deny packets. A new field will appear where you can Send Deny Response **dst-nat**: perform destination NAT on packets. New fields appear to specify the Dual NAT Pool and Dual NAT Port. **dual-nat**: perform both source and destination NAT on packets

Field	Default	Description
		permit: forward packets **redirect**: specify the location to which packets are redirected, which can be one of the following: - **Datapath Destination ID** (**0-65535**) - **ESI Server Group**: specify the ESI server group configured with the esi group command. - **Tunnel:** specify the ID of the tunnel configured with the interface tunnel command **src-nat**: perform source NAT on packets
ICMPv6 Message Type		Choose from the informational or error message types. This field appears if **IPv6** is enabled and **ICMPv6** is selected in the **Service Type** field.
Log if ACL is applied	No	Whether to generate a log message when the rule is applied.
Mirror all session packets	No	Whether to mirror all session packets to datapath or remote destination.
Queue Priority	low	Assigns a matching flow to a priority queue (high/low).
Time Range	None	Define a time range for this rule.
Pause ARM Scanning	No	Whether to pause Adaptive Radio Management scan activity when traffic is present. Note that the Scanning setting in the ARM profile should be activated in order to be paused.
Blacklist user if ACL is applied	No	Whether to blacklist any user.
TOS Value	None	Value of type of service (TOS) bits to be marked in the IP header of a packet matching this rule when it leaves the switch.
802.1p Priority	None	Specify 802.1p priority (0-7).

Select **Add** to complete the configuration of the **Policies** profile, or click **Save** to complete the editing of an existing profile. The new policy appears on the **Security** > **Policies** page.

Security > Policies > Destinations

The **Security** > **Policies** > **Destinations** page lists the destination names currently configured, with the Policy that uses the destination and the folder. To create a new destination to be referenced by a security policy, click the **Add New Net Destination** button. To edit an existing policy, click the pencil icon.

The **Security** > **Policies** > **Add New Destinations** page contains the following fields, as described in Table 13:

Table 13: *Security > Policies > Destinations Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the security policy is associated. The drop-down menu displays all folders available for association with the policy.

Field	Default	Description
Name	Blank	Enter the name of the destination.
Rules		
Invert	No	Use this field to invert the destination from one end of the VPN connection to the other.
IPv6	No	Select this button to create a new rule for this destination profile. Clicking this button displays the **Net Destination Rule** section for the selected protocol, which is comprised of two settings: ● **Rule Type**–Specify whether the rule applies to **Host**, **Network**, or **Range**. ● **IP Address**–Enter the IP address for the net destination rule.

Select **Add** to complete the configuration of the **Destination** policy profile, or click **Save** to complete the editing of an existing profile. The new destination appears on the **Security** > **Policies** > **Destinations** page.

Security > Policies > Services

The **Security** > **Policies** > **Services** page displays all Netservice profiles that are available for reference by Security policies. This page displays Netservice profile names, the protocol associated with it, the policy that uses this Netservice profile, and the folder.

Select **Add** to create a new Netservice profile, or click the pencil icon next to an existing Netservice profile to edit it. The **Security** > **Policies** > **Services** page contains the following fields, as described in Table 14:

Table 14: *Security > Policies > Services Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the security policy service is associated. The drop-down menu displays all folders available for association with the service.
Name	Blank	Enter the name of the destination.
Other Settings		
Protocol	TCP	Specify the protocol that is to support the security policy service being configured. The service options are: ● **TCP** ● **UDP** ● **IP** The remaining fields on this page change according to which protocol you have selected.
Port Selection	Range	Choose whether to list ports by **Range** (which causes the Port and Max Port fields to appear below) or **List** (which introduces a Port List field and requires a minimum version of 6.0.0.0).
TCP/UDP Port		Appears if **Range** is specified in Port Selection. Specify the TCP/UDP port or range of ports to support the service being configured.

Field	Default	Description
TCP/UDP Max Port		Appears if **Range** is specified in Port Selection. Specify the highest port that will support the TCP/UDP service being configured.
Port List		Appears if **List** is specified in Port Selection. Enter a comma separated list of ports. Requires a minimum version of 6.0.0.0.
IP Protocol Number (0-255)		Specify the numeric identifier of the upper layer IP protocol that an IP packet should use.
Configure Application Level Gateway	No	Specify whether to create an application level gateway, which filters incoming and outgoing information packets before copying and forwarding across the gateway. If you select **Yes** in this field, you are prompted with a new drop-down menu in which to select the Application Level Gateway type.
Application Level Gateway	dhcp	If you select **Yes** for **Configure Application Level Gateway**, then specify the gateway type from this drop-down menu. The following application level gateway types are supported: ● **dhcp** ● **dns** ● **ftp** ● **h323** ● **noe** ● **rtsp** ● **sccp** ● **sip** ● **sips** ● **svp** ● **tftp** ● **vocera**

Security > Server Groups

Server Groups Page Overview

The **Server** > **Server Groups** page displays all server groups currently configured, and the profiles and folders that are used by each server group, to include the following:

- AAA
- Captive Portal Auth
- Management Auth
- Stateful 802.1X Auth
- TACACS Accounting
- VPN Auth
- Folder

The list of servers in a server group is an ordered list. By default, the first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure the order of servers in the server group. In the Web UI, use the up or down arrows to order the servers (the top server is the first server in the list). In the CLI, use the position parameter to specify the relative order of servers in the list (the lowest value denotes the first server in the list).

The first available server in the list is used for authentication. If the server responds with an authentication failure, there is no further processing for the user or client for which the authentication request failed. You can optionally enable fail-through authentication for the server group so that if the first server in the list returns an authentication deny, the switch attempts authentication with the next server in the ordered list. The switch attempts authentication with each server in the list until either there is a successful authentication or the list of servers in the group is exhausted. This feature is useful in environments where there are multiple, independent authentication servers; users may fail authentication on one server but can be authenticated on another server.

Before enabling fail-through authentication, note the following:

- This feature is not supported for 802.1x authentication with a server group that consists of external EAP compliant RADIUS servers. You can, however, use fail-through authentication when the 802.1x authentication is terminated on the switch (AAA FastConnect).
- Enabling this feature for a large server group list may cause excess processing load on the switch. Best practices are to use server selection based on domain matching whenever possible.
- Certain servers, such as the RSA RADIUS server, lock out the switch if there are multiple authentication failures. Therefore you should not enable fail-through authentication with these servers.

When fail-through authentication is enabled, users that fail authentication on the first server in the server list should be authenticated with the second server.

Supported Servers

AOS-W supports the following external authentication servers:

- RADIUS (Remote Authentication Dial-In User Service)
- LDAP (Lightweight Directory Access Protocol)
- TACACS+ (Terminal Access Switch Access Control System)
- Windows

Additionally, you can use the switch's internal database to authenticate users. You create entries in the database for users and their passwords and default role.

You can create groups of servers for specific types of authentication. For example, you can specify one or more RADIUS servers to be used for 802.1x authentication. The list of servers in a server group is an ordered list. This means that the first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure servers of different types in one group — for example, you can include the internal database as a backup to a RADIUS server.

Server names are unique. You can configure the same server in multiple server groups. You must configure the server before you can add it to a server group.

Adding a New Server Group

The server group is assigned to the server group for 802.1x authentication.

To create a new server group, click the **Add** button, or to edit an existing group, click the pencil icon next to that group. The **Add New Server Group** page appears, and contains the following fields, as described in Table 15:

Table 15: *Security > Server Groups > Add or Edit Server Group Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server group.
Other Settings		

Field	Default	Description
Fail Through	No	Enable or disable a fail through server. When fail-through authentication is enabled, users that fail authentication on the first server in the server list should be authenticated with the second server. Theswitch attempts authentication with each server in the list until either there is a successful authentication or the list of servers in the group is exhausted. This feature is useful in environments where there are multiple, independent authentication servers; users may fail authentication on one server but can be authenticated on another server.
Add New Server		Select this button to add a new server to the Server Group being configured. A new **Server** section and Server Group Server Rules section appear with the following settings to be defined: Server Section ● **Trim FQDN**–Default setting is **No**. Change to **Yes** to enable. You can use the **match FQDN** option for a server match rule. With a match FQDN rule, the server is selected if the <domain> portion of the user information in the formats <domain>\<user> or <user>@<domain> exactly matches a specified string. This rule does not support client information in the **host/<pc-name>.<domain>** format, so it is not useful for 802.1x machine authentication. The **match FQDN** option performs matches on only the <domain> portion of the user information sent in an authentication request. The match-authstring option (described previously) allows you to match all or a portion of the user information sent in an authentication request. ● **Server Type**–Select the server type for the new server being added. Options are **RADIUS** (default), **LDAP**, **TACACS**, **Internal**, or **Windows**. ● **Server**–Select the server from the drop-down menu that the new server is to use. You can edit an existing server or create a new server. Server Group Server Rules Section Select the **Add** button to add a new rules section. The page that appears contains the following settings to define: ● **Match Type**–From the drop-down menu, select **Authstring** or **FQDN**. The following settings complete the configuration. ● **Operator**–For **Authstring** only, specify how to process the string (**contains, equals, starts with**). ● **Match String**–Enter the string or string fragment. Finish by clicking the **Add New Server Group Server Rules** button.
Server Group Rule		
Field to set	role	Specify whether the server group rule is a **role** or a **VLAN**. The **Role/VLAN** field at the bottom of the page changes in response to your selection here.
Attribute	ARAP-Features	From the drop-down menu, click the attribute that defines the server group rule being configured. Many options are supported.
Operation	contains	Select the criteria by which to process the **Operand**, which you specify in the following field.
Operand		Enter a text string.
Role/VLAN	ap-role	Select the role or VLAN to associate with this new server group rule from the drop-down menu.

Select **Add** to complete the configuration of the **Server Group**, or click **Save** to complete the editing of an existing server. The new server group appears on the **Security** > **Server Groups** page.

Security > Server Groups > LDAP

You can configure Lightweight Directory Access Protocol (LDAP) servers for use by a server group.
The **Security** > **Server Groups** > **LDAP** page displays current LDAP servers available for inclusion in server groups. Select **Add** to create a new LDAP server, or click the pencil icon next to an existing LDAP server to edit the configuration.

The **Security > Server Groups > Add LDAP Server** page contains the following fields, as described in Table 16:

Table 16: *Security > Server Groups > Add LDAP Server Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server.
Other Settings		
Host IP Address	0.0.0.0	Enter the IP address of the LDAP server.
Admin-DN		Enter the distinguished name for the admin user who has read/search privileges across all the entries in the LDAP database. The user need not have write privileges but the user should be able to search the database, and read attributes of other users in the database.
Admin Password		Enter the password for the admin user.
Allow Clear-text	No	Enable this setting to allows clear-text (unencrypted) communication with the LDAP server.
Auth Port	389	Enter the port number used for authentication on the LDAP server.
Base-DN		Enter the distinguished name of the node which contains the entire user database to use.
Filter	(objectclass=*)	Select the filter that should be applied to any search of the user in the LDAP database.
Key Attribute	sAMAccountName	Enter the attribute that should be used as a key in search for the LDAP server. For Active Directory, the value is sAMAccountName.
Timeout (1030 sec)	20	Define the timeout period of a LDAP request, in seconds.
Enable	Yes	Use this field to enable or disable the LDAP server being configured. You can configure the LDAP server as disabled, but return later to enable it.
Preferred Connection	ldap-s	Select the connection type for the LDAP server from the drop-

Field	Default	Description
Type		down menu. LDAP servers support the following connection types: ● clear-text–No encryption is used. ● ldap-s–Uses SSL encryption. ● start-tls–Uses TLS encryption.
Maximum Number of Non-admin Connections	4	The number of non-administrative connections that should not be exceeded.

Select **Add** to complete the configuration of the **LDAP Server**, or click **Save** to complete the editing of an existing server. The new LDAP server appears on the **Security** > **Server Groups** > **LDAP Server** page. This server is now available to be used by server groups.

Security > Server Groups > RADIUS

You can configure RADIUS servers for use by a server group. The **Security** > **Server Groups** > **RADIUS** page displays current RADIUS servers available for inclusion in server groups. Select **Add** to create a new RADIUS server, or click the pencil icon next to an existing RADIUS server to edit the configuration.

The **Security** > **Server Groups** > **Add New RADIUS Server** page contains the following fields, as described in Table 17:

Table 17: *Security > Server Groups > RADIUS*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server.
Other Settings		
Host IP Address		Set the IP address of the authentication server.
Key (Confirm Key)		Set the shared secret between the switch and the authentication server. The maximum length is 48 bytes.
Auth Port	1812	Set the authentication port on the server.
Acct Port	1813	Set the accounting port on the server.
Retransmits (0-3)	3	Set the Maximum number of retries sent to the server by the switch before the server is marked as down.
Timeout	(1-30 sec)	Set the maximum time, in seconds, that the switch waits before timing out the request and resending it.
NAS ID		Set the Network Access Server (NAS) identifier to use in RADIUS packets.
NAS IP		Set the NAS IP address to send in RADIUS packets.

Field	Default	Description
		You can configure a global NAS IP address that the switch uses for communications with all RADIUS servers. If you do not configure a server-specific NAS IP, the global NAS IP is used.
Use MD5	No	Enable or disable the use of MD5 hashing for cleartext passwords.
Enable	Yes	Enable or disable the RADIUS server.
Source Interface		Enter a VLAN number ID between 1-4094. Allows you to use source IP addresses to differentiate RADIUS requests. Associates a VLAN interface with the RADIUS server to allow the server-specific source interface to override the global configuration. If you associate a Source Interface (by entering a VLAN number) with a configured server, then the source IP address of the packet will be that interface's IP address. If you do not associate the Source Interface with a configured server (leave the field blank), the IP address of the global Source Interface will be used. Requires a minimum version of 6.1.0.0.

Select **Add** to complete the configuration of the **RADIUS** server, or click **Save** to complete the editing of an existing server. The new server appears on the **Security** > **Server Groups** > **RADIUS** page. This server is now available to be used by server groups.

Security > Server Groups > TACACS

You can configure TACACS+ servers for use by a server group. The **Security** > **Server Groups** > **TACACS** page displays current TACACS servers available for inclusion in server groups. Select **Add** to create a new RADIUS server, or click the pencil icon next to an existing TACACS server to edit the configuration.

The **Security** > **Server Groups** > **Add New TACACS Server** page contains the following fields, as described in Table 18:

Table 18: *Security > Server Groups > TACACS*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server.
Other Settings		
Host IP Address	0.0.0.0	
Key (Confirm Key)		Set the shared secret to authenticate communication between the TACACS+ client and server.
TCP Port	49	Set the TCP port to be used by the server.
Retransmits (0-3)	3	Set the maximum number of times a request is retried.

Field	Default	Description
Tmeout (1-30 sec)	20	Set the timeout period for TACACS+ requests, in seconds.
Enable	Yes	Enable or disable the TACACS server.
Session Authorization	No	Enables or disables session authoriaztion.Session authorization turns on the optional authorization session for admin users.

Select **Add** to complete the configuration of the **TACACS Server**, or click **Save** to complete the editing of an existing server. The new server appears on the **Security** > **Server Groups** > **TACACS** page. This server is now available to be used by server groups.

Security > Server Groups > Internal

An internal server group configures the internal database with the username, password, and role (student, faculty, or sysadmin) for each user. There is a default internal server group that includes the internal database. For the internal server group, configure a server derivation rule that assigns the role to the authenticated client.

The **Security** > **Server Groups** > **Add New Internal Server** page contains the following fields, as described in Table 19:

Table 19: *Security > Server Groups > Add Internal Server Field and Descriptions*

Field	Defaul-t	Description
General Settings		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name		Enter the name of the server.
Other Settings		
Maximum Expiration (mins)		Set the maximum expiration time (in minutes) for guest accounts. If the guest-provisioning user attempt to add a guest account that expires beyond this time period, an error message is displayed and the guest account is created with the maximum time you configured.
Internal Server Users		
Add New Internal Server User		This section displays internal server users currently configured for use on the Internal Server. Select this button to add a new user. The **Internal Server User** section appears with the following settings.
Internal Server User		
User Name		Enter the name of a user, or click **Generate** to create an anonymous ID for this user.
Password		Enter the password in plain text, or click **Generate** to create a random password for this user.
User Role	guest	From the drop-down menu, select the user role to associate with this user.

Field	Defaul-t	Description
		The role establishes read/write privileges, manage/monitor privileges, and other settings.
E-Mail		Enter the email address of the guest user.
Enabled	Yes	Specify whether this guest user is enabled or disabled on the internal server.
Expire User	No	Specify whether to expire the guest user after a period of time. If you click **Yes**, a new field appears with instructions about the date and time in which the guest user is expired from the internal server.

Select **Add** to complete the configuration of the **Internal Server**, or click **Save** to complete the editing of an existing server. The new server appears on the **Security** > **Server Groups** > **Internal Server** page. This server is now available to be used by server groups.

Security > Server Groups > XML API

Alcatel-Lucent Configuration supports server groups that can include XML API servers. XML API servers send and accept requests for information. XML API servers process such requests and act on these requests by performing requested actions. Such a server also compiles necessary reporting data and sends it back to requesting source.

The **Security** > **Server Groups** > **Server** page lists any XML API servers currently available for use by server groups. From this page, click **Add** to create a new XML API server, or click the pencil icon next to an existing server to edit. The **Security** > **Server Groups** > **Add New XML API Server** page contains the following fields, as described in Table 20:

Table 20: *Security > Server Groups > Add New XML API Server Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server.
Other Settings		
Key (Confirm Key)	Blank	Set the shared secret to authenticate communication between the XML API client and server.

Select **Add** to complete the configuration of the **XML API Server**, or click **Save** to complete the editing of an existing server. The new server appears on the **Security** > **Server Groups** > **XML API** page. This server is now available to be used by server groups.

Security > Server Groups > RFC 3576

RFC 3576 servers support dynamic authorization extensions to Remote Authentication Dial-In User Service (RADIUS). Alcatel-Lucent Configuration supports RFC 3576 servers that can be referenced by server groups.

To view currently configured RFC 3576 servers and where they are used, navigate to the **Security** > **Server Groups** > **RFC3576** page.

Select **Add** to create a new RFC3576 server, or click the pencil icon next to an existing server to edit it. The **Security** > **Server Groups** > **Add RFC 3576 Server** page contains the following fields, as described in Table 21.

Table 21: *Security > Server Groups > Add RFC 3576 Server Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server.
Other Settings		
Key (Confirm Key)	Blank	Set the shared secret to authenticate communication between the RFC 3576 client and server.

Select **Add** to complete the configuration of the **RFC 3576 Server**, or click **Save** to complete the editing of an existing server. The new server appears on the **Security** > **Server Groups** > **RFC 3576** page. This server is now available to be used by server groups.

Security > Server Groups > Windows

Perform these steps to configure a **Windows** profile.

1. Select **Security** > **Server Groups** > **Windows** in the **Navigation** pane. The details page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **Windows** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in Table 22:

Table 22: *Security > Server Groups > Windows Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Host		Enter the IP address of the Windows server.
Enable	No	Enable or disable the Windows server.
Windows Domain		The domain of the Windows server. Requires a minimum of AOS-W 6.0.

3. Select **Add** or **Save**. The added or edited profile appears on the **Windows** page and on the details page.

Security > TACACS Accounting

TACACS+ accounting allows commands issued on the switch to be reported to TACACS+ servers. You can specify the types of commands that are reported, and these are action, configuration, or show commands. You can have all commands reported as desired. Alcatel-Lucent Configuration supports TACACS Accounting servers that can be referenced by server groups.

To view currently configured TACACS Accounting profiles and where they are used, navigate to the **Security > TACACS Accounting** page. Select **Add** to create a new TACACS Accounting profile, or click the pencil icon to edit an existing profile.

The **Add/Edit TACACS Accounting Profile** page contains the following fields, as described in Table 23:

Table 23: *Security > Server Groups > Add/Edit TACACS Accounting Profile Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Enabled	No	Enable or disable the TACACS Accounting profile. If enabled, additional field appear, in which to define additional parameters, as follows.
Server Group	default	From the drop-down menu, select the server group that is to reference the TACACS Accounting profile. You can create a new group by clicking the add icon, or edit an existing group by clicking the pencil icon. once you are done adding or editing, the OV3600 interface returns you to the TACACS Accounting Profile page to complete the configuration.
Action	No	Select this option to have **Action** commands monitored and reported by the TACACS Accounting profile.
Configuration	No	Select this option to have **Configuration** commands monitored and reported by the TACACS Accounting profile.
Show	No	Select this option to have **Show** commands monitored and reported by the TACACS Accounting profile.

Select **Add** to complete the new TACACS Accounting profile, or click **Save** to complete the editing of an existing profile.

Security > Time Ranges

A time range profile establishes the boundaries by which users and guest users are to be supported on the network. This is a security and access-related profile, and several time range profiles can be configured to enable absolute or periodic access.

The **Security > Time Ranges** page displays all time ranges that are currently available in Alcatel-Lucent Configuration, time range profile type, the policy and WLAN that use time range profiles, and the folder in which each profile is visible.

To create a new time range profile, click the **Add New Time Range** button, or click the pencil icon next to an existing time range profile to adjust settings. The **Security** > **Time Range** > **Add/Edit New Time Range** page contains the following fields, as described in Table 24:

Table 24: *Security > Time Range > Add/Edit Time Range Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Type	Absolute	Specify whether the time range is Absolute, meaning a very specific range of time, or Periodic, meaning regularly occurring time ranges that occur repeatedly over time. If you select **Absolutely**, specify the **Start Date** and **End Date** and time as instructed. If you select **Periodic**, the **Add New Time Period** button appears. Select this button, then complete the three settings that follow: ● **Period**–Specify whether the time period is daily, weekday, weekend, or day. ● **Start Time**–Specify the hour and minute that the time period is to be begin. ● **End Time**–Specify the hour and minute that the time period is to end.

Select **Add** to complete the **Time Period** profile, or click **Save** to complete the editing of an existing profile.

Security > User Rules

The user role is a user derivation profile. User Rules can be derived from attributes from the client's association with an AP. For VoIP phones, you can configure the devices to be placed in their user role based on the SSID or the Organizational Unit Identifier (OUI) of the client's MAC address.

Navigate to the **Security** > **User Rules** page in the Alcatel-Lucent Configuration navigation pane. This page displays user rules that are currently configured, the AAA profile that references these rules, and the folder.

To add a new user rule, which is a derivation profile, click Add New User Derivation Profile. To edit an existing user rule, click the pencil icon next to an existing rule. Table 25 describes the contents of this page.

Table 25: *Security > User Rules > Add/Edit User Rules Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the rule set is associated. The drop-down menu displays all folders available for association with the rule set.
Name	Blank	Enter the name of the rule set.
User Derivation Rules		
Add New User Derivation Rule		Select this button to create a new rule. Additional fields appear that require configuration, as follows.

Field	Default	Description
Set Type	role	Select whether the rule is based on role, VLAN, or AAA profile (Requires a Public Wi-Fi Access licens).
Rule Type	bssid	Select one of the following options from the drop-down menu. Your selection in this field changes an ensuing field that must be completed, as follows: ● **bssid**–Selecting this option displays the **BSSID** field below. Specify the BSSID in text. ● **dhcp-option-77**–Selecting this option displays the **DHCP Option 77** field below. Enter this information in text. ● **dhcp-option** - Selecting this option displays a **DHCP Option** entry field below. ● **encryption-type**–Selecting this option displays the **Encryption Type** field below, in which you must select the encryption type from the drop-down menu. Select **open**, **static-wep**, or another other encryption type from the drop-down menu. ● **essid**–Selecting this option displays **ESSID** field below, in which you enter the ESSID in text. ● **location**–Selecting this option displays the **Location** field below, in which you enter the location in text. ● **macaddr**–Selecting this option displays the MAC Address field below, in which you must enter the MAC address.
Operator		Select the matching operator.
User Role/VLAN	ap-role	If you selected **role** for the **Set Type** field above, then select the specific user role from this drop-down menu. If you selected **VLAN** for the **Set Type** field above, then select the specific VLAN from this drop-down menu.

Local Config of SNMP Management

The Local Config component is used for local configuration of Alcatel-Lucent switches. Locally configured settings are not pushed to local switches by master switches.

SNMP trap settings for switches are managed locally. Trap settings for the AP are managed by group or global configuration in **Profiles** > **AP** > **SNMP**.

CAUTION

If you push configuration to a switch without having imported the contents of this profile, it will stop responding to the OV3600, because the default profile has no community strings in it.

To configure SNMP trap settings on a switch, navigate to the **Local Config** > **SNMP Management** page. Select **Add** to create a new SNMP Management profile, or click the pencil icon to edit an existing profile.

Table 26 describes the fields that appear in the Details page for this profile:

Table 26: *Local Config > SNMP Management Profile Settings*

Field	Description
General Settings	
Folder	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.

Field	Description
Name	Enter the name of the profile.
SNMP Settings	
Community Strings	Community strings used to authenticate requests for SNMP versions before version 3. **NOTE:** This is needed only if using SNMP v2c and is not needed if using version 3.
Enable Trap Generation	Enables generation of SNMP traps to configured SNMP trap receivers.
Engine ID	Sets the SNMP server engine ID as a hexadecimal number. 24 character maximum.
Inform Queue Length (100-350)	Specify the length for the SNMP inform queue. Default is 250.
Always use the switch's IP address as source address	Set whether to use the IP address of the switch as the trap source.
Trap Source IP Address	Enter the source IP address for sending traps.
SNMP Trap Hosts	
IP Address	Enter the IP address of the trap host.
SNMP Version	Configures the SNMP version as 1, 2c, or 3. ● If 2c is selected, the Send Inform field appears at the bottom of this section. ● If 3 is selected, the **SNMP User** field will appear as a drop-down menu containing any configured v3 users. Select the plus icon to add them via the **SNMP Management > SNMPv3 User** profile.
Community String	Configure the security string for notification messages. Does not appear if **SNMP Version** is set to 3.
UDP Port (1-65535)	The port number to which trap notification messages are sent. Default is 162.
Send Informs	Whether to send SNMP inform messages to the configured host. Displays when **2c** is selected in **SNMP Version**.
SNMPv3 Users If you are using SNMPv3 to obtain values from the Alcatel-Lucentswitch, navigate to **Local Config > SNMP Management > SNMPv3 User** to configure the following parameters:	
User name	A string representing the name of the user.
Authentication protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: ● MD5: HMAC-MD5-96 Digest Authentication Protocol ● SHA: HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.

Field	Description
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption Protocol).
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol.

Select **Add** to create this profile, or click **Save** to retain changes to an edited profile.

Advanced Services

This section describes the contents, parameters, and default settings for all **Advanced Services** components in **Alcatel-Lucent Configuration**. Alcatel-Lucent Configuration in OV3600 supports advanced services such as IP Mobility and VPN services. For additional information about IP Mobility domains, VPN services, and additional architecture or concepts, refer to the *Alcatel-Lucent AOS-W User Guide*.

Advanced Services > IP Mobility

Navigate to **Advanced Services** > **IP Mobility** page from the **Alcatel-Lucent Configuration** navigation pane. This page displays all currently configured profiles supporting IP Mobility, each group that uses each IP Mobility profile, and the folder for each IP Mobility profile.

Select **Add** to create a new **IP Mobility** profile, or click the pencil icon next to an existing profile to modify settings on an existing profile. The **Advanced Services** > **IP Mobility Profile Details** page contains the following fields, as described in Table 27:

Table 27: *Advanced Services > IP Mobility, Add/Edit Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Mobility Domains		
Mobility Domains	None selecte-d	This section displays all domains that are available for association with this IP mobility profile. You can show all, or show only selected domains. Select one or more mobility domains to associate with this IP Mobility profile.
Foreign Agent		
Registration Lifetime Requested by Proxy (10-65,534 sec)	180	Specify the client registration time on the foreign network. A foreign agent receives traffic that is intercepted by the home agent on the home network, and forwards to the client on the foreign network. This setting defines the registration time of a client on the foreign network.
Maximum Number of Active Visitors (0-5000)	5000	Set the maximum number of users to be supported by the foreign network.

Field	Default	Description
Maximum Number of Requests Retransmits (0-5)	3	Set the maximum number of times that a retransmit is to be supported on the foreign network by proxy.
Retransmit Interval (100-10000 msec)	1000	Set the foreign agent retransmit time in milliseconds. The retransmit interval defines retransmission between the home agent and the foreign agent.
Home Agent		
Replay Protection Time Value (0-300 sec)	7	Define the time period over which message replay is to be detected. Message replay detects if a message that is intended for a client has been intercepted and replayed. This setting defines how long replay detection is to monitor for replay.
Maximum Number of Active Bindings (0-5000)	5000	Define the maximum number of bindings in which the home agent network is to support a client when the client is out of range of the network, or otherwise disconnected.
Proxy Mobile IP		
Trigger Mobility on Station Association	Yes	Enable this setting to trigger client mobility processing on the network once a client has associated to the network in mobile fashion. The proxy mobile IP module in a mobility-enabled switch detects when a mobile client has moved to a foreign network and determines the home agent for a roaming client. The proxy mobile IP module performs the following functions: ● Derives the address of the home agent for a mobile client from the HAT using the mobile client's IP address. If there is more than one possible home agent for a mobile client in the HAT, the proxy mobile IP module uses a discovery mechanism to find the current home agent for the client. ● Detects when a mobile client has moved. Client moves are detected based on ingress port and VLAN changes and mobility is triggered accordingly. For faster roaming convergence between AP(s) on the same switch, it is recommended that you keep the **on station association** option enabled. This helps trigger mobility as soon as 802.11 association packets are received from the mobile client.
Enable Support for Standalone APs	No	Select this option to support standalone APs on the IP Mobility domain.
Log User Moves	Yes	Enable this option to log client movement in the IP Mobility domain. This setting is derived from station association in a foreign network.
Allow Roaming for Authenticated Stations Only	Yes	Enable this setting to require authentication for roaming stations.
Filter out DHCP Release from Stations	No	Enable or disable the filtering of DHCP information when a client is released from a station.
Re-home Idle Voice Capable Client	No	Enable or disable re-homing for idle voice-capable clients. This setting reassigns the home network in relation to a voice-capable client that is idle (non-roaming).
Maximum Number of Station Mobility Events Per Second	10	Set the maximum number of events, per second, that station mobility events can be supported.

Field	Default	Description
(1-65535)		
Maximum Interval Mobility Will Hold Inactive Host Trail (120-3600 sec)	600	Define how long inactive host trails are to be supported in IP mobility.
Maximum Entries in User Mobility Trail (1-30)	10	Define how many events are to be logged in IP mobility.
Mobility Host Entry Hold Time After Connectivity Loss (30-3600 sec)	60	Define how long IP mobility is to support hosts should there be a disconnection.
Mobility Host Entry LIfetime When Mobility Cannot Be Provided (30-60000 sec)	120	Define how long host entries in the IP mobility domain are to be maintained when they are without mobility.
Proxy DHCP		
Maximum Number of BOOTP Packets Per Transaction (0-65534)	25	Define the maximum number of BOOTP packets that can be supported for a given transaction in proxy DHCP. All BOOTP packets are at least 300 bytes in size, by specification. BOOTP packets are used when a host configures itself dynamically at boot time.
Maximum Time Allowed for a DHCP Transaction to Complete (10-600 sec)	60	Set the maximum allowable time for proxy DHCP transactions to complete.
Proxy DHCP Session Hold Time after Completion (dangerous) (1-600 sec)	5	Specify the length of time a proxy DHCP session is to be supported after DHCP processes are complete. Longer times are not considered advisable.
Terminate Proxy DHCP on Aggressive Transaction ID Change (dangerous)	No	If proxy DHCP is subject aggressive transaction ID change, this setting terminates upon detection.
Performs Proxy-DHCP for BOOTP Packets Without DHCP-options (dangerous)	No	Use this setting to support Proxy DHCP for BOOTP packets, but without DHCP options.
Revocation		
Retransmit Interval (100-10000 msec)	1000	Set the interval in milliseconds in which to retransmit in revocation. A home agent or foreign agent can send a registration revocation message, which revokes registration service for the mobile client. For example, when a mobile client roams from one foreign agent to another, the home agent can send a registration revocation message to the first foreign agent so that the foreign agent can free any resources held for the client.
Maximum Number of Request Retransmits (0-5)	3	Use this setting to define how many retransmits are supported before revocation is enacted.

Select **Add** to create this IP Mobility Profile, or click **Save** to retain changes to an edited IP Mobility Profile.

Advanced Services > IP Mobility > Mobility Domain

You configure mobility domains on masterswitches. All local switches managed by the master switch share the list of mobility domains configured on the master. Mobility is disabled by default and must be explicitly enabled on all switches that will support client mobility. Disabling mobility does not delete any mobility-related configuration.

The home agent table (HAT) maps a user VLAN IP subnet to potential home agent addresses. The mobility feature uses the HAT table to locate a potential home agent for each mobile client, and then uses this information to perform home agent discovery. To configure a mobility domain, you must assign a home agent address to at least one switches with direct access to the user VLAN IP subnet. (Some network topologies may require multiple home agents.)

Best practices are to configure the switch IP address to match the AP's local switches, or to define the Virtual Router Redundancy Protocol (VRRP) IP address to match the VRRP IP used for switches redundancy. Do not configure both a switch IP address and a VRRP IP address as a home agent address, or multiple home agent discoveries may be sent to the switches.

Configure the HAT with a list of every subnetwork, mask, VLAN ID, VRRP IP, and home agent IP address in the mobility domain. Include an entry for every home agent and user VLAN to which an IP subnetwork maps. If there is more than one switches in the mobility domain providing service for the same user VLAN, you must configure an entry for the VLAN for each switches. Best practices are to use the same VRRP IP used by the AP.

The mobility domain named **default** is the default active domain for all switches. If you need only one mobility domain, you can use this default domain. However, you also have the flexibility to create one or more user-defined domains to meet the unique needs of your network topology. Once you assign a switches to a user-defined domain, it automatically leaves the default mobility domain. If you want a switches to belong to both the default and a user-defined mobility domain at the same time, you must explicitly configure the default domain as an active domain for the switches.

Navigate to **Advanced Services > IP Mobility > Mobility Domain** from the **Alcatel-Lucent Configuration** navigation pane. This page displays all currently configured IP Mobility domains. Select **Add** to create a new **IP Mobility Domain**, or click the pencil icon next to an existing profile to modify an existing domain. The **Advanced Services > IP Mobility > Add/Edit IP Mobility Domain** page contains the following fields, as described in Table 28:

Table 28: *Advanced Services > IP Mobility > Add/Edit IP Mobility Domain Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the domain is associated. The drop-down menu displays all folders available for association with the domain.
Name	Blank	Enter the name of the domain.
Other Settings		
Active	No	Define whether the IP Mobility Domain is active or inactive.
Description		Add a description for the domain (requires AOS 6.0.0.0 or later)
Mobile IP Home Agents		
Add		Use this button to create new home agents. Once you click **Add**, the following additional fields appear in the Mobile IP Home Agent section. Complete these settings. ● **Subnet**–Define the subnet mask for the IP Mobility Domain. ● **Netmask**–Define the net mas for the IP Mobility Domain.

Field	Default	Description
		- **VLAN ID (1-4094)**–Set the VLAN to be supported on the IP Mobility Domain. - **Home Agent**–Set the home agent for the IP Mobility Domain. When you enable IP mobility in a mobility domain, the proxy mobile IP module determines the home agent for a roaming client. Select **Add** to create the home agent.

Select **Add** to create the new IP Mobility Domain, or click **Save** to save changes to a recon figured IP Mobility Domain. The domain is now available for use in IP Mobility profiles.

Advanced Services > VPN Services

For wireless networks, virtual private network (VPN) connections can be used to further secure the wireless data from attackers. The Alcatel-Lucentswitches can be used as a VPN concentrator that terminates all VPN connections from both wired and wireless clients.

You can configure the switches for the following types of VPNs:

- Remote access VPNs allow hosts, such as telecommuters or traveling employees, to connect to private networks such as a corporate network over the Internet. Each host must run VPN client software that encapsulates and encrypts traffic and sends it to a VPN gateway at the destination network. The switches supports the following remote access VPN protocols:
  - Layer-2 Tunneling Protocol over IPSec (L2TP/IPSec)
  - Point-to-Point Tunneling Protocol (PPTP)
- Site-to-site VPNs allow networks such as a branch office network to connect to other networks such as a corporate network. Unlike a remote access VPN, hosts in a site-to-site VPN do not run VPN client software. All traffic for the other network is sent and received through a VPN gateway that encapsulates and encrypts the traffic.

Before enabling VPN authentication, you must configure the following:

- The default user role for authenticated VPN clients—this is configured with roles and policies.
- The authentication server group the switches will use to validate the clients—this is configured with server groups.

You then specify the default user role and authentication server group in the VPN authentication profile.

The **Advanced Services** > **VPN Services** page displays all VPN service profiles that are currently configured, and allows you to add VPN service profiles or to edit existing profiles.

Select the **Add** button to add a new VPN Service profile, or click the pencil icon next to an existing profile to change its configuration. The **VPN Services** detail page appears, with settings defined in Table 29.

Table 29: *Advanced Services > VPN Services > Add/Edit VPN Service Profiles Fields and Descriptions*

Field	Defaul-t	Description
General Settings		
Folder	Top	Set the folder with which the VPN service profile is associated. The drop-down menu displays all folders available for association with the VPN services profile.
Name	Blank	Enter the name of the VPN services profile.
Other Settings		

Field	Default	Description
IKE Profile		Select an IKE profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing IKE profile. Refer to "Advanced Services > VPN Services > IKE" on page 73
PPTP Profile		Select a PPTK profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing PPTP profile. Refer to "Advanced Services > VPN Services > L2TP" on page 75.
L2TP Profile		Select an L2TP profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing L2TP profile. Refer to "Advanced Services > VPN Services > L2TP" on page 75.
IPSEC Profile		Select an IPSEC profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing IPSEC profile. Refer to "Advanced Services > VPN Services > IPSEC" on page 77.

Select **Add** to create the VPN Services profile, or click **Save** to change an existing profile. The new VPN Service profile appears on the **VPN Services** page.

Advanced Services > VPN Services > IKE

Navigate to **Advanced Services** > **VPN Services** > **IKE page** from the **Alcatel-Lucent Configuration** navigation pane. This page displays all Internet Key Exchange (IKE) profiles currently available for VPN Services. IKE is a part of the IPSEC protocol suite, supporting security for VPNs with a shared session secret that produces security keys.

NOTE

The IKE profile requires the switch to have a Remote Access Points license or a VPN Server license.

Select **Add** to create a new IKE profile, or click the pencil icon next to an existing profile to edit. Table 30 describes the fields on the **Advanced Services** > **VPN Services** > **IKE Add/Edit Detail** page.

Table 30: *Advanced Services > VPN Services > IKE Add/Edit Detail Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the IKE profile is associated. The drop-down menu displays all folders available for association with the IKE services profile.
Name	Blank	Enter the name of the IKE profile.
Other Settings		
IKE Aggressive Group Name		Enter the authentication group name for aggressive mode. Make sure that the group name matches the group name configured in the VPN client software. Aggressive Mode condenses the IKE SA negotiations into three

Field	Default	Description
		packets (versus six packets for Main Mode). A group associates the same set of attributes to multiple clients.
Enable IKE RAP PSKL Refresh/Caching	No	Use this setting to enable refresh and caching for IKE on remote APs.
IKE Shared Secrets		
Add		Select this button to add an IKE shared secret. The following settings appear. Complete these settings and click **Add** in this section. ● **Subnet**–Enter the subnet for the shared secret. ● **Subnet Mask**–Enter the subnet mask for the shared secret. ● **IKE Shared Secret**–Type the shared secret, and confirm.

Select **Add** to create the **VPN Services** > **IKE** profile, or click **Save** to retain the changes to an existing IKE profile. The profile appears on the **Advanced Services** > **VPN Services** > **IKE** page.

Advanced Services > VPN Services > IKE > IKE Policy

Navigate to **Advanced Services** > **VPN Services** > **IKE** > **IKE Policy page** from the **Alcatel-Lucent Configuration** navigation pane to add a new IKE policy, as follows:

Table 31: *Advanced Services > VPN Services > IKE > IKE Policy Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the IKE policy profile is associated. The drop-down menu displays all folders available for association with the IKE Policy profile.
Priority	Blank	Enter the priority number of this IKE policy.
Other Settings		
Encryption		From the drop-down menu, select the encryption type to be supported in the IKE policy. ● DES ● 3DES ● AES128 ● AES192 ● AES256
Hash Algorithm		Select the hash algorithm for this IKE policy. ● MD5 ● SHA ● SHA1-96 ● SHA2-256-128 ● SHA2-384-192 **NOTE:** ‘SHA2-256-128’ and ‘SHA2-384-192’ require an Advanced Cryptography license and a minimum version of 6.1.0.0.
Authentication		AOS-W VPNs support client authentication using pre-shared keys, RSA

Field	Default	Description
		digital certificates, or Elliptic Curve Digital Signature Algorithm (ECDSA) certificates. To set the authentication type for the IKE rule, click the **Authentication** drop-down list and select one of the following types: ● Pre-Share (for IKEv1 clients using pre-shared keys) ● RSA (for clients using certificates) ● ECDSA-256 (for clients using certificates) ● ECDSA-384 (for clients using certificates) **NOTE:** 'ECDSA-256' and 'ECDSA-384' require an Advanced Cryptography license and a minimum version of 6.1.0.0.
Diffie-Hellman Group		Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie Hellman Group for the ISAKMP policy, click the **Diffie Hellman Group** drop-down list and select one of the following groups: ● Group 1: 768-bit Diffie Hellman prime modulus group. ● Group 2: 1024-bit Diffie Hellman prime modulus group. ● Group 19: 256-bit random Diffie Hellman ECP modulus group. ● Group 20: 384-bit random Diffie Hellman ECP modulus group. **NOTE:** 'EC 256-bit (19)' and 'EC 384-bit (20)' require an Advanced Cryptography license and a minimum version of 6.1.0.0.
Lifetime	empty	Set the Security Association Lifetime to define the lifetime of the security association, in seconds.
Version	1	Select 1 to configure the VPN for IKEv1, or 2 for IKEv2.

Advanced Services > VPN Services > L2TP

The combination of Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec) is a highly secure technology that enables VPN connections across public networks such as the Internet. L2TP/IPSec provides both a logical transport mechanism on which to transmit PPP frames as well as tunneling or encapsulation so that the PPP frames can be sent across an IP network. L2TP/IPSec relies on the PPP connection process to perform user authentication and protocol configuration. With L2TP/IPSec, the user authentication process is encrypted using the Data Encryption Standard (DES) or Triple DES (3DES) algorithm.

L2TP/IPSec requires two levels of authentication:

- Computer-level authentication with a preshared key to create the IPSec security associations (SAs) to protect the L2TP-encapsulated data.
- User-level authentication through a PPP-based authentication protocol using passwords, SecureID, digital certificates, or smart cards after successful creation of the SAs.

Navigate to **Advanced Services > VPN Services > L2TP** page from the **Alcatel-Lucent Configuration** navigation pane. This page lists all L2TP profiles that are currently available. Select **Add** to create a new **L2TP** profile, or click the pencil icon next to an existing profile to modify settings. The **Advanced Services > VPN Services > L2TP Add/Edit Details** page contains the following fields, as described in Table 32.

Table 32: *Advanced Services > VPN Services > L2TP Add/Edit Details Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the L2TP profile is associated. The drop-

Field	Default	Description
		down menu displays all folders available for association with the L2TP profile.
Name	Blank	Enter the name of the L2TP profile.
Other Settings		
Enable L2TP	Yes	Enable or disable this L2TP profile.
PPP Authentication Modes	PAP	Select one or more authentication modes to support this L2TP profile.
Primary DNS Server		Enter the IP address of the primary DNS server.
Secondary DNS Server		Enter the IP address of the secondary DNS server.
Primary WINS Server		Enter the IP address of the primary Windows Internet Naming Service (WINS) server.
Secondary WINS Server		Enter the IP address of the secondary WINS server.
Hello Timeout (10-1440 secs)	60	Enter the time, in seconds, at which L2TP authentication times out.
SecurID Token Persistence Timeout (15-10080 Mins)	1440	Enter the time, in minutes, at which the SecurID Token expires. requiring reauthentication.

Select **Add** to complete the L2TP profile, or click **Save** to retain changes to an existing L2TP profile.

Advanced Services > VPN Services > PPTP

Point-to-Point Tunneling Protocol (PPTP) is an alternative to L2TP/IPSec. Like L2TP/IPSec, PPTP provides a logical transport mechanism to send PPP frames as well as tunneling or encapsulation so that the PPP frames can be sent across an IP network. PPTP relies on the PPP connection process to perform user authentication and protocol configuration.

With PPTP, data encryption begins after PPP authentication and connection process is completed. PPTP connections use Microsoft Point-to-Point Encryption (MPPE), which uses the Rivest-Shamir-Aldeman (RSA) RC-4 encryption algorithm. PPTP connections require user-level authentication through a PPP-based authentication protocol (MSCHAPv2 is the currently-supported method).

The PPTP page displays all PPTP profiles that are currently configured for use by VPN services. This page lists the PPTP profile names, the VPN Services that reference these PPTP profiles, and the folder for each PPTP profile. Select **Add** to create a new PPTP profile, or click the pencil icon next to an existing profile to edit. The **Add/Edit Details** page appears.

The **Advanced Services** > **VPN Services** > **PPTP Add/Edit Details** page contains the following fields, as described in Table 33.

Table 33: *Advanced Services > VPN Services > PPTP Add/Edit Details Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the PPTP profile is associated. The menu

Field	Default	Description
		displays all folders available for association with the PPTP profile.
Name	Blank	Enter the name of the PPTP profile.
Other Settings		
Enable PPTP	Yes	Enable or disable this PPTP profile.
Echo Timeout (10-300 sec)	60	Define the PPTP echo timeout, which is the time between request and sending echo reply. Should this require more time than specified in this field, the PPTP session times out.
PPP Authentication MSCHAP	No	Enable or disable the MSCHAP authentication protocol for this PPTP profile.
PPP Authentication MSCHAPv2	Yes	Enable or disable the MSCHAPv2 authentication protocol for this PPTP profile.
Primary DNS Server		Enter the IP address of the primary DNS server.
Secondary DNS Server		Enter the IP address of the secondary DNS server.
Primary WINS Server		Enter the IP address of the primary Windows Internet Naming Service (WINS) server.
Secondary WINS Server		Enter the IP address of the secondary WINS server.

Select **Add** to create the PPTP profile, or click **Save** to preserve changes to an existing profile. The PPTP profile appears on the **Advanced Services** > **VPN Services** > **PPTP** page.

Advanced Services > VPN Services > IPSEC

The combination of Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec) is a highly secure technology that enables VPN connections across public networks such as the Internet. L2TP/IPSec provides both a logical transport mechanism on which to transmit PPP frames as well as tunneling or encapsulation so that the PPP frames can be sent across an IP network. L2TP/IPSec relies on the PPP connection process to perform user authentication and protocol configuration. With L2TP/IPSec, the user authentication process is encrypted using the Data Encryption Standard (DES) or Triple DES (3DES) algorithm.

L2TP/IPSec requires two levels of authentication:

- Computer-level authentication with a preshared key to create the IPSec security associations (SAs) to protect the L2TP-encapsulated data.
- User-level authentication through a PPP-based authentication protocol using passwords, SecureID, digital certificates, or smart cards after successful creation of the SAs.

Navigate to **Advanced Services** > **VPN Services** > **IPSEC** from the **Alcatel-Lucent Configuration** navigation pane. This page displays the IPSEC profile name, the VPN services that use the IPSEC profile, and the folder associated with the IPSEC Profile.

Select **Add** to create a new **IPSEC** profile, or click the pencil icon next to an existing profile to modify settings. The **Add/Edit Details** page contains the following fields, as described in Table 34:

Table 34: *Advanced Services > VPN Services > IPSEC Add/Edit Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the IPSEC profile is associated. The drop-down menu displays all folders available for association with the IPSEC profile.
Name	Blank	Enter the name of the IPSEC profile.
Other Settings		
Maximum MTU Size (1034-1500 bytes)	1500	Define the Maximum transmission unit (MTU) size in bytes.
Dynamic Maps		
Dynamic Maps		Select one or more dynamic maps that the IPSEC profile is to reference. You can add or edit dynamic maps as required. Refer to "Advanced Services > VPN Services > IPSEC > Dynamic Map" on page 78.

Select **Add** to complete the creation of the IPSEC profile, or click **Save** to retain the changes to the IPSEC profile. This profile appears on the **Advanced Services** > **VPN Services** > **IPSEC** page.

Advanced Services > VPN Services > IPSEC > Dynamic Map

VPN Services may reference IPSEC profiles. IPSEC profiles reference Dynamic Maps, and Dynamic Maps reference Transform Sets. This interrelationship is conveyed in the navigation pane of **Device Setup** > **Alcatel-Lucent Configuration.**

Dynamic maps establish policy templates that are used during negotiation requests in IPSEC. This occurs during security associations from a remote IPSEC peer in the VPN, even when all cryptographic map parameters are not known during new security associations from a remote IPSEC peer. For instance, if you do not know about all the IPSec remote peers in your network, a Dynamic Map allows you to accept requests for new security associations from previously unknown peers. Note that these requests are not processed until the IKE authentication has completed successfully. In short, a Dynamic Map is a policy template used by IPSEC profiles. Dynamic Maps are not used for initiating IPSEC security associations, but for determining whether or not traffic should be protected in the VPN.

To view Dynamic Maps that are currently configured, navigate to **Advanced Services** > **VPN Services** > **IPSEC** > **Dynamic Map**. This page lists dynamic map names, IPSEC profiles that reference them, and the folder.

Select **Add** to create a new **Dynamic Map**, or click the pencil icon next to an existing map to modify settings. The **Add/Edit Details** page contains the fields as described in Table 35:

Table 35: *Advanced Services > VPN Services > IPSEC > Dynamic Map Add/Edit Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the Dynamic Map is associated. The drop-down menu displays all folders available for association with the Dynamic Map.
Name	Blank	Enter the name of the Dynamic Map.

Field	Default	Description
Other Settings		
Priority		Specify the priority in which this Dynamic Map should be processed in relation to additional Dynamic Maps that may be configured and used by IPSEC profiles.
Diffie-Hellman Group		Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie Hellman Group for the ISAKMP policy, click the **Diffie Hellman Group** drop-down list and select one of the following groups: ● Group 1: 768-bit Diffie Hellman prime modulus group. ● Group 2: 1024-bit Diffie Hellman prime modulus group. ● Group 19: 256-bit random Diffie Hellman ECP modulus group. ● Group 20: 384-bit random Diffie Hellman ECP modulus group. **NOTE:** ‘EC 256-bit (19)’ and ‘EC 384-bit (20)’ require an Advanced Cryptography license and a minimum version of 6.1.0.0.
Lifetime (300-86400 sec)		Define the lifetime in seconds for the dynamic map, when deployed in IPSEC profiles.
Transform Set 1-4		From the drop-down menu, select up to four transform sets in the sequence in which they should be referenced by the Dynamic Map. You can add a new Transform Set by clicking the add icon, or you can edit an existing Transform Set by clicking the pencil icon. Refer to "Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set" on page 79.
Version	1	Select 1 to configure the VPN for IKEv1, or 2 for IKEv2.

Select **Add** to complete the creation of the Dynamic Map, or click **Save** to retain changes to an existing Dynamic Map.

Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set

VPN Services may reference IPSEC profiles. Transform sets define the encryption and hash algorithm to be used by a dynamic map in an IPSEC profile that supports VPN Services.

Navigate to **Advanced Services** > **VPN Services** > **IPSEC** > **Dynamic Map** > **Transform Set** from the **Alcatel-Lucent Configuration** navigation pane. This page displays all currently configured Transform Sets, and which Dynamic Maps reference them.

Select **Add** to create a new **Transform Set**, or click the pencil icon next to an existing Transform Set to modify settings. The **Add/Edit Details** page contains the following fields, as described in Table 36:

Table 36: *Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set Add/Edit Details Fields and Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the Transform Set is associated. The drop-down menu displays all folders available for association with the Transform Set.

Field	Default	Description
Name	Blank	Enter the name of the Transform Set.
Other Settings		
Encryption	168-bit 3DES-CBC	Select the encryption for the transform set from the drop-down menu.
Hash Algorithm	SHA (HMAC Variant)	Select the hash algorithm from the drop-down menu.

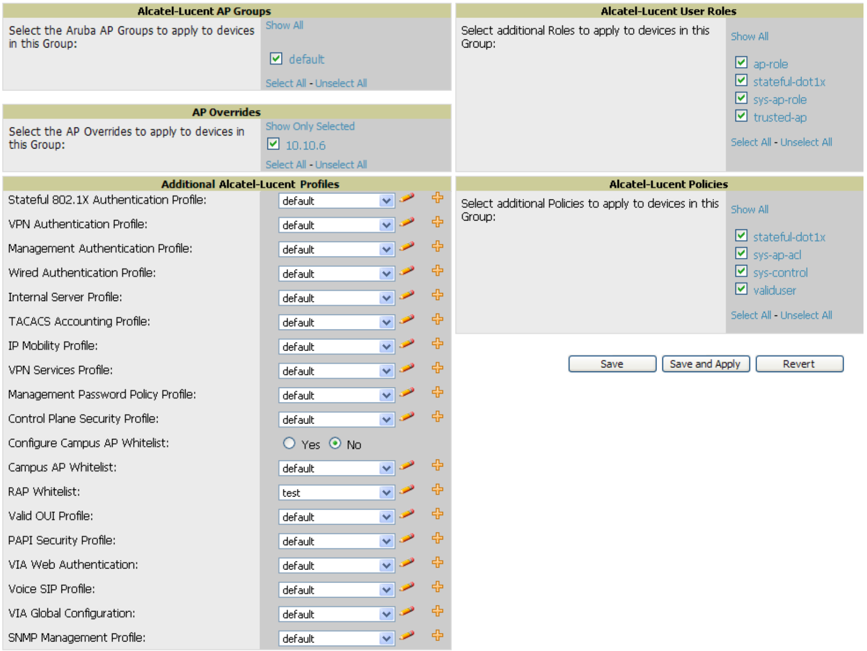
Select **Add** to create the new Transform Set, or click **Save** if editing an existing Transform Set. The Transform Set is available for reference by Dynamic Maps in support of IPSEC profiles and VPN services.

Groups > Alcatel-Lucent Config Page

With Global Alcatel-Lucent Configuration enabled in **OV3600 Setup > General**, create Alcatel-Lucent AP Groups with the **Device Setup > Alcatel-Lucent Configuration** page, as described in earlier in this document. To view and edit profile assignments for Alcatel-Lucent AP Groups, perform these steps.

1. Navigate to the **Groups > List** page.
2. Select the name of the Alcatel-Lucent AP Group to view and edit, and navigate to the **Alcatel-Lucent Config** page, illustrated in Figure 28:

Figure 28 *Groups > List > Alcatel-Lucent Config Page Illustration*



Alcatel-Lucent AP Groups

Select the Aruba AP Groups to apply to devices in this Group: Show All

☑ default

Select All - Unselect All

AP Overrides

Select the AP Overrides to apply to devices in this Group: Show Only Selected

☑ 10.10.6

Select All - Unselect All

Additional Alcatel-Lucent Profiles

Stateful 802.1X Authentication Profile:	default
VPN Authentication Profile:	default
Management Authentication Profile:	default
Wired Authentication Profile:	default
Internal Server Profile:	default
TACACS Accounting Profile:	default
IP Mobility Profile:	default
VPN Services Profile:	default
Management Password Policy Profile:	default
Control Plane Security Profile:	default
Configure Campus AP Whitelist:	○ Yes ● No
Campus AP Whitelist:	default
RAP Whitelist:	test
Valid OUI Profile:	default
PAPI Security Profile:	default
VIA Web Authentication:	default
Voice SIP Profile:	default
VIA Global Configuration:	default
SNMP Management Profile:	default

Alcatel-Lucent User Roles

Select additional Roles to apply to devices in this Group: Show All

☑ ap-role
☑ stateful-dot1x
☑ sys-ap-role
☑ trusted-ap

Select All - Unselect All

Alcatel-Lucent Policies

Select additional Policies to apply to devices in this Group: Show All

☑ stateful-dot1x
☑ sys-ap-acl
☑ sys-control
☑ validuser

Select All - Unselect All

3. Complete the profile assignments on this page, referring to additional topics in this appendix for additional information. Table 37 provides a summary of topics supporting these settings.

Table 37: *Information Resources for the Groups > List > Alcatel-Lucent Config Page*

Section	Additional Information Available In These Locations
Alcatel-Lucent AP Groups Section	● "Alcatel-Lucent AP Groups" on page 30 ● "Alcatel-Lucent AP Groups Procedures and Guidelines" on page 19 ● "Setting Up Initial Alcatel-Lucent Configuration" on page 13
AP Overrides	● "AP Overrides" on page 34 ● "Supporting APs with Alcatel-Lucent Configuration" on page 21
Alcatel-Lucent User Roles	● "Security > User Roles" on page 45 ● "Visibility in Alcatel-Lucent Configuration" on page 25
Alcatel-Lucent Policies	● "Security > Policies" on page 51 ● "Visibility in Alcatel-Lucent Configuration" on page 25

Index