

OmniVista 3600 Air Manager 8.2



Copyright

© 2016 Alcatel-Lucent. All rights reserved.

Specifications in this manual are subject to change without notice.

Originated in the USA.

AOS-W, Alcatel 4302, Alcatel 4304, Alcatel 4306, Alcatel 4308, Alcatel 4324, Alcatel 4504, Alcatel 4604, Alcatel 4704, Alcatel 6000, OAW-AP41, OAW-AP68, OAW-AP60/61/65, OAW-AP70, OAW-AP80, OAW-AP92/93, OAW-AP105, OAW-AP120/121, OAW-AP124/125, OAW-AP175, OAW-IAP92/93/105, OAW-RAP2, OAW-RAP5, and Omnivista 3600 Air Manager are trademarks of Alcatel-Lucent in the United States and certain other countries.

Any other trademarks appearing in this manual are the property of their respective companies. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al.

Controller Configuration in OV3600	7
Requirements, Restrictions, and AOS-W Support in OV3600	7
Requirements	7
Restrictions	7
AOS-W Support in OV3600	7
Overview of Alcatel-Lucent Configuration in OV3600	8
Device Setup > Alcatel-Lucent Configuration Page	9
Groups > Controller Config Page with Global Configuration Enabled	9
Groups > Controller Config when Global Configuration is Disabled	10
Support for Editing Multiple Device Settings	10
Controller Configuration Sections in the Tree View	11
Alcatel-Lucent AP Groups Section	11
AP Overrides Section	12
WLANs Section	12
Profiles Section	13
Security Section	13
Local Config Section	14
Advanced Services Section	14
APs/Devices > List Page	15
APs/Devices > Manage Page	16
APs/Devices > Monitor Page	17
APs/Devices > Audit Page	18
Groups > Basic Page	18
Additional Concepts and Components	18
Global Configuration and Scope	18
Referenced Profile Setup	19
Save, Save and Apply, and Revert Buttons	20
Additional Concepts and Benefits	21
Scheduling Configuration Changes	21
Auditing and Reviewing Configurations	21
Licensing and Dependencies in Alcatel-Lucent Configuration	21
Setting Up Initial Alcatel-Lucent Configuration	21
Prerequisites	22
Procedure	22
Additional Capabilities	25
Alcatel-Lucent Configuration in Daily Operations	27
Alcatel-Lucent AP Groups Procedures and Guidelines	27
Guidelines and Pages for Alcatel-Lucent AP Groups	27
Selecting Alcatel-Lucent AP Groups	27
Configuring Alcatel-Lucent AP Groups	28
General WLAN Guidelines	28
Guidelines and Pages for WLANs in Alcatel-Lucent Configuration	28
General Profiles Guidelines	28
General Controller Procedures and Guidelines	29
Using Master, Standby Master, and Local Controllers	29

Pushing Device Configurations to Controllers	29
Supporting APs with Alcatel-Lucent Configuration	30
AP Overrides Guidelines	30
Changing Adaptive Radio Management (ARM) Settings	30
Changing SSID and Encryption Settings	30
Changing the Alcatel-Lucent AP Group for an AP Device	30
Using OV3600 to Deploy Alcatel-Lucent APs	31
Using General OV3600 Device Groups and Folders	32
Visibility in Alcatel-Lucent Configuration	32
Visibility Overview	32
Defining Visibility for Alcatel-Lucent Configuration	33
Appendix A Controller Configuration Reference	37
Overview	37
Alcatel-Lucent AP Groups	39
About Alcatel-Lucent AP Groups	39
AP Overrides	42
WLANs	47
Overview of WLANs Configuration	47
WLANs	48
WLANs > Basic	48
WLANs > Advanced	48
Profiles	49
Understanding Alcatel-Lucent Configuration Profiles	49
Security	50
Security > User Roles	52
Security > User Roles > BW Contracts	52
Security > User Roles > VPN Dialers	53
Security > Policies	53
Security > Policies > Destinations	53
Security > Policies > Services	53
Security > Server Groups	54
Server Groups Page Overview	54
Supported Servers	54
Adding a New Server Group	55
Security > Server Groups > LDAP	55
Security > Server Groups > RADIUS	55
Security > Server Groups > TACACS	55
Security > Server Groups > Internal	55
Security > Server Groups > XML API	56
Security > Server Groups > RFC 3576	56
Security > Server Groups > Windows	56
Security > TACACS Accounting	56
Security > Time Ranges	57
Security > User Rules	57
Local Config	57
Local Config > Network	58
Local Config > Network > Controller	58
Local Config > Network > VLANs	58
Local Config > Network > Ports/Interfaces	59
Local Config > Network > IP	59

Local Config > Management	59
Local Config > Management >General	59
Local Config > Management >Administration	59
Local Config > Management >SNMP	60
Local Config > Management> Logging	60
Local Config > Management> Clock	60
Local Config > Advanced >Redundancy	60
Advanced Services	61
Advanced Services > AirGroup	61
Advanced Services > AirGroup > CPPM Server AAA	62
Advanced Services > AirGroup > Domain	62
Advanced Services > AirGroup > Service	62
Advanced Services > IP Mobility	63
Advanced Services > IP Mobility > Mobility Domain	63
Advanced Services > VPN Services	64
Advanced Services > VPN Services > IKE Profile	64
Advanced Services > VPN Services > IKE > Site to Site IKE	65
Advanced Services > VPN Services > IKE > IKE Policy	65
Advanced Services > VPN Services > IPSEC Profile	65
Advanced Services > VPN Services > IPSEC > Dynamic Map	66
Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set	66
Advanced Services > VPN Services > L2TP Profile	66
Advanced Services > VPN Services > PPTP Profile	67
Groups > Controller Config Page	67
Index	69

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



When configuring the controller, we recommend that you have access to the *Alcatel-Lucent AOS-W User Guide* and the *Alcatel-Lucent AOS-W CLI Guide* to use as a reference.

The Alcatel-Lucent Configuration feature in OV3600 consolidates 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 7](#)
- ["Additional Concepts and Components" on page 18](#)
- ["Setting Up Initial Alcatel-Lucent Configuration" on page 21](#)



OV3600 supports Alcatel-Lucent AP Groups, which should not be confused with standard Alcatel-Lucent Device Groups. This document provides information about the configuration and use of Alcatel-Lucent AP Groups and describes how Alcatel-Lucent AP Groups inter-operate with standard Alcatel-Lucent 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 version must be installed and operational on the network.
- Alcatel-Lucent controllers 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 **AirGroup**, **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 controllers.

AOS-W Support in OV3600

OV3600 provides the following options for configuring your devices:

- Template-based configuration for devices with firmware versions before Alcatel-Lucent AOS-W 3.3.2.10
- Global GUI configuration for organizations that have near-identical deployments on all of their controllers
- Group-level GUI configuration for organizations that have two or more configuration strategies

Configuration changes are pushed to the controller via SSH with no reboot required.

OV3600 only supports configuration of the settings that a master controller would push to the standby / local controllers (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, and the WLAN Wizard. Controller IP addresses, VLANs, and interfaces are also supported, as are AirGroup, VPN and IP Mobility Advanced services.

Other features of Alcatel-Lucent Configuration in OV3600 include:

- OV3600 understands AOS-W license dependencies.
- OV3600 supports a variety of Alcatel-Lucent firmware versions. Profiles and fields that are not supported by an older version will not be configured on the controller 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 in the Settings **section** of the **AP/Devices > Manage** page.
- Values for specific fields can be overwritten for individual controllers via overrides on the controller's **APs/Devices > Manage** page.

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 about the AOS-W version supported by each release, see the *OmniVista 3600 Air Manager Release Notes*.

Overview of Alcatel-Lucent Configuration in OV3600

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

OV3600 can be set up on **OV3600 Setup > General > Device Configuration** to configure Alcatel-Lucent devices globally (using the **Device Setup > Alcatel-Lucent Configuration** page) or by Device Group (in the **Groups > Controller Config** page). By default, global Alcatel-Lucent Configuration is enabled, (see [Figure 1](#)).

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

Device Configuration	
Guest User Configuration:	Enabled for device <input type="button" value="v"/>
Allow WMS Offload configuration in monitor-only mode:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow disconnecting users while in monitor-only mode:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use Global Alcatel-Lucent Configuration <small>Changing this setting may require importing configuration on your devices.</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No

OV3600 supports Alcatel-Lucent Configuration with the following pages:

- "Device Setup > Alcatel-Lucent Configuration Page" on page 9—Deploys and maintains *global* Alcatel-Lucent Configuration in OV3600. You can limit the view to a folder.
- "Groups > Controller Config Page with Global Configuration Enabled" on page 9—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 > Controller Config** page manages Alcatel-Lucent AP group and other controller-wide settings defined on the **Device Setup > Alcatel-Lucent Configuration** page.

- If global configuration is disabled, the **Groups > Controller Config** page resembles the **Device Setup > Alcatel-Lucent Configuration** tree navigation (the same sections listed in the previous bullet are available), but the **Groups > Controller Config** pages do not display the **Folder** as a column in the list tables or as a field in the individual profiles.
- "[Groups > Controller Config when Global Configuration is Disabled](#)" on page 10— this page modifies or reboots all devices when Global Alcatel-Lucent Configuration is disabled.
- "[APs/Devices > Manage Page](#)" on page 16—supports device-level settings and changes in OV3600.
- "[APs/Devices > Monitor Page](#)" on page 17—supports device-level monitoring in OV3600.
- "[APs/Devices > Audit Page](#)" on page 18—supports device level configuration importing in OV3600.
- "[Groups > Basic Page](#)" on page 18—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 UI Config are managed here.

Device Setup > Alcatel-Lucent Configuration Page



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

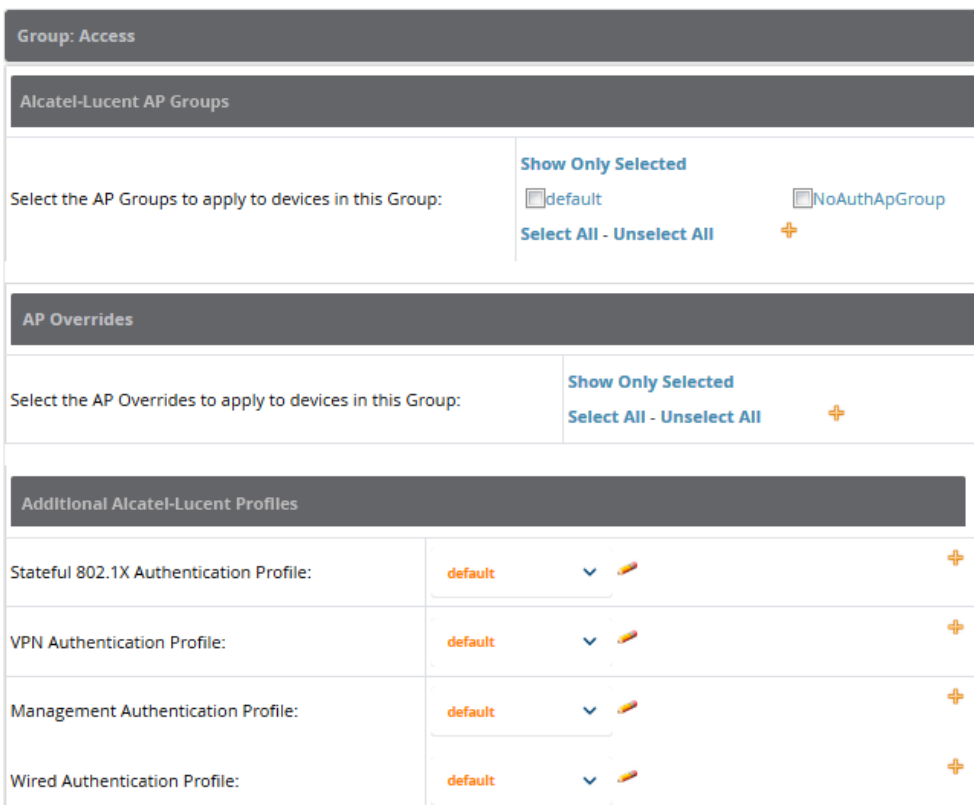
The **Device Setup > Alcatel-Lucent Configuration** page displays the expandable navigation pane shown in , allowing you to monitor and configure Alcatel-Lucent AP Groups, AP Overrides, WLANs, Profiles, Security, Local Config, and Advanced Services. Each section is summarized in "[Controller Configuration Sections in the Tree View](#)" on page 11.

Groups > Controller Config Page with Global Configuration Enabled

When **Use Global Alcatel-Lucent Configuration** is enabled in the **OV3600 Setup > General** page, a focused sub-menu page displays allowing you to edit all configured Alcatel-Lucent AP groups (see [Figure 2](#)):

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

Figure 2: Groups > Controller Config > Alcatel-Lucent AP Groups page illustration (partial display)



Groups > Controller Config when Global Configuration is Disabled

If **Use Global Alcatel-Lucent Configuration** in **OV3600 Setup > General** is set to **No**, the **Groups > Controller 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 "[Controller Configuration Sections in the Tree View](#)" on page 11.

Support for Editing Multiple Device Settings

OV3600 provides support for editing the settings for multiple controllers from one place. This feature is supported only for certain profiles on the controller. The supported profiles and the associated fields are listed in the following table:

Table 1: Editing Multiple Device Settings

Profile Path	Fields
Local Config >Network >VLANS >VLAN profile	VLAN ID
Local Config >Network >IP >Routed Virtual Interface	VLAN Interface ID, IP Address, IP Netmask
Local Config >Network >IP >Default Gateway	Default Gateway
Advanced Services >VPN Services >IKE >IKE Shared Secrets	IKE Shared Secret, Subnet, Subnet Mask
Advanced Services >VPN Services >IPSEC >IPSEC MAP	Source Network Address, Source Network Mask, Local FQDN ID for Aggressive Mode IPSEC Map, Peer Gateway IP Address

To edit these settings for individual devices, click the pencil icon by the profile name to edit the profile, then click the **Modify Per-Device Settings** link. Edit the fields for the selected devices as required, then click **Save**.

Controller Configuration Sections in the Tree View

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



The **Device Setup** > **Controller Config** page is not available if **Use Global Alcatel-Lucent Configuration** is disabled in **OV3600 Setup** > **General**.

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 11
- "AP Overrides Section" on page 12
- "WLANs Section" on page 12
- "Profiles Section" on page 13
- "Security Section" on page 13
- "Local Config Section" on page 14
- "Advanced Services Section" on page 14

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

Alcatel-Lucent AP Groups Section

An Alcatel-Lucent AP Group is a collection of configuration profiles that define specific settings on Alcatel-Lucent controllers 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 **Controller Config** > **Alcatel-Lucent AP Groups** page (see Figure 3).

Figure 3: *Groups > Controller Config > Alcatel-Lucent AP Groups Navigation*

		Name	APs	Used By		
		Search		User Role	RAP Whitelist	Auth
<input type="checkbox"/>		corp	44	-	-	-
<input type="checkbox"/>		corp-11ac	0	-	-	-
<input type="checkbox"/>		corp-no-scanning	0	-	-	-
<input type="checkbox"/>		default	96	-	-	-
<input type="checkbox"/>		NoAuthApGroup	0	-	-	defau



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 share the following characteristics:

- Any Alcatel-Lucent controllers 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 32.
- You can import a controller configuration file from AOS-W for Alcatel-Lucent AP Group deployment in OV3600.

For additional information, see:

- "[Setting Up Initial Alcatel-Lucent Configuration](#)" on page 21
- "[Alcatel-Lucent AP Groups Procedures and Guidelines](#)" on page 27

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.

AP Overrides operate as follows in Alcatel-Lucent Configuration:

- Custom-created AP Overrides appear in the Alcatel-Lucent Configuration navigation pane, as illustrated in .
- Alcatel-Lucent controllers 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 42.

Figure 4: AP Overrides

USED BY			
NAME	GROUP	CONTROLLER	FOLDER
1153-ac	-	-	Top
AP-225	-	-	Top

WLANs Section

Access WLANs with **Alcatel-Lucent Configuration > WLANs**, (see [Figure 5](#)). The following concepts govern the use of WLANs in Alcatel-Lucent configuration:

- WLANs are the same as virtual AP configuration profiles.

- WLAN profiles contain settings including SSIDs, referenced Alcatel-Lucent AP Groups, Traffic Management profiles, and device folders.

WLAN configurations are described in:

- "Setting Up Initial Alcatel-Lucent Configuration" on page 21
- "General WLAN Guidelines" on page 28
- "WLANs" on page 47

Figure 5: Alcatel-Lucent Configuration > WLANs Navigation

USED BY						
NAME	SSID	ARUBA AP GROUP	AP OVERRIDE	TRAFFIC MANAGEMENT	CONTROLLER	FOLDER
<input type="checkbox"/> ALU-AP	0V3600	default	-	-	-	Top
<input type="checkbox"/> default	aruba-ap	default	-	-	-	Top

Profiles Section

Use Profiles to organize and deploy groups of configurations for Alcatel-Lucent AP Groups, WLANs, and other profiles. Profiles are assigned to folders, which establishes visibility to Alcatel-Lucent AP Groups and WLAN settings. Access Profiles with **Alcatel-Lucent Configuration > Profiles** (see Figure 6). 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. Profile procedures and guidelines are described in:

- "Setting Up Initial Alcatel-Lucent Configuration" on page 21
- "General Profiles Guidelines" on page 28
- "Profiles" on page 49

Figure 6: Alcatel-Lucent Configuration > Profiles Navigation

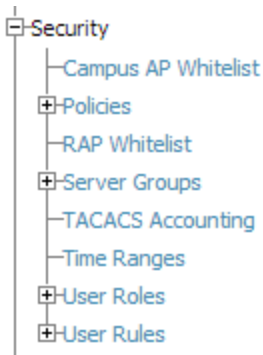
- Profiles
 - AAA
 - AP
 - Controller
 - IDS
 - Mesh
 - QoS
 - RF
 - SSID
 - Wireless LAN

Security Section

Use the **Security** section to add, edit, or delete 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, (see Figure 7). The following general guidelines apply to **Security** profiles in Alcatel-Lucent configuration:

- Roles can have multiple policies, and 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 the rules deployed in AOS-W. For additional information about Security, refer to "Security" on page 50 in the Appendix.

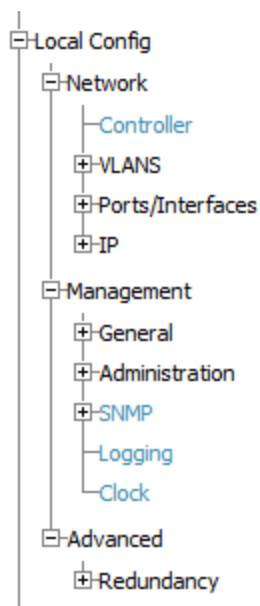
Figure 7: Alcatel-Lucent Configuration > Security Navigation



Local Config Section

Use the Local Config section for local configuration of Alcatel-Lucent controllers (see Figure 3). Locally configured settings are not pushed to local controllers by master controllers. SNMP trap settings for controllers are also managed locally. For additional information, refer to "Local Config" on page 57.

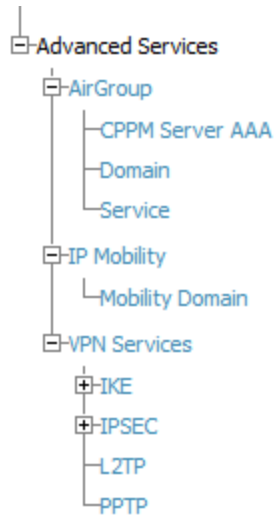
Figure 8: Alcatel-Lucent Configuration > Local Config Navigation



Advanced Services Section

Navigate to Advanced Services with the **Alcatel-Lucent Configuration > Advanced Services** path. The **Advanced Services** section includes AirGroup, IP Mobility and VPN Services (see Figure 9). For additional information about AirGroup, IP Mobility and VPN Services, refer to "Advanced Services" on page 61.

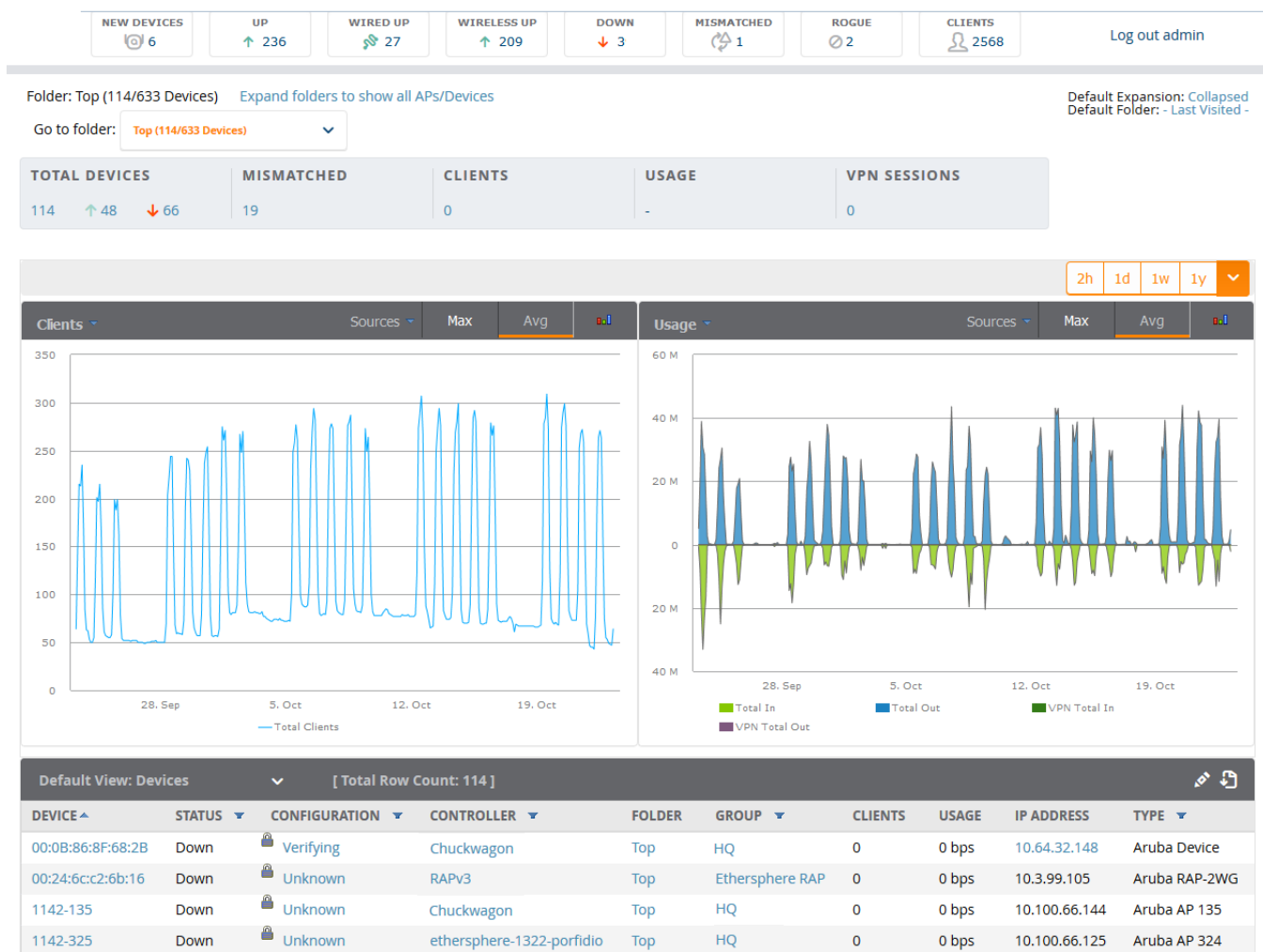
Figure 9: Alcatel-Lucent Configuration > Advanced Services Navigation



APs/Devices > List Page

This page supports all OV3600 devices. This page supports controller reboot, re-provisioning, changing Alcatel-Lucent AP groups, and updating thin AP settings (see [Figure 10](#)). Click the pencil icon () in the Device Table titlebar to perform these tasks and more. The device table also includes an option to configure a custom view using search filters.

Figure 10: APs/Devices List Page (Partial Display)



APs/Devices > Manage Page

This page configures device-level settings, including **Manage** mode, that enable pushing configurations to controllers. For additional information, refer to "Pushing Device Configurations to Controllers" on page 29.

You can create controller 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 or more settings. Controller overrides can be added from the controller's **APs/Devices > Manage** page (see Figure 11).

Figure 11: APs/Devices > Manage Page (Split View)

General	
Name:	ethersphere-1322-porfidio
Status:	Up (OK)
Configuration:	Good
Last Contacted:	1/26/2016 9:10 AM PST
Type:	Aruba 7220
Firmware:	6.4.4.4
Group:	HQ
Folder:	Top
Management Mode:	<input checked="" type="radio"/> Monitor Only + Firmware Upgrades <input type="radio"/> Manage Read/Write
Enable Planned Downtime Mode:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Notes	
<div style="border: 1px solid #ccc; height: 40px;"></div>	
Device Communication	
If this device is down because its IP address or management ports have changed, update ...	
IP Address:	10.11.0.21
SNMP Port (1-65535):	161
SSH Port (1-65535):	22
If this device is down because the credentials on the device have changed, update the fiel... This device is currently using SNMP version 2c.	
Community String:	••••••••
Confirm Community String:	••••••••
SNMPv3 Username:	Enter a Value
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:	1322-Master
Location:	1322
Contact:	1322
Latitude:	Enter a Value
Longitude:	Enter a Value
Altitude (m):	Enter a Value
Group:	Aruba HQ
Folder:	Top
Auto Detect Upstream Device:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Upstream device will automatically be updated when the device is polled.	
Automatically clear Down Status Message w...:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Down Status Message:	<div style="border: 1px solid #ccc; height: 40px;"></div>
Aruba Overrides	
Add New Aruba Controller Override	
Network Settings	
Gateway:	10.11.0.1
Maintenance Windows	
Add New AP Maintenance Window	

Save and Apply
Revert
Delete
Import Settings

Update Firmware
Reboot

APs/Devices > Monitor Page

Used in conjunction with the **Manage** page, the **Monitor** page enables review of device-level settings. The contents of this page varies, depending on the device type being monitored, and can provide a large volume of information, including:

- Status info
- Controller's license link
- Radio statistics about some Alcatel-Lucent thin APs

- **Clients** and **Usage** and interactive graphs showing the numbers of clients connected to the network, and upstream and downstream bandwidth usage over the selected period.
- CPU Utilization and memory utilization interactive graphs.
- APs managed by this controller list (when viewing a controller)
- Alert summary
- An option to poll the controller
- Recent OV3600 Device Events
- Links to the **System Event** and **Audit** Logs
- Information about wired interfaces
- Information about RF Neighbors

For additional information, refer to ["Pushing Device Configurations to Controllers"](#) on page 29.

APs/Devices > Audit Page

Use the **APs/Devices > Audit** page 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 configuration mismatches
- View archived device configurations
- Create and restore flash backups.

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 the Instant WebUI Configuration is not currently running, you can enable the **Enable Instant GUI Config** option in the Alcatel-Lucent Instant section so that the IGC initializes when the OV3600 server starts for the first time.
- If you want to configure your controllers using templates instead, disable Alcatel-Lucent GUI configuration from the **Groups > Basic** page and use template-based configuration. See the *OmniVista 3600 Air Manager 8.2 User Guide* in **Home > Documentation** for more information about templates.

Additional Concepts and Components

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

- ["Global Configuration and Scope"](#) on page 18
- ["Referenced Profile Setup"](#) on page 19
- ["Save, Save and Apply, and Revert Buttons"](#) on page 20
- ["Additional Concepts and Benefits"](#) on page 21

Global Configuration and Scope

OV3600 supports global configuration from both a master-local controller deployment and an all-master-controller deployment:

- In a master-local controller deployment, AOS-W is the agent that pushes global configurations from master controller to local controllers. OV3600 supports this AOS-W functionality.
- In an all-master-controller scenario, every master controller operates independently of other master controllers. OV3600 provides the ability to push configurations to all master controllers 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, see "[General Controller Procedures and Guidelines](#)" on page 29.









































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. For example, after you create an Alcatel-Lucent AP Group from the **Device Setup > Alcatel-Lucent Configuration** page, the **Referenced Profile** section appears (see [Figure 12](#)).

Click the **Add** icon (the plus symbol) on the right to add a referenced profile to a new AP Group. After you click **Save** or **Save and Apply**, OV3600 automatically returns you to the original Alcatel-Lucent AP Group configuration page.

This configuration is also supported on the **Additional Alcatel-Lucent Profiles** section of the **Groups > Controller Config** page.

Figure 12: 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: <small>Requires version ≥ 3.3.0.0 and < 5.0.0.0</small>	default	▼	 
Ethernet Interface 0 Link Profile: <small>Requires version ≥ 3.3.0.0 and < 5.0.0.0</small>	default	▼	 
Ethernet Interface 1 Link Profile: <small>Requires version ≥ 3.3.0.0 and < 5.0.0.0</small>	default	▼	 
AP System Profile:	default	▼	 
Regulatory Domain Profile:	default	▼	 
SNMP Profile: <small>Requires a version earlier than 3.4.0.0</small>	default	▼	 
VoIP Call Admission Control Profile: <small>Requires a Voice Service/Policy Enforcement Firewall license</small>	default	▼	 
802.11a Traffic Management Profile:	--None--	▼	
802.11g Traffic Management Profile:	--None--	▼	
IDS Profile:	ids-low-setting	▼	 
Mesh Radio Profile: <small>Requires an Outdoor Mesh Access Points license</small>	default	▼	 
AP Authorization Profile: <small>Requires a Remote Access Points license and version 5.0.0.0 and above, or RN 3.0</small>	--None--	▼	
AP Provisioning Profile: <small>Requires version 5.0.0.0 and above, or RN 3.0</small>	--None--	▼	
Ethernet Interface 0 Port Configuration: <small>Requires version 5.0.0.0 and above, or RN 3.0</small>	default	▼	 
Ethernet Interface 1 Port Configuration: <small>Requires version 5.0.0.0 and above, or RN 3.0</small>	default	▼	 
Ethernet Interface 2 Port Configuration: <small>Requires version 5.0.0.0 and above, or RN 3.0</small>	shutdown	▼	 
Ethernet Interface 3 Port Configuration: <small>Requires version 5.0.0.0 and above, or RN 3.0</small>	shutdown	▼	 
Ethernet Interface 4 Port Configuration: <small>Requires version 5.0.0.0 and above, or RN 3.0</small>	shutdown	▼	 

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 might see an alert on other Alcatel-Lucent

Configuration pages warning that you have unapplied Alcatel-Lucent Configuration Changes, and that you must click **Save and Apply** to make the changes take effect. You can apply the configuration after all changes are complete.

- **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 controllers in **Manage** mode. If you have controllers 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 Controllers](#)" on page 29.
- **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 Controllers](#)" on page 29.



If your controllers 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 WebUI to the Alcatel-Lucent controllers as a set of CLI commands using Secure Shell (SSH). No controller 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 controller, you can click **Import** from the **APs/Devices > Audit** page to import the controller'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-Lucent controllers. If you push a policy to a controller without this license, a **Good** configuration will not result, and the controller 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.



Alcatel-Lucent Configuration is enabled by default in OV3600.

Prerequisites

- Complete the OV3600 upgrade to OV3600 6.4 or later. Upon upgrade, global Alcatel-Lucent Configuration is enabled by default in groups with devices in monitor-only mode that have AOS-W firmware 3.3.2.10 or greater.
- Back up AOS-W controller configuration file. Information about backing up OV3600 is available in the *OmniVista 3600 Air Manager 8.2 User Guide*.

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 controller 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. If this feature is disabled, the user will only be able to configure Aruba devices using templates.
3. Authorize Alcatel-Lucent controllers into the device group in **Monitor Only** mode, to prevent OV3600 from changing the controllers' configurations.



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

4. Navigate to the **AP/s/Devices > Audit** page for the first controller to and select Import to importing an existing configuration file. [Figure 13](#) illustrates the information available on this page if the device is mismatched.

Figure 13: APs/Devices > Audit Page Illustration

Device Configuration of Chuck in group Access Points in folder Top

This Device is in monitor-only mode.

Configuration read from device at 1/26/2016 10:08 AM PST
 Configuration: Mismatched

Audit Audit the device's current configuration.

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

Create Backup Now Backup device's flash and current configuration.

[More Archived Configs](#)
[View Running Configuration](#)
[View Telnet/SSH Command log](#)

Show entire config

Customize Choose settings to ignore during configuration audits.

AP GROUP SETTINGS		
	CURRENT DEVICE CONFIGURATION	DESIRED CONFIGURATION
AP Group '1341-hq' Virtual AP Profile 'HPE+BYOD' Status	Present	Delete
AP Group 'Ch36-48' Virtual AP Profile 'HPE+BYOD' Status	Present	Delete
WLAN SETTINGS		
	CURRENT DEVICE CONFIGURATION	DESIRED CONFIGURATION
WLAN '1341-HPE+' Status	Present	Delete
WLAN '1341-hq-ARUBA-VISITOR-vap-prof' Hotspot 2.0 Profile	(not set)	default
WLAN '1341-hq-MFA' Hotspot 2.0 Profile	(not set)	default
WLAN '1341-hq-ethersphere-wpa2-vap-prof' Hotspot 2.0 Profile	(not set)	default
WLAN '1344-hq-ethersphere-wpa2-vap-prof' Hotspot 2.0 Profile	(not set)	default
WLAN 'HPE+BYOD' Status	Present	Delete
WLAN 'corp1341-ethersphere-voip-vap_prof' Hotspot 2.0 Profile	(not set)	default
WLAN 'corp1341-ethersphere-wap2-vap_prof' Hotspot 2.0 Profile	(not set)	default
WLAN 'corp1344-ethersphere-voip-vap_prof' Hotspot 2.0 Profile	(not set)	default
WLAN 'corp1344-ethersphere-wap2-vap_prof' Hotspot 2.0 Profile	(not set)	default
WLAN 'default' Hotspot 2.0 Profile	(not set)	default
AAA PROFILE SETTINGS		
	CURRENT DEVICE CONFIGURATION	DESIRED CONFIGURATION

If the page reports a device mismatch, the page will display an **Import** button that allows you to import the Alcatel-Lucent controller settings from an Alcatel-Lucent controller that has already been configured. To import the complete configuration from the controller (including any unreferenced profiles) select the **Include unreferenced profiles** check box. If you deselect the check box, OV3600 will not import those files, and will delete the unreferenced profiles/AP Groups on the controller when that configuration is pushed.

In Global Configuration:

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

In Group Configuration:

Importing the group configuration creates Profiles and Alcatel-Lucent AP Groups in the controller's **Groups > Controller Config** page.

5. After configuration file import is complete, refresh the page to verify the results of the import and add or edit the imported parameters as required.
6. Navigate to the **Controller Configuration** page.
 - This page displays a list of APs authorized on 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 52](#).
 - *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 32](#).
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 New Alcatel-Lucent AP Group** 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.

For additional information about configuring Alcatel-Lucent AP Groups, see ["Alcatel-Lucent AP Groups Procedures and Guidelines" on page 27](#).

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 it can display only selected WLANs.
 - b. Click **Add** to create a WLAN, or click the pencil icon to edit a 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 controller. 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 28](#)
 - ["WLANs" on page 47](#) for details on all WLAN settings
9. Add or edit Alcatel-Lucent Configuration Profiles as required.
 - a. Navigate to the **Alcatel-Lucent Configuration > Profiles** section of the navigation pane.
 - b. Select the type of profile in the navigation pane to configure: **AAA, AP, Controller, 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 controller 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 controllers 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 28](#)

10. Provision multiple Alcatel-Lucent AP Groups on one or more controllers by putting the controllers 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 > Controller 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 27](#)

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

["Selecting Alcatel-Lucent AP Groups" on page 27](#)

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 controller using that controller's OV3600 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 30](#).

13. Navigate to the **APs/Devices > Audit** page for the controller 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.

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 *OmniVista 3600 Air Manager 8.2 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 the following additional resources for more information:

- *Alcatel-Lucent AOS-W User Guide*
- *OmniVista 3600 Air Manager 8.2 User Guide*
- *OmniVista 3600 Air Manager 8.2 Best Practices Guide*

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 21. This chapter emphasizes frequent procedures as follows:

- ["Alcatel-Lucent AP Groups Procedures and Guidelines"](#) on page 27
- ["General WLAN Guidelines"](#) on page 28
- ["General Controller Procedures and Guidelines"](#) on page 29
- ["Supporting APs with Alcatel-Lucent Configuration"](#) on page 30
- ["Visibility in Alcatel-Lucent Configuration"](#) on page 32
- ["Using OV3600 to Deploy Alcatel-Lucent APs"](#) on page 31



For a complete reference on all Configuration pages, field descriptions, and certain additional procedures that are more specialized, refer to ["Controller Configuration Reference"](#) on page 37.

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 39. 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 controller's OV3600 group or to an OV3600 group by themselves.
- All configurations of Alcatel-Lucent AP Groups must be pushed to Alcatel-Lucent controllers to become active on the network.
- Additional dynamics between master, standby master, and local controllers still apply. In this case, refer to ["Using Master, Standby Master, and Local Controllers"](#) on page 29.

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 > Controller 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 27.
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 controllers by clicking **Save and Apply**. The principles of Monitor and Manage mode still apply. For additional information, refer to "[Pushing Device Configurations to Controllers](#)" on page 29.

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 controllers 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 controllers with the steps described in "[Setting Up Initial Alcatel-Lucent Configuration](#)" on page 21.

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 additional information about Profiles, refer to "[Profiles](#)" on page 49.

General Controller Procedures and Guidelines

Using Master, Standby Master, and Local Controllers

OV3600 implements the following general approaches to controllers:

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

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

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

Pushing Device Configurations to Controllers

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

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

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



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 controllers. 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 controller 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 controller.
5. As desired, return devices to Monitor mode until the next set of configuration changes is ready to push to controllers.

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 28](#)
- ["Alcatel-Lucent AP Groups Procedures and Guidelines" on page 27](#)
- ["Profiles" on page 49](#)

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 28](#)
- ["Guidelines and Pages for WLANs in Alcatel-Lucent Configuration" on page 28](#)
- ["Profiles" on page 49](#)

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 controller 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 controller that is to support this AP device. For additional information, refer to ["Pushing Device Configurations to Controllers" on page 29](#).

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 controllers 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 controller. 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 controller 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.
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 the Alcatel-Lucent controller with the **show ap databaseaosw** 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 Group** below the list of the devices, select the appropriate group, and then click **Move**.



If the list of Alcatel-Lucent AP Groups is not there, 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 controllers 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 controller.

Using General OV3600 Device 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.



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:

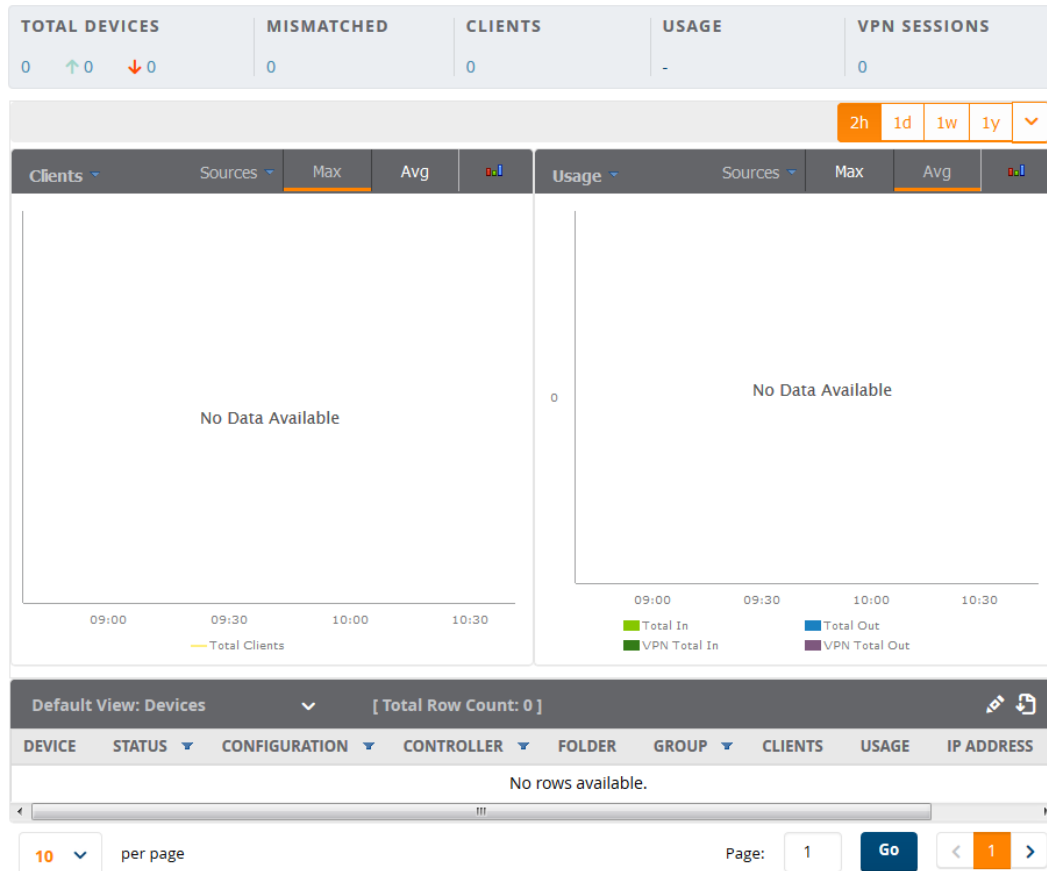
- Administrative and Management users in OV3600 can view the **Alcatel-Lucent Configuration** page and the **APs/Devices > Manage** pages.
 - Administrative users are enabled to view all configurations.
 - Management users have access to all profiles and Alcatel-Lucent AP groups for their respective 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 52](#)
 - ["Security > Policies" on page 53](#)
- OV3600 continues to support the standard operation of folders, users, and user roles as described in the *OmniVista 3600 Air Manager 8.2 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.
 - c. Enter a name for the folder and (optionally) select a parent folder.
 - d. 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 14](#) illustrates an unpopulated device page for an example folder.

Figure 14: APs/Devices > List Page with no devices



2. Add Alcatel-Lucent controller devices to that folder as required. Use the **Device Setup > Add** page following instructions available in the *OmniVista 3600 Air Manager 8.2 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 15](#).

Figure 15: OV3600 Setup > Roles > Add/Edit Role Page Illustration

Security Verification	
Current password for 'admin':	<input type="text"/>
Role	
Name:	<input type="text" value="Enter a Value"/>
Enabled:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Type:	<input type="text" value="AP/Device Manager"/>
AP/Device Access Level:	<input type="text" value="Monitor (Read Only)"/>
Top Folder:	<input type="text" value="Top"/>
RAPIDS:	<input type="text" value="None"/>
VisualRF:	<input type="text" value="Read Only"/>
Aruba Controller Single Sign-on Role:	<input type="text" value="Disabled"/>
Display client diagnostics screens by default:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow user to disable timeout:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow reboot of APs/Devices:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Guest User Preferences	
Allow creation of Guest Users:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow accounts with no expiration:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow sponsor to change sponsorship username:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Custom Message:	<input type="text" value="Enter a Value"/>
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

- 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 controller, 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 controllers 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 8.2 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 8.2 User Guide*.
7. Continue to other elements of Alcatel-Lucent Configuration described in the Reference section of this document.

Overview

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

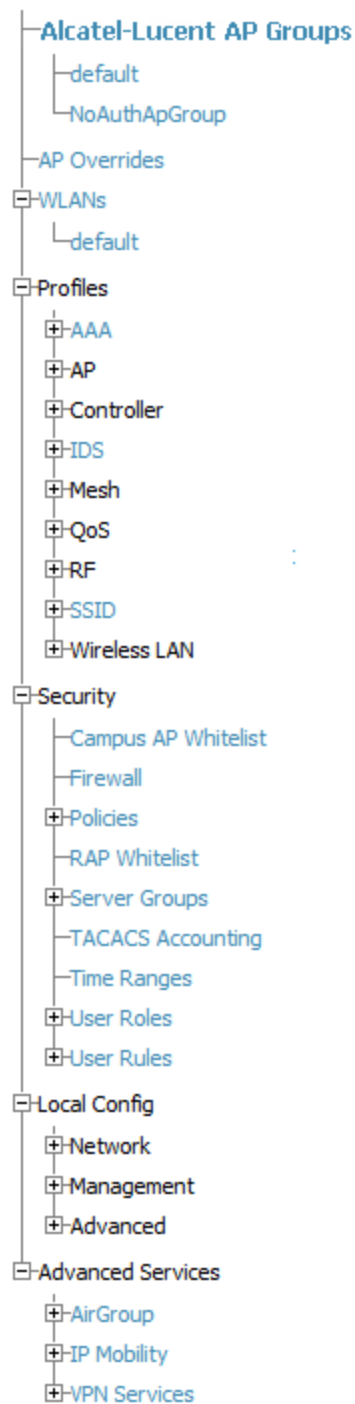
- Controller Configuration components are summarized in "Additional Concepts and Components" on page 18.
- For procedures that use several of these components, refer to earlier chapters in this document.
- For architectural information about AOS-W, refer to the *Alcatel-Lucent AOS-W User Guide*.



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 > Controller Configuration** page, illustrated in [Figure 16](#). The one exception is the additional **Groups > Controller Config** page that you access from the standard OV3600 navigation menu.

Figure 16: Controller Configuration Components



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

- "Groups > Controller Config Page" on page 67
- "Alcatel-Lucent AP Groups" on page 39
- "AP Overrides" on page 42
- "WLANs" on page 47
- "Profiles" on page 49
- "Security" on page 50

- "Local Config " on page 57
- "Advanced Services" on page 61

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 27.

The **Alcatel-Lucent AP Groups** page displays the name of the AP Group, the number of APs in the group, and the User Role, RAP Whitelist, Authorization, and Controller that reference this AP Group.

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, (see [Table 2](#)).

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

Field	Default	Description
General Settings		
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 selected	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.

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

Field	Default	Description
802.11g Radio Profile	2.4_am	<p>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.</p> <p>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.</p> <p>The drop-down menu displays these options:</p> <ul style="list-style-type: none"> • default • nchannel too high • nchannel too low <p>Select the pencil icon next to this field to edit profile settings in the RF > 802.11a/g Radio page.</p>
RF Optimization Profile	default	<p>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.</p> <p>Select the pencil icon next to this field to display the Profiles > RF section and edit these settings as desired.</p>
Event Thresholds Profile	default	<p>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:</p> <ul style="list-style-type: none"> • default • all additional RF profiles currently configured in Alcatel-Lucent Configuration <p>Select the pencil icon next to this field to display the Profiles > RF > Events Threshold section and edit these settings as desired.</p>
Wired AP Profile	default	<p>Controls whether 802.11 frames are tunneled to the controller 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.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Wired page and adjust these settings as desired.</p>

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

Field	Default	Description
Ethernet Interface 0 Link Profile	default	<p>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.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Ethernet Link details page and adjust these settings as desired.</p>
Ethernet Interface 1 Link Profile	default	<p>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.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Ethernet Link details page and adjust these settings as desired.</p>
AP System Profile	default	<p>Defines administrative options for the controller, including the IP addresses of the local, backup, and master controllers, Real-Time Locating Systems (RTLS) server values, and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps.</p> <p>This field is a drop-down menu with the following options:</p> <ul style="list-style-type: none"> ● Non-integer RTLS Server Station Message Frequency ● Too-high RTLS Server Port ● Too-low AeroScout RTLS Server Port ● Too-low RTLS Server Port <p>Select the pencil icon next to this field to display the Profiles > AP > System details page and adjust these settings as desired.</p>
Regulatory Domain Profile	default	<p>Defines an AP's country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Regulatory Domain page and adjust these settings as desired.</p>
SNMP Profile	default	<p>Selects the SNMP profile to associate with this AP group. The drop-down menu lists all SNMP profiles currently enabled in OV3600.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > SNMP page and adjust these settings as desired.</p>
VoIP Call Admission Control Profile	default	<p>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.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Regulatory Domain page and adjust these settings as desired.</p>

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

Field	Default	Description
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	<p>Selects the IDS profile to be associated with the new AP Group. The drop-down menu contains these options:</p> <ul style="list-style-type: none"> ids-disabled ids-high-setting ids -low-setting ids-medium-setting <p>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.</p> <p>Select the pencil icon next to this field to display the Profiles > IDS page and adjust these settings as desired.</p>
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.
Mesh Cluster Profiles		
Add New Mesh Cluster Profile		<p>Select to display a new Mesh Cluster Profile section to this page. This section has two fields, as follows:</p> <ul style="list-style-type: none"> 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. <p>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.</p>

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 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. 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.

Figure 17: Groups > Controller Config > AP Overrides page illustration (partial view)

Adding: AP Override

Folder: Top ▼

Name:

WLANs

Show Only Selected

WLANs: 1.0.0_ethersphere-voip 1.0.0_ethersphere-wpa2
 1.0.0_guest 10.0.0_ethersphere-voip
 11.0.0_ethersphere-voip

Excluded WLANs

Show Only Selected

1.0.0_ethersphere-voip 1.0.0_ethersphere-wpa2
 1.0.0_guest 10.0.0_ethersphere-voip
 11.0.0_ethersphere-voip

Referenced Profiles

802.11a Radio Profile: -Inherit- ▼ +

802.11g Radio Profile: -Inherit- ▼ +

Table 3 describes the fields on the **AP Overrides > Add/Edit Details** page.

Table 3: 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.
WLANs		

Table 3: AP Overrides Add or Edit page fields (Continued)

Field	Default	Description
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 <i>not</i> 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: <ul style="list-style-type: none"> • 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.

Table 3: AP Overrides Add or Edit page fields (Continued)

Field	Default	Description
Event Thresholds Profile	default	<p>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:</p> <ul style="list-style-type: none">• default• all additional RF profiles currently configured in Alcatel-Lucent Configuration <p>Select the pencil icon next to this field to display the Profiles > RF > Events Threshold section and edit these settings as desired.</p>
Wired AP Profile	default	<p>Controls whether 802.11 frames are tunneled to the controller 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.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Wired page and adjust these settings as desired.</p>
Ethernet Interface 0 Link Profile	default	<p>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.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Ethernet Link details page and adjust these settings as desired.</p>
Ethernet Interface 1 Link Profile	default	<p>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.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Ethernet Link details page and adjust these settings as desired.</p>
AP System Profile	default	<p>Defines administrative options for the controller, including the IP addresses of the local, backup, and master controllers, Real-time Locating Systems (RTLS) server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps.</p> <p>This field is a drop-down menu with the following options:</p> <ul style="list-style-type: none">• Non-integer RTLS Server Station Message Frequency• Too-high RTLS Server Port• Too-low AeroScout RTLS Server Port• Too-low RTLS Server Port <p>Select the pencil icon next to this field to display the Profiles > AP > System details page and adjust these settings as desired.</p>

Table 3: AP Overrides Add or Edit page fields (Continued)

Field	Default	Description
Regulatory Domain Profile	default	<p>Defines an AP's country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Regulatory Domain page and adjust these settings as desired.</p>
SNMP Profile	default	<p>Selects the SNMP profile to associate with this AP group. The drop-down menu lists all SNMP profiles currently enabled in OV3600.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > SNMP page and adjust these settings as desired.</p>
VoIP Call Admission Control Profile	default	<p>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.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Regulatory Domain page and adjust these settings as desired.</p>
802.11g Traffic Management Profile	default	<p>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.</p>
802.11a Traffic Management Profile	default	<p>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.</p>
IDS Profile	default	<p>Selects the IDS profile to be associated with the new AP Group. The drop-down menu contains these options:</p> <ul style="list-style-type: none"> • ids-disabled • ids-high-setting • ids -low-setting (the default) • ids-medium-setting <p>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.</p> <p>Select the pencil icon next to this field to display the Profiles > IDS page and adjust these settings as desired.</p>

Table 3: AP Overrides Add or Edit page fields (Continued)

Field	Default	Description
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: <ul style="list-style-type: none"> • default • NoWiredAuthPort • shutdown
Mesh Cluster Profiles		
Add New Mesh Cluster Profile	Hidden by default until the Add button is clicked	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 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 8.2 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 28](#).

The **WLANs** page contains additional information as described in [Table 4](#):

Table 4: *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.
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.
Controller	Lists the controller for the WLAN.
Folder	Name of the folder in which the configuration resides.

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.

Refer to the 802.1X Authentication chapter in the *Alcatel-Lucent AOS-W User Guide* for information about WLAN Configuration. Refer to the "wlan ssid-profile" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

An alternate way to create or edit WLANs is from the **Advanced** page. Refer to ["WLANs > Advanced" on page 48](#).

WLANs > Advanced

From the **Alcatel-Lucent Configuration > WLANs** page, click **Add** to create a new WLAN, then click **Advanced**. The **Advanced** page allows you to configure many more sophisticated settings when creating or

editing WLANs.

Refer to the 802.1X Authentication chapter in the *Alcatel-Lucent AOS-W User Guide* for information about WLAN Configuration. Refer to the "wlan ssid-profile" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

Profiles

Understanding Alcatel-Lucent Configuration Profiles

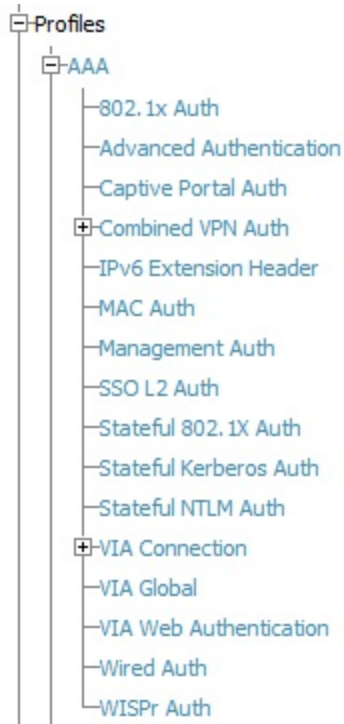
In AOS-W, related configuration parameters are grouped into a profile that you can apply as needed to an AP group or to individual APs. This section lists each category of AP profiles that you can configure and then apply to an AP group or to an individual AP. Note that some profiles reference other 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 > AAA** menu by clicking the plus sign (+) next to it. The following profile options appear:

- 802.1X Auth
- Advanced Authentication
- Captive Portal Auth
- Combined VPN Auth
- IPv6 Extension Header
- MAC Auth
- Management Auth
- SSO L2 Auth
- Stateful 802.1X Auth
- Stateful Kerberos Auth
- Stateful NTLM Auth
- VIA Connection
- VIA Global
- VIA Web Authentication
- Wired Auth
- WISPr Auth

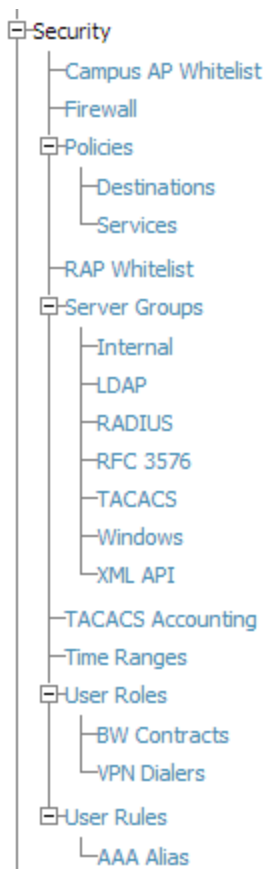
Figure 18: AAA Profiles



Security

Controller Configuration supports user roles, policies, server groups, and additional security parameters with the profiles listed in the **Security** portion of the navigation pane on the **Controller Configuration** page, as illustrated in [Figure 19](#):

Figure 19: 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:

- Campus AP Whitelist
- "Security > Policies" on page 53
 - "Security > Policies > Destinations" on page 53
 - "Security > Policies > Services" on page 53
- Security RAP Whitelist
- "Security > Server Groups" on page 54
 - "Security > Server Groups > Internal" on page 55
 - "Security > Server Groups > LDAP" on page 55
 - "Security > Server Groups > RADIUS" on page 55
 - "Security > Server Groups > RFC 3576" on page 56
 - "Security > Server Groups > TACACS" on page 55
 - "Security > Server Groups > Windows" on page 56
 - "Security > Server Groups > XML API" on page 56
- "Security > TACACS Accounting" on page 56
- "Security > Time Ranges" on page 57
- "Security > User Roles" on page 52
 - "Security > User Roles > BW Contracts" on page 52

- "Security > User Roles > VPN Dialers" on page 53
- "Security > User Rules" on page 57
 - Security > User Rules > AAA Alias

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).



You must install the Policy Enforcement Firewall license in the controller

This page displays the current user roles in Alcatel-Lucent Configuration and where they are used. Select **Add** to create a new user role.

Refer to the Roles and Policies chapter in the *Alcatel-Lucent AOS-W User Guide* for information about roles. Refer to the "user-role" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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 controller (upstream traffic)
- from the controller 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 controller 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.

Select **Add** to create a new **BW Contract** profile,

Refer to the Roles and Policies chapter in the *Alcatel-Lucent AOS-W User Guide* for information about bandwidth contracts. Refer to the "user-role" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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.

Select **Add** to create a new **VPN Dialer** profile,

Refer to the Virtual Private Networks chapter in the *Alcatel-Lucent AOS-W User Guide* for information about VPN Dialers. Refer to the "vpn-dialer" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

Security > Policies

The **Security > Policies** page displays all currently configured policies, including the policy name and the user role, the system, and the controller that use this policy. To create a new policy, click the **Add New Policy** button. To edit an existing policy, click the pencil icon.

Refer to the "ip access-list session" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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.

Refer to the "ip access-list session" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

Security > Policies > Services

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

Select **Add** to create a new Netservice profile, or click the pencil icon next to an existing Netservice profile to edit it.

Refer to the "ip access-list session" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

Security > Server Groups

Server Groups Page Overview

The **Server > Server Groups** page displays all server groups currently configured along with the profiles and controllers that are used by each server group:

- AAA
- Captive Portal Auth
- Stateful Kerberos Auth
- Management Auth
- Stateful NTLM Auth
- Stateful 802.1X Auth
- TACACS Accounting
- VIA Auth
- VPN Auth
- WISPr Auth
- Controller

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 WebUI, 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 controller attempts authentication with the next server in the ordered list. The controller 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 controller (AAA FastConnect).
- Enabling this feature for a large server group list may cause excess processing load on the controller. Best practices are to use server selection based on domain matching whenever possible.
- Certain servers, such as the RSA RADIUS server, lock out the controller 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

Alcatel-Lucent AOS-W supports the following external authentication servers:

- LDAP (Lightweight Directory Access Protocol)
- RADIUS (Remote Authentication Dial-In User Service)
- RFC 3576
- TACACS+ (Terminal Access Controller Access Control System)
- Windows

- XML API

Additionally, you can use the controller'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.

Refer to the Authentication Servers chapter in the *Alcatel-Lucent AOS-W User Guide* for information about servers and server groups. Refer to the "aaa server-group" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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.

Refer to the Authentication Servers chapter in the *Alcatel-Lucent AOS-W User Guide* for information about LDAP. Refer to the "aaa authentication-server ldap" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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. Click **Add** to create a new RADIUS server, or click the pencil icon next to an existing RADIUS server to edit the configuration.

Refer to the Authentication Servers chapter in the *Alcatel-Lucent AOS-W User Guide* for information about RADIUS servers. Refer to the "aaa authentication-server radius" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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 TACACS server, or click the pencil icon next to an existing TACACS server to edit the configuration.

Refer to the Authentication Servers chapter in the *Alcatel-Lucent AOS-W User Guide* for information about TACACS. Refer to the "aaa authentication-server tacacs" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

Security > Server Groups > Internal

An internal server group configures the internal database with the username, password, and role (student, faculty, sysadmin, etc.) 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.

Refer to the Authentication Servers chapter in the *Alcatel-Lucent AOS-W User Guide* for information about internal databases. Refer to the "aaa authentication-server internal" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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.



This profile requires that the controller has an External Services Interface license.

The **Security > Server Groups > XML API** 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.

Refer to the External User Management chapter in the *Alcatel-Lucent AOS-W User Guide* for information about XML API Servers. Refer to the "aaa xml-api" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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.

Refer to the Authentication Servers chapter in the *Alcatel-Lucent AOS-W User Guide* for information about RFC 3576. Refer to the "aaa rfc-3576-server" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

Security > Server Groups > Windows

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

Refer to the Authentication Servers chapter in the *Alcatel-Lucent AOS-W User Guide* for information about Windows servers. Refer to the "aaa authentication-server windows" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

Security > TACACS Accounting

TACACS+ accounting allows commands issued on the controller 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, so a TACACS Server Group must be configured first.

To edit or create a TACACS Accounting profile, navigate to the **Security > TACACS Accounting** page.

Refer to the Authentication Servers chapter in the *Alcatel-Lucent AOS-W User Guide* for information about TACACS Accounting. Refer to the "aaa tacacs-accounting" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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.

Refer to the Creating a Time Range section of the Captive Portal Authentication chapter in the *Alcatel-Lucent AOS-W User Guide* for information about time ranges. Refer to the "time-range" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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.

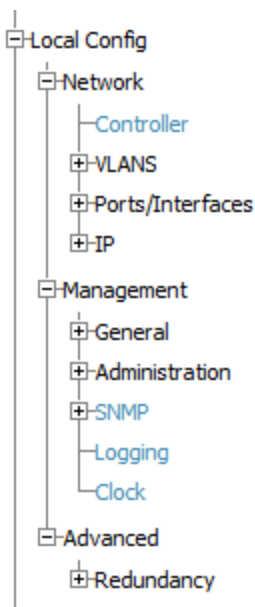
To add a new user rule, which is a derivation profile, click the Add New User Derivation Profile button. To edit an existing user rule, click the pencil icon next to an existing rule.

Refer to the Authentication Servers chapter in the *Alcatel-Lucent AOS-W User Guide* for information about Server Derivation Rules. Refer to the "aaa derivation-rules" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

Local Config

Alcatel-Lucent Configuration in OV3600 supports local configuration of system and network settings for controllers, such as VLANs, Ports and Interfaces, IP addresses and controller management access. This section describes the **Local Config** components in **Alcatel-Lucent Configuration**. For additional information about controller system settings and network configuration settings, refer to the *Alcatel-Lucent AOS-W User Guide*.

Figure 20: Local Config menu



Local Config > Network

This section describes the Local Config Network settings available in the **Device setup > Alcatel-Lucent Config > Network** page.

Local Config > Network > Controller

To configure local controller settings, navigate to the **Local Config > Network > Controller** page. This profile contains the following categories of controller configuration settings:

- **Controller IP details:** Allows you to set the controller IP to the loopback interface address or a specific VLAN interface address. If the controller IP command is not configured, then the controller IP defaults to the loopback interface address. If the loopback interface address is not configured, the controller uses the first configured VLAN interface address.
- **IPsec key:** Define the IPsec key used for secure communication between master and local controllers. Select **Add** to create a new Controller System profile, or click the pencil icon next to an existing profile to edit the configuration
- **Spanning Tree Configuration:** Enables and configures Rapid Spanning Tree Protocol (RSTP) and Per VLAN Spanning Tree (PVST+) settings.

Select **Add** to create a new Controller System profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. For more information, refer to the *Alcatel-Lucent AOS-W User Guide* and the "**controller-ip**" and "**spanning-tree**" commands in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide*.

Local Config > Network > VLANs

To configure local VLAN settings, navigate to the **Local Config > Network > VLANs** page. These profiles contain the following categories of VLAN configuration settings:

- **VLAN Settings:** Define a VLAN ID, VLAN description and associated AAA profile settings.
- **Named VLAN:** Create a VLAN Pool and define an assignment type and list of VLAN IDs for the pool. The **Hash** assignment type means that the VLAN assignment is based on the station MAC address. The **Even** assignment type is based on an even distribution of VLAN pool assignments.

Select **Add** to create a new VLAN or Named VLAN profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. Refer to the *Alcatel-Lucent AOS-W User Guide* and the "vlan" and "vlan-name" commands in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide* for more information about controller VLAN configuration.

Local Config > Network > Ports/Interfaces

Navigate to the **Local Config > Network > Ports/Interfaces** page to edit port settings and the Gigabit Ethernet Interface profiles for Alcatel-Lucent controllers. These profiles contain the following categories of port and interface configuration settings:

- **Gigabit Interface Settings:** Enable or disable the interface, and define switchport modes, duplex settings, access control lists (ACLs), and LACP and LLDP values.
- **Interface Port Channel:** Enable or disable the interface, and define port channel members, ACLs and security settings

Select **Add** to create a new Interface or Port profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. Refer to the *Network Configuration Parameters* chapter of the *Alcatel-Lucent AOS-W User Guide* and the "**interface port-channel**" and "**interface gigabitethernet**" commands in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide* for more information about controller Port and Interface configuration.

Local Config > Network > IP

Navigate to the **Local Config > Network > IP** page to edit settings for the Routed Virtual Interface and Gateway profiles. These profiles contain the following categories of controller connectivity settings:

- **Routed Virtual Interface:** Define how the VLAN obtains its IP address, enable inside NAT addresses, BCMC optimization, Inter-VLAN routing and ARP settings. This profile also allows users to define DHCP helper addresses and enable IGMP and OSPF features.
- **Default Gateway:** Define the default gateway, enable DNS translation.

Select **Add** to create a new IP profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. Refer to the *Network Configuration Parameters* chapter of the *Alcatel-Lucent AOS-W User Guide* and the "**ip default-gateway**" and "**interface vlan**" commands in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide* for more information about controller IP configuration.

Local Config > Management

This section describes the Local Config Management settings available in the **Device setup > Alcatel-Lucent Config > Management** page.

Local Config > Management > General

Navigate to the **Local Config > Management > General** page to create a management server profile for the controller that defines how the OV3600 server or an Analytics Location Engine (ALE) should receive Advanced Monitoring (AMON) protocol messages. The default profiles provided for the OV3600 server (default-amp) and ALE (default-ale) are editable. The **Local Config > Management > General** page also allows you to define management authentication settings for SSH, password and certificate authentication.

Select **Add** to create a new Management Server profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. For details on the configuration settings available in this profile, refer to the *Management Access* chapter of the *Alcatel-Lucent AOS-W User Guide* or the **mgmt-server-profile** command in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide*.

Local Config > Management > Administration

Define controller management users and management user passwords. The settings in this profile also allows network administrators to bypass the enable password prompt and go directly to the privileged commands

(config mode) after logging on to the controller. Select **Add** to create a new management administration profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. For more information, refer to the *Management Access* chapter of the *Alcatel-Lucent AOS-W User Guide* and the **mgmt-user** command in the *Alcatel-Lucent AOS-W Command-line Interface Reference Guide*.

Local Config > Management >SNMP

To configure SNMP Management Profile settings on a controller, navigate to the **Local Config >Management > SNMP** page. Refer to the "Configuring SNMP" section of the Management Access chapter in the *Alcatel-Lucent AOS-W User Guide* for information about SNMP Management. Also refer to the "snmp-server" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available in the SNMP Management profile.

SNMPv3 users are defined in the **Local Config >Management > SNMP > SNMPv3** page. Use this page to view existing SNMPv3 users, or create a new user by defining the authentication type and folder access for that user.

The traps, **apUp** and **apDown**, allow the AP MAC address and the AP name to be added. They support rogue containment so there is no mismatch in the AP list when the AP is in **monitor_only** mode and the IGC is enabled.

Because the error is not set in the configuration response from the AP when the IGC is enabled, the error is displayed by the IGC instead.



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

Local Config > Management> Logging

The Logging profile specifies the IP address of a syslog server to which the controller sends log files, as well as the logging server facility, and the logging levels of the log files that will be sent to the server. By default, the controller sends log files with a severity of **warning** or higher.

Select **Add** to create a new Logging profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. For more information on controller log files, refer to the Management Access chapter of the *Alcatel-Lucent AOS-W User Guide* and the "logging" command in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide*.

Local Config > Management> Clock

The clock profile configured on the **Local Config > Management >Clock** page defines an NTP Server, and timezone settings for the controller .

Select **Add** to create a new Logging profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. For more information on controller log files, refer to the Management Access chapter of the *Alcatel-Lucent AOS-W User Guide* and the "**logging**" command in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide*.

Local Config > Advanced >Redundancy

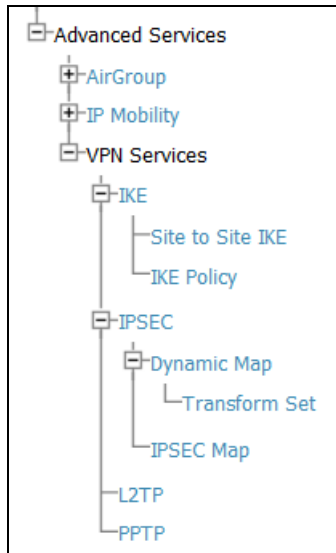
This section contains a configuration profile that defines the Virtual Router Redundancy Protocol (VRRP) values for the controller. You can configure VRRP to support controller redundancy solutions, including pairs of local controllers acting in an active-active mode or a hot-standby mode, a master controller backing up a set of local controllers or a pair of controllers acting as a redundant pair of master controllers in a hot-standby mode.

Select **Add** to create a new IPV4 VRRP profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. For more information, refer to the *Redundancy and VRRPs* chapter of the *Alcatel-Lucent AOS-W User Guide* and the "**vrrp**" command in the *Alcatel-Lucent AOS-W Commmand-line Interface Reference Guide*.

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 AirGroup, IP Mobility and VPN services. For additional information about the AirGroup feature, IP Mobility domains, VPN services, and additional architecture or concepts, refer to the *Alcatel-Lucent AOS-W User Guide*.

Figure 21: *Advanced Services menu*



Advanced Services > AirGroup

AirGroup is a unique enterprise-class capability that leverages zero configuration networking to allow mobile device technologies, such as the AirPrint™ wireless printer service and the AirPlay™ mirroring service, to communicate over a complex access network topology. Controllers running Alcatel-Lucent AOS-W 6.4.0.0 or later can use AirGroup to perform the following functions:

- Discover network services across IP subnet boundaries in enterprise wireless and wired networks.
- Enable users to access the available AirGroup services such as AirPrint and AirPlay.
- Permit users to access conference room Apple TV during presentations, based on group-based access privileges.
- Provide and maintains seamless connectivity of clients and services across VLANs and SSIDs. It minimizes the mDNS traffic across the wired and wireless network, thereby preserving wired network bandwidth and WLAN airtime.

The **Advanced Services > AirGroup** page displays the following categories of parameters for configuring the AirGroup feature:

- AirGroup Global: settings for location discovery and ClearPass PolicyManager (CPPM) configuration.
- Disallowed VLANs: Define VLANs not allowed for use by the AirGroup feature
- AirGroup Services: Enable or disable supported AirGroup services.

Select **Add** to create a new AirGroup profile, or click the pencil icon next to an existing profile to modify settings on an existing profile. Refer to the AirGroup chapter in the *Alcatel-Lucent AOS-W User Guide* and the "airgroup" command in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide* for information about the options that are available on this form.

Advanced Services > AirGroup > CPPM Server AAA

If the Controller is configured to support the ClearPass PolicyManager (CPPM) portal, WLAN administrators can register shared devices such as a conference room Apple TV and printer. The ClearPass Guest portal allows WLAN end users to register their personal devices.

The AirGroup CPPM Server AAA profile configured in the **Advanced Services > AirGroup > CPPM Server AAA** page defines RADIUS and RFC 3576 Server settings for CPPM authentication. Select **Add** to create a new CPPM AAA profile, or click the pencil icon next to an existing profile to view or edit the profile configuration.

Refer to the AirGroup chapter in the *Alcatel-Lucent AOS-W User Guide* and the "airgroup" command in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide* for information about the options that are available on this form. For more information on AirGroup configuration on CPPM, see the *ClearPass Policy Manager User Guide* and *ClearPass Guest Deployment Guide*.

Advanced Services > AirGroup > Domain

An AirGroup domain is a set of controllers that are part of an AirGroup cluster. An administrator can configure multiple AirGroup domains for a site-wide deployment. Individual local controllers can independently select relevant multiple AirGroup domains to form a multi-controller AirGroup cluster.

The AirGroup domain profile configured in the **Advanced Services > AirGroup > Domain** page specifies the IP addresses of devices within a specified domain. Select **Add** to create a new AirGroup Domain profile, or click the pencil icon next to an existing profile to view or edit the profile configuration.

Refer to the AirGroup chapter in the *Alcatel-Lucent AOS-W User Guide* and the **airgroup** command in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide* for information about the options that are available on this form.

Advanced Services > AirGroup > Service

The AirGroup Services profile configured in the **Advanced Services > AirGroup > Services** page configures, enables and disables AirGroup services. (Several AirGroup services are preconfigured and are available as part of the factory default configuration.) The administrator can also enable or disable individual services by using the controller WebUI.

The following services are enabled by default on the controller:

- AirPlay — Apple AirPlay allows wireless streaming of music, video, and slide shows from your iOS device to Apple TV and other devices that support the AirPlay feature.
- AirPrint — Apple AirPrint allows you to print from an iPad, iPhone, or iPod Touch directly to any AirPrint compatible printers.
- ChromeCast — A Wi-Fi-enabled dongle device that connects to a television through an HDMI port to wirelessly stream video and music content from a smart phone (Android and Apple iOS), tablet, laptop or desktop computer device to the TV screen.

The following services are disabled by default on the controller:

- iTunes — iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt — Use this service for remote login, remote management, and FTP utilities on Apple devices.
- Sharing — Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple devices.
- Chat — The iChat (Instant Messenger) application on Apple devices uses this service.
- DLNA Media — Applications such as Windows Media Player use this service to browse and play media content on a remote device.
- DLNA Print — This service is used by printers which support DLNA.

Select **Add** to create a new AirGroup Services profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. Refer to the AirGroup chapter in the *Alcatel-Lucent AOS-W User Guide* and the **airgroup** command in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide* for information about the options that are available on this form.

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.

Refer to the IP Mobility chapter in the *Alcatel-Lucent AOS-W User Guide* for information about IP Mobility. Also refer to the "**ip mobile domain**" command in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide* for information about the options that are available on this form.

Advanced Services > IP Mobility > Mobility Domain

You configure mobility domains on master controllers. All local controllers managed by the master controller share the list of mobility domains configured on the master. Mobility is disabled by default and must be explicitly enabled on all controllers 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 controller with direct access to the user VLAN IP subnet. (Some network topologies may require multiple home agents.)

A best practice is to either configure the switch IP address to match the AP's local controllers or to define the Virtual Router Redundancy Protocol (VRRP) IP address to match the VRRP IP used for controller 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 controllers.

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 controller in the mobility domain providing service for the same user VLAN, you must configure an entry for the VLAN for each controller. 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 controllers. 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 controller to a user-defined domain, it automatically leaves the default mobility domain. If you want a controller 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 controller.

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.

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

Refer to the IP Mobility chapter in the *Alcatel-Lucent AOS-W User Guide* for information about IP Mobility. Also refer to the "**ip mobile**" commands in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on this form.

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-Lucent controllers can be used as a VPN concentrator that terminates all VPN connections from both wired and wireless clients.

You can configure the controllers 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 controllers support 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 controllers 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.

Refer to [Table 5](#) for a list of VPN services that can be configured.

Table 5: *Advanced Services > VPN Services*

Profile Type	Refer to
IKE Profile	Refer to " Advanced Services > VPN Services > IKE Profile " on page 64
IPSEC Profile	Refer to " Advanced Services > VPN Services > IPSEC Profile " on page 65.
L2TP Profile	Refer to " Advanced Services > VPN Services > L2TP Profile " on page 66.
PPTP Profile	Refer to " Advanced Services > VPN Services > PPTP Profile " on page 67.

Advanced Services > VPN Services > IKE Profile

Navigate to the **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.



The IKE profile requires the controller 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.

Refer to the Virtual Private Networks chapter in the *Alcatel-Lucent AOS-W User Guide* for information about IKE.

Advanced Services > VPN Services > IKE > Site to Site IKE

The Site to Site IKE configuration page under **Controller Config > Advanced Services > VPN Services > IKE > Site to Site IKE** as shown in Figure 1. This page lets you configure Site to Site IKE on a controller. Refer to the *Virtual Private Networks* chapter in the *ArubaOS User Guide* for more information about IKE.

Figure 22: Site to Site IKE

Adding: Site to Site IKE

Configure DPD: Yes No

Permit Invalid Certificates: Yes No

Disable Aggressive Mode: Yes No

Disable IP COMP: Yes No
Requires a minimum version of 6.4.3.0

XAuth: Yes No

CA-Certificate for VPN Clients: Certificate Name, type uniqueness conflicts between "Aruba Config" and "Controller Override" may result in pushing unintended certificate to the controller. --None--

Server-Certificate for VPN Clients: Certificate Name, type uniqueness conflicts between "Aruba Config" and "Controller Override" may result in pushing unintended certificate to the controller. --None--

Configure IKE Certificate-Group for VPN C... Yes No

Site to Site IKE Shared Secrets

Add New Site to Site IKE Shared Secret

Advanced Services > VPN Services > IKE > IKE Policy

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

Refer to the *Virtual Private Networks* chapter in the *Alcatel-Lucent AOS-W User Guide* for information about IKE. Also refer to the "vpn-dialer" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on the IKE Policy form.

Advanced Services > VPN Services > IPSEC Profile

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 the **Advanced Services > VPN Services > IPSEC** page 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.

Refer to the Virtual Private Networks chapter in the *Alcatel-Lucent AOS-W User Guide* for information about IPSEC profiles.

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.

Refer to the Virtual Private Networks chapter in the *Alcatel-Lucent AOS-W User Guide* for information about IPSEC Dynamic Maps. Also refer to the "vpn-dialer" command in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on the IPSEC Dynamic Map form.

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.

Refer to the Virtual Private Networks chapter in the *Alcatel-Lucent AOS-W User Guide* for information about Transform Sets.

Advanced Services > VPN Services > L2TP Profile

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 the **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.

Refer to the Virtual Private Networks chapter in the *Alcatel-Lucent AOS-W User Guide* for information about L2TP. Also refer to the "vpn-dialer" and "vpn group pptp" commands in the *Alcatel-Lucent AOS-W CLI Guide* for information about the options that are available on the L2TP Profile form.

Advanced Services > VPN Services > PPTP Profile

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.

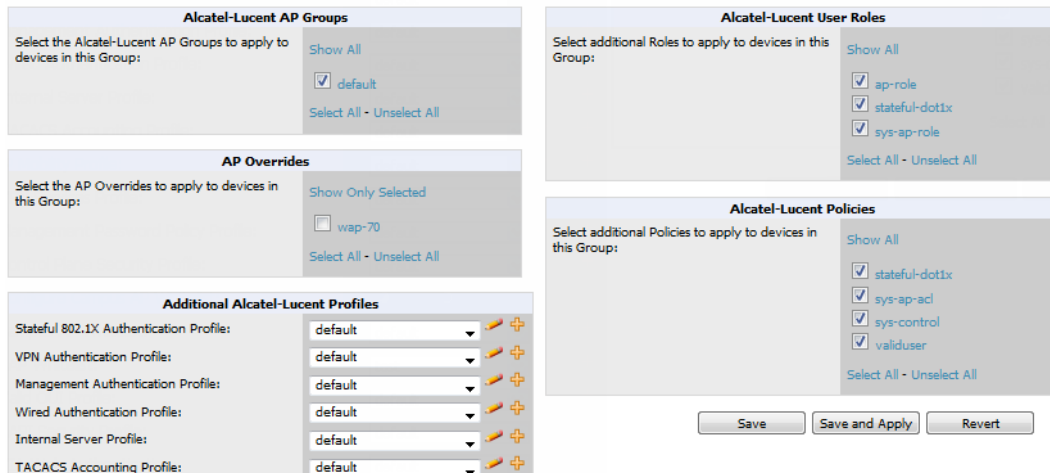
Refer to the Virtual Private Networks chapter in the *Alcatel-Lucent AOS-W User Guide* for information about PPTP. Also refer to the "vpn-dialer" and "vpdn group pptp" commands in the *Alcatel-Lucent AOS-W Command-Line Interface Reference Guide* for information about the options that are available on the PPTP Profile form.

Groups > Controller 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 **Controller Config** page, illustrated in [Figure 23](#):

Figure 23: *Groups > Controller Config Page (partial view)*



3. Complete the profile assignments on this page, referring to additional topics in this appendix for additional information. [Table 6](#) provides a summary of topics supporting these settings.

Table 6: *Information Resources for the Groups > Controller Config Page*

Section	Additional Information Available In These Locations
Alcatel-Lucent AP Groups Section	<ul style="list-style-type: none"> "Alcatel-Lucent AP Groups" on page 39 "Alcatel-Lucent AP Groups Procedures and Guidelines" on page 27 "Setting Up Initial Alcatel-Lucent Configuration" on page 21
AP Overrides	<ul style="list-style-type: none"> "AP Overrides" on page 42 "Supporting APs with Alcatel-Lucent Configuration" on page 30
Alcatel-Lucent User Roles	<ul style="list-style-type: none"> "Security > User Roles" on page 52 "Visibility in Alcatel-Lucent Configuration" on page 32
Alcatel-Lucent Policies	<ul style="list-style-type: none"> "Security > Policies" on page 53 "Visibility in Alcatel-Lucent Configuration" on page 32

A

- Adaptive Radio Management (ARM) 30
- Advanced Services 61
 - defined 14
 - pages and field descriptions 57
- Advanced Services > IP Mobility 61, 63
- Advanced Services > IP Mobility > Mobility Domain 63
- Advanced Services > IP Mobility page 61, 63
- Advanced Services > VPN Services 64
- Advanced Services > VPN Services > IKE 64
- Advanced Services > VPN Services > IKE > IKE Policy 65
- Advanced Services > VPN Services > IKE > Site to Site IKE 65
- Advanced Services > VPN Services > IPSEC 65
- Advanced Services > VPN Services > IPSEC > Dynamic Map 66
- Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set 66
- Advanced Services > VPN Services > L2TP 66
- Advanced Services > VPN Services > PPTP 67
- AMP
 - Additional Capabilities 25
 - Deploy APs 31
 - Setup
 - Device Configuration 8
- AP Groups
 - Configuration 27-28, 30, 39
 - General Procedures and Guidelines 27
 - Selection 27
- AP Overrides
 - guidelines 30
 - pages and field descriptions 42
- APs
 - Using in Groups and Folders 32
- APs/Devices > Audit 18, 29
- APs/Devices > List 8, 10, 15, 30, 33
- APs/Devices > Manage 8, 16, 31, 33
- APs/Devices > Mismatched 29
- APs/Devices > Monitor 17

C

- CLI Commands
 - Controller 7

Configuration

- AirWave 7-8
- AMP 8
- AP Groups 27-28, 30, 39
- Controllers 7, 37
- Device to Controller 29
- Mobility Domains 63
- WLANs 28

Configuration Concepts and Components 18

Configuration Requirements, Restrictions, and Support

- Requirements 7
- Restrictions 7

Configuration Setup 27

Configuration Visibility 32

Contents iii

Controller Procedures 29

Controllers

- Configuration 7, 37
- Global Configuration 18

D

- Define Visibility
 - Aruba Configuration 33
- Deploying APs 31
- Device Configuration
 - Advanced Services 14
 - Folders, Users, and Visibility 21
 - Initial Setup 21
 - Initial Setup Procedure 22
 - Prerequisites 22
 - Profiles 13
 - Push to Controllers 29
 - Security 13
 - WLANs 12
- Device Groups
 - using with APs 32
- Device Setup 9
 - AP Groups 9, 67
 - Aruba Configuration 8, 33, 66
 - Controller Configuration 37
- Device Setup > Communication 31
- Device Setup > Discover 31
- Dynamic Maps 66

E

Encryption 30

F

Folders

Using with APs 32

G

Global Configuration 9, 18

Groups

Controller Config 8-9, 29, 67

Using with APs 32

Groups > Basic 18

Groups > Monitor 29

I

IKE Policy 65

Index 69

M

Modify Devices 31

P

Profiles 28

defined 13

embedded configuration 19

overview 49

pages and field descriptions 49

S

Save, Save and Apply, and Revert Buttons 20

Security

defined 13

pages and field descriptions 50

Security > Policies 53

Security > Policies > Destinations 53

Security > Policies > Services 53

Security > Server Groups 54

Security > Server Groups > Internal 55

Security > Server Groups > LDAP 55

Security > Server Groups > RADIUS 55

Security > Server Groups > RFC 3576 56

Security > Server Groups > TACACS 55

Security > Server Groups > Windows 56

Security > Server Groups > XML API 56

Security > TACACS Accounting 56

Security > Time Ranges 57

Security > User Roles 52

Security > User Roles > BW Contracts 52

Security > User Roles > VPN Dialers 53

Security > User Rules 57

Selecting AP Groups 27

SSIDs 12-13, 24, 30, 42, 47-48

T

Title i

Transform Set 66

V

Visibility 32

W

WLAN Guidelines 28

WLANs 48

defined 12

pages and field descriptions 47

WLANs > Advanced 48

WLANs > Basic 48