



OmniVista 3600 Air Manager

Version 7.3.0

Alcatel-Lucent Configuration Guide

Copyright

© 2011 Alcatel-Lucent. All rights reserved.

Specifications in this manual are subject to change without notice.

Originated in the USA.

AOS-W-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 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.

Legal Notice

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

Preface	7
Document Audience and Organization.....	7
Note, Caution, and Warning Icons	7
Contacting AirWave Wireless and Alcatel-Lucent Networks.....	8
Chapter 1 Alcatel-Lucent Configuration in AirWave	9
Introduction	9
Requirements, Restrictions, and AOS-W Support in AirWave	9
Requirements.....	9
Restrictions	9
AOS-W Support in AirWave.....	9
Overview of Alcatel-Lucent Configuration in AirWave.....	10
Device Setup > Alcatel-Lucent Configuration Page	11
Groups > Alcatel-Lucent Config Page With Global Configuration Enabled	12
Groups > Alcatel-Lucent Config When Global Configuration is Disabled	12
Alcatel-Lucent Configuration Sections in the Tree View.....	13
Alcatel-Lucent AP Groups Section.....	13
AP Overrides Section	14
WLANs Section.....	15
Profiles Section.....	16
Security Section.....	16
Local Config Section	17
Advanced Services Section.....	17
APs/Devices > List Page.....	18
APs/Devices > Manage Page	18
APs/Devices > Monitor Page	19
Groups > Basic Page.....	19
Additional Concepts and Components of Alcatel-Lucent Configuration	20
Global Configuration and Scope.....	20
Referenced Profile Setup in Alcatel-Lucent Configuration	20
Save, Save and Apply, and Revert Buttons.....	21
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	22
Prerequisites	22
Procedure	22
Additional Capabilities of Alcatel-Lucent Configuration	27
Chapter 2 Using Alcatel-Lucent Configuration in Daily Operations	29
Introduction	29
General Alcatel-Lucent AP Groups Procedures and Guidelines	29
Guidelines and Pages for Alcatel-Lucent AP Groups in Alcatel-Lucent Configura- tion.....	29
Selecting Alcatel-Lucent AP Groups	30
Configuring Alcatel-Lucent AP Groups.....	30
General WLAN Guidelines	30
Guidelines and Pages for WLANs in Alcatel-Lucent Configuration	30
General Profiles Guidelines	30

General Controller Procedures and Guidelines.....	31
Using Master, Standby Master, and Local Controllers in Alcatel-Lucent Configuration	31
Pushing Device Configurations to Controllers	31
Supporting APs with Alcatel-Lucent Configuration.....	32
AP Overrides Guidelines	32
Changing Adaptive Radio Management (ARM) Settings	32
Changing SSID and Encryption Settings	32
Changing the Alcatel-Lucent AP Group for an AP Device	32
Using OV3600 to Deploy Alcatel-Lucent APs for the First Time.....	33
Using General OV3600 Device Groups and Folders.....	34
Visibility in Alcatel-Lucent Configuration.....	34
Visibility Overview	34
Defining Visibility for Alcatel-Lucent Configuration.....	35

Appendix A Alcatel-Lucent Configuration Reference 37

Introduction	37
Alcatel-Lucent AP Groups.....	38
Alcatel-Lucent AP Groups.....	38
AP Overrides	42
AP Overrides	42
WLANs	47
Overview of WLANs Configuration.....	47
WLANs	47
WLANs > Basic	48
WLANs > Advanced	48
Profiles	52
Understanding Alcatel-Lucent Configuration Profiles.....	52
Profiles > AAA Overview	52
Profiles > AAA	53
Profiles > AAA > 802.1x Auth.....	55
Profiles > Advanced Authentication.....	60
Profiles > AAA > Captive Portal Auth.....	61
Profiles > AAA > IPv6 Extension Header.....	63
Profiles > AAA > MAC Auth.....	64
Profiles > AAA > Stateful 802.1X Auth	65
Profiles > AAA > Wired Auth	66
Profiles > AAA > Combined VPN Auth.....	66
Profiles > AAA > Management Auth.....	67
Profiles > AAA > Stateful NTLM Auth.....	68
Profiles > AAA > WISPr Auth.....	69
Profiles > AP.....	70
Profiles > AP > Authorization	71
Profiles > AP > Ethernet Link	72
Profiles > AP > Provisioning.....	73
Profiles > AP > Regulatory Domain.....	74
Profiles > AP > SNMP	75
Profiles > AP > SNMP > SNMP User	76
Profiles > AP > System	76
Profiles > AP > Wired Port	80
Profiles > AP > Wired	81
Profiles > IDS	82
Profiles > IDS > General.....	84
Profiles > IDS > Signature Matching.....	85
Profiles > IDS > Signature Matching > Signature	86
Profiles > IDS > Denial of Service	87
Profiles > IDS > Denial of Service > Rate Threshold.....	90
Profiles > IDS > Impersonation	91
Profiles > IDS > Unauthorized Device.....	92
Profiles > Mesh	95

Profiles > Mesh > Cluster.....	96
Profiles > Mesh > Radio.....	96
Profiles > Mesh > Radio > Mesh HT SSID.....	99
Profiles > QoS.....	100
Profiles > QoS > Traffic Management.....	101
Profiles > QoS > VoIP Call Admission Control	101
Profiles > QoS > WMM Traffic Management	103
Profiles > RF.....	104
Profiles > RF > 802.11a/g Radio.....	105
Profiles > RF > 802.11a/g Radio > AM Scanning	109
Profiles > RF > 802.11a/g Radio > ARM.....	110
Profiles > RF > 802.11a/g Radio > HT Radio.....	113
Profiles > RF > 802.11a/g Radio > Spectrum.....	114
Profiles > RF > Event Thresholds	115
Profiles > RF > Optimization	117
Profiles > SSID.....	119
Profiles > SSID.....	119
Profiles > SSID > EDCA AP	124
Profiles > SSID > EDCA Station.....	127
Profiles > SSID > HT SSID	130
Profiles > SSID > 802.11K	131
Security.....	133
Security > User Roles	134
Security > User Roles > BW Contracts.....	136
Security > User Roles > VPN Dialers	137
Security > Policies	140
Security > Policies > Destinations	142
Security > Policies > Services.....	142
Security > Server Groups.....	143
Server Groups Page Overview	143
Supported Servers.....	144
Adding a New Server Group.....	144
Security > Server Groups > LDAP	146
Security > Server Groups > RADIUS	147
Security > Server Groups > TACACS	148
Security > Server Groups > Internal.....	149
Security > Server Groups > XML API.....	150
Security > Server Groups > RFC 3576	150
Security > Server Groups > Windows.....	151
Security > TACACS Accounting	151
Security > Time Ranges.....	152
Security > User Rules	153
Local Config of SNMP Management.....	155
Advanced Services.....	157
Overview of IP Mobility Domains	157
Advanced Services > IP Mobility	158
Advanced Services > IP Mobility > Mobility Domain	160
Advanced Services > VPN Services	161
Advanced Services > VPN Services > IKE.....	163
Advanced Services > VPN Services > IKE > IKE Policy	164
Advanced Services > VPN Services > L2TP.....	165
Advanced Services > VPN Services > PPTP	165
Advanced Services > VPN Services > IPSEC.....	166
Advanced Services > VPN Services > IPSEC > Dynamic Map	167
Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set.....	168
Groups > Alcatel-Lucent Config Page and Section Information	170
Index.....	171

Document Audience and Organization

This configuration guide is intended for wireless network administrators and helpdesk personnel who deploy AOS-W on the network and wish to manage it with the OmniVista 3600 Air Manager (OV3600). OV3600 versions 6.3 and later support Alcatel-Lucent Configuration. This document provides instructions for using Alcatel-Lucent Configuration and contains the following chapters:

Table 1 *Document Organization and Purposes*

Chapter	Description
Chapter 1, “Alcatel-Lucent Configuration in OV3600” on page 9	Introduces the concepts, components, navigation, and initial setup of Alcatel-Lucent Configuration.
Chapter 2, “Using Alcatel-Lucent Configuration in Daily Operations” on page 27	Provides a series of procedures for configuring, modifying, and using Alcatel-Lucent Configuration once initial setup is complete. This chapter is oriented around the most common tasks in Alcatel-Lucent Configuration.
Appendix A, “Alcatel-Lucent Configuration Reference” on page 35	Provides an encyclopedic reference to the fields, settings, and default values of all Alcatel-Lucent Configuration components, to include a few additional procedures supporting more advanced configurations.

Note, Caution, and Warning Icons

This document uses the following notice icons to emphasize advisories for certain actions, configurations, or concepts:



Indicates helpful suggestions, pertinent information, and important things to remember.



Indicates a risk of damage to your hardware or loss of data.



Indicates a risk of personal injury or death.

Contacting Alcatel-Lucent

Table 2 *Contact Information*

Online Contact and Support	
Main Website	http://www.alcatel-lucent.com/enterprise
Support Website	http://service.esd.alcatel-lucent.com
Alcatel-Lucent Enterprise Service and OmniVista 3600 Email Support	Esd.support@alcatel-lucent.com

Introduction

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

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](#)
- [Additional Concepts and Components of Alcatel-Lucent Configuration](#)
- [Setting Up Initial Alcatel-Lucent Configuration](#)



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

Requirements, Restrictions, and AOS-W Support in OV3600

Requirements

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

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

Restrictions

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

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

AOS-W Support in OV3600

OV3600 provides three options for configuring Alcatel-Lucent devices:

- Template-based configuration for devices with firmware versions before AOS-W 3.3.2.10
- Global GUI config for organizations who have near-identical deployments on all of their controllers

- Group-level GUI config for organizations who have two or more configuration strategies
- Configuration changes are pushed to the switch via SSH with no reboot required.

OV3600 only supports configuration of the settings which a master switch would push to the standby / local controllers (global features). OV3600 supports all master, master-standby, and master-local deployments.

All settings for Profiles, Alcatel-Lucent AP Groups, Servers and Roles are supported, as is the AOS-W WLAN Wizard. Switch IP addresses, VLANs, and interfaces are not supported, nor are Advanced Services with the exception of VPN and IP Mobility.

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

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

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

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

Overview of Alcatel-Lucent Configuration in OV3600

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

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

Figure 1 OV3600 Setup > General Setting for Global or Group Alcatel-Lucent Configuration

Device Configuration	
Guest User Configuration:	Enabled for devices in Mai <input type="text"/>
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
Allow non-UTF8 characters:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use Global Alcatel-Lucent Configuration: Changing this setting may require importing configuration on your devices.	<input checked="" type="radio"/> Yes <input type="radio"/> No

OV3600 supports Alcatel-Lucent Configuration with the following pages:

- [Device Setup > Alcatel-Lucent Configuration Page](#)—deploys and maintains *global* Alcatel-Lucent Configuration in OV3600. You can limit the view to a folder.
- [Groups > Alcatel-Lucent Config Page With Global Configuration Enabled](#)—the way this page displays depends on whether global or group configuration is enabled in **OV3600 Setup > General > Device Configuration**:

- If global configuration is enabled, the **Groups > Alcatel-Lucent Config** page manages Alcatel-Lucent AP group and other switch-wide settings defined on the **Device Setup > Alcatel-Lucent Configuration** page.
- If global configuration is disabled, the **Groups > Alcatel-Lucent Config** page resembles the **Device Setup > Alcatel-Lucent Configuration** tree navigation (the same sections listed in the previous bullet are available), but the **Groups > Alcatel-Lucent Config** pages do not display the **Folder** as a column in the list tables or as a field in the individual profiles.
- **Groups > Alcatel-Lucent Config When Global Configuration is Disabled**— this page modifies or reboots all devices when Global Alcatel-Lucent Configuration is enabled.
- **APs/Devices > Manage Page**—supports device-level settings and changes in OV3600.
- **APs/Devices > Monitor Page**—supports device-level monitoring in OV3600.
- **APs/Devices > Audit Page**—supports device level configuration importing in OV3600.
- **Groups > Basic Page**—For device groups containing Alcatel-Lucent devices, basic information such as the group’s name, regulatory domain, the use of Global Groups, SNMP Polling periods, and turning on the Alcatel-Lucent GUI Config are managed here.

Device Setup > Alcatel-Lucent Configuration Page



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

The **Device Setup > Alcatel-Lucent Configuration** page uses an expandable navigation pane to support Alcatel-Lucent AP Groups, AP Overrides, WLANs, Profiles, Security, Local Config, and Advanced Services. Each of these sections is summarized in “[Alcatel-Lucent Configuration Sections in the Tree View](#)” on page 13.

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

Limit to Folder: Top

Alcatel-Lucent AP Groups

- default
- NoAuthApGroup

AP Overrides

WLANs

Profiles

Security

Local Config

Advanced Services

Add New Alcatel-Lucent AP Group

1-2 of 2 Alcatel-Lucent AP Groups Page 1 of 1 Choose columns Export CSV

	Name	Number of APs	Group	User Role	Used By		
					RAP Whitelist	Authorization	Controller
<input type="checkbox"/>	default	4	Access Points	-	-	-	-
<input type="checkbox"/>	NoAuthApGroup	0	-	-	-	default	-

1-2 of 2 Alcatel-Lucent AP Groups Page 1 of 1

Select All - Unselect All

Delete

Groups > Alcatel-Lucent Config Page With Global Configuration Enabled

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

- Alcatel-Lucent AP Groups must be defined from the **Device Setup > Alcatel-Lucent Configuration** page before they are visible on the **Groups > Alcatel-Lucent Config** page.
- Use this page to select the Alcatel-Lucent AP Groups that you push to switches.
- Use this page to associate a device group to one or more Alcatel-Lucent AP Groups.
- From this page, you can select other profiles that are defined on the switch, like an internal server.

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

The screenshot displays the configuration interface for Alcatel-Lucent AP groups. It is divided into several sections:

- Alcatel-Lucent AP Groups:** Select the Aruba AP Groups to apply to devices in this Group. Includes a 'Show All' link, a checked 'default' option, and 'Select All - Unselect All' buttons.
- AP Overrides:** Select the AP Overrides to apply to devices in this Group. Includes a 'Show Only Selected' link, a checked '10.10.6' option, and 'Select All - Unselect All' buttons.
- Additional Alcatel-Lucent Profiles:** A list of profiles with dropdown menus and edit/delete icons. Profiles include: Stateful 802.1X Authentication Profile, VPN Authentication Profile, Management Authentication Profile, Wired Authentication Profile, Internal Server Profile, TACACS Accounting Profile, IP Mobility Profile, VPN Services Profile, Management Password Policy Profile, Control Plane Security Profile, Configure Campus AP Whitelist (radio buttons for Yes/No), Campus AP Whitelist, RAP Whitelist, Valid OUI Profile, PAPI Security Profile, VIA Web Authentication, Voice SIP Profile, VIA Global Configuration, and SNMP Management Profile.
- Alcatel-Lucent User Roles:** Select additional Roles to apply to devices in this Group. Includes a 'Show All' link, checked options for 'ap-role', 'stateful-dot1x', 'sys-ap-role', and 'trusted-ap', and 'Select All - Unselect All' buttons.
- Alcatel-Lucent Policies:** Select additional Policies to apply to devices in this Group. Includes a 'Show All' link, checked options for 'stateful-dot1x', 'sys-ap-acl', 'sys-control', and 'validuser', and 'Select All - Unselect All' buttons.

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

Groups > Alcatel-Lucent Config When Global Configuration is Disabled

If **Use Global Alcatel-Lucent Configuration** in **OV3600 Setup > General** is set to **No**, the **Groups > Alcatel-Lucent Config** page can be used to manage two or more distinctive configuration strategies using the same tree navigation as the **Device Setup > Alcatel-Lucent Configuration** page, as shown in [Figure 4](#).

Each of the sections is summarized in “[Alcatel-Lucent Configuration Sections in the Tree View](#)” on page 13, with full details in “[Alcatel-Lucent Configuration Reference](#)” on page 35.

Figure 4 *Groups > Alcatel-Lucent Config with Group-Level Configuration*

Alcatel-Lucent Configuration Sections in the Tree View

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

- [Alcatel-Lucent AP Groups Section](#)
- [AP Overrides Section](#)
- [WLANs Section](#)
- [Profiles Section](#)
- [Security Section](#)
- [Local Config Section](#)
- [Advanced Services Section](#)



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

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

Alcatel-Lucent AP Groups Section

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

Navigate to the **Alcatel-Lucent Configuration > Alcatel-Lucent AP Groups** page. [Figure 5](#) illustrates one example of this page.

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

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

Alcatel-Lucent AP Groups have the following characteristics:

- Any Alcatel-Lucent switch can support multiple Alcatel-Lucent AP Groups.
- Alcatel-Lucent AP Groups are assigned to folders, and folders define visibility. Using conventional OV3600 folders to define visibility, Alcatel-Lucent AP Groups can provide visibility to some or many components while blocking visibility to other users for more sensitive components, such as SSIDs. Navigate to the **Users** pages to define folder visibility, and refer to “[Visibility in Alcatel-Lucent Configuration](#)” on page 33.
- You can import a switch configuration file from AOS-W for Alcatel-Lucent AP Group deployment in OV3600.

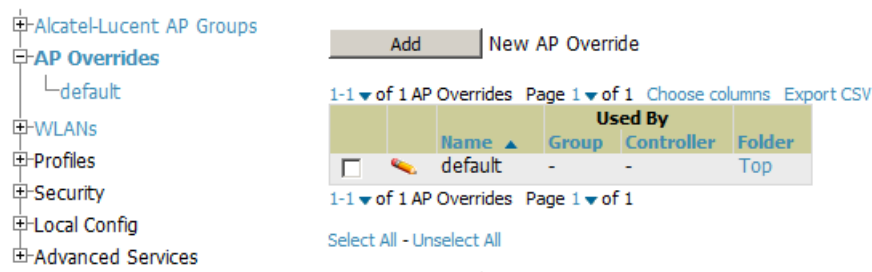
For additional information, refer to the following sections in this document:

- “[Setting Up Initial Alcatel-Lucent Configuration](#)” on page 21
- “[General 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. [Figure 6](#) illustrates this location:

Figure 6 *Alcatel-Lucent Configuration > AP Overrides Navigation*



AP Overrides operate as follows in Alcatel-Lucent Configuration:

- Custom-created AP Overrides appear in the Alcatel-Lucent Configuration navigation pane, as illustrated in [Figure 6](#).
- Alcatel-Lucent switches 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 these topics:
 - “[AP Overrides Guidelines](#)” on page 30
 - “[AP Overrides](#)” on page 40 in the Appendix

WLANs Section

Access WLANs with **Alcatel-Lucent Configuration > WLANs**, illustrated in [Figure 7](#).

Figure 7 Alcatel-Lucent Configuration > WLANs Navigation

Limit to Folder: Top

Add New WLAN

1-20 of 49 WLANs Page 1 of 3 > | Edit Columns

	Name	SSID	Aruba AP Group	Used By	Traffic Management	Folder
<input type="checkbox"/>	1.0.0_ethersphere-voip	ethersphere-voip	corpTest, corp, voip-test	-	-	Top
<input type="checkbox"/>	1.0.0_ethersphere-wpa2	ethersphere-wpa2	corpTest, voip-test-nokia, corp, voip-test	-	-	Top
<input type="checkbox"/>	1.0.0_guest	guest	corpTest, voip-test-nokia, corp, voip-test	-	-	Top
<input type="checkbox"/>	ethersphere-vocera	ethersphere-vocera	-	-	-	Top
<input type="checkbox"/>	office	office	-	-	-	Top
<input type="checkbox"/>	office-ethersphere-voip	ethersphere-voip	aire-office	-	-	Top

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

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

This document describes WLAN configuration in the following section and chapter:

- “Setting Up Initial Alcatel-Lucent Configuration” on page 21
- “General WLAN Guidelines” on page 28
- “WLANs” on page 45

Profiles Section

Profiles provide a way to organize and deploy groups of configurations for Alcatel-Lucent AP Groups, WLANs, and other profiles. Profiles are assigned to folders; this establishes visibility to Alcatel-Lucent AP Groups and WLAN settings. Access **Profiles** with **Alcatel-Lucent Configuration > Profiles**, illustrated in [Figure 8](#).

Figure 8 Alcatel-Lucent Configuration > Profiles Navigation

Limit to Folder: Top

Add New IDS Profile

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

	Name	Dell PowerConnect W AP Group	Used By	Controller	Folder
<input type="checkbox"/>	default	-	-	-	Top
<input type="checkbox"/>	ids-disabled	-	-	-	Top
<input type="checkbox"/>	ids-high-setting	-	-	-	Top
<input type="checkbox"/>	ids-low-setting	default,	-	-	Top
<input type="checkbox"/>	ids-medium-setting	NoAuthApGroup	-	-	Top

1-5 of 5 IDS Profiles Page 1 of 1

Select All - Unselect All

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

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

- “Setting Up Initial Alcatel-Lucent Configuration” on page 21
- “General Profiles Guidelines” on page 28
- “Profiles” on page 50 in the Appendix

Security Section

The **Security** section displays, adds, edits, or deletes security profiles in multiple categories, including user roles, policies, rules, and servers such as RADIUS, TACACS+, and LDAP servers. Navigate to Security with the **Alcatel-Lucent Configuration > Security** path, illustrated in Figure 9.

Figure 9 Alcatel-Lucent Configuration > Security Navigation

The screenshot shows the navigation interface for the Security section. On the left, a tree view lists categories: Alcatel-Lucent AP Groups, AP Overrides, WLANs, Profiles, Security (selected), Campus AP Whitelist, Policies, RAP Whitelist, Server Groups, TACACS Accounting, Time Ranges, User Roles, and User Rules. The main content area displays a table of 'Campus AP Whitelists'. The table has columns for Name, Group, Controller, and Folder. A single entry is shown: 'default' under the 'Access Points' group, with a '-' in the Controller column and 'Top' in the Folder column. Above the table, there is an 'Add' button and the text 'New Campus AP Whitelist'. Below the table, there is a 'Delete' button. The interface also shows pagination information: '1-1 of 1 Campus AP Whitelists Page 1 of 1' and a 'Select All - Unselect All' link.

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

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

For additional information about Security, refer to “Security” on page 131 in the Appendix.

Local Config Section

The Local Config section, introduced in OV3600 7.2, is used for local configuration of Alcatel-Lucent switches. Locally configured settings are not pushed to local controllers by master switches.

SNMP trap settings for switches are managed locally.

Figure 10 Alcatel-Lucent Configuration > Local Config Navigation

Limit to Folder: Top

- Alcatel-Lucent AP Groups
 - AP Overrides
 - WLANs
 - Profiles
 - Security
 - Local Config**
 - SNMP Management**
 - SNMPv3 User**
 - Advanced Services

Add New SNMPv3 User

1-1 of 1 SNMPv3 Users Page 1 of 1 Choose columns Export CSV

	Name	SNMP Management	Controller	Folder	Used By
<input type="checkbox"/>	default	-	-	Top	

1-1 of 1 SNMPv3 Users Page 1 of 1

Select All - Unselect All

Delete

Save and Apply Revert All

For complete details on the Local Config section, refer to “Local Config of SNMP Management” on page 153 in the Appendix.

Advanced Services Section

Navigate to Advanced Services with the **Alcatel-Lucent Configuration > Advanced Services** path. The **Advanced Services** section includes IP Mobility and VPN Services. Figure 11 illustrates this navigation and the components.

Figure 11 Alcatel-Lucent Configuration > Advanced Services Navigation

Note: This profile depends on the controller having a Remote Access Points license or a VPN Server license

- Alcatel-Lucent AP Groups
 - AP Overrides
 - WLANs
 - Profiles
 - Security
 - Local Config
 - Advanced Services**
 - IP Mobility
 - VPN Services**
 - IKE
 - IPSEC**
 - Dynamic Map**
 - Transform Set
 - L2TP
 - PPTP

Add New IPSEC Dynamic Map

1-3 of 3 IPSEC Dynamic Maps Page 1 of 1 Choose columns Export CSV

	Name	Priority	IPSEC	VIA Connection	Controller	Folder	Used By
<input type="checkbox"/>	default-dynamicmap	10000	default	default	-	Top	
<input type="checkbox"/>	default-ikev2-dynamicmap	10000	-	default	-	Top	
<input type="checkbox"/>	default-rap-ipsecmap	10001	-	-	-	Top	

1-3 of 3 IPSEC Dynamic Maps Page 1 of 1

Select All - Unselect All

Delete

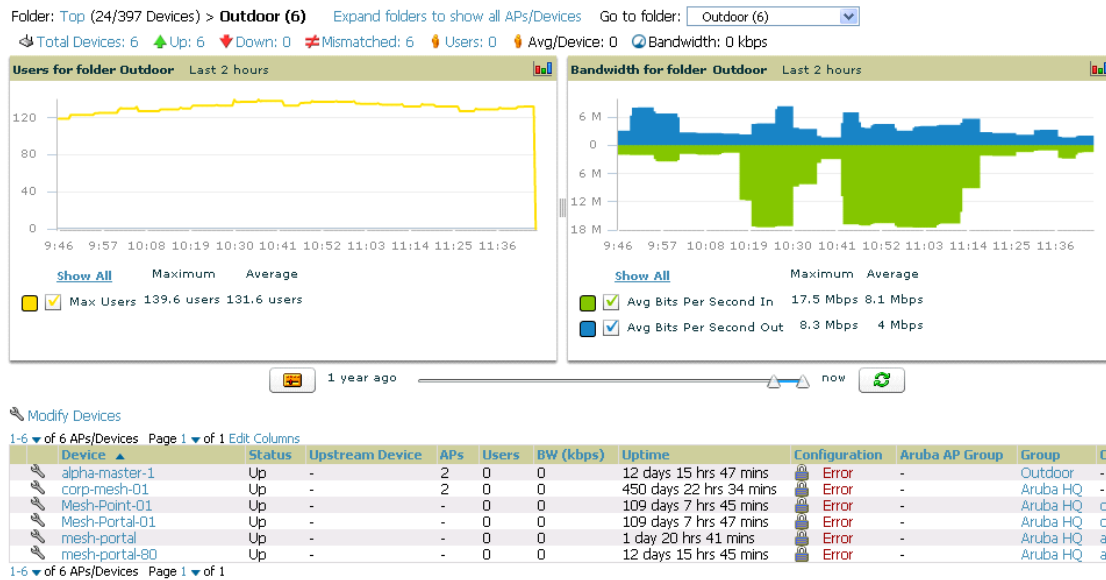
Save and Apply Revert All

For additional information about IP Mobility and VPN Services, refer to “Advanced Services” on page 155.

APs/Devices > List Page

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

Figure 12 APs/Devices List Page Illustration (Partial Display)



APs/Devices > Manage Page

This page configures device-level settings, including **Manage** mode that enables pushing configurations to switches. For additional information, refer to “Pushing Device Configurations to Switches” on page 29.

You can create switch overrides for entire profiles or a specific profile setting per profile. This allows you to avoid creating new profiles or Alcatel-Lucent AP Groups that differ by one more settings. Switch overrides can be added from the switch's APs/Devices > **Manage** page. Figure 13 illustrates an APs/Devices > **Manage** page with switch overrides:

Figure 13 APs/Devices > Manage Page Illustration (Partial Display)

General

Name: Alcatel-Lucent-4308

Status: Up (OK)

Configuration: Error (Too many errors fetching existing configuration)

Last Contacted: 6/16/2011 5:39 PM

Type: Alcatel-Lucent OAW-4308

Firmware: 3.3.2.23

Group: Access Points

Folder: Top

Management Mode: Monitor Only + Firmware Upgrades Manage Read/Write

Settings

Name: Alcatel-Lucent-4308

Location: Sunnyvale

Contact: John

Latitude:

Longitude:

Altitude (m):

Group: Access Points

Folder: Top

Auto Detect Upstream Device: Yes No

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

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

Down Status Message:

Notes

Device Communication

[View Device Credentials](#)

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

IP Address:

SNMP Port (1-65535):

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

This device is currently using SNMP version 2c.

Community String:

Confirm Community String:

SNMPv3 Username:

Auth Password:

Alcatel-Lucent Overrides

Alcatel-Lucent Controller Override

Profile: -- Select a profile type --

Network Settings

Gateway:

APs/Devices > Monitor Page

Used in conjunction with the **Manage** page, the **Monitor** page enables review of device-level settings. This page includes the following sections:

- **Status** information
- Switch's **License** link (see [“Licensing and Dependencies in Alcatel-Lucent Configuration”](#) on page 21)
- **Radio Statistics** of some Alcatel-Lucent thin APs
- **User** and **Bandwidth** interactive graphs
- **CPU Utilization** and **Memory Utilization** interactive graphs
- **APs Managed by this Controller** list (when viewing a switch)
- **Alert Summary**
- **Recent Events**
- **Audit Log**

For additional information, refer to [“Pushing Device Configurations to Switches”](#) on page 29.

Groups > Basic Page

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

- Use this page to control which device settings appear on the **Groups** pages.
- If you want to configure your controllers using templates instead, you should disable Alcatel-Lucent GUI configuration from the **Groups > Basic** page and use template-based configuration. See the Templates chapter of the *OmniVista 3600 Air Manager 7.3 User Guide* in **Home > Documentation** for more information on templates.

Additional Concepts and Components of Alcatel-Lucent Configuration

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

Global Configuration and Scope

Alcatel-Lucent Configuration supports AOS-W as follows:

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

For additional information about these and additional functions, refer to [“General Switch Procedures and Guidelines”](#) on page 29.

Referenced Profile Setup in Alcatel-Lucent Configuration

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

- When you create a new Alcatel-Lucent AP Group from the **Device Setup > Alcatel-Lucent Configuration** page, the **Referenced Profile** section appears as shown in [Figure 14](#):

Figure 14 Referenced Profile Configuration for an Alcatel-Lucent AP Group

Referenced Profiles		
802.11a Radio Profile:	default	+
802.11g Radio Profile:	default	+
RF Optimization Profile:	default	+
Event Thresholds Profile:	default	+
Wired AP Profile:	default	+
Ethernet Interface 0 Link Profile:	default	+
Ethernet Interface 1 Link Profile:	default	+
AP System Profile:	corp	+
Regulatory Domain Profile:	corp-channel-profile	+
SNMP Profile:	default	+
VoIP Call Admission Control Profile: <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:	default	+
Mesh Radio Profile: <small>Requires an Outdoor Mesh Access Points license</small>	default	+

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

Save, Save and Apply, and Revert Buttons

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

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

Figure 15 Unapplied Alcatel-Lucent Configuration Changes Message

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

- **Save and Apply** —This button saves and applies the configuration with reference to Manage and Monitor modes. For example, you must click **Save and Apply** for a configuration profile to propagate to all switches is 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 Switches”](#) 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 Switches” 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 GUI to the Alcatel-Lucent switches as a set of CLI commands using Secure Shell (SSH). No switch reboot is required.

Auditing and Reviewing Configurations

OV3600 supports auditing or reviewing in these ways:

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

Licensing and Dependencies in Alcatel-Lucent Configuration

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

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

Alcatel-Lucent Configuration includes several settings or functions that are dependent on special licenses. The user interface conveys that a special license is required for any such setting, function, or profile. OV3600 does not push such configurations when a license related to those configurations is unavailable. For details on the licenses required by a specific version of AOS-W, refer to the *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 in OV3600 6.4 or later versions.

Prerequisites

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

Procedure

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

1. Determine whether you are using global or group configuration, and set **OV3600 Setup > General > Device Configuration > Use Global Alcatel-Lucent Configuration** accordingly.
1. On the **Groups > Basic** page, enable device preferences for Alcatel-Lucent devices. [Figure 17](#) illustrates this page.

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.

2. Authorize Alcatel-Lucent switches into the device group in **Monitor Only** mode.



CAUTION

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



NOTE

Alcatel-Lucent Configuration is enabled by default in OV3600.

3. Navigate to the **APs/Devices > Audit** page for the first switch to prepare for importing an existing Alcatel-Lucent switch configuration file. [Figure 16](#) illustrates the information available on this page if the device is mismatched.

Figure 16 *APs/Devices > Audit Page Illustration*

Device Configuration of **ethersphere-lms3** in group **ADC-HQ** in folder **Top**

This Device is in monitor-only-with-firmware-upgrades mode.
Configuration read from device at 8/29/2010 8:55 PM

Configuration: Mismatched

Audit the device's current configuration.

[Show Archived Device Configuration](#)

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

Include unreferenced profiles.

Choose settings to ignore during configuration audits.

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

In Global Configuration:

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

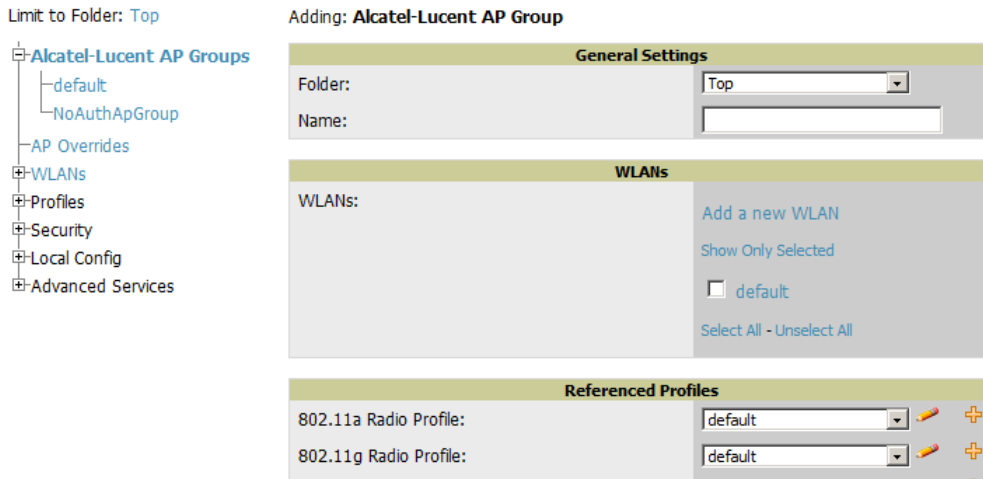
The folder for all the Profiles and Alcatel-Lucent AP Groups is set to the top folder of the OV3600 user who imports the configuration. This folder is **Top** in the case of managing administrators with read/write privileges.

In Group Configuration:

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

4. After configuration file import is complete, refresh the page to verify the results of the import and add or edit as required.
5. Navigate to the **Alcatel-Lucent Configuration** page.
 - This page displays a list of APs authorized on the OV3600 that are using the Alcatel-Lucent AP Group.
 - The **User Role** is the Alcatel-Lucent User Role used in firewall settings. For additional information, refer to “[Security > User Roles](#)” on page 132.
 - **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 33.
6. Add or modify **Alcatel-Lucent AP Groups** as required.
 - a. Navigate to the **Alcatel-Lucent Configuration > Alcatel-Lucent AP Groups** page.
 - b. Click **Add** from the **Alcatel-Lucent AP Groups** page to create a new Alcatel-Lucent AP Group. To edit an Alcatel-Lucent AP Group, click the pencil icon next to the group. The Details page for the Alcatel-Lucent AP Group appears. This page allows you to select the profiles to apply to the Alcatel-Lucent AP Group, and to select one or more WLANs that support that Alcatel-Lucent AP Group. [Figure 17](#) illustrates this page.

Figure 17 *Alcatel-Lucent Configuration > Alcatel-Lucent AP Groups > Add/Edit Details Page (Partial View)*



The following section of this configuration guide provide additional information about configuring Alcatel-Lucent AP Groups:

- “[General Alcatel-Lucent AP Groups Procedures and Guidelines](#)” on page 27

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

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

- **Basic**—This display is essentially the same as the AOS-W Wizard View on the Alcatel-Lucent switch.
- **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 provide additional information and illustrations for configuring WLANs:

- “[General WLAN Guidelines](#)” on page 28

- “WLANs” on page 45 in the Appendix for details on all WLAN settings
8. Add or edit Alcatel-Lucent Configuration Profiles as required.
 - a. Navigate to **Alcatel-Lucent Configuration > Profiles** section of the navigation pane.
 - b. Select the type of profile in the navigation pane to configure: **AAA, AP, 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 switch WebUI. The primary difference in OV3600 is that **AAA** and **SSID** profiles are not listed under the **WLAN** column, but under **Profiles**.
 - d. Save changes to each element as you proceed through profile and WLAN configuration.

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

 - “General Profiles Guidelines” on page 28
 9. Provision multiple Alcatel-Lucent AP Groups on one or more switches by putting the switches into an OV3600 group and configuring that group to use the selected Alcatel-Lucent AP Groups. With global configuration enabled, configure such Alcatel-Lucent AP Groups settings on the **Group > Alcatel-Lucent Config** page. With group configuration, use Alcatel-Lucent AP Groups. The following section of this document provides additional information:
 - “General Alcatel-Lucent AP Groups Procedures and Guidelines” on page 27
 10. As needed, add or edit AP devices. The following section of this document has additional information:
 - “Supporting APs with Alcatel-Lucent Configuration” on page 30
 11. Each AP can be assigned to a single Alcatel-Lucent AP Group. Make sure to choose an AP Group that has been configured on that switch using that switch'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.
 12. Navigate to the **APs/Devices > Audit** page for the switch to view mismatched settings. This page provides links to display additional and current configurations. You can display all mismatched devices by navigating to the **APs/Devices > Mismatched** page.

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

Device Configuration of **Alcatel-Lucent-4308** in group **Access Points** in folder **Top**
 This Device is in monitor-only-with-firmware-upgrades mode.
 Configuration read from device at 6/16/2011 2:00 PM
 Configuration: Error (Too many errors fetching existing configuration)

Audit Audit the device's current configuration.

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

Customize Choose settings to ignore during configuration audits.

[Show entire config](#)
[View Telnet/SSH Command log](#)

[Refresh this page](#)

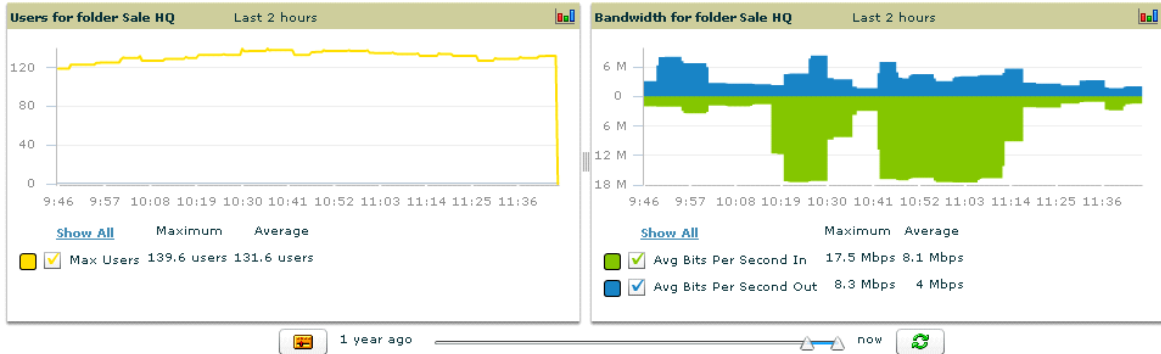
Group Basic Settings		
	Current Device Configuration	Desired Configuration
Offload WMS Database	(not set)	No
Alcatel-Lucent AP Group Settings		
	Current Device Configuration	Desired Configuration
Alcatel-Lucent AP Group 'default' 802.11a Radio Profile	(not set)	default
Alcatel-Lucent AP Group 'default' 802.11g Radio Profile	(not set)	default
Alcatel-Lucent AP Group 'default' AP Regulatory Domain Profile	(not set)	default
Alcatel-Lucent AP Group 'default' AP SNMP Profile	(not set)	default
Alcatel-Lucent AP Group 'default' AP System Profile	(not set)	default
Alcatel-Lucent AP Group 'default' Ethernet Interface 0 Link Profile	(not set)	default
Alcatel-Lucent AP Group 'default' Ethernet Interface 1 Link Profile	(not set)	default
Alcatel-Lucent AP Group 'default' Event Thresholds Profile	(not set)	default
Alcatel-Lucent AP Group 'default' IDS Profile	(not set)	ids-low-setting
Alcatel-Lucent AP Group 'default' RF Optimization Profile	(not set)	default
Alcatel-Lucent AP Group 'default' Status	(not set)	Create
Alcatel-Lucent AP Group 'default' Virtual AP Profile 'default' Status	(not set)	Create
Alcatel-Lucent AP Group 'default' Wired AP Profile	(not set)	default
Alcatel-Lucent WLAN Settings		
	Current Device Configuration	Desired Configuration
WLAN 'default' AAA Profile	(not set)	default
WLAN 'default' Allowed Band	(not set)	all

Figure 19 APs/Devices > Mismatched Page Illustration

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

Sale HQ (3/74)

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



Modify Devices

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

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

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

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

Version	Firmware Status	IP Address	LAN MAC Address	Radio MAC Address
3.4.0.2-vowifi	-	10.6.1.228	00:1A:1E:00:1A:1E	00:1A:1E:00:1A:1E
3.4.0.2-vowifi	-	10.6.1.240	00:1A:1E:00:1A:1E	00:1A:1E:00:1A:1E
3.4.0.2-vowifi	-	10.6.2.253	00:08:86:00:08:86	-

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

4 Folders

Add New Folder

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

- Once Alcatel-Lucent Configuration is deployed in OV3600, you can perform debugging with Telnet/SSH. Review the `telnet_cmds` file in the `/var/log` folder from the command line interface, or access this file from the **System > Status** page. Refer to the *OV3600 User Guide* for additional information.
- 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 of Alcatel-Lucent Configuration

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

- *AOS-W User Guide*
- *OV3600 User Guide*
- *Alcatel-Lucent and OV3600 Best Practices Guide*

Introduction

This chapter presents the more 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:

- [General Alcatel-Lucent AP Groups Procedures and Guidelines](#)
- [General WLAN Guidelines](#)
- [General Switch Procedures and Guidelines](#)
- [Supporting APs with Alcatel-Lucent Configuration](#)
- [Visibility in Alcatel-Lucent Configuration](#)
- [Using OV3600 to Deploy Alcatel-Lucent APs for the First Time](#)



For a complete reference on all Alcatel-Lucent Configuration pages, field descriptions, and certain additional procedures that are more specialized, refer to [Appendix A, “Alcatel-Lucent Configuration Reference”](#) on page 35.

General Alcatel-Lucent AP Groups Procedures and Guidelines

Guidelines and Pages for Alcatel-Lucent AP Groups in Alcatel-Lucent Configuration

The fields and default settings for Alcatel-Lucent AP Groups are described in “[Alcatel-Lucent AP Groups](#)” on page 36 in the Appendix. The following guidelines govern the configuration and use of Alcatel-Lucent AP Groups across OV3600:

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

- You modify devices in Alcatel-Lucent AP Groups with the **APs/Devices > List** page, clicking **Modify Devices**. This is the page where you assign devices to a given group and Alcatel-Lucent AP Group.

Selecting Alcatel-Lucent AP Groups

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

Configuring Alcatel-Lucent AP Groups

Perform the following steps to display, add, edit, or delete Alcatel-Lucent 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” on page 36](#).
3. Click **Add** or **Save** to finish creating or editing the Alcatel-Lucent AP Group. Click **Cancel** to back out of this screen and to cancel the AP Group configurations.
4. New AP groups appear in the **AP Groups** section of the Alcatel-Lucent Configuration navigation pane, and clicking the group name takes you to the **Details** page for that group.
5. When this and other procedures are completed, push the configuration to the Alcatel-Lucent switches by clicking **Save and Apply**. The principles of Monitor and Manage mode still apply. For additional information, refer to [“Pushing Device Configurations to Switches” on page 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 switches to become active on the network.

General Profiles Guidelines

AOS-W elements can be added or edited after an AOS-W configuration file is imported to OV3600 and pushed to switches with the steps described in [“Setting Up Initial Alcatel-Lucent Configuration” on page 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 the 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 you to your place in Alcatel-Lucent AP Group or WLAN setup.

For complete Profiles inventory and field descriptions, refer to “Profiles” on page 50 in the Appendix.

General Switch Procedures and Guidelines

Using Master, Standby Master, and Local Switches in Alcatel-Lucent Configuration

OV3600 implements the following general approaches to switches:

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

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

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

Pushing Device Configurations to Switches

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

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

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



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

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

1. Make all device changes using the **Alcatel-Lucent Configuration** pages. Click **Save and Apply** as you complete device-level changes. This builds an inventory of pending configuration changes that have not been pushed to the switch and APs.
2. Review the entire set of newly mismatched devices on the **APs/Devices > Mismatched** page.
3. For each mismatched device, navigate to the **APs/Devices > Audit** page to audit recent configuration changes as desired.

4. Once all mismatched device configurations are verified to be correct from the **APs/Devices > Audit** page, use the **Modify Devices** link on the **Groups > Monitor** page to place these devices into **Manage** mode. This instructs OV3600 to push the device configurations to the switch.
5. As desired, return devices to **Monitor** mode until the next set of configuration changes is ready to push to switches.

Supporting APs with Alcatel-Lucent Configuration

AP Overrides Guidelines

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

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

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

Changing Adaptive Radio Management (ARM) Settings

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

- [“Configuring Alcatel-Lucent AP Groups” on page 28](#)
- [“Alcatel-Lucent AP Groups” on page 36](#)
- [“Profiles > RF > 802.11a/g Radio > ARM” on page 108](#) in the Appendix.

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 > SSID” on page 117](#) and related profiles in the Appendix.

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 Alcatel-Lucent AP Group for an AP device:

1. As needed, 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 Alcatel-Lucent AP Groups that are currently configured in OV3600.
2. Navigate to the **APs/Devices > List** page to view all devices currently seen by OV3600.
3. If necessary, add the device to OV3600 using the **APs/Devices > New** page.
To discover additional devices, ensure that the switch is set to perform a thin AP poll period.
4. On the **APs/Devices > List** page, you can specify the **Group** and **Folder** to which a device belongs. Click **Modify Devices** to change more than one device, or click the **Wrench** icon associated with any specific device to make changes. The **APs/Devices > Manage** page appears.
5. In the **Settings** section of the **APs/Devices > Manage** page, select the new Alcatel-Lucent AP Group to assign to the device. Change or adjust any additional settings as desired.
6. Click **Save and Apply** to retain these settings and to propagate them throughout OV3600, or click one of the alternate buttons as follows for an alternative change:
 - Click **Revert** to cancel out of all changes on this page.
 - Click **Delete** to remove this device from OV3600.
 - Click **Ignore** to keep the device in OV3600 but to ignore it.
 - Click **Import Settings** to define device settings from previously created configurations.
 - Click **Replace Hardware** to replace the AP device with a new AP device.
 - Click **Update Firmware** to update the Firmware that operates this device.
7. Push this configuration change to the AP switch that is to support this AP device. For additional information, refer to [“Pushing Device Configurations to Switches” on page 29](#).

Using OV3600 to Deploy Alcatel-Lucent APs for the First Time

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

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

For efficiency, 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 the bottom of the page and put APs in the appropriate OV3600 group and folder. Set the devices to **Manage Read/Write** mode.
7. Click **Add**. Wait approximately five to 10 minutes. You can observe that the APs have been renamed not only in OV3600 but also on the Alcatel-Lucent AP Group and Alcatel-Lucent switch with the **show ap database aosw** command.
8. To set the appropriate Alcatel-Lucent AP Group, select the **AP/Devices** or **Groups** page and locate your APs.
9. Click **Modify Devices**.
10. Select the APs you want to re-group.
11. In the field that states **Move to Alcatel-Lucent AP Group** below the list of the devices, select the appropriate group and click **Move**.



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

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

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, Aruba 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 visibility through user roles, AP/Device access level, and folders (in *global* configuration). These and 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](#)
 - [Security > Policies](#)
- OV3600 continues to support the standard operation of folders, users, and user roles as described in the *OV3600 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:

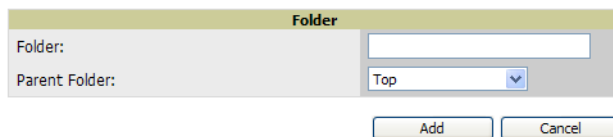
1. As needed, create a new OV3600 device folder with management access.
 - a. Navigate to the **APs/Devices > List** page and scroll to the bottom of the page. (An alternate page supporting new folders is **Users > Connected** page).

Figure 1 Add New Folder link at the bottom of the APs/Devices > List



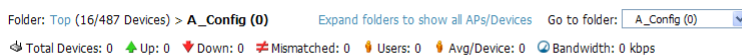
- b. Click the **Add New Folder** link shown in [Figure 1](#). The **Folder** detail page appears, as illustrated in [Figure 2](#):

Figure 2 APs/Devices > Add New Folder > Folders Page Illustration

A form titled "Folder" with a light green header. It contains two input fields: "Folder:" with a text box and "Parent Folder:" with a dropdown menu showing "Top". At the bottom are "Add" and "Cancel" buttons.

- c. Enter a name and select **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 3](#) illustrates an unpopulated device page for an example folder.

Figure 3 APs/Devices > List Page With No Devices



2. Add Alcatel-Lucent switch devices to that folder as required. Use the **Device Setup > Add** or **Device Setup > Discover** page following instructions available in the *OV3600 User Guide*.
3. As needed, create or edit a user role that is to have rights and manage privileges required to support their function in Alcatel-Lucent Configuration. 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.

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 as illustrated in [Figure 4](#).

Figure 4 *OV3600 Setup > Roles > Add/Edit Role Page Illustration*

The image shows two stacked configuration panels. The top panel, titled 'Role', contains the following fields: 'Name' (text input with 'New Role'), 'Enabled' (radio buttons for 'Yes' and 'No'), 'Type' (dropdown menu with 'AP/Device Manager'), 'AP/Device Access Level' (dropdown menu with 'Monitor (Read Only)'), 'Top Folder' (dropdown menu with 'Top'), 'RAPIDS' (dropdown menu with 'None'), 'VisualRF' (dropdown menu with 'Read Only'), and 'Helpdesk' (radio buttons for 'Yes' and 'No'). The bottom panel, titled 'Guest User Preferences', contains: 'Allow creation of Guest Users' (radio buttons for 'Yes' and 'No'), 'Allow accounts with no expiration' (radio buttons for 'Yes' and 'No'), 'Allow sponsor to change sponsorship username' (radio buttons for 'Yes' and 'No'), and 'Custom Message' (text input). At the bottom of the form are 'Add' and 'Cancel' buttons.

- d. As per standard OV3600 configuration, complete the settings on this page. The most important fields with regard to Alcatel-Lucent Configuration, device visibility and user rights are as follows:
 - **Type**—Specify the type of user. Important consideration should be given to whether the user is an administrative user with universal access, or an AP/Device manager to specialize in device administration, or additional users with differing rights and access.
 - **AP/Device Access Level**—Define the access level that this user is to have in support of Alcatel-Lucent switches, devices, and general Alcatel-Lucent Configuration operations.
 - **Top Folder**—Specify the folder created earlier in this procedure, or specify the **Top** folder for an administrative user.
- e. Click **Add** to complete the role creation, or click **Save** to retain changes to an existing role. The **OV3600 Setup > Roles** page now displays the new or revised role.
4. As needed, add or edit one or more users to manage and support Alcatel-Lucent Configuration. This step creates or edits users to have rights appropriate to Alcatel-Lucent Configuration. This user inherits visibility to Alcatel-Lucent switches and Alcatel-Lucent Configuration data based on the role and device folder created earlier in this procedure.
 - a. Navigate to the **OV3600 Setup > Users** 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 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 adding devices is available in the *OmniVista 3600 Air Manager User Guide*.
7. Continue to other elements of Alcatel-Lucent Configuration described in this document.

Introduction

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

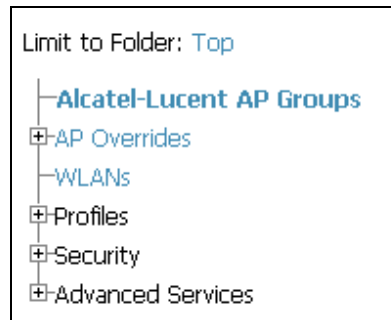
- Alcatel-Lucent Configuration components are summarized in “[Additional Concepts and Components of Alcatel-Lucent Configuration](#)” on page 19.
- For procedures that use several of these components, refer to earlier chapters in this document.
- For architectural information about AOS-W, refer to the *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 > Alcatel-Lucent Configuration** page, illustrated in [Figure 1](#). The one exception is the additional **Groups > Alcatel-Lucent Config** page that you access from the standard OV3600 navigation menu.

Figure 1 Alcatel-Lucent Configuration Components



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

- Alcatel-Lucent AP Groups
- AP Overrides
- WLANs
- Profiles
- Security
- Local Config of SNMP Management
- Advanced Services
- Groups > Alcatel-Lucent Config Page and Section Information

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.

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 “[General Alcatel-Lucent AP Groups Procedures and Guidelines](#)” on page 27.

Limit to Folder: Top Add

Alcatel-Lucent AP Groups 1-20 of 64 Alcatel-Lucent AP Groups Page 1 of 4 > | [Choose Columns](#) [CSV Export](#)

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

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

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

Column	Description
Name	Displays the name of the Alcatel-Lucent AP Group. Select the pencil icon next to any group to edit.
(Used by) Group	Displays the OV3600 device groups that define this Alcatel-Lucent AP Group. Select the name of any group in this column to display the detailed Groups > Alcatel-Lucent Config page. The device groups in this column receive the profile configurations from the associated Alcatel-Lucent AP Group. Any Alcatel-Lucent AP Group profiles can define device groups.
(Used by) Number of AP	Displays the number of APs in this Alcatel-Lucent AP Group. A detailed list of each AP by name can be displayed by navigating to the Groups > List page and selecting that group.
(Used By) User Role	Displays the user role or roles that support the respective Alcatel-Lucent AP Group, when defined.
Folder	Displays the folder that is associated with this Alcatel-Lucent AP Group, when defined. A Top viewable folder for the role is able to view all devices and groups contained by the top folder. The top folder and its subfolders must contain all the devices in any groups it can view. Clicking any folder name takes you to the APs/Devices > List page for folder inventory and configuration.

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

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

Field	Default	Description
General Settings		
Folder	Top	Displays the folder with which the AP Group is associated. The drop-down menu displays all folders available for association with the AP Group. Folders provide a way to organize the visibility of device parameters that is separate from the configuration groups of devices. Using folders, you can view basic statistics about device, and define which users have visibility to which device parameters.
Name	Default	Enter the name of the AP Group.
WLANs		
Add a new WLAN		Select this link to create a new WLAN to support Alcatel-Lucent Configuration. Once created, that new WLAN will appear with others on this page.
Show only selected/Show All		To set the WLANs that appear on this page, select (check) the desired WLANs, then click Show Only Selected .
WLANs	None 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.
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 profile settings in the RF > 802.11a/g Radio page.
RF Optimization Profile	default	Enables or disables load balancing based on a user-defined number of clients or degree of AP utilization on an AP. Use this profile to detect coverage holes, radio interference and STA association failures and configure Received signal strength indication (RSSI) metrics. Select the pencil icon next to this field to display the Profiles > RF section and edit these settings as desired.

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

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 switch using Generic Routing Encapsulation (GRE) tunnels, bridged into the local Ethernet LAN (for remote APs), or a configured for combination of the two (split-mode). This profile also configures the switching mode characteristics for the port, and sets the port as either trusted or untrusted.</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 switch, including the IP addresses of the local, backup, and master switches, Real-time Locating Systems (RTLS) server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps.</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>Alcatel-Lucent's 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

Field	Default	Description
802.11g Traffic Management Profile	default	Specifies 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	Specifies 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 to 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 allow you to define device-specific settings for an AP device without having to remove that device from an existing Alcatel-Lucent AP Group or create a new Alcatel-Lucent AP Group specifically for that device. The **AP Overrides** page is for custom AP devices that otherwise comply with most settings in the Alcatel-Lucent AP Group in which it is managed.

AP Overrides

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

Figure 2 *AP Overrides Page Illustration*

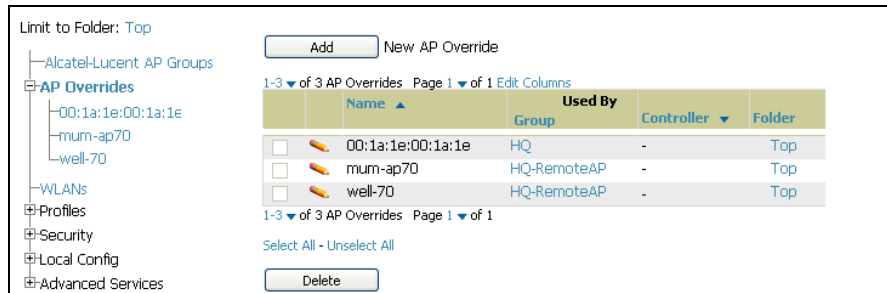


Table 3 describes the fields on this page.

Table 3 *AP Overrides Fields and Descriptions*

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

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

Table 4 *AP Overrides Add or Edit Page Fields*

Field	Default	Description
Name	Blank	Name of the AP Override. Use the name of the AP device to which it applies.
Folder	Top	Displays the folder with which the WLAN is associated. The drop-down menu displays all folders available for association with the WLAN.
WLANs		
WLANs		This section lists the WLANs currently defined in Alcatel-Lucent Configuration by default. You can display selected WLANs or all WLANs. Select one or more WLANs for which AP Override is to apply.

Table 4 AP Overrides Add or Edit Page Fields (Continued)

Field	Default	Description
Excluded WLANs		
Excluded WLANs		This section displays WLANs currently defined in Alcatel-Lucent Configuration by default. This section can display selected WLANs or all WLANs. Use this section to specify which WLANs are not to support AP Override .
Referenced Profiles		
802.11a Radio Profile	5_am	<p>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.</p> <p>Select the pencil icon next to this field to edit or create additional profile settings in the RF > 802.11a/g Radio page.</p> <p>For additional information, refer to “Profiles > RF > 802.11a/g Radio” on page 103.</p>
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 or create additional profile settings in the RF > 802.11a/g Radio page of Alcatel-Lucent Configuration.</p> <p>For additional information, refer to “Profiles > RF > 802.11a/g Radio” on page 103.</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> <p>For additional information, refer to “Profiles > RF > 802.11a/g Radio” on page 103.</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> <p>For additional information, refer to “Profiles > RF > Event Thresholds” on page 113.</p>

Table 4 AP Overrides Add or Edit Page Fields (Continued)

Field	Default	Description
Wired AP Profile	default	<p>Controls whether 802.11 frames are tunneled to the switch using Generic Routing Encapsulation (GRE) tunnels, bridged into the local Ethernet LAN (for remote APs), or a configured for combination of the two (split-mode). This profile also configures the switching mode characteristics for the port, and sets the port as either trusted or untrusted.</p> <p>Select the pencil icon next to this field to display the Profiles > AP > Wired page and adjust these settings as desired.</p> <p>For additional information, refer to “Profiles > AP > System” on page 74.</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> <p>For additional information, refer to “Profiles > AP > SNMP” on page 73.</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> <p>For additional information, refer to “Profiles > AP > SNMP” on page 73.</p>
AP System Profile	default	<p>Defines administrative options for the switch, including the IP addresses of the local, backup, and master switches, Real-time Locating Systems (RTLS) server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps.</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> <p>For additional information, refer to “Profiles > AP > System” on page 74.</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> <p>For additional information, refer to “Profiles > AP > Regulatory Domain” on page 72.</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> <p>For additional information, refer to “Profiles > AP > SNMP” on page 73.</p>

Table 4 AP Overrides Add or Edit Page Fields (Continued)

Field	Default	Description
VoIP Call Admission Control Profile	default	<p>Alcatel-Lucent's 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> <p>For additional information, refer to "Profiles > AP > SNMP" on page 73.</p>
802.11g Traffic Management Profile	default	<p>Specifies 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> <p>For additional information, refer to "Profiles > QoS > Traffic Management" on page 99</p>
802.11a Traffic Management Profile	default	<p>Specifies 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> <p>For additional information, refer to "Profiles > QoS > Traffic Management" on page 99</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> <p>For additional information, refer to "Profiles > IDS" on page 80</p>
Mesh Radio Profile	default	<p>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.</p> <p>For additional information, refer to "Profiles > Mesh" on page 93.</p>
AP Authorization Profile		<p>Selects the AP Authorization profile to be associated with the new AP Group. This profile requires a Remote Access Points license. Refer to "Profiles > AP > Authorization" on page 69.</p>
AP Provisioning Profile		<p>Selects the AP Provisioning profile to be associated with the new AP Group. Refer to "Profiles > AP > Provisioning" on page 71.</p>

Table 4 AP Overrides Add or Edit Page Fields (Continued)

Field	Default	Description
Ethernet Interface 0-4 Port Configuration		<p>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:</p> <ul style="list-style-type: none"> • default • NoWiredAuthPort • shutdown <p>Refer to “Select Add or Save. The added or edited Wired Port profile appears on the Profiles page, and on the Wired Port details page.” on page 79.</p>
Mesh Cluster Profiles		
Add New Mesh Cluster Profile	Hidden by default until the Add button is clicked	<p>Clicking this Add button displays a new Mesh Cluster Profile field. The drop-down menu displays all supported profiles. Select one from the menu.</p> <p>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.</p> <p>For additional information about Mesh Cluster profiles, refer to these sections:</p> <ul style="list-style-type: none"> • “Profiles > Mesh” on page 93 • “Profiles > QoS” on page 98.
Excluded Mesh Cluster Profiles		
Excluded Mesh Cluster Profiles		<p>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. For additional information about Mesh Cluster profiles, refer to “Profiles > QoS” on page 98.</p>

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 *AOS-W 6.0 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 your place on 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 **Alcatel-Lucent Configuration > WLANs** page contains additional information as described in [Table 5](#):

Table 5 *Alcatel-Lucent Configuration > WLANs* Page Field 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.
Folder	Lists the folder for the WLAN.

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

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

WLANs > Basic

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

Table 6 *WLANs > Basic* Page Field Descriptions

Field	Default	Description
Name	Blank	Enter the name of the WLAN.
Folder	Top	Displays the folder with which the WLAN is associated. The drop-down menu displays all folders available for association with the WLAN.
SSID		Select the SSID profile that defines encryption, EDCA or high-throughput SSID parameters. Access these SSID profiles by clicking Profiles > SSID in the navigation pane at left. For additional information, refer to “Profiles > SSID” on page 117 .
Radio Type		Define whether the supported radio type on the WLAN is 802.11a, 802.11g, or all.
Enable 802.11n	Yes	Define whether the WLAN is to support 802.11n.
VLAN	1	Select the VLAN ID number to be supported on this WLAN.
Intended Use	Internal	Define whether this WLAN is Internal to the enterprise or to support Guest users.
Encryption	opensystem	Select one or more encryption types, as desired, to be supported by this WLAN.
Use Captive Portal	No	Select whether this WLAN will use captive portal authentication. Captive portal authentication directs clients to a special web page that typically requires them to enter a username and password before accessing the network. For additional information about this profile type, refer to “Profiles > AAA > Captive Portal Auth” on page 60 .
Authenticated User Role	logon	For the captive portal authentication profile, you specify the previously-created auth-guest user role as the default user role for authenticated captive portal clients and the authentication server group (“Internal”). For additional information, refer to “Security > User Roles” on page 132 .

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

The alternate way to create or edit WLANs is from the **Advanced** page. For additional information, refer to [“WLANs > Advanced” on page 46](#).

WLANs > Advanced

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

Table 7 WLANs > Advanced Page Fields

Field	Default	Description
General Settings		
Folder	Top	Displays the folder with which the WLAN is associated. The drop-down menu displays all folders available for association with the WLAN.
Name	Blank	Name of the WLAN.
Referenced Profiles		
SSID Profile		Select the SSID profile that defines encryption, EDCA or high-throughput SSID parameters. Access these SSID profiles by clicking Profiles > SSID in the navigation pane at left. For additional information, refer to “Profiles > SSID” on page 117 .
AAA Profile		Select the AAA profile that defines RADIUS, TACACS+, or other AAA server configurations for this WLAN. Access these SSID profiles by clicking Profiles > AAA in the navigation pane at left. For additional information, refer to “Profiles > AAA Overview” on page 50 .
802.11k Profile		Manages settings for the 802.11k protocol. The 802.11k protocol allows APs and clients to dynamically query their radio environment and take appropriate connection actions. For example: In a 802.11k network if the AP with the strongest signal reaches its CAC (Call Admission Control) limits for voice calls, then on-hook voice clients may connect to an under utilized AP with a weaker signal. You can configure the following options in 802.11k profile: <ul style="list-style-type: none"> • Enable or disable 802.11K support on the AP • Forceful disassociation of on-hook voice clients • Measurement mode for beacon reports. For more details, see the “Configuring 802.11k Protocol” topic in the <i>AOS-W 6.0 User Guide</i> .
WMM Traffic Management Profile		Manages settings for the bandwidth management profile for Wi-Fi Multimedia (WMM). Refer to “Profiles > QoS > Traffic Management” on page 99 .
Other Settings		
Virtual AP Enable	Yes	Enable this setting to allow virtual AP configurations to be deployed on this WLAN. This profile defines your WLAN by enabling or disabling the bandsteering, fast roaming, and DoS prevention features. It defines radio band, forwarding mode and blacklisting parameters, and includes references an AAA Profile, an EDCA Parameters AP Profile and a High-throughput SSID profile
Allowed Band	all	Select whether this WLAN is to support 802.11a, 802.11g, or both.
VLAN		Enter the VLAN or range of VLANs to be supported with this WLAN.
Forward Mode	tunnel	Define whether this WLAN is to support tunnel, bridge, or split-mode IP forwarding.
Deny Time Range	none	Define the time range restrictions for the roles in this WLAN, if any.
Mobile IP	Yes	Enable or disable mobile IP functions. This setting specifies whether the switch is the home agent for a client. When enabled, this setting detects when a mobile client has moved to a foreign network and determines the home agent for a roaming client.

Table 7 WLANs > Advanced Page Fields (Continued)

Field	Default	Description
HA Discovery on Association	No	<p>Enable or disable HA discovery on Association. In normal circumstances a switch performs an HA discovery only when it is aware of the client's IP address which it learns through the ARP or any L3 packet from the client. This limitation of learning the client's IP and then performing the HA discovery is not effective when the client performs an inter switch move silently (does not send any data packet when in power save mode). This behavior is commonly seen with various handheld devices, Wi-Fi phones, etc. This delays HA discovery and eventually resulting in loss of downstream traffic if any meant for the mobile client.</p> <p>With HA discovery on association, a switch can perform a HA discovery as soon as the client is associated. By default, this feature is disabled. You can enable this on virtual APs with devices in power-save mode and requiring mobility. This option will also poll for all potential HAs.</p>
DoS Prevention	No	Enable or disable DoS prevention functions, as defined in virtual AP profiles.
Station Blacklisting	Yes	<p>Enable or disable DoS prevention functions, as defined in virtual AP profiles. The blacklisting option can be used to prevent access to clients that are attempting to breach the security.</p> <p>When a client is blacklisted in the Alcatel-Lucent system, the client is not allowed to associate with any AP in the network for a specified amount of time. If a client is connected to the network when it is blacklisted, a de-authentication message is sent to force the client to disconnect. While blacklisted, the client cannot associate with another SSID in the network.</p>
Blacklist Time	3600	If station blacklisting is enabled, specify the time in seconds for which blacklisting is enabled. When a client is blacklisted in the Alcatel-Lucent system, the client is not allowed to associate with any AP in the network for a specified amount of time.
Authentication Failure Blacklist Time	3600	<p>You can configure a maximum authentication failure threshold in seconds for each of the following authentication methods:</p> <ul style="list-style-type: none"> ● 802.1x ● MAC ● Captive portal ● VPN <p>When a client exceeds the configured threshold for one of the above methods, the client is automatically blacklisted by the switch, an event is logged, and an SNMP trap is sent. By default, the maximum authentication failure threshold is set to 0 for the above authentication methods, which means that there is no limit to the number of times a client can attempt to authenticate.</p> <p>With 802.1x authentication, you can also configure blacklisting of clients who fail machine authentication.</p> <p>NOTE: This requires that the External Services Interface (ESI) license be installed in the switch.</p> <p>NOTE: When clients are blacklisted because they exceed the authentication failure threshold, they are blacklisted indefinitely by default. You can configure the duration of the blacklisting.</p>
Fast Roaming	No	Fast roaming is a component of virtual AP profiles in which client devices are allowed to roam from one access point to another without requiring reauthentication by the main RADIUS server.
Strict Compliance	No	Define whether clients should have strict adherence to settings on this page for network access.
VLAN Mobility	No	Define whether clients in the WLAN and VLAN should have mobility or roaming privileges.

Table 7 WLANs > Advanced Page Fields (Continued)

Field	Default	Description
Remote AP Operation	standard	<p>Define the rights for remote APs in this WLAN. Options are as follows:</p> <ul style="list-style-type: none"> • standard • persistent • backup • always <p>Remote APs connect to a switch using Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec). AP control and 802.11 data traffic are carried through this tunnel. Secure Remote Access Point Service extends the corporate office to the remote site. Remote users can use the same features as corporate office users. Secure Remote Access Point Service can also be used to secure control traffic between an AP and the switch in a corporate environment. In this case, both the AP and switch are in the company's private address space.</p>
Drop Broadcast and Multicast	No	Specify whether the WLAN should drop broadcast and multicast mesh network advertising on the WLAN.
Convert Broadcast ARP Requests to Unicast	No	Specify whether ARP table information should be distributed in broadcast (default) or unicast fashion.
Deny Inter User Traffic	No	If enabled, this setting disables traffic between all untrusted users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic. Requires a minimum version of 6.1.0.0.
Band Steering	No	Enable or disable band steering on the WLAN. Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5GHz band than on the 2.4GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40MHz or 20MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.
Steering Mode	prefer-5ghz	<p>Band steering supports three different band steering modes.</p> <ul style="list-style-type: none"> • Force-5GHz: When the AP is configured in force-5GHz band steering mode, the AP will try to force 5Ghz-capable APs to use that radio band. • Prefer-5GHz (Default): If you configure the AP to use prefer-5GHz band steering mode, the AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. • Balance-bands: In this band steering mode, the AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5Ghz band has more channels than the 2.4 GHz band, and that the 5Ghz channels operate in 40MHz while the 2.5Ghz band operates in 20MHz. <p>NOTE: Steering modes do not take effect until the band steering feature has been enabled. The band steering feature in AOS-W versions 3.3.2-5.0 does not support multiple band-steering modes. The band-steering feature in these versions of AOS-W functions the same way as the default prefer-5GHz steering mode available in AOS-W 6.0 and later.</p>
Dynamic Multicast Optimization (DMO)	No	If enabled, DMO techniques will be used to reliably transmit video data.
Dynamic Multicast Optimization (DMO) Threshold (2-255)	6	Maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops.

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

Profiles

Understanding Alcatel-Lucent Configuration Profiles

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

You can apply the following types of profiles to an AP or AP group. For additional details and configuration instructions, continue to the related procedures in this section.

Perform the following initial steps to configure profiles.

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

This document section describes the profiles and settings supported in Alcatel-Lucent Configuration in the following sections:

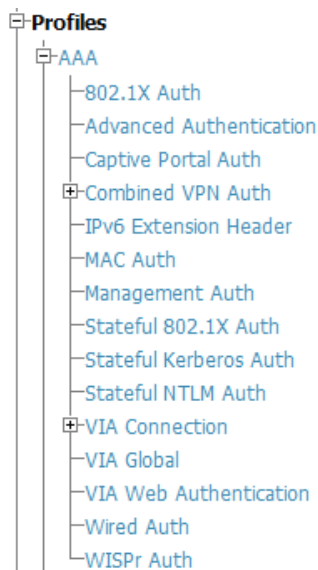
- [Profiles > AAA Overview](#)
- [Profiles > AP](#)
- [Profiles > IDS](#)
- [Profiles > Mesh](#)
- [Profiles > QoS](#)
- [Profiles > RF](#)
- [Profiles > SSID](#)

Profiles > AAA Overview

This profile type defines authentication settings for the WLAN users, including the role for unauthenticated users, and the different roles that should be assigned to users authenticated via 802.1x, MAC or SIP authentication. Perform these steps to determine the need for and to configure AAA profiles.

1. Select the **Profiles > AAA** profile heading in the navigation pane. The **AAA Profiles** page appears and lists the current profiles. [Figure 3](#) illustrates this page.

Figure 3 AAA Profiles Navigation of Alcatel-Lucent Configuration



2. From the navigation pane, you can configure the following profile types:

- **AAA Profile**—The AAA profile defines the authentication method and the default user role for unauthenticated users. This profile type references additional profiles. Refer to “[Profiles > AAA](#)” on page 51.
- **802.1x Auth**—Manages settings for the 802.11k protocol. In a 802.1k network, if the AP with the strongest signal reaches its maximum capacity, clients may connect to an underutilized AP with a weaker signal underutilized APs. Refer to “[Profiles > AAA > Advanced Authentication](#)” on page 58.
- **Advanced Authentication**—Manages timers to apply to all clients and servers. Refer to “[Profiles > AAA > Advanced Authentication](#)” on page 58.
- **Captive Portal Auth**—Captive portal authentication directs clients to a special web page that typically requires them to enter a username and password before accessing the network. This profile defines login wait times and the URLs for login and welcome pages, and manages the default user role for authenticated captive portal clients. You can also use this profile to set the maximum number of authentication failures allowed per user before that user is blacklisted. This profile includes a reference to an Server group profile. Refer to “[Profiles > AAA > Captive Portal Auth](#)” on page 60.
- **Combined VPN Auth**—Identifies the default role for authenticated VPN clients. This profile also references a server group. Refer to “[Profiles > AAA > Combined VPN Auth](#)” on page 64.
- **IPv6 Extension Header**—This profile allows you to edit the packet filter options in the IPv6 Extension Header (EH). Refer to “[Profiles > AAA > IPv6 Extension Header](#)” on page 61.
- **MAC Auth**—Defines parameters for MAC address authentication, including the case of MAC string (upper- or lower-case), the format of the diameters in the string, and the maximum number of authentication failures before a user is blacklisted. Refer to “[Profiles > AAA > MAC Auth](#)” on page 62.
- **Management Auth**—Enables or disables management authentication, and identifies the default role for authenticated management clients. This profile also references a server group. Refer to “[Profiles > AAA > Management Auth](#)” on page 65.
- **Stateful 802.11 Auth**—Enables or disables 802.1x authentication for clients on non-Alcatel-Lucent APs, and defines the default role for those users once they are authenticated. This profile also references a server group to be used for authentication. Refer to “[Profiles > AAA > Stateful 802.1X Auth](#)” on page 63.
- **Stateful NTLM Auth**—Requires that you specify a server group which includes the servers performing NTLM authentication, and a default role to be assigned to authenticated users. Refer to “[Profiles > AAA > Stateful NTLM Auth](#)” on page 66.
- **Wired Auth**—This profile merely references an AAA profile to be used for wired authentication. Refer to “[Profiles > AAA > Wired Auth](#)” on page 64.
- **WISPr Auth**—The Wireless Internet Service Provider roaming (WISPr) protocol allows users to roam between service providers. A RADIUS server is used to authenticate subscriber credentials. Refer to “[Profiles > AAA > WISPr Auth](#)” on page 67.

Profiles > AAA

Perform these steps to configure a AAA profile.

1. Select **Profiles > AAA** in the Navigation pane.
2. Select the **Add** button to create a new AAA profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 8](#).

Table 8 Profiles > AAA > New AAA Profile Settings

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

Table 8 Profiles > AAA > New AAA Profile Settings

Field	Default	Description
Referenced Profiles		
MAC Authentication Profile	None	Select a MAC Authentication profile to be referenced by the AAA profile being configured. If necessary, click the pencil or add icon to add or edit a MAC Authentication profile. Refer to “Profiles > AAA > MAC Auth” on page 62 if required. NOTE: Not supported with WLAN RAP Operation “always” after version 6.0.0.0.
MAC Authentication Server Group	default	Select a MAC Authentication server group. You can add a new server group by clicking the add icon or edit an existing server group by clicking the pencil icon.
802.1X Authentication Profile	None	Select the 802.1X Authentication Profile to be referenced by the AAA profile being configured. You can add a new profile by clicking the add icon or edit an existing profile by clicking the pencil icon. Refer to “Profiles > AAA > Advanced Authentication” on page 58 .
802.1X Authentication Server Group	None	Select the 802.1X Authentication server group. You can add a new server group by clicking the add icon or edit an existing server group by clicking the pencil icon.
RADIUS Accounting Server Group	None	Select the RADIUS accounting server group to be referenced by the AAA profile being configured. Select the add icon to create a new RADIUS server group.
Other Settings		
Initial Role	logon	Select the initial role to be referenced by the AAA profile being configured. Add a new role by clicking the add icon, or edit an existing role by clicking the pencil icon.
MAC Authentication Default Role	guest	Select the MAC authentication default role to be referenced by the AAA profile being configured. Add a new role by clicking the add icon, or edit an existing role by clicking the pencil icon. This setting requires a policy enforcement firewall license.
802.1X Authentication Default Role	guest	Select the 802.1X authentication default role to be referenced by the AAA profile being configured. Add a new role by clicking the add icon, or edit an existing role by clicking the pencil icon. This setting requires a policy enforcement firewall license.
User Derivation Rules	None	Select the user derivation rules to be referenced by the AAA profile being configured. User derivation rules are executed before client authentication. The user role can be derived from attributes from the client’s association with an AP. You configure the user role to be derived by specifying condition rules; when a condition is met, the specified user role is assigned to the client. You can specify more than one condition rule; the order of rules is important as the first matching condition is applied. Add a new rule by clicking the add icon, or edit an existing rule by clicking the pencil icon.
Wired to Wireless Roaming	Yes	Enable or disable support for roaming from wired to wireless networks.
SIP Authentication Role	None	Select the role to function for SIP authentication. The switch supports the stateful tracking of session initiation protocol (SIP) authentication between a SIP client and a SIP registry server. Upon successful registration, a user role is assigned to the SIP client. Select the add icon to create a new role, or click the pencil icon to edit an existing role. This setting requires a voice service license.

Table 8 Profiles > AAA > New AAA Profile Settings

Field	Default	Description
Enforce DHCP		When you select this option, clients must obtain an IP using DHCP before they are allowed to associate to an AP. Enable this option when you create a user rule that assigns a specific role or VLAN based upon the client device's type. Note: If a client is removed from the user table by the "Logon user lifetime" AAA timer, then that client will not be able to send traffic until it renews its DHCP.
Radius Interim Accounting		By default, the RADIUS accounting feature sends only start and stop messages to the RADIUS accounting server. Issue the interim-radius-accounting command to allow the switch to send Interim-Update messages with current user statistics to the server at regular intervals. Requires a minimum version of 6.1.0.0.
Device Type Classification		When you select this option, the switch will parse user-agent strings and attempt to identify the type of device connecting to the AP. When the device type classification is enabled, the Global client table shown in the Monitoring >Network > All WLAN Clients window shows each client's device type, if that client device can be identified. Requires a minimum version of 6.1.0.0.
L2 Authentication Fail through		When MAC authentication fails, enable this option to perform 802.1x authentication. Requires a minimum version of 6.1.0.0.
XML API Servers		
XML API Servers		Select the XML API server to support the AAA profile being configured, if required. This section is blank if there are no XML API servers.
RFC 3576 Servers		
RFC 3576 Servers		Select the RFC 3576 RADIUS server to support the AAA profile being configured, if required. This section is blank if there are no such servers.

3. Select **Add** or **Save**. The added or edited **AAA** profile appears on the **AAA Profiles** page.

Profiles > AAA > 802.1x Auth

802.1x authentication consists of three components:

- The *supplicant*, or *client*, is the device attempting to gain access to the network. You can configure the Alcatel-Lucent user-centric network to support 802.1x authentication for wired users as well as wireless users.
- The *authenticator* is the gatekeeper to the network and permits or denies access to the supplicants. The Alcatel-Lucent switch acts as the authenticator, relaying information between the authentication server and supplicant. The EAP type must be consistent between the authentication server and supplicant and is transparent to the switch.
- The *authentication server* provides a database of information required for authentication and informs the authenticator to deny or permit access to the supplicant.

The 802.1x authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS) server which can authenticate either users (through passwords or certificates) or the client computer.

An example of an 802.1x authentication server is the Internet Authentication Service (IAS) in Windows (see <http://technet2.microsoft.com/windowsserver/en/technologies/ias.mspx>).

In Alcatel-Lucent user-centric networks, you can terminate the 802.1x authentication on the switch. The switch passes user authentication to its internal database or to a "backend" non-802.1x server. This feature,

also called “AAA FastConnect,” is useful for deployments where an 802.1x EAP-compliant RADIUS server is not available or required for authentication.

Perform these steps to configure an **802.1X Auth** profile.

1. Select **Profiles > AAA > 802.1x Auth** in the Navigation pane. The details page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **802.1x Auth** profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 9](#):

Table 9 Profiles > AAA > 802.1x Auth Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Max Authentication Failures	0	Number of times a user can try to login with wrong credentials after which the user will be blacklisted as a security threat. Set to 0 to disable blacklisting, otherwise enter a non-zero integer to blacklist the user after the specified number of failures. This setting requires a wireless intrusion protection license.
Enforce Machine Authentication	No	(For Windows environments only) Select this option to enforce machine authentication before user authentication. If selected, either the Machine Authentication Default Role or the User Authentication Default Role is assigned to the user, depending on which authentication is successful. This setting requires a policy enforcement firewall license.
Machine Authentication: Default Machine Role	ap-role	Select the default role to be assigned to the user after completing machine authentication.
Machine Authentication Cache Timeout (1-1000 hrs)	24	When a Windows device boots, it logs onto the network domain using a machine account. Within the domain, the device is authenticated before computer group policies and software settings can be executed; this process is known as machine authentication. Machine authentication ensures that only authorized devices are allowed on the network. You can configure 802.1x for both user and machine authentication (select the Enforce Machine Authentication option described in Table 51 on page 272). This tightens the authentication process further since both the device and user need to be authenticated. When you enable machine authentication, there are two additional roles you can define in the 802.1x authentication profile: <ul style="list-style-type: none"> • Machine authentication default machine role • Machine authentication default user role While you can select the same role for both options, you should define the roles as per the policies that need to be enforced. Also, these roles can be different from the 802.1x authentication default role configured in the AAA profile. With machine authentication enabled, the assigned role depends upon the success or failure of the machine and user authentications. In certain cases, the role that is ultimately assigned to a client can also depend upon attributes returned by the authentication server or server derivation rules configured on the switch. This setting requires a policy enforcement firewall license.

Table 9 Profiles > AAA > 802.1x Auth Profile Settings (Continued)

Field	Default	Description
Blacklist on Machine Authentication Failure	No	Define whether the user is blacklisted upon authentication failure. This setting requires a policy enforcement firewall license.
Machine Authentication: Default User Role	ap-role	Select the default role to be assigned to the user after completing 802.1x authentication. This setting requires a policy enforcement firewall license.
Interval Between Identity Requests (1-65535 sec)	30	Specify the interval in which identity requests are to be spaced between each other.
Quiet Period after Failed Authentication (1-65535 sec)	30	Specify the amount of time in seconds in which failed authentication denies access to a user, after failed authentication.
Reauthentication Interval (60-864000 sec)	86,400 seconds	Select this option to force the client to do a 802.1x re-authentication after the expiration of the default timer for re-authentication. The default value of the timer (Reauthentication Interval) is 24 hours. If the user fails to re-authenticate with valid credentials, the state of the user is cleared. If derivation rules are used to classify 802.1x-authenticated users, then the Reauthentication timer per role overrides this setting.
Use Server Provided Reauthentication Interval	No	802.1x re-authentication can be attempted after the expiration of the default timer for re-authentication. Specify whether this is to be supported from the authentication server.
Multicast Key Rotation (60-864000 sec)	No	Define whether Multicast Key Rotation is enabled or disabled. When enabled, unicast and multicast keys are updated after each reauthorization. It is a best practice to configure the time intervals for reauthentication, multicast key rotation, and unicast key rotation to be at least 15 minutes.
Multicast Key Rotation Time Interval (60-86400 sec)	1800	When enabled, unicast and multicast keys are updated after each reauthorization. It is a best practice to configure the time intervals for reauthentication, multicast key rotation, and unicast key rotation to be at least 15 minutes. Make sure these intervals are mutually prime, and the factor of the unicast key rotation interval and the multicast key rotation interval is less than the reauthentication interval.
Unicast Key Rotation Time Interval (60-864000 sec)	900	
Authentication Server Retry Interval (5-65535 sec)	30	Specify the interface at which reauthentication is supported. The supported range is from 1 to 6,535 seconds.
Authentication Server Retry Count (0-3)	2	Define the number of times that failed authentication should be allowed to retry authentication.
Framed MTU (500-1500)	1100	Define the size, in bytes, for framed maximum transmission units.
Number of Times ID-Requests are Retried (1-10)	3	Define the number of allowable times that failed ID requests are allowed to retry the request.

Table 9 Profiles > AAA > 802.1x Auth Profile Settings (Continued)

Field	Default	Description
Maximum Number of Reauthentication Attempts (1-10)	3	Set the number of times that reauthentication is to be attempted if the first authentication attempt fails.
Maximum Number of Times Held State Can Be Bypassed (0-3)	0	Define whether a held state can be bypassed, and the number of times this is to be allowed.
Dynamic WEP Key Message Retry Count (1-3)	1	Define the number of times that failed authentication with a WEP key should be allowed to retry authentication. The range is from 0 to 3 attempts. A primary means of cracking WEP keys is to capture 802.11 frames over an extended period of time and searching for such weak implementations that are still used by many legacy devices.
Dynamic WEP Key Size (bits)	128	Specify the maximum size of the WEP key in bits. The options are 40 or 128.
Interval Between WPA/WPA2 Key Messages (10-5000 msec)	1000	Specify the key message interval in milliseconds.
Display Between EAP-Success and WPA2 Unicast Key Exchange (0-2000 msec)	0	Define EAP for RADIUS server authentication. 802.1x uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1x framework that are suitable for wireless networks include EAP-Transport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAP-Tunneled TLS (EAP-TTLS). These protocols allow the network to authenticate the client while also allowing the client to authenticate the network.
Delay between WPA/WPA2 Unicast Key Exchange (0-2000 msec)	0	Specify the delay between processing these two key times during authentication.
WPA/WPA2 Key Message Retry Count (1-10)	3	Specify the number of times that WPA or WPA2 keys are allowed to retry. The supported range is from 1 to 10.
Multicast Key Rotation	No	Enable or disable multicast key rotation, and define the related settings on this page for multicast key rotation time and interval if this field is enabled.
Unicast Key Rotation	No	Enable or disable unicast key rotation, and define the related settings on this page for unicast key rotation time and interval if this field is enabled.
Reauthentication	No	Enable or disable reauthentication. Although reauthentication and rekey timers are configurable on a per-SSID basis, an 802.1x transaction during a call can affect voice quality. If a client is on a call, 802.1x reauthentication and rekey are disabled by default until the call is completed. You disable or re-enable the "voice aware" feature in the 802.1x authentication profile.
Opportunistic Key Caching	Yes	Enable or disable opportunistic key caching (also configured in the 802.1x Authentication profile). This supports WPA2 clients.
Validate PMKID	No	Define whether PMKID authentication should be validated.
Use Session Key	No	Specify whether a client session should use a security key.

Table 9 Profiles > AAA > 802.1x Auth Profile Settings (Continued)

Field	Default	Description
Use Static Key	No	The IEEE 802.1x authentication standard allows for the use of keys that are dynamically generated on a per-client basis, or as a static key that is the same on all devices in the network). Define whether to use a static key with this setting.
xSec MTU (1024 - 1500 Bytes)	1300 bytes	Define the maximum transmission unit size in bytes.
Termination	No	Select this option to terminate 802.1x authentication on the switch.
Termination EAP-Type TLS	No	Specify if the EAP termination type is TLS.
Termination EAP-Type PEAP	0	Specify EAP-PEAP termination. 802.1x authentication based on PEAP with MS-CHAPv2 provides both computer and user authentication. If a user attempts to log in without the computer being authenticated first, the user is placed into a more limited "guest" user role. Windows domain credentials are used for computer authentication, and the user's Windows login and password are used for user authentication. A single user sign-on facilitates both authentication to the wireless network and access to the Windows server resources.
Termination Inner EAP-Type MSCHAPv2	No	Enable or disable this setting. You can enable caching of user credentials on the switch as a backup to an external authentication server. The EAP-Microsoft Challenge Authentication Protocol version 2 (MS-CHAPv2), described in RFC 2759, is widely supported by Microsoft clients.
Termination Inner EAP-Type GTC	No	Enable or disable GTC. EAP-Generic Token Card (GTC): Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the switch as a backup to an external authentication server.
Token Caching	Disabled	Specify whether EAP token caching is enabled or disabled.
Token Caching Period (1-240 hrs)	24	Specify token caching, in hours. The supported range is from 1 to 240 hours.
CA-Certificate		Type the CA certificate imported into the switch.
Server-Certificate		Specify a server certificate. The list of available certificates is taken from the computer certificate store on which IAS is running. In this case, a self-signed certificate was generated by the local certificate authority and installed on the IAS system. On each wireless client device, the local certificate authority is added as a trusted certificate authority, thus allowing this certificate to be trusted.
TLS Guest Access	No	Specify if TLS authentication supports guest users. User-level authentication is performed by an external RADIUS server using PPP EAP-TLS. In this scenario, client and server certificates are mutually authenticated during the EAP-TLS exchange. During the authentication, the switch encapsulates EAP-TLS messages from the client into RADIUS messages and forwards them to the server.
TLS Guest Role	ap-role	Specify the TLS authentication role that will support guests. This setting requires a policy enforcement firewall license.

Table 9 Profiles > AAA > 802.1x Auth Profile Settings (Continued)

Field	Default	Description
Ignore EAPOL-START After Authentication	No	Enable or disable this setting. EAP authentication starts with a EAPOL-start frame that is sent by the wireless client to the AP. Upon reception of such a frame, the AP responds back to the wireless client with an EAP-Identify-Request and also does internal resource allocation. Attackers can use this vulnerability by sending a lot of EAPOL-start frames to the Access point, either by spoofing the MAC address or by emulating wireless clients. This forces the AP to allocate increasing resource and eventually bringing it down. Enable this setting to reduce the risk.
Handle EAPOL-Logoff	No	Specify whether authentication should manage logoff activity.
Ignore EAP ID During Negotiation	No	Specify whether EAP should be ignored during authentication.
WPA-Fast-Handover	No	In the 802.1x Authentication profile, the WPA fast handover feature allows certain WPA clients to use a pre-authorized PMK, significantly reducing handover interruption. Check with the manufacturer of your handset to see if this feature is supported. This feature is disabled by default.
Disable Rekey and Reauthentication for Clients on Call	No	Although reauthentication and rekey timers are configurable on a per-SSID basis, an 802.1x transaction during a call can affect voice quality. If a client is on a call, 802.1x reauthentication and rekey are disabled by default until the call is completed. You disable or re-enable the “voice aware” feature in the 802.1x authentication profile. This setting requires a voice service license.

Select **Add** or **Save**. The added or edited **802.1x Auth** profile appears on the **AAA Profiles** page, and on the **802.1x Auth** details page.

Profiles > AAA > Advanced Authentication

In Advanced Authentication, you can apply timers and DNS query intervals. Follow these steps to configure an Advanced Authentication profile.

1. Select **Profiles > AAA > Advanced Authentication** in the **Alcatel-Lucent Navigation** pane. The details page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **Advanced Authentication** profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 10](#):

Table 10 Profiles > AAA > Advanced Authentication Profile Settings

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

Table 10 Profiles > AAA > Advanced Authentication Profile Settings

Field	Default	Description
Authentication Timers		
User Idle Timeout	300 seconds	Maximum period, in seconds, after which a client is considered idle if there is no user traffic from the client. The timeout period is reset if there is a user traffic. After this timeout period has elapsed, the switch sends probe packets to the client; if the client responds to the probe, it is considered active and the User Idle Timeout is reset (an active client that is not initiating new sessions is not removed). If the client does not respond to the probe, it is removed from the system. Range: 30 to 15300 seconds
User Stats Timeout	600	Set the timeout value for user stats reporting in seconds. The supported range is 300-600 seconds, or 5-10 minutes, and the default value is 600 seconds. Requires a minimum version of 6.1.0.0.
Fast Aging of Multiple Instances of User		When this feature is enabled, the switch actively sends probe packets to all users with the same MAC address but different IP addresses. The users that fail to respond are purged from the system. This command enables quick detection of multiple instances of the same MAC address in the user table and removal of an “old” IP address. This can occur when a client (or an AP connected to an untrusted port on the switch) changes its IP address.
Dead Time for down Authentication Server (0-60 min)	10 minutes	Maximum period, in minutes, that the switch considers an unresponsive authentication server to be “out of service”. This timer is only applicable if there are two or more authentication servers configured on the switch. If there is only one authentication server configured, the server is never considered out of service and all requests are sent to the server. If one or more backup servers are configured and a server is unresponsive, it is marked as out of service for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as down for the dead time. Range: 0–50
Unauthenticated User Lifetime (0-255 min)	5 minutes	Maximum time, in minutes, unauthenticated clients are allowed to remain logged on. Range: 0–255
RADIUS Client		
RFC 3576 Server UDP Port (1-65535)	3799	Configures the UDP port to receive requests from a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576, “Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)”. NOTE: This parameter can only be used on the master switch.
DNS Query Interval		
DNS Query Interval (1-1440 min)	15	If you define a RADIUS server using the FQDN of the server rather than its IP address, the switch will periodically generate a DNS request and cache the IP address returned in the DNS response. By default, DNS requests are sent every 15 minutes

3. Select **Add** or **Save**. The added or edited **Advanced Authentication** profile appears on the **Profiles > AAA** page.

Profiles > AAA > Captive Portal Auth

In this section, you create an instance of the captive portal authentication profile and the AAA profile. For the captive portal authentication profile, you specify the previously-created auth-guest user role as the default user role for authenticated captive portal clients and the authentication server group (“Internal”).

Perform these steps to configure a **Captive Portal Authentication** profile.

1. Select **Profiles > AAA > Captive Portal Auth** in the **Alcatel-Lucent Configuration Navigation** pane.
2. Select the **Add** button to create a new **Captive Portal Auth** profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 11](#).

Table 11 Profiles > AAA > Captive Portal Auth Profile Settings

Field	Default	Description
General Settings		
Name	Blank	Enter the name of the Captive Portal Authentication profile.
Referenced Profiles		
Server Group	default	Enter the name of the internal VPN authentication server group, or the server group that performs 802.1x authentication.
Other Settings		
Default Role	default	Role assigned to the Captive Portal user upon login. When both user and guest logon are enabled, the default role applies to the user logon; users logging in using the guest interface are assigned the guest role. The Policy Enforcement Firewall license must be installed.
Default Guest Role	default	Role assigned to a guest user upon login.
Redirect Pause (0-60 sec)	10	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link.
User Login	Yes	Enables Captive Portal with authentication of user credentials.
Guest Login	No	Enables Captive Portal logon without authentication.
Logout Popup Window	Yes	Enables a pop-up window with the Logout link for the user to logout after logon. If this is disabled, The user remains logged in until the user timeout period has elapsed or the station reloads.
Use HTTP Authentication	No	Use HTTP protocol on redirection to the Captive Portal page. If you use this option, modify the captive portal policy to allow HTTP traffic.
Logon Wait Minimum Wait (1-10 sec)	5	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter.
Logon Wait Maximum Wait (0-10 sec)	10	Maximum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter.
Logon Wait CPU Utilization Threshold (0-100%)	60	CPU utilization percentage above which the Logon wait interval is applied when presenting the user with the logon page.
Max Authentication Failures	0	Maximum number of authentication failures before the user is blacklisted. The range is 1-10. Requires a Wireless Intrusion Protection license or an RFprotect license.
Show FQDN	No	Allows the user to see and select the fully-qualified domain name (FQDN) on the login page.

Table 11 Profiles > AAA > Captive Portal Auth Profile Settings (Continued)

Field	Default	Description
Use CHAP (Non-standard)	No	Use CHAP protocol. You should not use this option unless instructed to do so by a representative from Alcatel-Lucent.
Sygate-on-demand-agent	No	Enables client remediation with Sygate-on-demand-agent (SODA). Requires a Client Integrity license and a version earlier than 6.0.0.0.
Login Page	/auth/index.html	URL of the page that appears for the user logon. This can be set to any URL.
Welcome Page	/auth/welcome.html	URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL.
Show Welcome Page	Yes	Enables the display of the welcome page. If this option is disabled, redirection to the web URL happens immediately after logon.
Add switch IP address in redirection URL	No	Sends the switch IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the switch from which a request originated by parsing the 'switchip' variable in the URL.
Allow Only One Active User Session	No	Allows only one active user session at a time. Requires a minimum version of 3.4.0.0.
Add a Controller Interface in Redirection URL	0.0.0.0	Select this option to send the switch's IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the switch from which a request originated by parsing the 'switchip' variable in the URL. Requires a Public Wi-Fi Access license and a minimum version of 3.4.1.0
Show the Acceptable Use Policy Page		Show the acceptable use policy page before the logon page. Requires a minimum version of 3.4.0.3.
Add User VLAN in Redirection URL	No	Enable this option to send the user VLAN in the redirection URL when external captive portal servers are used. Requires a Public Wi-Fi Access license and a minimum version of 3.4.1.0
White List Net Destinations		This setting allows you to select net destinations for your whitelist. Requires a Public Wi-Fi Access license.
Black List Net Destinations		This setting allows you to select net destinations for your blacklist. Requires a Public Wi-Fi Access license.

3. Select **Add** or **Save**. The added or edited **Captive Portal Auth** profile appears on the **AAA Profiles** page.

The captive portal authentication profile specifies the captive portal login page and other configurable parameters. The initial user role configuration must include the applicable captive portal authentication profile instance. Therefore, you need to modify the guest-logon user role configuration to include the guestnet captive portal authentication profile.

Profiles > AAA > IPv6 Extension Header

This profile allows you to edit the packet filter options in the IPv6 Extension Header (EH). AOS-W firewall is enhanced to process the EH to enable IPv6 packet filtering. You can now filter the incoming IPv6 packets based on the EH type. You can edit the packet filter options in the default EH.



This profile depends on the switch having a Policy Enforcement Firewall license and a minimum version of 6.1.0.0.

Perform these steps to configure an **IPv6 Extension Header** profile.

1. Select **Profiles > AAA > IPv6 Extension Header** in the Navigation pane.

Select the **Add** button to create a new **IPv6 Extension Header** profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 12](#):

Table 12 Profiles > AAA > IPv6 Extension Header

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the IPv6 Extension Header profile.
Denied Extension Header Filter Items		
Match IPv6 Header Type (0-255)	hop-by-hop	Specify one of the following EH types: <ul style="list-style-type: none"> ● authentication: Matches the IPv6 authentication header ● dest-option: Matches the IPv6 destination-option header ● esp: Matches the IPv6 encapsulation security payload header ● fragment: Matches the IPv6 fragment header ● hop-by-hop: Matches the IPv6 hop-by-hop header ● mobility: Matches the IPv6 mobility header ● routing: Matches the IPv6 routing header

2. Select **Add** or **Save**. The added or edited **IPv6 Extension Header** profile appears on the **IPv6 Extension Header** details page.

Profiles > AAA > MAC Auth

Before configuring MAC-based authentication, you must configure the following:

- The user role that will be assigned as the default role for the MAC-based authenticated clients. You configure the default user role for MAC-based authentication in the AAA profile. If derivation rules exist or if the client configuration in the internal database has a role assignment, these values take precedence over the default user role.
- Authentication server group that the switch uses to validate the clients. The internal database can be used to configure the clients for MAC-based authentication.

Perform these steps to configure a **MAC Auth** profile.

1. Select **Profiles > AAA > MAC Auth** in the Navigation pane.
2. Select the **Add** button to create a new **MAC Auth** profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 13](#):

Table 13 Profiles > AAA > MAC Auth Profile Settings

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

Table 13 Profiles > AAA > MAC Auth Profile Settings (Continued)

Field	Default	Description
Other Settings		
Delimiter	none	Delimiter used in the MAC string: <ul style="list-style-type: none"> colon specifies the format xx:xx:xx:xx:xx:xx dash specifies the format xx-xx-xx-xx-xx-xx none specifies the format xxxxxxxxxxxx oui-nic specifies the format xxxxxx-xxxxxx (use the client device's OUI as a delimiter) - for 6.1.0.0 versions or later
Case	lower	The case (upper or lower) used in the MAC string.
Max Authentication Failures (0-10)	0	Number of times a station can fail to authenticate before it is blacklisted. A value of 0 disables blacklisting.

3. Select **Add** or **Save**. The added or edited **MAC Auth** profile appears on the **Profiles > AAA** page, and on the **MAC Auth** details page.

Profiles > AAA > Stateful 802.1X Auth

This profile type enables or disables 802.1x authentication for clients on non-Alcatel-Lucent APs, and defines the default role for those users once they are authenticated. This profile also references a server group to be used for authentication.

Perform these steps to configure a **Stateful 802.1X Auth** profile.

1. Select **Profiles > AAA > Stateful 802.11 Auth** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Stateful 802.11 Auth** profile, or click the pencil icon next to an existing profile to edit. Complete the settings described in [Table 14](#):

Table 14 Profiles > AAA > Stateful 802.1X Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Referenced Profiles		
Server Group		Select the AAA authentication server group. Select the pencil icon to edit an existing server group or click the add icon to create a new server group.
Other Settings		
Default Role	ap-role	The user role to be associated with this authentication profile.
Timeout (1-20 sec)	10	Maximum time, in seconds, that the server waits before timing out the request.
Enabled	No	When enabled with Yes , activates the authentication server.

3. Select **Add** or **Save**. The added or edited **Stateful 802.11 Auth** profile appears on the **AAA Profiles** page, and on the **Stateful 802.11 Auth** details page.

Profiles > AAA > Wired Auth

This profile type references an AAA profile to be used for wired authentication.

Perform these steps to configure a **Wired Auth** profile.

1. Select **Profiles > AAA > Wired Auth** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Wired Auth** profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 15](#):

Table 15 Profiles > AAA > Wired Auth Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the Wired Authentication profile.
Referenced Profiles		
AAA	None	From the drop-down menu, select the AAA profile for wired authentication. Select the pencil icon to edit an existing profile or click the add icon to create a new profile.

3. Select **Add** or **Save**. The added or edited **Wired Auth** profile appears on the **AAA Profiles** page, and on the **Wired Auth** details page.

Profiles > AAA > Combined VPN Auth

A VPN Authentication profile identifies the default role for authenticated VPN clients. This profile also references a server group.

Before you enable VPN authentication, you must configure the authentication server(s) and server group that the switch will use to validate the remote AP. When you provision the remote AP, you configure IPsec settings for the AP, including the username and password. This username and password must be validated by an authentication server before the remote AP is allowed to establish a VPN tunnel to the switch. The authentication server can be any type of server supported by the switch, including the switch's internal database.

Perform these steps to configure a **Combined VPN Auth** profile.

1. Select **Profiles > AAA > Combined VPN Auth** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **VPN Auth** profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 16](#):

Table 16 Alcatel-Lucent Configuration > Profiles > AAA > VPN Auth Profile Settings

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

Table 16 Alcatel-Lucent Configuration > Profiles > AAA > VPN Auth Profile Settings

Field	Default	Description
Referenced Profiles		
Server Group		Select the AAA authentication server group. Select the pencil icon to edit an existing server group or click the add icon to create a new server group.
Other Settings		
Default Role	default-vpn-role	Select the role to be associated with this authentication profile.
Max Authentication failures (0-10)	0	Enter the number of times a station can fail to authenticate before it is blacklisted. A value of 0 disables blacklisting.
Check Certificate Common Name against AAA Server	Yes	This field appears if you are adding or modifying a RAP VPN Authentication Profile. If you use client certificates for user authentication, enable this option to verify that the certificate's common name exists in the server. This parameter is enabled by default in the default-cap and default-rap VPN profiles, and disabled by default on all other VPN profiles. Requires a minimum version of 6.1.0.0.

3. Select **Add** or **Save**. The added or edited **Combined VPN Auth** profile appears on the **AAA Profiles** page, and on the **VPN Auth** details page.

Profiles > AAA > Management Auth

Users who need to access the switch to monitor, manage, or configure the Alcatel-Lucent user-centric network can be authenticated with RADIUS, TACACS+, or LDAP servers or the internal database.

Perform these steps to configure a **Management Auth** profile.

1. Select **Profiles > AAA > Management Auth** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Management Auth** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 17](#):

Table 17 Profiles > AAA > Management Auth Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Referenced Profiles		
Server Group		Select the AAA authentication server group. Select the pencil icon to edit an existing server group or click the add icon to create a new server group.

Table 17 Profiles > AAA > Management Auth Profile Settings

Field	Default	Description
Other Settings		
Default Role	root	The role to be associated with this authentication profile: <ul style="list-style-type: none"> ● guest-provisioning: Allows the user to create guest accounts. ● location-api-mgmt: Permits access to location API information. You can log in, however, you cannot use any commands. ● network-operations: Permits access to Monitoring, Reports, and Events pages in the WebUI. You can log in; however, you can only use a subset of commands to monitor the switch. ● read-only: Permits access to monitoring pages only. ● root: Permits access to all management functions on the switch.
Enable	No	When enabled, this setting activates the authentication server.

3. Select **Add** or **Save**. The added or edited **Management Auth** profile appears on the **AAA Profiles** page, and on the **Management Auth** details page.

Profiles > AAA > Stateful NTLM Auth

When the user logs off or shuts down the client machine, this profile allows the user to remain in the authenticated role until the user ages out. Aging out means the user has sent no traffic for the amount of time specified for the **Timeout** parameter of this profile.

The Stateful NT LAN Manager (NTLM) Authentication profile requires that you specify the following components:

- a server group that includes the servers performing NTLM authentication
- a default role to be assigned to authenticated users.

The Wireless Internet Service Provider roaming (WISPr) protocol allows users to roam between service providers. A RADIUS server is used to authenticate subscriber credentials.

For details on defining a Windows server used for NTLM authentication, refer to [“Security > Server Groups > Windows” on page 149](#).

Perform these steps to configure a **Stateful NTLM Auth** profile.

1. Select **Profiles > AAA > Stateful NTLM Auth** in the **Alcatel-Lucent Navigation** pane. The details page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **Stateful NTLM Auth** profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 18](#):

Table 18 Profiles > AAA > Stateful NTLM Auth Profile Settings

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

Table 18 Profiles > AAA > Stateful NTLM Auth Profile Settings (Continued)

Field	Default	Description
Other Settings		
Timeout	10	Set the aging out or timeout period, which is the amount of time for which the user sends no traffic. The user's role remains authenticated unless this period of time is exceeded.
Server Group	default	Select a server from the drop-down menu. You can edit servers with the Pencil icon or add additional servers with the Add icon.
Default Role	guest	Select a user role to associate with the user from the drop-down menu. You can edit roles with the Pencil icon or add additional roles with the Add icon.
Mode	No	Indicates whether this profile is enabled or disabled. A minimum of AOS-W 6.0.0.0 is required.

3. Select **Add** or **Save**. The added or edited profile appears on the **Stateful NTLM Auth** page, and on the details page.

Profiles > AAA > WISPr Auth

The Wireless Internet Service Provider roaming (WISPr) protocol allows users to roam between service providers. A RADIUS server is used to authenticate subscriber credentials.

AOS-W supports stateful 802.1x authentication, stateful NTLM authentication and authentication for Wireless Internet Service Provider roaming (WISPr). Stateful authentication differs from 802.1x authentication in that the switch does not manage the authentication process directly, but monitors the authentication messages between a user and an external authentication server, and then assigns a role to that user based upon the information in those authentication messages. WISPr authentication allows clients to roam between hotspots using different ISPs.

Refer to the *AOS-W User Guide* for additional information about stateful NTLM and WISPr authentication.

Perform these steps to configure a **WISPr Auth** profile.

1. Select **Profiles > AAA > WISPr Auth** in the **Alcatel-Lucent Navigation** pane. The details page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **Stateful NTLM Auth** profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 19](#):

Table 19 Profiles > AAA > WISPr Auth Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Server Group	default	Select the AAA authentication server group. Select the pencil icon to edit an existing server group or click the add icon to create a new server group.
Default Role	guest	Select the default role assigned to users that complete WISPr authentication.

Table 19 Profiles > AAA > WISPr Auth Profile Settings (Continued)

Field	Default	Description
Max Authentication Failures	0	Number of times a user can try to login with wrong credentials after which the user will be blacklisted as a security threat. Set to 0 to disable blacklisting, otherwise enter a non-zero integer to blacklist the user after the specified number of failures. This setting requires a wireless intrusion protection license.
Logon Wait Minimum Wait	5	Define the minimum wait time for additional logon attempts. If the switch's CPU utilization has surpassed the Logon Wait CPU utilization threshold value, this wait parameter defines the minimum number of seconds a user will have to wait prior to retrying a login attempt. The supported range is 1 to 10 seconds.
Logon Wait Maximum Wait	10	Define the maximum wait time for additional logon attempts. If the switch's CPU utilization has surpassed the Login wait CPU utilization threshold value, this wait parameter defines the maximum number of seconds a user will have to wait prior to retrying a login attempt. The supported range is form 1 to 10 seconds.
Logon Wait CPU Utilization Threshold	60	Set the percentage of CPU utilization at which the maximum and minimum logon wait times are enforced. The supported range is from 1% to 100%.
WISPr Location-ID ISO Country Code		Enter the ISO Country Code section of the WISPr Location ID.
WISPr Location-ID E.164 Area Code		Enter the E.164 Area Code section of the WISPr Location ID.
WISPr Location-ID SSID/zone		Enter the SSID/Zone section of the WISPr Location ID.
WISPr Operator Name		Enter a name identifying the hotspot operator.
WISPr Location Name		Enter a name identifying the hotspot location. If no name is defined, the parameter will use the name of the AP to which the user has associated.

3. Select **Add** or **Save**. The added or edited profile appears on the **Stateful NTLM Auth** page, and on the details page.

Profiles > AP

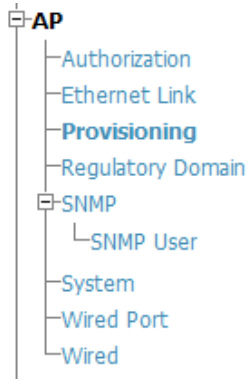
Display the currently configured AP profiles by navigating to **Device Setup > Profiles > AP**.

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 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 the following types of profiles to an AP or AP group:

Perform these steps to configure AP profiles.

1. Select the **Profiles > AP** profile heading in the navigation pane.

Figure 4 Profiles > AP in Alcatel-Lucent Configuration



2. From the navigation pane, you can configure the following profile types. The following AP profiles configure AP operation parameters, regulatory domain, SNMP information, and more:
 - **Authorization**—Allows you to assign an to a provisioned but unauthorized AP to a AP group with a restricted configuration profile. Refer to “[Profiles > AP > Authorization](#)” on page 69.
 - **Ethernet Link**—Sets the duplex mode and speed of AP’s Ethernet link. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link. Refer to “[Profiles > AP > SNMP](#)” on page 73.
 - **Provisioning** —Defines a group of provisioning parameters for an AP or AP group. Refer to “[Profiles > AP > Provisioning](#)” on page 71.
 - **Regulatory Domain**—Defines an AP’s country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios. Refer to “[Profiles > AP > Regulatory Domain](#)” on page 72.
 - **Wired Port**—Allows you to enable or disable the wired port, define an AAA profile for wired port devices, and associate the port with an ethernet link profile that defines its speed and duplex values. Refer to “[Profiles > AP > Wired Port](#)” on page 78.
 - **Wired**—Controls whether 802.11 frames are tunneled to the switch using Generic Routing Encapsulation (GRE) tunnels, bridged into the local Ethernet LAN (for remote APs), or a configured for combination of the two (split-mode). This profile also configures the switching mode characteristics for the port, and sets the port as either trusted or untrusted. Refer to “[Profiles > AP > System](#)” on page 74.
 - **SNMP**—Defines and enables SNMP settings, to include community string and SNMP user profiles. “[Profiles > AP > SNMP](#)” on page 73.
 - **SNMP User**—Sets the SNMP user name and authentication profile to support more general SNMP profiles. Refer to “[Profiles > AP > SNMP > SNMP User](#)” on page 74.
 - **System**—Defines administrative options for the switch, including the IP addresses of the local, backup, and master switches, Real-time Locating Systems (RTLS) server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps. Refer to “[Profiles > AP > System](#)” on page 74.

Profiles > AP > Authorization

Remote AP configurations include an authorization profile that specifies which profile settings should be assigned to a remote AP that has been provisioned but not yet authenticated at the remote site. By default, these yet-unauthorized APs are assigned the pre-defined profile **NoAuthApGroup**. This configuration allows the user to connect to an unauthorized remote AP via a wired port then enter a corporate username and password.

Once a valid user has authorized the AP and the remote AP will be marked as authorized on the network. The remote AP will then download the configuration assigned to that AP by its permanent AP group.

Perform these steps to configure an **Authorization** profile.

1. Select **Profiles > AP > Authorization** in the Navigation pane.
2. Select the **Add** button to create a new profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 20](#):

Table 20 Profiles > AP > Authorization Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Referenced Profiles		
AP Authorization Group	None	Designates the profile to reference. The dropdown menu includes the following options: <ul style="list-style-type: none"> • default • NoAuthApGroup

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

Profiles > AP > Ethernet Link

The configurable speed defined in this profile is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link.

Perform these steps to configure a **Ethernet Link** profile.

1. Select **Profiles > AP > Ethernet Link** in the Navigation pane.
2. Select the **Add** button to create a new profile, or click the pencil icon next to an existing profile to edit. Complete the settings as described in [Table 21](#):

Table 21 Profiles > AP > Ethernet Link Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Speed (Mbps)	auto	Designates the speed of the Ethernet link for this profile. Options are 10 , 100 , or 1000 Mbits.
Duplex	auto	Defines this profile to support duplex Ethernet. Options are full , half , or auto .

3. Select **Add** or **Save**. The added or edited **Ethernet Link** profile appears on the **AAA Profiles** page, and on the **802.1x Auth** details page.

Profiles > AP > Provisioning

Perform these steps to define a provisioning profile for an AP or group of APs:

1. Select **Profiles > AP > System** in the **Alcatel-Lucent Navigation** pane. This page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **System** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 22](#):

Table 22 Profiles > AP > Provisioning Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Remote-AP	No	Whether the AP you are provisioning is a remote AP.
Set or Clear Master IP/FQDN		Whether to specify or clear the definition for the Master IP or fully qualified domain name of the AP.
Domain Name		Fully-qualified domain name (FQDN) for the AP. Requires a version <i>earlier</i> than 6.1.0.0.
PPPoE User Name		Point-to-Point Protocol over Ethernet (PPPoE) username for the AP.
PPPoE Password		PPPoE password for the AP.
PPPoE Service Name		PPPoE service name for the AP.
USB User Name		The PPP username provided
USB Password		A PPP password, if provided
USB Device Type		The USB device type.
USB Device Identifier		The USB device identifier.
USB Dial String		The dial string for the USB modem.
USB Initialization String		The initialization string for the USB modem.
USB TTY Device Path		The TTY device path for the USB modem.
USB TTY Device Control Path		Requires a minimum version of 6.1.0.0.
Link Priority Ethernet (0-255)	0	Set the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary switch link.

Table 22 Profiles > AP > Provisioning Profile Settings (Continued)

Field	Default	Description
Link Priority Cellular (0-255)	0	Set the priority of the wired uplink. Each uplink type has an associated priority; wired ports having the highest priority by default.
Uplink VLAN (0-4095)	0	If you configure an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink VLAN of 0, which disables this feature. NOTE: If an AP is provisioned with an uplink VLAN, it <i>must be connected to a trunk mode port</i> or the AP's frames will be dropped.

Profiles > AP > Regulatory Domain

This profile type defines an AP's country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios.

With the implementation of the high-throughput IEEE 802.11n draft standard, 40 MHz channels were added in addition to the existing 20 MHz channel options. Available 20 MHz and 40 MHz channels are dependent on the country code entered in the regulatory domain profile.

The following channel configurations are now available in AOS-W:

- A 20 MHz channel assignment consists of a single 20 MHz channel assignment. This channel assignment is valid for 802.11a/b/g and for 802.11n 20 MHz mode of operation.
- A 40 MHz channel assignment consists of two 20 MHz channels bonded together (a bonded pair). This channel assignment is valid for 802.11n 40 MHz mode of operation and is most often utilized on the 5 GHz frequency band. If high-throughput is disabled, a 40 MHz channel assignment can be configured, but only the primary channel assignment will be utilized. 20 MHz clients can also associate using this configuration, but only the primary channel will be utilized.

A high-throughput (HT) AP can use a 40 MHz channel pair comprised of two adjacent 20 MHz channels available in the regulatory domain profile for your country. When ARM is configured for a dual-band AP, it will dynamically select the primary and secondary channels for these devices. It can, however, continue to scan all changes in the a+b/g bands to calculate interference and detect rogue APs.

Perform these steps to configure a **Regulatory Domain** profile.

1. Select **Profiles > AP > Regulatory Domain** in the Navigation pane. This page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **Regulatory Domain** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 23](#):

Table 23 Profiles > AP > Regulatory Domain Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Country Code		Designate the country with the 802.1X regulatory standard relevant to this WLAN.

Table 23 Profiles > AP > Regulatory Domain Profile Settings (Continued)

Field	Default	Description
Valid 802.11a 40MHz Channel Pairs		Select a 40MHz channel pair for 802.11a. A high-throughput (HT) AP can use a 40 MHz channel pair comprised of two adjacent 20 MHz channels available in the regulatory domain profile for your country. When ARM is configured for a dual-band AP, it will dynamically select the primary and secondary channels for these devices. It can, however, continue to scan all changes in the a+b/g bands to calculate interference and detect rogue APs.
Valid 802.11g 40 MHz Channel Pairs		Select a 40MHz channel pair for 802.11g
Valid 802.11a 40MHz Channels		Specify the valid channels for 40MHz channel pairing in 802.11a.
Valid 802.11g 40 MHz Channels		Specify the valid channels for 40MHz channel pairing in 802.11g.

3. Select **Add** or **Save**. The added or edited **Regulatory Domain** profile appears on the **Regulatory Domain Profiles** page.

Profiles > AP > SNMP

Alcatel-Lucent switches and APs support versions 1, 2c, and 3 of Simple Network Management Protocol (SNMP) for reporting purposes only. In other words, SNMP cannot be used for setting values in an Alcatel-Lucent system in the current AOS-W version. Perform these steps to configure a **SNMP** profile.

1. Select **Profiles > AP > SNMP** in the Navigation pane.
2. Select the **Add** button to create a new **SNMP** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 24](#):

Table 24 Profiles > AP > SNMP Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
SNMP Enable	Yes	Enable or disable SNMP in this profile.
Enter Community String		Text field allows you to type one or multiple SNMP community strings applied to this profile.
Select SNMP User Profile		
Select SNMP User Profile		If SNMP is enabled in this profile, and one or more profiles have been configured, select the corresponding SNMP profile from this list.

3. Select **Add** or **Save**. The added or edited **SNMP** profile appears on the **SNMP** profiles page.

Profiles > AP > SNMP > SNMP User

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

1. Select **Profiles > AP > SNMP > SNMP User** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new user, or click the **pencil** icon next to an existing user to edit that user. Complete the settings as described in [Table 25](#):

Table 25 Profiles > AP > SNMP > SNMP User Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Name of the SNMP user profile. This is the name by which the SNMP user is managed and accessed when cited by SNMP profiles
Other Settings		
User Name	Blank	Actual name of the network user to be supported by this SNMP profile in Alcatel-Lucent Configuration
Authentication Profile	none	Select a protocol from the drop-down menu. Options are as follows: <ul style="list-style-type: none">● none—Uses no authentication type for the user being defined.● md5—Sets the MD5 hashing algorithm for the user that hashes a cleartext password.● sha—Sets the SHA hashing algorithm for the user that hashes a cleartext password.

3. Select **Add** or **Save**. The added or edited **SNMP** user appears on the **SNMP User** page. This user can now be referenced in SNMP profiles.

Refer to the *AOS-W 6.1 MIB* guide for additional information about SNMP traps.

Profiles > AP > System

Using DNS, the remote AP receives multiple IP addresses in response to a host name lookup. Known as the backup switch list, remote APs go through this list to associate with a switch. If the primary switch is unavailable or does not respond, the remote AP continues through the list until it finds an available switch. This provides redundancy and failover protection.

If the remote AP loses connectivity on the IPsec tunnel to the switch, the remote AP establishes connectivity with a backup switch from the list and automatically reboots. Network connectivity is lost during this time. You can also configure a remote AP to revert back to the primary switch when it becomes available. To complete this scenario, you must also configure the LMS IP address and the backup LMS IP address.

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

1. Select **Profiles > AP > System** in the **Alcatel-Lucent Navigation** pane. This page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **System** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 26](#):

Table 26 Profiles > AP > System Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
LMS IP		In multi-switch networks, this parameter specifies the IP address of the local management switch (LMS)—the Alcatel-Lucent switch—which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. This can be the IP address of the local or master switch. When using redundant controllers as the LMS, set this parameter to be the VRRP IP address to ensure that APs always have an active IP address with which to terminate sessions. For those APs that need to boot off the local switch, configure the LMS IP address to point to the new local switch.
LMS IPv6		The IPv6 address of the local management switch (LMS)—the Alcatel-Lucent switch which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. Requires a minimum version of 6.1.0.0
Backup LMS IP		In multi-switch networks, specify the IPv4 address of a <i>backup</i> to the IP address specified with the LMS IP field.
Backup LMS IPv6		For multi-switch networks, specify the IPv6 address of a backup to the IP address specified with the LMS IPv6 field.
LMS Preemption	No	The AP fallback feature allows an AP associated with the backup switch (backup LMS) to fail back to the primary switch (primary LMS) if it becomes available. Enable LMS preemption with this field.
LMS Hold-down Period (1-3600 sec)	600	Enter the amount of time the remote AP must wait before moving back to the primary switch.
Number of IPSEC Retries	360	Number of times the AP will try to create an IPsec tunnel with the master switch before the AP will reboot. If you specify a value of 0, and AP will not reboot if it cannot create the IPsec tunnel. The supported range of values is 0-1000 retries, and the default value is 360 retries.
Master switch IP Address		Enter the IP address of the master switch.
LED Operating Mode	normal	The operating mode for the AP LEDs. Options are normal and off.
RF Band	g	Indicates the band for mesh operation for multiband radios. Select a or g. Important: If you create more than one mesh cluster profile for an AP or AP group, each mesh cluster profile must use the same band.
RF Band for AM mode scanning	all	Scanning band for multiple RF radios. Options are all, a, or g. Requires a minimum of 6.0.0.0.
Double Encrypt	No	The double encryption feature applies only for traffic to and from a wireless client that is connected to a tunneled SSID. When this feature is enabled, all traffic (which is already encrypted using Layer-2 encryption) is re-encrypted in the IPsec tunnel. When this feature is disabled, the wireless frame is only encapsulated inside the IPsec tunnel. All other types of data traffic between the switch and the AP (wired traffic and traffic from a split-tunneled SSID) are always encrypted in the IPsec tunnel.

Table 26 Profiles > AP > System Profile Settings (Continued)

Field	Default	Description
Native VLAN ID (0-4094)	1	Enter the ID of the native VLAN. The supported range is from 0 to 4094.
SAP MTU		Specify the Service Access Point (SAP) maximum transmission unit (MTU) in bytes. The range is 1024 to 1578 bytes.
Bootstrap Threshold (1-65535)	8	Enter a threshold value from 0 to 65,535. Adjust the bootstrap threshold to 30 if the network experiences packet loss. This makes the AP recover more slowly in the event of a failure, but it will be more tolerant to heartbeat packet loss. The default maximum request retries and bootstrap threshold settings for most mesh networks is recommended; however, if you must keep your mesh network alive, you can modify the settings as described in this section. The modified settings are not applicable if mesh portals are directly connected to the switch.
Request Retry Interval	10	Enter in seconds the amount of time for retries. The supported range is from 1 to 65,535 seconds.
Maximum Request Retries	10	Maximum number of times to retry AP-generated requests. The default is 10 times. If you must modify this setting, the recommended value is 10,000. The range is from 1 to 65,535.
Keepalive Interval (30-65535)	60	Define the keepalive interval in a range of 30 to 65,535 seconds.
Dump Server		Enter the IP address for the dump server.
Telnet	No	Enables Telnet in this system profile.
SNMP Sys-contact		Enter an IP address to the value for SNMP sys_contact, the SNMP system Sys location.
RFprotect Server IP		Enter the IP address of the RFprotect server.
RFprotect Backup Server IP		Enter an IP address. When an Alcatel-Lucent switch is present in an Alcatel-Lucent RFprotect system, an Alcatel-Lucent AP that is acting as an RFprotect sensor can be configured and managed from the switch. As a Managed Sensor, the Alcatel-Lucent AP is managed by the switch but sends collected security data about the wireless environment to an RFprotect Server.
Configure Aeroscout RTLS Server	No	Enable this option if you wish to support an Aeroscout RTLS server.
Ortonics Walljack	Yes	Specify whether the Alcatel-Lucent switch uses an Ortonics walljack. Ortonics® Wi-Jack™ and Wi-Jack Duo™ thin client access points are centrally configured and managed by the Alcatel-Lucent Networks wireless switches to provide a high performance wireless network that integrates seamlessly into the structured cabling infrastructure. When enabled, this setting requires an Ortonics Access Point License.
Ortonics LED Off Time-Out	Yes	Enable the LED time-out function for Ortonics wall jacks when used. When enabled, this setting requires an Ortonics Access Point License.
Ortonics Low Temp	100	Enter the low and high temperatures in Celsius for Ortonics wall jacks. The range is from 0C to 255C degrees. When Ortonics is enabled, these settings require an Ortonics Access Point License.
Ortonics High Temp	110	
Configure RTLS Server	No	Enable this setting for Real-time Locating Systems (RTLS) server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps.

Table 26 Profiles > AP > System Profile Settings (Continued)

Field	Default	Description
Remote-AP DHCP Server VLAN (1-4094)		Specify the VLAN to be associated with the remote-AP DHCP server. This field requires a remote access points license, when used.
Remote-AP DHCP Server ID		Specify the IP address of the remote-AP DHCP server.
Remote-AP DHCP Default Router		Specify the IP address of the remote-AP DHCP default router. This field requires a remote AP license. This field requires a remote access points license, when used.
Remote-AP DHCP DNS Server		Enter the IP address or addresses of one or more remote-AP DHCP DNS servers.
Remote-AP DHCP Pool Start		Specify the DHCP IP address pool. This configures the pool of IP addresses from which the remote AP uses to assign IP addresses.
Remote-AP DHCP Pool End		At the Remote-AP-DHCP Pool Start and End fields, enter the first and last IP addresses of the pool. These fields require a remote access point license, when used.
Remote-AP DHCP Pool Netmask	255.255.255.0	Enter the subnet mask. This field requires a remote access points license, when used.
Remote-AP DHCP Lease Time (0-30 days)	0	Specify the amount of time that the IP address of the DHCP server is valid. The supported range is from 0 to 30 days. A value of 0 disables this function. This field requires a remote access points license, when used.
Heartbeat DSCP (0-63)	0	This setting defines DSCP for low-speed networks. The supported range is from 0 to 63. To enable this function, enter a value greater than 0.
Session ACL	none	Select an access control list for user sessions. To add a new policy for access control, click the plus sign and refer to “Security > Policies” on page 138 .
Corporate DNS Domain		Enter the domain name service (DNS) domain or domains, one per line.
Image URL		If an AP developers license is active, enter the image URL in a range from 1 to 1024. This setting requires an AP Developer license.
Maintenance Mode	No	You can configure APs to suppress traps and syslog messages related to those APs. Known as AP maintenance mode, this setting in the AP system profile is particularly useful when deploying, maintaining, or upgrading the network. If enabled, APs stop flooding unnecessary traps and syslog messages to network management systems or network operations centers during a deployment or scheduled maintenance. The switch still generates debug syslog messages if debug logging is enabled. After completing the network maintenance, disable AP maintenance mode to ensure all traps and syslog messages are sent. AP maintenance mode is disabled by default.
WISPr Location-ID ISO Country Code		The ISO Country Code section of the WISPr Location ID. Requires a minimum version of 5.0.0.0 and a version earlier than 6.0.0.0
WISPr Location-ID E.164 Country Code		The E.164 Country Code section of the WISPr Location ID. Requires a minimum version of 5.0.0.0 and a version earlier than 6.0.0.0
WISPr Location-ID E.164 Area Code		The E.164 Area Code section of the WISPr Location ID. Requires a minimum version of 5.0.0.0 and a version earlier than 6.0.0.0
WISPr Location-ID SSID/Zone		The SSID/Zone section of the WISPr Location ID. Requires a minimum version of 5.0.0.0 and a version earlier than 6.0.0.0

Table 26 Profiles > AP > System Profile Settings (Continued)

Field	Default	Description
WISPr Operator Name		A name identifying the hotspot operator. Requires a minimum version of 5.0.0.0 and a version earlier than 6.0.0.0
WISPr Location Name		A name identifying the hotspot location. If no name is defined, the parameter will use the name of the AP to which the user has associated. Requires a minimum version of 5.0.0.0 and a version earlier than 6.0.0.0

3. Select **Add** or **Save**. The added or edited **System** profile appears on the **System** profiles list page.

Profiles > AP > Wired Port

APs with multiple wired Ethernet ports include an wired port profile that can enable or disable the wired port, define an AAA profile for wired port devices, and associate the port with an ethernet link profile that defines its speed and duplex values.

Perform these steps to configure a **Wired Port** profile.

1. Select **Profiles > AP > Wired Port** in the Navigation pane. This page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **Wired Port** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 27](#):

Table 27 Profiles > AP > Wired Port Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Referenced Profiles		
Wired AP Profile	default	Profile that defines wired port settings for APs assigned to the AP group. Refer to “Profiles > AP > Wired” on page 79.
Ethernet Interface Link Profile	default	Specify an ethernet link profile to be used by devices connecting to the AP’s wired port profile. This profile defines the duplex value and speed to be used by the port.
AAA Profile	None	Name of an AAA profile to be used by devices connecting to the AP’s wired port. Refer to “Profiles > AAA Overview” on page 50.
Other Settings		
Shut down	No	Whether to disable the wired AP port.
Remote-AP Backup	Yes	Select the Remote AP Backup checkbox to use the wired port on a Remote AP for local connectivity and troubleshooting when the AP cannot reach the switch. If the AP is not connected to the switch, no firewall policies will be applied when this option is enabled. (The AAA profile will only be applied when the AP is connected to switch).

Table 27 Profiles > AP > Wired Port Profile Settings (Continued)

Field	Default	Description
Bridge Role	none	
Time To Wait for Authentication To Succeed	20	Authentication timeout value, in seconds, for devices connecting the AP's wired port. The supported range is 1-65535 seconds.

3. Select **Add** or **Save**. The added or edited **Wired** Port profile appears on the **Profiles** page, and on the **Wired** Port details page.

Profiles > AP > Wired

The wired AP profile controls the configuration of the Ethernet port(s) on your AP. You can use the wired AP profile to configure Ethernet ports for bridging or secure jack operation using the wired AP profile.

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

1. Select **Profiles > AP > Wired** in the **Navigation** pane. This page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **Wired** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 28](#):

Table 28 Profiles > AP > Wired Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Wired AP Enable	No	Designate whether Wired APs are to be enabled or disabled.
Forward Mode	tunnel	If Wired AP is enabled, designate whether forwarding is to be bridge-based or tunnel-based.
Switchport Mode	Access	Select access or trunk . These options only apply to bridge mode configurations. <ul style="list-style-type: none"> • Access mode forwards untagged packets received on the port to the switch and they appear on the configured access mode VLAN. Tagged packets are dropped. All packets received from the switch and sent via this port are untagged. Define the access mode VLAN in the Access mode VLAN field. • Trunk mode contains a list of allowed VLANs. Any packet received on the port that is tagged with an allowed VLAN is forwarded to the switch. Untagged packets are forwarded to the switch on the configured Native VLAN. Packets received from the switch and sent out the port remain tagged unless the tag value in the packet is the Native VLAN, in which case the tag is removed. Define the Native VLAN in the Trunk mode native VLAN field and the other allowed VLANs in the Trunk mode allowed VLANs field.
Access Mode VLAN (1-4096)	1	Access mode forwards untagged packets received on the port to the switch and they appear on the configured access mode VLAN. Tagged packets are dropped. All packets received from the switch and sent via this port are untagged. Define the access mode VLAN in the Access mode VLAN field. The VLAN range is from 1 to 4096.

Table 28 Profiles > AP > Wired Profile Settings (Continued)

Field	Default	Description
Trunk Mode Native VLAN (1-4096)	1	Trunk mode contains a list of allowed VLANs. Any packet received on the port that is tagged with an allowed VLAN is forwarded to the switch. Untagged packets are forwarded to the switch on the configured Native VLAN. Packets received from the switch and sent out the port remain tagged unless the tag value in the packet is the Native VLAN, in which case the tag is removed. Define the Native VLAN in the Trunk mode native VLAN field and the other allowed VLANs in the Trunk mode allowed VLANs field.
Trunk Mode Allowed VLANs		Define whether the trunk mode settings defined in additional fields of this profile are to allow VLANs. The VLAN range is from 1 to 4094. Enter a list or a range of numbers. The VLAN range is from 1 to 4096. You can enter a range of numbers, specific numbers or a combination of range and specific VLAN numbers, as desired.
Trusted	No	Use this option if the wired port is a trusted port.
Broadcast	Yes	Use this option if the wired port is a broadcast port.

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

Profiles > IDS

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.

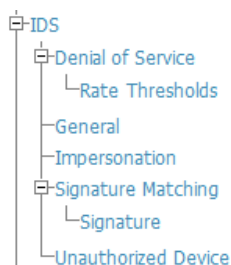
The top-level IDS profile, assigned to an Alcatel-Lucent AP group or AP name, references additional IDS profiles that are also described in this section. AOS-W includes predefined top-level IDS profiles that provide different levels of sensitivity. The following are predefined IDS profiles:

- ids-disabled
- ids-high-setting
- ids-low-setting (the default setting)
- ids-medium-setting

You apply the top-level IDS profile to an AP group or specific AP.

To view IDS profiles, click **Profiles > IDS** in the Alcatel-Lucent Configuration navigation pane.

Figure 5 IDS Profiles



A predefined IDS profile refers to specific instances of the other IDS profiles. You cannot create new instances of a profile within a predefined IDS profile. You can modify parameters within the other IDS profiles.

IDS profiles reference other profiles. These additional profiles can be created before, during, or after the configuration of the IDS profile.

Select the **Add** button to create a new **IDS** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 29](#):

Table 29 Profiles > IDS > General Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings and AP SNMP User Profiles		
IDS Unauthorized Device Profile	default	Select the IDS Unauthorized Device Profile from the drop-down menu. This profile is referenced by the overriding IDS profile currently being configured. The drop-down menu contains any profiles that you have configured. To create a new profile of this type, click the add icon. To edit an existing profile, select that profile then click the pencil icon. For additional information about configuring IDS Unauthorized Device Profiles, refer to “Profiles > IDS > Unauthorized Device” on page 90.
IDS Signature Matching Profile	default	Select the IDS Signature Matching Profile from the drop-down menu. The drop-down menu lists all signature matching profiles that are currently configured and available. To create a new profile of this type, click the add icon. To edit an existing profile, select that profile then click the pencil icon. For additional information about configuring IDS Unauthorized Device Profiles, refer to “Profiles > IDS > Signature Matching” on page 83.
IDS General Profile	default	Select the IDS General Profile from the drop-down menu. The drop-down menu lists all General IDS profiles that are currently configured and available. To create a new profile of this type, click the add icon. To edit an existing profile, select that profile then click the pencil icon. For additional information about configuring IDS Unauthorized Device Profiles, refer to “Profiles > IDS > General” on page 82.
IDS Impersonation Profile	default	Select the IDS Impersonation Profile from the drop-down menu. The drop-down menu lists all such profiles that are currently configured and available. To create a new profile of this type, click the add icon. To edit an existing profile, select that profile then click the pencil icon. For additional information about configuring IDS Impersonation Profiles, refer to “Profiles > IDS > Impersonation” on page 89.
IDS DoS Profile	default	Select the IDS Impersonation Profile from the drop-down menu. The drop-down menu lists all such profiles that are currently configured and available. To create a new profile of this type, click the add icon. To edit an existing profile, select that profile then click the pencil icon. For additional information about configuring IDS Impersonation Profiles, refer to “Profiles > IDS > Denial of Service” on page 85.

4. Select the profile type to view or configure:

- **Denial of Service**—Configures traffic anomaly settings for Denial of Service (DoS) attacks. Refer to [“Profiles > IDS > Denial of Service”](#) on page 85.
 - **Rate Thresholds**—Defines thresholds assigned to the different frame types for rate anomaly checking. Refer to [“Profiles > IDS > Denial of Service > Rate Threshold”](#) on page 88.
- **General**—Configures general AP attributes. Refer to [“Profiles > IDS > General”](#) on page 82.

- **Impersonation**—Configures anomaly settings for impersonation attacks. Refer to “[Profiles > IDS > Impersonation](#)” on page 89.
 - **Signature Matching**—Configures signatures and signature matching for intrusion detection. Refer to “[Profiles > IDS > Signature Matching](#)” on page 83.
 - **Signature**—Defines a predefined signature. Refer to “[Profiles > IDS > Signature Matching > Signature](#)” on page 84.
 - **Unauthorized Device**—Configures detection for unauthorized devices. Also configures rogue AP detection and containment. Refer to “[Profiles > IDS > Unauthorized Device](#)” on page 90.
5. Select **Add** or **Save**. The added or edited **IDS** profile appears on the **IDS** profiles page.

Profiles > IDS > General

Perform these steps to configure a **General IDS** profile.

1. Select **Profiles > IDS > General** in the **Alcatel-Lucent Navigation** pane. The list of current IDS profiles appears on this page.
2. Select the **Add** button to create a new **General** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 30](#):

Table 30 *Profiles > IDS > General Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings and AP SNMP User Profiles		
Stats Update Interval (60-36000 sec)	60	Set the time interval, in seconds, for the AP to update the switch with statistics. NOTE: This setting takes effect only if the Alcatel-Lucent Mobility Manager is configured. Otherwise, statistics update to the switch is disabled.
AP Max Unseen Timeout (5-36000 sec)	600	Sets the time, in seconds, after which an AP is aged out. NOTE: This setting requires a minimum of AOS-W 6.0.0.0.
AP Inactivity Timeout (5-36000 sec)	5	Set the time, in seconds, after which an AP is aged out.
STA Max Unseen Timeout (5-36000 sec)	600	Sets the time, in seconds, after which a station is aged out. NOTE: This setting requires a minimum of AOS-W 6.0.0.0.
STA Inactivity Timeout (30-36000 sec)	60	Set the time, in seconds, after which a station is aged out.
Min Potential AP Beacon Rate (0-100%)	25	Set the minimum beacon rate acceptable from a potential AP, in percentage of the advertised beacon interval.
Min Potential AP Monitor Time (0-36000 sec)	2	Set the minimum time, in seconds, a potential AP has to be up before it is classified as a real AP.

Table 30 Profiles > IDS > General Profile Settings (Continued)

Field	Default	Description
Signature Quiet Time (60-360000 sec)	900	Set the time to wait, in seconds, after which the check can be resumed when detecting a signature match.
Wireless Containment	Deauth only	Enable wireless containment including Tarpit Shielding. Tarpit shielding works by steering a client to a tarpit so that the client associates with it instead of the AP that is being contained. <ul style="list-style-type: none"> • deauth-only—Containment using deauthentication only • none—Disable wireless containment • tarpit-all-sta—Wireless containment by tarpit of all stations • tarpit-non-valid-sta—Wireless containment by tarpit of non-valid clients NOTE: Tarpit requires a minimum version of 6.0.0.0.
Debug Wireless Containment	No	Enable/disable debug of containment from the wireless side. Note: Enabling this debug option will cause containment to <i>not</i> function properly.
Wired Containment	No	Enable containment from the wired side.
Wired Containment of AP's Adj MACs	No	Enable/disable wired containment of MACs offset by one from APs BSSID. NOTE: This setting requires a minimum of AOS-W 6.0.0.0.
Monitored Device Stats Update Interval (0-36000 sec)	0	Time interval, in seconds, for AP to update the switch with stats for monitored devices. Minimum is 60.
Mobility Manager RTLS	No	Enable/disable RTLS communication with the configured mobility-manager
Send Ad-hoc Info to Controller	Yes	Enable or disable sending Ad hoc information to the switch from the AP. NOTE: This setting requires a WIPS or RFprotect license and a minimum of AOS-W 6.0.0.0.
Ad-hoc AP Max Unseen Timeout (5-36000 sec)	180	Ageout time in seconds since ad hoc (IBSS) AP was last seen. NOTE: This setting requires a minimum of AOS-W 6.0.0.0.
Ad-hoc (IBSS) AP Inactivity Timeout (5-36000 sec)	5	Ad hoc (IBSS) AP inactivity timeout in number of scans. NOTE: This setting requires a minimum of AOS-W 6.0.0.0.
IDS Event Generation on AP	None	Enable or disable IDS event generation from the AP. Event generation from the AP can be enabled for syslogs, traps, or both. This does not affect generation of IDS correlated events on the switch.

3. Select **Add** or **Save**. The added or edited **General** profile appears on the **IDS > General** profiles page.

Profiles > IDS > Signature Matching

The IDS signature matching profile contains signatures for intrusion detection. This profile can include predefined or custom signatures. [Table 31](#) describes the predefined signatures that you can add to the profile.

Perform these steps to configure a **Signature Matching** profile.

1. Select **Profiles > IDS > Signature Matching** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Signature Matching** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 31](#):

Table 31 Profiles > IDS > Signature Matching Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Signature Profiles		
Select Signature Profiles		Select from signature options as follows: <ul style="list-style-type: none"> ● AirJack ● ASLEAP ● Deauth-Broadcast ● default ● Disassoc-Broadcast ● Netstumbler Generic ● Netstrumbler Version 3.3.0x ● Null-Probe-Response ● Wellenreiter

3. Select **Add** or **Save**. The added or edited **Signature Matching** profile appears on the **IDS > Signature Matching** profiles page.

Profiles > IDS > Signature Matching > Signature

Perform these steps to create signatures for use with **Signature Matching** profiles.

1. Select **Profiles > IDS > Signature Matching > Signature** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Signature**, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 32](#):

Table 32 Profiles > IDS > Signature Creation Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the signature.
IDS Signatures		
Add		Select this button to add a new IDS signature. Complete the settings as follows: <ul style="list-style-type: none"> ● Parameter, which can be one of the following: <ul style="list-style-type: none"> ■ bssid ■ dst-mac ■ frame-type ■ payload ■ seq-num ■ src-mac ● BSSID Select Add when these signature settings are defined.

3. Select **Add** or **Save** on the **Signature** page. The added or edited **Signature** appears on the **IDS > Signature Matching > Signatures** page.

Profiles > IDS > Denial of Service

This profile type defines traffic anomaly settings that detect and process denial-of-service attacks. This profile type defines the parameters that are monitored and acted upon when detecting and blacklisting an offending client from the Alcatel-Lucent system. When a client is blacklisted in the Alcatel-Lucent system, the client is not allowed to associate with any AP in the network for a specified amount of time. If a client is connected to the network when it is blacklisted, a de-authentication message is sent to force the client to disconnect. While blacklisted, the client cannot associate with another SSID in the network.

[Table 33](#) summarizes the predefined IDS Denial of Service profiles. These profiles are viewable with the **Profiles > IDS > Denial of Service** path in the navigation pane.

Table 33 *Predefined IDS DoS Profiles*

Parameter	ids-dosdisabled	ids-dos-lowsetting	ids-dosmedium-setting	ids-dos-highsetting
Detect Disconnect Station Attack	disabled	enabled	enabled	enabled
Disconnect STA Detection Quiet Time	900 seconds	900 seconds	900 seconds	900 seconds
Spoofed Deauth Blacklist	disabled	disabled	disabled	disabled
Detect AP Flood Attack	disabled	disabled	disabled	disabled
AP Flood Threshold	50	50	50	50
AP Flood Increase Time	3 seconds	3 seconds	3 seconds	3 seconds
AP Flood Detection Quiet Time	900 seconds	900 seconds	900 seconds	900 seconds
Detect EAP Rate Anomaly	disabled	disabled	enabled	enabled
EAP Rate Threshold	60	60	30	60
EAP Rate Time Interval	3 seconds	3 seconds	3 seconds	3 seconds
EAP Rate Quiet Time	900 seconds	900 seconds	900 seconds	900 seconds
Detect Rate Anomalies	disabled	disabled	disabled	enabled
Detect 802.11n 40 MHz Intolerance Setting	disabled	enabled	enabled	enabled
Client 40 MHz Intolerance Detection Quiet Time	900 seconds	900 seconds	900 seconds	900 seconds
Rate Thresholds for Assoc Frames	default	default	default	default
Rate Thresholds for Disassoc Frames	default	default	default	default
Rate Thresholds for Deauth Frames	default	default	default	default
Rate Thresholds for Probe Request Frames	default	probe-request-response-thresholds	probe-request-response-thresholds	probe-request-response-thresholds

Table 33 Predefined IDS DoS Profiles (Continued)

Parameter	ids-dosdisabled	ids-dos-lowsetting	ids-dosmedium-setting	ids-dos-highsetting
Rate Thresholds for Probe Response Frames	default probe-request-response-thresholds	probe-request-response-thresholds	probe-request-response-thresholds	Rate Thresholds for Auth Frames
default	default	default	default	

Perform these steps to configure or edit an IDS **Denial of Service** profile, and to create or edit profiles that are referenced by a DOC profile.

1. Select **Profiles > IDS > Denial of Service** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Signature Matching** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 34](#):

Table 34 Profiles > IDS > Denial of Service Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Referenced Profiles		
Rate Thresholds for Assoc Frames	default	Select a profile from the drop-down menu, or click the edit (icon) or add (icon) to edit or create a profile that sets the rate threshold for association frames. The IDS rate threshold profile defines thresholds assigned to the different frame types for rate anomaly checking.
Rate Thresholds for Disassoc Frames	default	Select a profile from the drop-down menu, or click the edit (icon) or add (icon) to edit or create a profile that sets the rate threshold for disassociation frames. The IDS rate threshold profile defines thresholds assigned to the different frame types for rate anomaly checking.
Rate Thresholds for Deauth Frames	default	Select a profile from the drop-down menu, or click the edit (icon) or add (icon) to edit or create a profile that sets the rate threshold for de-authentication frames. The IDS rate threshold profile defines thresholds assigned to the different frame types for rate anomaly checking.
Rate Thresholds for Probe Request Frames	default	Select a profile from the drop-down menu, or click the edit (icon) or add (icon) to edit or create a profile that sets the rate threshold for probe request frames. The IDS rate threshold profile defines thresholds assigned to the different frame types for rate anomaly checking.
Rate Thresholds for Probe Response Frames	default	Select a profile from the drop-down menu, or click the edit (icon) or add (icon) to edit or create a profile that sets the rate threshold for probe response frames. The IDS rate threshold profile defines thresholds assigned to the different frame types for rate anomaly checking.
Rate Thresholds for Auth Frames	default	Select a profile from the drop-down menu, or click the edit (icon) or add (icon) to edit or create a profile that sets the rate threshold for authentication frames. The IDS rate threshold profile defines thresholds assigned to the different frame types for rate anomaly checking.
Other Settings		
Detect Disconnect Station Attack	Yes	Enables or disables detection of station disconnection attacks.

Table 34 Profiles > IDS > Denial of Service Profile Settings (Continued)

Field	Default	Description
Disconnect STA Assoc Response Threshold	5	The number of successful Association Response or Reassociation response frames seen in an interval of 10 seconds that should trigger this event. Requires a minimum version of 6.0.0.0.
Disconnect STA Deauth and Disassoc Threshold	8	Rate thresholds for Disassociate frames. Requires a minimum version of 6.0.0.0
Disconnect STA Detection Quiet Time	900	After a station disconnection attack is detected, sets the time (in seconds) that must elapse before another identical alarm can be generated.
Spoofed Deauth Blacklist	No	Enables or disables automatic client blacklisting of spoofed de-authentication.
Detect AP Flood Attack	No	Enables or disables the detection of flooding with fake AP beacons to confuse legitimate users and to increase the amount of processing need on client operating systems.
AP Flood Threshold	50	Sets the number of Fake AP beacons that must be received within the Flood Increase Time to trigger an alarm.
AP Flood Increase Time	3	Sets the time, in seconds, during which a configured number of Fake AP beacons must be received to trigger an alarm.
AP Flood Detection Quiet Time	900	After an alarm has been triggered by a Fake AP flood, the time (in seconds) that must elapse before an identical alarm may be triggered.
Detect Client Flood Attack	No	Enable/disable detection of client flood attack. There are fake AP tools that can be used to attack wireless intrusion detection itself by generating a large number of fake clients that fill internal tables with fake information. If successful, it overwhelms the wireless intrusion system, resulting in a DoS. Requires a Wireless Intrusion Protection license or an RFprotect license and a minimum version of 6.0.0.0.
Client Flood Threshold	150	Threshold for the number of spurious clients in the system. Requires a Wireless Intrusion Protection license or an RFprotect license and a minimum version of 6.0.0.0
Client Flood Increase Time	3	Number of consecutive seconds over which the client count is more than the threshold. Requires a Wireless Intrusion Protection license or an RFprotect license and a minimum version of 6.0.0.0
Client Flood Detection Quiet Time	900	Time to wait, in seconds, after detecting a client flood before continuing the check. Requires a Wireless Intrusion Protection license or an RFprotect license and a minimum version of 6.0.0.0
Detect EAP Rate Anomaly	No	Enables or disables Extensible Authentication Protocol (EAP) handshake analysis to detect an abnormal number of authentication procedures on a channel and generates an alarm when this condition is detected.
EAP Rate Thresholds	60	Sets the number of EAP handshakes that must be received within the EAP Rate Time Interval to trigger an alarm.
EAP Rate Time Interval	3	Sets the time, in seconds, during which the configured number of EAP handshakes must be received to trigger an alarm.
EAP Rate Quiet Time	900	After an alarm has been triggered, sets the time (in seconds) that must elapse before another identical alarm may be triggered.
Detect Rate Anomalies	No	Enables or disables detection of rate anomalies.

Table 34 Profiles > IDS > Denial of Service Profile Settings (Continued)

Field	Default	Description
Detect 802.11n 40MHz Intolerance Setting	Yes	Enables or disables detection of 802.11n 40 MHz intolerance setting, which controls whether stations and APs advertising 40 MHz intolerance will be reported.
Client 40 MHz Intolerance Detection Quiet Time	900	Controls the quiet time (when to stop reporting intolerant STAs if they have not been detected), in seconds, for detection of 802.11n 40 MHz intolerance setting.

3. Select **Add** or **Save**. The added or edited **Denial of Service** profile appears on the **IDS > Denial of Service** profiles page.

Profiles > IDS > Denial of Service > Rate Threshold

The IDS rate threshold profile defines thresholds assigned to the different frame types for rate anomaly checking. A profile of this type is attached to each of the following 802.11 frame types in the IDS Denial of Service profile:

- Association frames
- Disassociation frames
- Deauthentication frames
- Probe Request frames
- Probe Response frames
- Authentication frames

A channel threshold applies to an entire channel, while a node threshold applies to a particular client MAC address. Alcatel-Lucent provides predefined default IDS rate thresholds profiles for each of these types of frames. Default values depend upon the frame type.

Perform these steps to create Rate Threshold Profiles for use with **Denial of Service** profiles.

1. Select **Profiles > IDS > Denial of Service > Rate Thresholds** in the **Alcatel-Lucent Navigation** pane. This page summarizes the current thresholds available.
2. Select the **Add** button to create a new **Rate Threshold**, or click the **pencil** icon next to an existing threshold to edit. Complete the settings as described in [Table 35](#):

Table 35 Profiles > IDS > Denial of Service, Rate Threshold Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the rate threshold profile.
Other Settings		
Channel Increase Time (0--360000 sec)	15	Set the time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.
Channel Quiet Time (60-360000 sec)	900	Set the time that must elapse before another identical alarm may be triggered, after an alarm has been triggered, Use this option to prevent excessive messages in the log file.

Table 35 Profiles > IDS > Denial of Service, Rate Threshold Settings (Continued)

Field	Default	Description
Channel Threshold (0-100000)	300	Specify the number of a specific type of frame. This number must be exceeded within a specific interval in an entire channel to trigger an alarm.
Node Time Interval (1-120 sec)	15	Set the time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.
Node Quiet Time (60-360000 sec)	900	Set the time that must elapse before another identical alarm may be triggered, after an alarm has been triggered. This option prevents excessive messages in the log file.
Node Threshold (0-100000)	200	Specify the number of a specific type of frame that must be exceeded within a specific interval for a particular client MAC address to trigger an alarm.

3. Select **Add** or **Save**. The added or edited **Rate Threshold** appears on the **Profiles > IDS > Denial of Service > Rate Thresholds** page.

Profiles > IDS > Impersonation

Perform these steps to create IDS **Impersonation** profiles.

1. Select **Profiles > IDS > Impersonation** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Impersonation** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 36](#):

Table 36 Profiles > IDS > Impersonation Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the impersonation profile.
Other Settings		
Detect AP Impersonation	Yes	Enable or disable detection of AP impersonation. In AP impersonation attacks, the attacker sets up an AP that assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for man-in-the-middle attacks, a rogue AP attempting to bypass detection, or a honeypot attack.
Protect from AP Impersonation	No	When AP impersonation is detected, use this control to set both the legitimate and impersonating AP to be disabled using a denial of service attack.
Beacon Diff Threshold (0-100%)	50	Set the percentage increase in beacon rate that triggers an AP impersonation alert.
Beacon Increase Wait Time (0-360000 sec)	3	Set the time, in seconds, after the Beacon Diff Threshold is crossed before an AP impersonation event is generated.
Detect Sequence Anomaly	No	Enable or disable detection of anomalies between sequence numbers seen in 802.11 frames. During an impersonation attack, the attacker may spoof the MAC address of a client or AP — if two devices are active on the network with the same MAC address, the sequence numbers in the frames will not match since the sequence number is generated by NIC firmware.

Table 36 Profiles > IDS > Impersonation Settings (Continued)

Field	Default	Description
Sequence Number of Difference (0-100000)	300	Set the maximum allowable tolerance between sequence numbers within the Sequence Number Time Tolerance period.
Sequence Number Time Tolerance (0-360000 sec)	300	Time, in seconds, during which sequence numbers must exceed the Sequence Number Difference value for an alarm to be triggered.
Sequence Number Quiet Time (60-360000 sec)	900	After an alarm has been triggered, the time (in seconds) that must elapse before another identical alarm may be triggered.
Detect AP Spoofing	Yes	Whether to detect AP Spoofing. NOTE: Requires a WIDS license.
AP Spoofing Quiet Time	900	Time to wait, in seconds, after a spoofing attempt to resume the check.
Detect Beacon Wrong Channel	No	Enable/disable detection of beacons advertising the incorrect channel.
Beacon Wrong Channel Detection Quiet Time	900	Time to wait in seconds after detecting an attempt of beacons advertising the incorrect channel, after which the check can be resumed.
Detect Hotspotter Attack	No	Enable/disable detection of the Hotspotter attack to lure away valid clients.
Hotspotter Quiet Time	900	Time to wait in seconds after detecting an attempt to use the Hotspotter tool against clients.

3. Select **Add** or **Save**. The added or edited **Impersonation** profile appears on the **Profiles > IDS > Impersonation** page.

Profiles > IDS > Unauthorized Device

Unauthorized device detection includes the ability to detect and disable rogue APs and other devices that can potentially disrupt network operations.

The most important IDS functionality offered in the Alcatel-Lucent system is the ability to classify an AP as either a rogue AP or an interfering AP. 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. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat since it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.



Rogue device classification for Alcatel-Lucent WMS Offload infrastructure is also described in the *OV3600 User Guide*.

You can enable a policy to automatically disable APs that are classified as a rogue APs by the Alcatel-Lucent system. When a rogue AP is disabled, no wireless stations are allowed to associate to that AP.

Perform these steps to create IDS **Unauthorized Device** profiles.

1. Select **Profiles > IDS > Unauthorized Devices** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Unauthorized Devices** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 37](#):

Table 37 Profiles > IDS > Unauthorized Devices Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Detect Adhoc Networks	Yes	Enable or disable detection of adhoc networks.
Protect from Adhoc Networks	No	Enable or disable protection from adhoc networks. When adhoc networks are detected, they are disabled using a denial of service attack.
Detect Windows Bridge	Yes	Enable or disable detection of Windows station bridging.
Detect Wireless Bridge	Yes	Enable or disable detection of wireless bridging.
Detect Devices with An Invalid MAC OUI	No	Enable or disable the checking of the first three bytes of a MAC address, known as the MAC organizationally unique identifier (OUI), assigned by the IEEE to known manufacturers. Often clients using a spoofed MAC address do not use a valid OUI and instead use a randomly generated MAC address. Enabling MAC OUI checking causes an alarm to be triggered if an unrecognized MAC address is in use.
MAC OUI Detection Quiet Time (60-360000 sec)	900	Set the time, in seconds, that must elapse after an invalid MAC OUI alarm has been triggered before another identical alarm may be triggered.
Adhoc Network Detection Quiet Time (60-360000 sec)	900	Set the time, in seconds, that must elapse after an adhoc network detection alarm has been triggered before another identical alarm may be triggered.
Wireless Bridge Detection Quiet Time (60-360000 sec)	900	Set the time, in seconds, that must elapse after a wired bridging alarm has been triggered before another identical alarm may be triggered.
Rogue AP Classification	Yes	Enable or disable rogue AP classification. A rogue AP is one that is unauthorized and plugged into the wired side of the network. Any other AP seen in the RF environment that is not part of the valid enterprise network is considered to be “interfering” — it has the potential to cause RF interference but it is not connected to the wired network and thus does not represent a direct threat.
Overlay Rogue AP Classification	Yes	Set Overlay Rogue Classification, which is classification through valid/rogue APs. A switch uses the wired-mac table of other valid and rogue APs as equivalents of the wired MACs that it sees on our network. When this match is triggered, it makes a note of the AP that helped in this process, and this info will be displayed as the Helper-AP.
Valid Wired MACs		Set a list of MAC addresses of wired devices in the network, typically gateways or servers.
Rogue Containment	No	By default, rogue APs are only detected but are not automatically disabled. This option automatically shuts down rogue APs. When this option is enabled, clients attempting to associate to a rogue AP will be disconnected from the rogue AP through a denial of service attack.

Table 37 Profiles > IDS > Unauthorized Devices Profile Settings (Continued)

Field	Default	Description
Allow Well Known MAC		<p>Allow devices with known MAC addresses to classify rogues APs. Depending on your network, configure one or more of the following options for classifying rogue APs:</p> <ul style="list-style-type: none"> ● hsrp—Routers configured for HSRP, a Cisco-proprietary redundancy protocol, with the HSRP MAC OUI 00:00:0c. ● iana—Routers using the IANA MAC OUI 00:00:5e. ● local-mac—Devices with locally administered MAC addresses starting with 02. ● vmware—Devices with any of the following VMWare OUIs: 00:0c:29, 00:05:69, or 00:50:56 ● vmware1—Devices with VMWare OUI 00:0c:29. ● vmware2—Devices with VMWare OUI 00:05:69. ● vmware3—Devices with VMWare OUI 00:50:56. <p>If you modify an existing configuration, the new configuration overrides the original configuration.</p>
Suspected Rogue Containment	No	<p>Use this setting to treat suspected rogue APs as interfering APs; thereby the switch attempts to reclassify them as rogue APs. By default, suspected rogue APs are not automatically contained.</p> <p>In combination with the suspected rogue containment confidence level, this option automatically shuts down suspected rogue APs. When this option is enabled, clients attempting to associate to a suspected rogue AP will be disconnected from the suspected rogue AP through a denial of service attack.</p>
Suspected Rogue Containment Confidence Level (50-100)	60	<p>Set the confidence level. When an AP is classified as a suspected rogue AP, it is assigned a 50% confidence level. If multiple APs trigger the same events that classify the AP as a suspected rogue, the confidence level increases by 5% up to 95%.</p> <p>In combination with suspected rogue containment, this option configures the threshold by which containment should occur. Suspected rogue containment occurs only when the configured confidence level is met.</p>
Protect Valid Stations	No	Use this setting to disallow valid stations from connecting to a non-valid AP.
Detect Bad WEP	No	Enable or disable detection of WEP initialization vectors that are known to be weak. A primary means of cracking WEP keys is to capture 802.11 frames over an extended period of time and searching for such weak implementations that are still used by many legacy devices.
Detect Misconfigured AP	No	<p>Enable or disable detection of misconfigured APs. An AP is classified as misconfigured if it does not meet any of the following configurable parameters:</p> <ul style="list-style-type: none"> ● Valid channels ● Encryption type ● Short preamble ● List of valid AP MAC OUIs ● Valid SSID list
Protect Misconfigured AP	No	Enable or disable protection of misconfigured APs.
Detect Valid SSID Misuse	No	If an unauthorized AP (neighbor or interfering) is using the same SSID as an authorized network, a valid client may be tricked into connecting to the wrong network. If a client connects to a malicious network, security breaches or attacks can occur. Enable/disable detection of Interfering or Neighbor APs using valid/protected SSIDs. Requires a Wireless Intrusion Protection license or an RFprotect license and a minimum version of 6.1.0.0
Protect SSID	No	Enable or disable use of SSID by only valid APs.

Table 37 Profiles > IDS > Unauthorized Devices Profile Settings (Continued)

Field	Default	Description
Privacy	No	Enable or disable encryption as valid AP configuration.
Require WPA	No	Enable or disable “misconfigured” flagging of any valid AP that is not using WPA encryption.
Detect Unencrypted Valid Clients		Enable/disable detection of unencrypted valid clients. Requires a Wireless Intrusion Protection license or an RFprotect license and a minimum version of 6.0.0.0
Unencrypted Valid Client Detection Quiet Time	900	Time to wait, in seconds, after detecting an unencrypted valid client after which the check can be resumed.Requires a Wireless Intrusion Protection license or an RFprotect license and a minimum version of 6.0.0.0
Valid 802.11g Channel for Policy Enforcement		Enter the list of valid 802.11g channels that third-party APs are allowed to use.
Valid 802.11a Channel for Policy Enforcement		Enter the list of valid 802.11a channels that third-party APs are allowed to use.
Valid MAC OUIs		Enter the list of MAC OUIs of wired devices in the network, typically gateways or servers.
Valid and Protected SSIDs		Enter the list of valid and protected SSIDs.
Protect 802.11n High Throughput Devices	No	Enable or disable protection of high-throughput 802.11n devices not operating in 40 MHz mode.
Protect 40MHz 802.11n High Throughput Devices	No	Enable or disable protection of high-throughput (802.11n) devices operating in 40 MHz mode.
Detect Active 802.11 Greenfield Mode	Yes	Enable or disable detection of high-throughput devices advertising greenfield preamble capability.

3. Select **Add** or **Save**. The added or edited profile appears on the **Profiles > IDS > Unauthorized Devices** page.

Profiles > Mesh

Mesh profiles help define and bring-up the mesh network. This section describes the mesh radio and mesh cluster profiles in more detail.

- **Cluster**—Mesh clusters are grouped and defined by a mesh cluster profile, which provides the framework of the mesh network. Similar to virtual AP profiles, the mesh cluster profile contains the MSSID (mesh cluster name), authentication methods, security credentials, and cluster priority required for mesh nodes to associate with their neighbors and join the cluster. Associated mesh nodes store this information in flash memory.

Although most mesh deployments will require only a single mesh cluster profile, you can configure and apply multiple mesh cluster profiles to an AP group or an individual AP. If you have multiple cluster profiles, the mesh portal uses the profile with the highest priority to bring up the mesh network. Mesh points, in contrast, go through the list of mesh cluster profiles in order of priority to decide which profile to use to associate themselves with the network. The mesh cluster priority determines the order by which the mesh cluster profiles are used. This allows you, rather than the link metric algorithm, to explicitly segment the network by defining multiple cluster profiles. AirWave provides a “default” version of the mesh cluster profile. You can use the “default” version or create a new instance of a

profile which you can then edit as you need. You can configure a maximum of 16 mesh cluster profiles on a mesh node. Refer to “[Profiles > QoS](#)” on page 98.

- **Radio**—Alcatel-Lucent provides a “default” version of the mesh radio profile. You can use the “default” version or create a new instance of a profile which you can then edit as you need. The mesh radio profile allows you to specify the set of rates used to transmit data on the mesh link. Refer to “[Profiles > Mesh > Radio](#)” on page 95.
- **Radio > Mesh HT SSID**—The mesh high-throughput SSID profile enables or disables high-throughput (802.11n) features for the SSID specified in the profile. Refer to “[Profiles > Mesh > Radio > Mesh HT SSID](#)” on page 97.

Profiles > Mesh > Cluster

AirWave provides a “default” version of the mesh cluster profile. You can use the “default” version or create a new instance of a profile which you can then edit as you need. You can configure a maximum of 16 mesh cluster profiles on a mesh node.

Perform these steps to create or edit Mesh Cluster profiles.

1. Select **Profiles > Mesh > Cluster** in the Navigation pane.
2. Select the **Add** button to create a new **Cluster** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 38](#):

Table 38 *Profiles > Mesh > Cluster Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Cluster Name	alcatel-lucent-mesh	Enter the mesh cluster name. The name can have a maximum of 32 characters, which is used as the MSSID. When you create a new cluster profile, it is a member of the “alcatel-lucent-mesh” cluster. NOTE: Each mesh cluster profile should have a unique MSSID. Configure a new MSSID before you apply the mesh cluster profile. To view existing mesh cluster profiles, use the command: show ap mesh-cluster-profile. A mesh portal chooses the best cluster profile and provisions it for use. A mesh point can have a maximum of 16 cluster profiles
RF Band	a	Use this setting to indicate the band for mesh operation for multiband radios. Select a or g . Important: If you create more than one mesh cluster profile for an AP or AP group, each mesh cluster profile must use the same band.
Encryption	Open System	Use this setting to configure the data encryption, which can be either open system (no authentication or h) or WPA2-PSK-AES (WPA2 with AES encryption using a preshared key). The recommended selection is WPA2-PSK-AES with passphrase. Keep the passphrase in a safe place.

3. Select **Add** or **Save**. The added or edited **Cluster** profile appears on **Profiles > Mesh > Cluster**.

Profiles > Mesh > Radio

The mesh radio profile allows you to specify the transmit power and set of rates used to transmit data on the mesh link.

Perform these steps to create or edit Mesh Radio profiles.

1. Select **Profiles > Mesh > Radio** in the Navigation pane.
2. Select the **Add** button to create a new **Radio** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 39](#):

Table 39 Profiles > Mesh > Radio Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Maximum Children (1-64)	64	Use this field to indicate the maximum number of children a mesh node can accept. The supported range is from 1 to 64.
Maximum Hop Count (1-32)	8	Use this field to indicate the maximum hop count from the mesh portal. The supported range is from 1 to 32.
Heartbeat Threshold (1-255)	10	Use this field to indicate the maximum number of heartbeat messages that can be lost between neighboring mesh nodes. The supported range is from 1 to 255.
Link Threshold (1-255)	12	Use this setting to optimize operation of the link metric algorithm. Indicates the minimal RSSI value. If the RSSI value is below this threshold, the link may be considered a subthreshold link. A sub-threshold link is one whose average RSSI value falls below the configured link threshold. If this occurs, the mesh node may try to find a better link on the same channel and cluster (only neighbors on the same channel are considered). The supported threshold is hardware dependent, with a practical range of 1 to 255.
Reselection Mode	startup-subthreshold	Use this setting to optimize operation of the link metric algorithm. Specifies the method a mesh node uses to find a better uplink to create a path to the mesh portal. Only neighbors on the same channel in the same mesh cluster are considered. Available options are: <ul style="list-style-type: none"> ● reselect-anytime—Connected mesh nodes evaluate mesh links every 30 seconds. If a mesh node finds a better uplink, the mesh node connects to the new parent to create an improved path to the mesh portal. ● reselect-never—Connected mesh nodes do not evaluate other mesh links to create an improved path to the mesh portal. ● startup-subthreshold—When bringing up the mesh network, mesh nodes have 3 minutes to find a better uplink. After that time, each mesh node evaluates alternative links only if the existing uplink falls below the configured threshold level (the link becomes a sub-threshold link). The reselection process is cancelled if the average RSSI on the existing uplink rises above the configured link-threshold. ● subthreshold-only—Connected mesh nodes evaluate alternative links only if the existing uplink becomes a sub-threshold link. NOTE: The default value is recommended for this setting.

Table 39 Profiles > Mesh > Radio Profile Settings (Continued)

Field	Default	Description
Metric Algorithm	distributed-tree-rssi	Use this setting to optimize operation of the link metric algorithm. Specifies the algorithm used by a mesh node to select its parent. Available options are: <ul style="list-style-type: none"> • best-link-rssi—Selects the parent with the strongest RSSI, regardless of the number of children a potential parent has. • distributed-tree-rssi—Selects the parent based on link-RSSI and node cost based on the number of children. This option evenly distributes the mesh points over high quality uplinks. Low quality uplinks are selected as a last resort. NOTE: Using the default value is recommended.
802.11g Portal Channel (1-14)	Blank	Each 802.11a and 802.11g radio profile references an Adaptive Radio Management (ARM) profile. When you assign an active ARM profile to a mesh radio, ARM's automatic power-assignment and channel-assignment features automatically select the radio channel with the least amount of interference for each mesh portal, maximizing end user performance. In earlier versions of this software, an AP with a mesh radio received its beacon period, transmission power and 11a/11g portal channel settings from its mesh radio profile. Mesh-access AP portals now inherit these radio settings from their dot11a or dot11g radio profiles. NOTE: Do not delete or modify mesh cluster profiles once you use them to provision mesh nodes. You can recover the mesh point if the original cluster profile is still available. Creating a new mesh cluster profile if needed is recommended.
802.11a Portal Channel (34-165)	Blank	
Beacon Period (60-999999 msec)	100	Define the beacon period supporting mesh profiles, as described for the fields immediately above.
Transmit Power (0-30 dBm)	30	Define the transmission power supporting mesh profiles, as described for the portal channel settings immediately above. This setting supports a range from 0 to 30 dBm.
Retry Limit (0-15)	4	Indicate the number of times a mesh node can re-send a packet. This setting supports a range from 0 to 15.
RTS Threshold (256-2346 bytes)	2333	Define the packet size sent by mesh nodes. Mesh nodes transmitting frames larger than this threshold must issue request to send (RTS) and wait for other mesh nodes to respond with clear to send (CTS) to begin transmission. This helps prevent mid-air collisions. The supported range is from 256 to 2346 bytes.
802.11a Transmit Rates	All selected	Indicate the transmit rates for the 802.11a radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.
802.11g Transmit Rates	All selected	Indicate the transmit rates for the 802.11g radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.
Mesh Private VLAN (0-4094)	0	Enter a VLAN ID for control traffic between an remote mesh portal and mesh nodes. This VLAN ID must not be used for user traffic. Range: 0-4094. Default: 0 (disabled).
BC/MC Rate Optimization	Yes	Enable or disable scanning of all active stations currently associated to a mesh point to select the lowest transmission rate based on the slowest connected mesh child. When enabled, this setting dynamically adjusts the multicast rate to that of the slowest connected mesh child. Multicast frames are not sent if there are no mesh children. NOTE: Using the default value is recommended.

3. Select **Add** or **Save**. The added or edited **Radio** profile appears on the **Profiles > Mesh > Radio** page.

Profiles > Mesh > Radio > Mesh HT SSID

The mesh high-throughput SSID profile enables or disables high-throughput (802.11n) features for the SSID specified in the profile. This parameter is enabled by default. The mesh high-throughput profile can have a maximum of 32 characters.

Perform these steps to configure a **Mesh HT SSID** profile.

1. Select **Profiles > Mesh > Radio > Mesh HT SSID** in the **Alcatel-Lucent Navigation** pane. The details page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **Mesh HT SSID** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 40](#):

Table 40 *Mesh > Radio > Mesh HT SSID Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile. This profile name can have a maximum of 32 characters.
Other Settings		
40 MHz Channel Usage	Yes	Enable or disable the use of 40 MHz channels. This parameter is enabled by default.
Low-density Parity Check		If enabled, the AP will advertise Low-density Parity Check (LDPC) support. LDPC improves data transmission over radio channels with high levels of background noise. Requires a minimum version of 6.1.0.0.
MPDU Aggregation		Enable or disable MAC protocol data unit (MPDU) aggregation. High-throughput mesh APs are able to send aggregated MAC protocol data units (MDPUs), which allow an AP to receive a single block acknowledgment instead of multiple ACK signals. This option, which is enabled by default, reduces network traffic overhead by effectively eliminating the need to initiate a new transfer for every MPDU.
Max Received A-MPDU Size (bytes)	65535	Set the maximum size of a received aggregate MAC Protocol Data Unit (A-MPDU), in bytes. The allowed values in AOS-W 3.4 and later are 8191, 16383, 32767, or 65535 bytes. OV3600 may support additional options.
Min MPCU Start Spacing (usec)	8	Set the minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds. The allowed values 0 (No restriction on MPDU start spacing), .25 usec, .5 usec, 1 usec, 2 usec, 4 usec, 8 usec, and 16 usec.
High Throughput Enable (SSID)	Yes	Enable or disable high-throughput (802.11n) features on this SSID. This parameter is enabled by default.
Supported MCS Set	0-15	Set a list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20MHz vs. 40MHz) and the number of spatial streams used by the mesh node. The default value is 1-15; the complete set of supported values. To specify a smaller range of values, enter a hyphen between the lower and upper values. To specify a series of different values, separate each value with a comma. Enter a list or range of numbers. The overall supported range is from 0-15. The following are two potential examples of supported ranges: <ul style="list-style-type: none"> ● 2-10 ● 1,3,6,9,12

Table 40 Mesh > Radio > Mesh HT SSID Profile Settings (Continued)

Field	Default	Description
Short Guard Interval in 40 MHz Mode	Yes	<p>Enable or disable use of short (400ns) guard interval in 40 MHz mode. A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data.</p> <p>The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput.</p> <p>This parameter is enabled by default.</p>
Short Guard Interval in 20 MHz Mode	Yes	<p>Enable or disable use of short (400ns) guard interval in 20 MHz mode. This parameter is enabled by default.</p> <p>A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput.</p> <p>Requires a minimum version of 6.1.0.0.</p>
Maximum Number of Spatial Streams Usable for STBC Transmission		<p>Controls the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on AP-90 series, AP-175, AP-130 Series and AP-105 only. The configured value will be adjusted based on AP capabilities.)</p>
Maximum Number of Spatial Streams Usable for STBC Reception		<p>Controls the maximum number of spatial streams usable for STBC reception. 0 disables STBC reception, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on AP-90 series, AP-175, AP-130 Series and AP-105 only. The configured value will be adjusted based on AP capabilities.)</p>
Legacy Stations	Yes	<p>Allow or disallow associations from legacy (non-HT) stations. This parameter is enabled by default (legacy stations are allowed).</p>
Max Transmitted A-MPDU Size	65535	<p>Sets maximum size of a transmitted aggregate MPDU, in bytes. Specify size in the supported range of 1576 to 65535 bytes.</p>

3. Select **Add** or **Save**. The added or edited profile appears on the **Mesh HT SSID** page.

Profiles > QoS

The following QoS profiles configure traffic management and VoIP functions.

- **Traffic Management**—Specifies 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. Refer to “[Profiles > QoS > Traffic Management](#)” on page 99.
- **VoIP Call Admission Control**—Alcatel-Lucent’s 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. Refer to “[Profiles > QoS > VoIP Call Admission Control](#)” on page 99.
- **WMM Traffic Management**—Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance specification based on the IEEE 802.11e wireless Quality of Service (QoS) standard. WMM works with 802.11a, b, g, and n physical

layer standards. WMM supports four access categories (ACs): voice, video, best effort, and background. The 802.1D priority value is contained in a two-byte QoS control field in the WMM data frame. Refer to “Profiles > QoS > WMM Traffic Management” on page 101.

Profiles > QoS > Traffic Management

Perform these steps to create or edit Traffic Management profiles.

1. Select **Profiles > QoS > Traffic Management** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Traffic Management** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 41](#):

Table 41 Profiles > QoS > Traffic Management Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Name of the threshold profile.
Other Settings		
Report Interval	5	Set the time in minutes between the bandwidth usage report. The supported range is from 1 to 9,999,999 minutes.
Station Shaping Policy	default-access	Select the policy from the drop-down menu, with these options: <ul style="list-style-type: none"> ● default-access ● fair access ● preferred access
WLAN Bandwidths		
WLAN		Select the Add button to specify, edit, or add a WLAN bandwidth allocation, and the associated WLAN.
Bandwidth Allocation		Use this control to allow you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network. Define this as a percentage.

3. Select **Add** or **Save**. The added or edited profile appears on the **Profiles > QoS > Traffic Management** page.

Profiles > QoS > VoIP Call Admission Control

Alcatel-Lucent’s 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. VoIP call admission control prevents any single AP from becoming congested with voice calls. You configure call admission control options in the VoIP CAC profile which you apply to an AP group or a specific AP.

In the VoIP Call Admission Control (CAC) profile, you can limit the number of active voice calls allowed on a radio. This feature is disabled by default. When the disconnect extra call feature is enabled, the system monitors the number of active voice calls, and if the defined threshold is reached, any new calls are disconnected. The AP denies association requests from a device that is on call.

You enable this feature in the VoIP CAC profile. You also need to enable call admission control, which is disabled by default, in this profile. Perform these steps to create or edit VoIP Call Admission Control profiles.

1. Select **Profiles > QoS > VoIP Call Admission Control** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **VoIP Call Admission Control** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 42](#):

Table 42 Profiles > QoS > VoIP Call Admission Control Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the threshold profile.
Other Settings		
VoIP Call Admission Control	No	Enable or disable VoIP Call Admission Control in this profile.
VoIP Active Load Balancing	No	Enable or disable load balancing in this profile.
VoIP Vocera Call Capacity (0-255)	20	Specify the bandwidth allocation to Vocera voice calls when Admission Control is enabled.
VoIP NOE Call Capacity (0-255)	10	Specify the bandwidth allocation to New Office Environment (NOE) voice calls when Admission Control is enabled.
VoIP SIP Call Capacity (0-255)	10	Specify the bandwidth allocation to Session Initiated Protocol (SIP) voice calls when Admission Control is enabled.
VoIP SVP Call Capacity (0-255)	10	Specify the bandwidth allocation to SpectraLink Voice Priority (SVP) voice calls when Admission Control is enabled.
VoIP SCCP Call Capacity (0-255)	10	Specify the bandwidth allocation to Cisco Skinny Client Control Protocol (SCCP) voice calls when Admission Control is enabled.
VoIP H.323 Call Capacity (0-255)	10	Specify the bandwidth allocation to H323 protocol traffic when Admission Control is enabled.
VoIP T-Spec Call Capacity (0-255)	10	<p>A WMM client can send a Traffic Specification (TSPEC) signaling request to the AP before sending traffic of a specific AC type, such as voice. You can configure the switch so that the TSPEC signaling request from a client is ignored if the underlying voice call is not active; this feature is disabled by default. If you enable this feature, you can also configure the number of seconds that a client must wait to start the call after sending the TSPEC request (the default is one second).</p> <p>You enable TSPEC signaling enforcement in the VoIP Call Admission Control profile. This field specifies the bandwidth allocation to T-Spec voice calls when Admission Control is enabled.</p>
VoIP Call Handoff Reservation (0-100%)	20	Specify the total bandwidth to be reserved for call handoff. This field is a percentage of entire bandwidth.
VoIP High-capacity Threshold (0-100%)	20	Specifies the threshold that defines high-capacity VoIP. This field is a percentage of entire bandwidth.

Table 42 Profiles > QoS > VoIP Call Admission Control Profile Settings (Continued)

Field	Default	Description
VoIP Send SIP 100 Trying	No	The SIP invite call setup message is time-sensitive, as the originator retries the call as quickly as possible if it does not proceed. You can direct the switch to immediately reply to the call originator with a “SIP 100 - trying” message to indicate that the call is proceeding and to avoid a possible timeout. This is useful in conditions where the SIP invite may be redirected through a number of servers before reaching the switch. Enable or disable SIP call setup keepalive with this field.
VoIP Disconnect Extra Call	No	In the VoIP Call Admission Control (CAC) profile, you can limit the number of active voice calls allowed on a radio. This feature is disabled by default. When the disconnect extra call feature is enabled, the system monitors the number of active voice calls, and if the defined threshold is reached, any new calls are disconnected. The AP denies association requests from a device that is on call. Enable or disable this feature in this field. You also need to enable call admission control, which is disabled by default, in this profile.
VoIP TSPEC Enforcement	No	A WMM client can send a Traffic Specification (TSPEC) signaling request to the AP before sending traffic of a specific AC type, such as voice. You can configure the switch so that the TSPEC signaling request from a client is ignored if the underlying voice call is not active; this feature is disabled by default. If you enable this feature, you can also configure the number of seconds that a client must wait to start the call after sending the TSPEC request (the default is one second). You enable TSPEC signaling enforcement in the VoIP Call Admission Control profile. This field enables or disables TSPEC Enforcement.
VoIP TSPEC Enforcement Period (0-100)	1	When TSPEC is enabled, this field sets the number of seconds that a client must wait to start the call after sending the TSPEC request.
VoIP Drop SIP Invite and Send Status Code (Client)	486	The SIP invite call setup message is time-sensitive, as the originator retries the call as quickly as possible if it does not proceed. You can direct the switch to immediately reply to the call originator with a “SIP 100 - trying” message to indicate that the call is proceeding and to avoid a possible timeout. This is useful in conditions where the SIP invite may be redirected through a number of servers before reaching the switch. Use this field to enable or disable SIP call setup keepalive in the VoIP Call Admission Control profile for the client.
VoIP Drop SIP Invite and Send Status Code (Server)	486	The SIP invite call setup message is time-sensitive, as the originator retries the call as quickly as possible if it does not proceed. You can direct the switch to immediately reply to the call originator with a “SIP 100 - trying” message to indicate that the call is proceeding and to avoid a possible timeout. This is useful in conditions where the SIP invite may be redirected through a number of servers before reaching the switch. Use this field to enable or disable SIP call setup keepalive in the VoIP Call Admission Control profile for the server.

3. Select **Add** or **Save**. The added or edited profile appears on **Profiles > QoS > VoIP Call Admission Control**.

Profiles > QoS > WMM Traffic Management

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance specification based on the IEEE 802.11e wireless Quality of Service (QoS) standard. WMM works with 802.11a, b, g, and n physical layer standards.

WMM supports four access categories (ACs): voice, video, best effort, and background. The 802.1D priority value is contained in a two-byte QoS control field in the WMM data frame.



Configure the virtual AP traffic management profile before applying the WMM traffic management profile to the virtual AP profile.

Perform these steps to configure a **WMM Traffic Management** profile.

1. Select **Profiles > QoS > WMM Traffic Management** in the **Alcatel-Lucent Navigation** pane. The details page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **WMM Traffic Management** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 43](#):

Table 43 Profiles > QoS > WMM Traffic Management Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Enable Shaping Policy	No	Enable or disable Quality of Service with the WMM Traffic Management profile. Define the percentage of QoS for each type of service to be supported in WMM. NOTE: If you enable this profile with Yes, ensure that the four percentage values you specify immediately below this field do not exceed 100%.
Voice Share	25%	Set the total bandwidth share to be reserved for voice traffic in this field. Supported range is 1 to 100%.
Best-effort Share	25%	Set the total bandwidth share to be reserved for best-effort traffic in this field. Supported range is 1 to 100%.
Video Share	25%	Set the total bandwidth share to be reserved for video traffic in this field. Supported range is 1 to 100%.
Background Share	25%	Set the total bandwidth share to be reserved for background traffic in this field. Supported range is 1 to 100%.

Select **Add** or **Save**. The added or edited profile appears on the **WMM Traffic Management** page, and on the details page.

Profiles > RF

The RF management profiles configure radio tuning and calibration, AP load balancing, coverage hole detection, and RSSI metrics.

- **802.11a Radio**—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. Refer to [“Profiles > RF > 802.11a/g Radio”](#) on page 103.
- **802.11g Radio**—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 dynamically select 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. Refer to “[Profiles > RF > 802.11a/g Radio](#)” on page 103.

- **AM Scanning**—Defines AP radio settings for Air Monitor network and radio frequency (RF) monitoring.
- **ARM**—Defines the Adaptive Radio Management (ARM) settings for scanning, acceptable coverage levels, transmission power and noise thresholds. In most network environments, ARM does not need any adjustments from its factory-configured settings. However, if you are using VoIP or have unusually high security requirements you may want to manually adjust the ARM thresholds. Refer to “[Profiles > RF > 802.11a/g Radio > ARM](#)” on page 108.
- **HT Radio**—Manages high-throughput (802.11n) radio settings for 802.11n-capable APs. A high-throughput profile determines 40 MHz tolerance settings, and controls whether or not APs using this profile will advertise intolerance of 40 MHz operation. (This option is disabled by default, allowing 40 MHz operation.) Refer to “[Profiles > RF > 802.11a/g Radio > HT Radio](#)” on page 111.
- **Spectrum**—Defines AP radio settings for spectrum analysis on specific Alcatel-Lucent AP models that can examine the RF environment in which the Wi-Fi network is operating, identify interference, and classify its sources. Refer to “[Profiles > RF > 802.11a/g Radio > Spectrum](#)” on page 112.
- **Event Thresholds**—Defines error event conditions, based on a customizable percentage of low-speed frames, non-unicast frames, or fragmented, retry or error frames. “[Profiles > RF > Event Thresholds](#)” on page 113
- **Optimization**—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. “[Profiles > RF > Optimization](#)” on page 115

Profiles > RF > 802.11a/g Radio

The two 802.11a and 802.11g RF management profiles for an AP configure its 802.11a (5 GHz) and 802.11b/g (2.4 GHz) radio settings. Use these profile settings to determine the channel, beacon period, transmit power, and ARM profile for a mesh AP’s 5 GHz and 2.5 GHz frequency bands. You can either use the “default” version of each profile, or create a new 802.11a or 802.11g profile which you can then configure as necessary. Each RF management profile also has a radio-enable parameter that allows you to enable or disable the AP’s ability to simultaneously carry WLAN client traffic and mesh-backhaul traffic on that radio.

Radios are enabled by default.

Perform these steps to create or edit radio profiles for 802.11a or g. This type of radio profile references additional profiles such as ARM and High-throughput Radio profiles. You have the chance to add or edit supporting profiles as you define **802.11a/g Radio** profiles.

1. Select **Profiles > RF > 802.11a/g** in the **Alcatel-Lucent Configuration** navigation pane.
2. Select the appropriate **Add** button to create a new **802.11a** or **g** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 44](#):

Table 44 Profiles > RF > 802.11a/g Profile Settings

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

Table 44 Profiles > RF > 802.11a/g Profile Settings (Continued)

Field	Default	Description
Referenced Profiles		
Adaptive Radio Management (ARM) Profile	default	Select an ARM profile from the drop-down menu to define ARM settings for your 802.11a/g radio profile. Select the pencil icon to edit an existing ARM profile, or click the plus sign to create a new ARM profile. You are directed to the ARM Profile setup page. Once you have configured this referenced ARM profile, OV3600 returns you to the 802.11a/g radio profile page. For additional ARM profile information, refer to “Profiles > RF > 802.11a/g Radio > ARM” on page 108.
Spectrum Profile		Select a profile to define settings for Spectrum scanning. Select the pencil icon to edit an existing Spectrum profile, or click the plus sign to create a new AM Scanning profile. You are directed to the Spectrum Profile setup page. NOTE: OV3600 displays an error message if you try to select an incompatible spectrum profile. A '2ghz' spectrum band profile cannot be referenced by an '802.11a' profile and vice-versa.
AM Scanning Profile		Select a profile to define settings for Air Monitor Scanning. Select the pencil icon to edit an existing AM Scanning profile, or click the plus sign to create a new AM Scanning profile.
High-throughput Radio Profile	default-a	Select a high-throughput (HT) profile from the drop-down menu to define HT settings for your 802.11a/g radio profile. Select the pencil icon to edit an existing HT Radio profile, or click the plus sign to create a new HT Radio profile. You are directed to the HT Radio Profile setup page. Once you have configured this referenced profile, OV3600 returns you to the 802.11a/g Profile page. For additional HT radio profile information, refer to “Profiles > RF > 802.11a/g Radio > HT Radio” on page 111.
Other Settings		
Radio Enable	Yes	Enable transmissions on this radio band.
Mode	ap-mode	Set the access Point operating mode. Available options are as follows: <ul style="list-style-type: none"> • am-mode—Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc. • ap-mode—Access Point mode • sensor-mode—RFprotect sensor mode • spectrum-mode—Spectrum sensor mode. Device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
High Throughput Enable (Radio)	Yes	Enable or disable high-throughput (802.11n) features on the radio.
Channel (34-165)		Set the transmit channel for this radio.
Secondary Channel	None	Sets a secondary channel in relation to the primary channel defined just above. Select an option as follows: <ul style="list-style-type: none"> • None—no secondary channel • Above—secondary channel is just above the channel defined in Channel field • Below—secondary channel is just below the channel defined in the Channel field
Beacon Period	100	Sets the Beacon Period for the AP in milliseconds. The supported range is from 60 to 30,000 milliseconds.
Beacon Regulate	No	Enabling this setting introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air.

Table 44 Profiles > RF > 802.11a/g Profile Settings (Continued)

Field	Default	Description
Transmit Power	15	Sets the maximum transmit power (EIRP) in dBm from 0 to 30 in 0.5 dBm increments. This setting is limited further by regulatory domain constraints and AP capabilities.
TPC Power	15	The transmit power advertised in the TPC IE of beacons and probe responses. Range: 0-51 dBm
Advertise 802.11d and 802.11h Capabilities	No	Enable or disable the radio to advertise its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities.
Advertised Regulatory Max EIRP	0	The maximum transmit power (EIRP) advertised.
Spectrum Load Balancing	No	The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the switch is responding to the wireless clients' probe requests. If enabled, the switch compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Alcatel-Lucent AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.
Spectrum Load Balancing Mode	channel	SLB Mode allows control over how to balance clients. Select one of the following options <ul style="list-style-type: none"> channel: Channel-based load-balancing balances clients across channels. This is the default load-balancing mode radio: Radio-based load-balancing balances clients across APs
Spectrum Load Balancing Domain		Define a spectrum load balancing domain to manually create RF neighborhoods. Use this option to create RF neighborhood information for networks that have disabled Adaptive Radio Management (ARM) scanning and channel assignment. <ul style="list-style-type: none"> If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is <i>not</i> defined, AOS-W uses the ARM feature to calculate RF neighborhoods. If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain <i>is also</i> defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by the ARM feature.
Spectrum Load Balancing Update Interval	30	Specify how often spectrum load balancing calculations are made (in seconds). The range is 1-2147483647 seconds.
RX Sensitivity Tuning Based Channel Reuse		In some dense deployments, it is possible for APs to hear other APs on the same channel. This creates co-channel interference and reduces the overall utilization of the channel in a given area. Channel reuse enables dynamic control over the receive (Rx) sensitivity in order to improve spatial reuse of the channel. This feature is disabled by default. To enable this feature, click the drop-down list and select either static or dynamic . To disable this feature, click the drop-down list and select disable . For details on each of these modes, see the "RX Sensitivity Tuning Based Channel Reuse" topic in the <i>AOS-W 6.0 User Guide</i> .
RX Sensitivity Threshold (-dBm)	0	RX sensitivity tuning based channel reuse threshold, in - dBm. If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (in -dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. If the value for this parameter is set to zero, the feature will automatically determine an appropriate threshold.

Table 44 Profiles > RF > 802.11a/g Profile Settings (Continued)

Field	Default	Description
Non 802.11 Interference Immunity	Level 2	<p>When an AP attempts to decode a non-802.11 signal, that attempt can momentarily interrupt its ability to receive traffic. The noise immunity feature can help improve network performance in environments with a high level of non-802.11 noise from devices such as Bluetooth headsets, video monitors and cordless phones.</p> <p>You can configure the noise immunity feature for any one of the following levels of noise sensitivity. Note that increasing the level makes the AP slightly 'deaf' to its surroundings, causing the AP to lose a small amount of range.</p> <ul style="list-style-type: none"> • Level 0: no ANI adaptation. • Level 1: Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. • Level 2: Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. • Level 3: Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4Ghz appliances such as cordless phones. • Level 4: Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. • Level 5: The AP completely disables PHY error reporting, improving performance by eliminating the time the switch would spend on PHY processing. <p>You can manage Non-802.11 Noise Immunity settings through the 802.11g RF management profile. Do not raise the noise immunity feature's default setting if the RX Sensitivity Tuning Based Channel Reuse feature is also enabled. A level-3 to level-5 Noise Immunity setting is not compatible with the Channel Reuse feature. Requires a minimum version of 6.1.0.0.</p>
Enable CSA	No	Enable or disable Channel Switch Announcements (CSAs), as defined by IEEE 802.11h. This setting enables an AP to announce that it is switching to a new channel before it begins transmitting on that channel. This allows clients that support CSA to transition to the new channel with minimal downtime.
CSA Count (1-16)	4	Set the number of channel switch announcements that must be sent prior to switching to a new channel.
Management Frame Throttle Interval	1	Set the averaging interval for rate limiting management frames from this radio, in seconds. A management frame throttle interval of 0 seconds disables rate limiting.
Management Frame Throttle Limit	20	Set the maximum number of management frames that can come in from this radio in each throttle interval.
ARM/WIDS Override	No	If selected, this option disables Adaptive Radio Management (ARM) and Wireless IDS functions and slightly increases packet processing performance. If a radio is configured to operate in Air Monitor mode, then the ARM/WIDS override functions are always enabled, regardless of whether or not this check box is selected.

Table 44 Profiles > RF > 802.11a/g Profile Settings (Continued)

Field	Default	Description
Maximum Distance	0	Maximum client distance, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km. The upper limit for this parameter varies from 24–58km, depending on the radio's band (a/g) and 20/40 MHz mode. Note that if you configure a value above the supported maximum, the maximum supported value will be used instead. Values below 600m will use default settings.
Spectrum Monitoring	No	Select this option to convert APs using this radio profile to a hybrid APs that will continue to serve clients as an Access Point, but will also scan and analyze spectrum analysis data for a single radio channel. Requires a Wireless Intrusion Protection license or an RFprotect license and a minimum version of 6.1.0.0.

3. Select **Add** or **Save**. The added or edited **802.11a/g** profile appears on the **Profiles > RF > 802.11a/g** page.

Profiles > RF > 802.11a/g Radio > AM Scanning

Air Monitor (AM) devices establish and monitor RF activity on the network. This profile depends on the switch having a minimum version of 6.0.0.0.

Perform these steps to create or edit an Air Monitor Scanning profile.

1. Select **Profiles > RF > 802.11a/g Radio > AM Scanning** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **AM Scanning** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 45](#):

Table 45 Profiles > RF > 802.11a/g Radio > AM Scanning Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the AM scanning profile.
Scan Mode	all-reg-domain	Set the scanning mode for the radio: <ul style="list-style-type: none"> • all-reg-domain: Scan channels in all regulatory domain • rare: Scan all channels (all regulatory domains and rare channels) • reg-domain: Scan channels in the APs regulatory domain
Dwell Time Settings		
Regulatory Domain Channels (100-32768)	250	Dwell time (in ms) for AP's Regulatory domain channels
Rare Channels (100-32768)	100	Dwell time (in ms) for rare channels.

Table 45 Profiles > RF > 802.11a/g Radio > AM Scanning Profile Settings

Field	Default	Description
Active Channels (100-32768)	500	Dwell time (in ms) for channels where there is wireless activity.
Non-regulatory Domain Channels (100-32768)	200	Dwell time (in ms) for channels not in the APs regulatory domain.

Profiles > RF > 802.11a/g Radio > ARM

Each 802.11a and 802.11g radio profile references an Adaptive Radio Management (ARM) profile. When you assign an active ARM profile to a mesh radio, ARM's automatic power-assignment and channel-assignment features will automatically select the radio channel with the least amount of interference for each mesh portal, maximizing end user performance. In earlier versions of this software, an AP with a mesh radio received its beacon period, transmission power and 11a/11g portal channel settings from its mesh radio profile. Mesh-access AP portals now inherit these radio settings from their dot11a or dot11g radio profiles.

Each ARM-enabled mesh portal monitors defined thresholds for interference, noise, errors, rogue APs and radar settings, then calculates interference and coverage values and selects the best channel for its radio band(s). The mesh portal communicates its channel selection to its mesh points via Channel Switch Announcements (CSAs), and the mesh points will change their channel to match their mesh portal. Although channel settings can still be defined for a mesh point via that mesh point's 802.11a and 802.11g radio profiles, these settings will be overridden by any channel changes from the mesh portal. A mesh point will take the same channel setting as its mesh portal, regardless of its associated clients. If you want to manually assign channels to mesh portals or mesh points, disable the ARM profile associated with the 802.11a or 802.11g radio profile by setting the ARM profile's assignment parameter to disable. The ARM power adjustment feature does not apply to all ARM-enabled Mesh portals. Indoor mesh portals can take advantage of this feature to adjust power settings according to their ARM profiles, but outdoor mesh portals will continue to run at configured power level to maximize their range.



Do not delete or modify mesh cluster profiles once you use them to provision mesh nodes. You can recover the mesh point if the original cluster profile is still available. It is recommended to create a new mesh cluster profile if needed.

Perform these steps to create or edit an adaptive radio management (ARM) profile.

1. Select **Profiles > RF > 802.11a/g Radio > ARM** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **ARM** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 46](#):

Table 46 Profiles > RF > 802.11a/g Radio > ARM Profile Settings

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

Table 46 Profiles > RF > 802.11a/g Radio > ARM Profile Settings (Continued)

Field	Default	Description
Other Settings		
Assignment	single-band	<p>Activates one of four ARM channel/power assignment modes.</p> <ul style="list-style-type: none"> ● disable—Disables ARM calibration and reverts APs back to default channel and power settings specified by the AP's radio profile ● maintain—APs maintain their current channel and power settings. This setting can be used to maintain AP channel and power levels after ARM has initially selected the best settings. ● multi-band—For single-radio APs, this value computes ARM assignments for both 5 GHz (802.11a) and 2.4 GHz (802.11b/g) frequency bands. ● single-band—For dual-radio APs, this value enables APs to change transmit power and channels within their same frequency band, and to adapt to changing channel conditions.
Allowed Bands for 40MHz Channels	a-only	<p>Set the 802.11 radio bands to be supported by this ARM profile. The drop-down menu supports the following options:</p> <ul style="list-style-type: none"> ● a-only—802.11a radio bands ● g-only—802.11g radio bands ● all—both 802.11a and g bands
Client Aware	Yes	<p>If the Client Aware option is enabled, the AP does not change channels if there is active client traffic on that AP. If Client Aware is disabled, the AP may change to a more optimal channel, but this change may also disrupt current client traffic.</p>
Max Tx Power (dBm)	30	<p>Set the highest transmit power levels for the AP, from 0-30 dBm in 3 dBm increments. Higher power level settings may be constrained by local regulatory requirements and AP capabilities. In the event that an AP is configured for a Max Tx Power setting it cannot support, this value will be reduced to the highest supported power setting.</p> <p>NOTE: Power settings will not change if the Assignment option is set to disabled or maintain.</p>
Min Tx Power (dBm)	9	<p>Set the lowest transmit power levels for the AP, from 0-30 dBm, in 3 dBm increments. Note that power settings will not change if the Assignment option is set to disabled or maintain.</p> <p>NOTE: Consider configuring a Min Tx Power setting higher than the default value if most of your APs are placed on the ceiling. APs on a ceiling often have good line of sight between them, which will cause ARM to decrease their power to prevent interference. However, if the wireless clients down on the floor do not have such a clear line back to the AP, you could end up with coverage gaps.</p>
Multi Band Scan	Yes	<p>If enabled, single radio channel APs scans for rogue APs across multiple channels. This option requires that Scanning is also enabled.</p> <p>The Multi Band Scan option does not apply to APs that have two radios, such as an Alcatel-Lucent AP-65 or AP-70, as these devices already scan across multiple channels. If one of these dual-radio devices are assigned an ARM profile with Multi Band enabled, that device will ignore this setting.</p>
Rogue AP Aware	No	<p>If you have enabled both the Scanning and Rogue AP options, Alcatel-Lucent APs may change channels to contain off-channel rogue APs with active clients. This security feature allows APs to change channels even if the Client Aware setting is disabled.</p> <p>This setting is disabled by default, and should only be enabled in high-security environments where security requirements are allowed to consume higher levels of network resources. You may prefer to receive Rogue AP alerts via SNMP traps or syslog events.</p>

Table 46 Profiles > RF > 802.11a/g Radio > ARM Profile Settings (Continued)

Field	Default	Description
Scan Interval (sec)	10	<p>If Scanning is enabled, the Scan Interval defines how often the AP will leave its current channel to scan other channels in the band.</p> <p>Off-channel scanning can impact client performance. Typically, the shorter the scan interval, the higher the impact on performance. If you are deploying a large number of new APs on the network, you may want to lower the Scan Interval to help those APs find their optimal settings more quickly. Raise the Scan Interval back to its default setting after the APs are functioning as desired.</p> <p>The supported range for this setting is 0 to 2,147,483,647 seconds.</p>
Active Scan	No	<p>When the Active Scan checkbox is selected, an AP initiates active scanning via probe request. This option elicits more information from nearby APs, but also creates additional management traffic on the network.</p> <p>Active Scan is disabled by default, and should not be enabled except under the direct supervision of AirWave or Alcatel-Lucent Support.</p>
Scanning	Yes	<p>The Scanning field enables or disables AP scanning across multiple channels. Disabling this option also disables the following scanning features:</p> <ul style="list-style-type: none"> • Multi Band Scan • Rogue AP Aware • VoIP Aware Scan • Power Save Aware Scan <p>Do not disable Scanning unless you want to disable ARM and manually configure AP channel and transmission power.</p>
Scan Time	110 msec	<p>The amount of time, in milliseconds, an AP will drift out of the current channel to scan another channel. The supported range for this setting is 50 to 2,147,483,647 milliseconds. A scan time between 50 to 200 msec is recommended.</p>
VoIP Aware Scan	No	<p>Alcatel-Lucent's VoIP Call Admission Control (CAC) prevents any single AP from becoming congested with voice calls. When you enable CAC, you should also enable this ARM profile setting so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that Scanning is also enabled, as well as a Voice Service/Policy Enforcement Firewall license.</p>
Power Save Aware Scan	Yes	<p>If enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode.</p>
Ideal Coverage Index	10	<p>The Alcatel-Lucent coverage index metric is a weighted calculation based on the RF coverage for all Alcatel-Lucent APs and neighboring APs on a specified channel. The Ideal Coverage Index specifies the ideal coverage that an AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. The range of possible values is 2 to 20.</p>
Acceptable Coverage Index	4	<p>For multi-band implementations, the Acceptable Coverage Index specifies the minimal coverage an AP it should achieve on its channel. The denser the AP deployment, the lower this value should be. The range of possible values is 1 to 6.</p>
Free Channel Index	25	<p>The Alcatel-Lucent Interference index metric measures interference for a specified channel and its surrounding channels. This value is calculated and weighted for all APs on those channels (including 3rd-party APs). An AP will only move to a new channel if the new channel has a lower interference index value than the current channel.</p> <p>Free Channel Index specifies the required difference between the two interference index values before the AP moves to the new channel. The lower this value, the more likely it is that the AP will move to the new channel. The range of possible values is 10 to 40.</p>
Backoff Time	240	<p>Sets the backoff time in seconds. After an AP changes channel or power settings, it waits for the backoff time interval before it asks for a new channel/power setting. The range of possible values is 120 to 3,600 seconds.</p>

Table 46 Profiles > RF > 802.11a/g Radio > ARM Profile Settings (Continued)

Field	Default	Description
Error Rate Threshold	50	Sets the minimum percentage of PHY errors and MAC errors in the channel that will trigger a channel change.
Error Rate Wait Time	30	Sets the minimum time in seconds the error rate has to exceed the Error Rate Threshold before it triggers a channel change.
Noise Threshold (-dBm)	-75	Sets the maximum level of noise in channel that triggers a channel change. The range of possible values is 0 to -2,147,483,647 dBm.
Noise Wait Time	120	Sets the minimum time in seconds the noise level has to exceed the Noise Threshold before it triggers a channel change. The range of possible values is 120-3600 seconds.
Minimum Scan Time	8	Sets the minimum number of times a channel must be scanned before it is considered for assignment. The supported range for this setting is 0 to 2,147,483,647 scans. A Minimum Scan Time between 1 to 20 scans is recommended.
Load Aware Scan Thresholds	1,250,000	Sets the traffic throughput level an AP must reach before it stops scanning. Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high. The supported range for this setting is 0 to 20000000 bytes/second. (Specify 0 to disable this feature.)
Mode Aware Arm	No	Sets mode aware functions on the APs. If enabled, ARM turns APs into Air Monitors (AMs) if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (for example, less than 60 feet apart).
Scan Mode	all-reg-domain	Set the scanning mode for the radio: <ul style="list-style-type: none"> all-reg-domain: Scan channels in all regulatory domain reg-domain: Scan channels in the APs regulatory domain

3. Select **Add** or **Save**. The added or edited profile appears on the **Profiles > RF > 802.11a/g Radio > ARM** page.
4. Repeat this procedure or continue to additional procedures to complete profile configuration, then reference this profile as desired.

Profiles > RF > 802.11a/g Radio > HT Radio

Perform these steps to create or edit High Throughput (HT) Radio profiles.

1. Select **Profiles > RF > HT Radio** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **HT Radio** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 47](#):

Table 47 Profiles > RF > HT Radio Profile Settings

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

Table 47 Profiles > RF > HT Radio Profile Settings (Continued)

Field	Default	Description
Other Settings		
40MHz Intolerance	No	Allows a radio using this profile to stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.
Honor 40MHz Intolerance	Yes	Select 40 MHz intolerance if you want to enable 40 MHz intolerance. This parameter controls whether or not APs using this high-throughput profile will advertise intolerance of 40 MHz operation. By default, this option is disabled and 40 MHz operation is allowed.
Legacy Station Workaround	No	Use this setting to allow or disallow associations from legacy (non-HT) stations.

3. Select **Add** or **Save**. The added or edited profile appears on the **Profiles > RF > HT Radio** page.

Profiles > RF > 802.11a/g Radio > Spectrum



Note: This profile depends on the switch having an RFprotect license and a minimum version of 6.0.0.0

Perform these steps to create or edit Spectrum profiles.

1. Select **Profiles > RF > Spectrum** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Spectrum** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 48](#):

Table 48 Profiles > RF > Spectrum Profile Settings

Field	Default	Description
General Settings		
Name	Blank	Enter the name of the profile.
Spectrum Band	2ghz	Define one of the following spectrum bands for the spectrum profile. If you do not select a spectrum band, the profile will use a default setting of 2Ghz. <ul style="list-style-type: none"> • 2ghz: Scan 2GHz channels • 5ghz-lower: Scan 5GHz channels 36-64 • 5ghz-middle: Scan 5GHz channels 100-140 • 5ghz-upper: Scan 5GHz channels 149-165 NOTE: If its in use, you cannot change the band if it makes it incompatible to the radio profile that uses it.
Other Settings		
WIFI	600 seconds	Define the ageout time for Wi-Fi devices.
Generic Interferer	600 seconds	Define the ageout time for generic devices.
Microwave	15 seconds	Define the ageout time for microwave ovens.
Microwave (Inverter type)	15 seconds	Define the ageout time for inverter microwave ovens.
Video Device	10 seconds	Define the ageout time for video devices.

Table 48 Profiles > RF > Spectrum Profile Settings (Continued)

Field	Default	Description
Audio Device	10 seconds	Define the ageout time for audio devices.
Cordless Phone Fixed Frequency	10 seconds	Define the ageout time for fixed frequency cordless phones.
Generic Fixed Frequency	10 seconds	Define the ageout time for generic fixed-frequency devices.
Bluetooth	25 seconds	Define the ageout time for Bluetooth devices.
XBox	25 seconds	Define the ageout time for Xbox consoles.
Cordless Network Frequency Hopper	25 seconds	Define the ageout time for cordless network frequency hopping devices.
Cordless Base Frequency Hopper	25 seconds	Define the ageout time for cordless base frequency hopping devices.
Generic Frequency Hopper	25 seconds	Define the ageout time for Generic Frequency Hopper devices.

Profiles > RF > Event Thresholds

Perform these steps to create or edit **Event Threshold** profiles.

1. Select **Profiles > RF > Event Thresholds** in the **Alcatel-Lucent Navigation** pane.
2. Select the **Add** button to create a new **Event Thresholds** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 49](#):

Table 49 Profiles > RF > Event Thresholds Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the thresholds profile.
Other Settings		
Detect Frame Rate Anomalies	No	Enables or disables alerts for frame rate anomalies.
Bandwidth Rate High Watermark	0	Sets a high percentage watermark for bandwidth rate. When exceeded, this threshold triggers a high-watermark-exceeded alert. Defining 0% disables this function.
Bandwidth Rate Low Watermark	0	Sets a low percentage watermark for bandwidth rate. When exceeded, this threshold triggers a low-watermark-exceeded alert. Defining 0% disables this function.
Frame Error Rate High Watermark	50	Sets a high percentage watermark for frame error rates. When frame error rates exceed this threshold, this setting triggers a high-watermark-exceeded alert. Defining 0% disables this function.

Table 49 Profiles > RF > Event Thresholds Profile Settings (Continued)

Field	Default	Description
Frame Error Rate Low Watermark	10	Sets a low percentage watermark for frame error rates. When frame error rates exceed this threshold, this setting triggers a low-watermark-exceeded alert. Defining 0% disables this function.
Frame Fragmentation Rate High Watermark	0	Sets a high percentage watermark for frame fragmentation rates. When frame fragmentation rates exceed this threshold, this setting triggers a high-watermark-exceeded alert. Defining 0% disables this function.
Frame Fragmentation Rate Low Watermark	0	Sets a low percentage watermark for frame fragmentation rates. When frame fragmentation rates exceed this threshold, this setting triggers a low-watermark-exceeded alert. Defining 0% disables this function.
Frame Low Speed Rate High Watermark	0	Sets a high percentage watermark for low speed rates. When the percentage of received and transmitted frames at low speed (less than 5.5Mbps for 802.11b and less than 24 Mbps for 802.11a) exceeds the configured high watermark, the system generates an alert. Defining 0% disables this function.
Frame Low Speed Rate Low Watermark	0	Sets a low percentage watermark for low speed rates. When the percentage of received and transmitted frames at low speed (less than 5.5Mbps for 802.11b and less than 24 Mbps for 802.11a) exceeds the configured Low Watermark, the system generates an alert. Defining 0% disables this function.
Frame Non Unicast Rate High Watermark	0	Sets a high percentage watermark for non-Unicast frame rate. When the percentage of non-Unicast frames exceeds the configured high watermark, the system generates an alert. Defining 0% disables this function.
Frame Non Unicast Rate Low Watermark	0	Sets a low percentage watermark for non-Unicast frame rate. When the percentage of non-Unicast frames exceeds the configured low watermark, the system generates an alert. Defining 0% disables this function.
Frame Receive Error Rate High Watermark	50	Sets a high percentage watermark for frame-receive errors. When the percentage of errors in received frames exceeds the configured high watermark, the system generates an alert. Defining 0% disables this function.
Frame Receive Error Rate Low Watermark	10	Sets a low percentage watermark for frame-receive errors. When the percentage of errors in received frames exceeds the configured low watermark, the system generates an alert. Defining 0% disables this function.
Frame Retry Rate High Watermark	50	Sets a high percentage watermark for frame retry levels. When the percentage of frame retries exceeds the configured high watermark, the system generates an alert. Defining 0% disables this function.
Frame Retry Rate Low Watermark	10	Sets a low percentage watermark for frame retry levels. When the percentage of frame retries exceeds the configured low watermark, the system generates an alert. Defining 0% disables this function.

3. Select **Add** or **Save**. The added or edited profile appears on the **Profiles > RF > Event Thresholds** page.

Profiles > RF > Optimization

The RF Optimization profile 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.

Perform these steps to create or edit Optimization profiles.

1. Select **Profiles > RF > Optimization** in the **Alcatel-Lucent Navigation** pane. This page summarizes the current cluster profiles.
2. Select the **Add** button to create a new **Optimization** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 50](#):

Table 50 Profiles > RF > Optimization Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the threshold profile.
Other Settings		
AP Load Balancing	No	Enable or disable AP load balancing based on a user-defined number of clients or the degree of AP utilization on an AP.
AP Load Balancing Max Retries (0-100,000)	8	Set the maximum number of times that an AP attempts load balancing before timing out.
AP Load Balancing User High Watermark (0-100,000)	0	Set the high watermark level for the number of users that AP load balancing is to support. The supported range is 0 to 100,000 users, and setting this field to 0 users disables this function. When the number of users exceeds the high watermark, it triggers an alert.
AP Load Balancing User Low Watermark (0-100,000)	0	Set the low watermark level for the number of users that AP load balancing is to support. The supported range is 0 to 100,000 users, and setting this field to 0 users disables this function. When the number of users exceeds the low watermark, it triggers an alert.
AP Load Balancing Util High Watermark (0-100%)	0	Set the high watermark level as a percentage of load balancing utilization. The supported range is 0 to 100%, and a value of 0% disables this function. When this watermark is exceeded, it triggers an alert or wait time.
AP Load Balancing Util Low Watermark (0-100%)	0	Set the low watermark level as a percentage of load balancing utilization. The supported range is 0 to 100%, and a value of 0% disables this function. When this watermark is exceeded, it triggers an alert or wait time.
AP Load Balancing Util Wait Time (0-360,000 sec)	0	Set the wait time for the AP when AP load balancing is enabled. When load balancing thresholds are exceeded, this setting defines the length of time before AP load balancing restarts on the AP. The supported range is 0 to 360,000 seconds, and defining a value of 0 disables this function.
Station Handoff Assist	No	Enable or disable the ability of APs to hand users over to another adjacent AP, as available, in order to optimize or improve general network load.
Detect Association Failure	No	Enable or disable an AP's ability to detect failures in wireless user associations.

Table 50 Profiles > RF > Optimization Profile Settings (Continued)

Field	Default	Description
Coverage Hole Detection	No	Enable or disable an AP's ability to detect areas where an otherwise good RF signal is not reaching wireless clients to an adequate level. NOTE: This setting requires a Wireless Intrusion Protection license.
Hole Good RSSI Threshold (0-65,535)	20	Set the amount of time in seconds during which Received Signal Strength Indication (RSSI) is to check coverage holes. NOTE: This setting requires a Wireless Intrusion Protection license.
Hole Good Station Ageout (sec)	30	Set the amount of time in seconds that an AP is unseen by any probes before it is deleted from the database. Enter 0 to disable ageout. NOTE: This setting requires a Wireless Intrusion Protection license.
Hole Detection Interval (sec)	180	Sets the amount of time in seconds in which automatic hole detection should check for coverage holes. Enter 0 to disable this function. NOTE: This setting requires a Wireless Intrusion Protection license.
Hole Idle Station Timeout (sec)	90	Sets the amount of time in seconds before which an idle AP is deleted from the database, once it has become idle. Enter 0 to disable this function. NOTE: This setting requires a Wireless Intrusion Protection license.
Hole Poor RSSI Threshold (0-65,535)	10	Sets the threshold at which RSSI deems coverage to be poor.
Detect Interference	No	Enables or disables interference detection for the APs to be configured with this optimization profile.
Interference Threshold (0-100%)	100	Sets the maximum allowable interference to be tolerated by APs that are configured with this optimization profile, as a percentage.
Interference Threshold Exceed Time (0-360000 sec)	60	Sets the amount of time in seconds during which interference is allowed to exceed the threshold percentage. When interference exceeds the threshold percentage longer than the amount of time specified in this field, the threshold has been exceeded.
Interference Baseline Time (0-360000 sec)	600	Sets the period of time in seconds during which interference levels are to be monitored. This setting governs the deployment of the interference percentage threshold and the threshold exceed time.
RSSI Falloff Wait Time (0-8 sec)	0	Sets the maximum time to wait with decreasing received signal strength indication (RSSI) before de-authorization is sent to the client.
Low RSSI Threshold (0-255)	0	Sets the low threshold for received signal strength indication (RSSI). If the RSSI for a specific client falls below this threshold and continues to fall for the RSSI Falloff Wait Time, then the AP sends a de-authorization command to the client. Such de-authorization removes the client from the current AP and forces it to re-authentication on a nearby AP.
RSSI Check Frequency (0-255)	0	Sets the amount of time in seconds between RSSI coverage checks.

3. Select **Add** or **Save**. The added or edited profile appears on the **Profiles > RF > Optimization** page.

Profiles > SSID

Configures network authentication and encryption types. This profile also includes references an EDCA Parameters Station Profile, an EDCA Parameters AP Profile and a High-throughput (HT) SSID profile.

- **SSID**—Configures network authentication and encryption types. The SSID profile defines SSID settings and references additional EDCA and HT profiles. Refer to “[Profiles > SSID](#)” on page 117.
- **EDCA AP**—AP to client traffic prioritization, including EDCA parameters for background, best-effort, voice and video queues. Refer to “[Profiles > SSID > EDCA AP](#)” on page 122.
- **EDCA Station**—Client to AP traffic prioritization parameters, including Enhanced Distributed Channel Access (EDCA) parameters for background, best-effort, voice and video queues. Refer to “[Profiles > SSID > EDCA Station](#)” on page 125.
- **HT SSID**—High-throughput APs support additional settings not available in legacy APs. A High-throughput SSID profile can enable or disable high-throughput (802.11n) features and 40 MHz channel usage, and define values for aggregated MAC protocol data units (MDPUs) and Modulation and Coding Scheme (MCS) ranges. If none of the APs in your mesh deployment are 802.11n-capable APs, you do not need to configure a high-throughput SSID profile. If you modify a currently provisioned and running high-throughput SSID profile, your changes take affect immediately. You do not reboot the switch or the AP. Refer to “[Profiles > SSID > HT SSID](#)” on page 128.
- **802.11k**—Manages settings for the 802.11k protocol. The 802.11k protocol provides mechanisms to APs and clients to dynamically query the radio environment and take appropriate connection actions. In a 802.11k enabled network, APs and clients can send neighbor reports, beacon reports, and link measurement reports to each other. Refer to “[Profiles > SSID > 802.11K](#)” on page 129.

Profiles > SSID

Perform these steps to create or edit SSID profiles.

1. Select **Profiles > SSID** in the **Alcatel-Lucent Navigation** pane. This page summarizes the SSID profiles currently configured.
2. Select the **Add** button to create a new SSID profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 51](#):

Table 51 *Profiles > SSID Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Displays the name of the profile.
SSID Enable	Yes	Enables/disables this SSID.
Hide SSID		Enables or disables hiding of the SSID name in beacon frames. Note that hiding the SSID does very little to increase security.
ESSID		Name that uniquely identifies a wireless network. The ESSID can be up to 31 characters. If the ESSID includes spaces, you must enclose it in quotation marks.

Table 51 Profiles > SSID Profile Settings (Continued)

Field	Default	Description
Referenced Profiles		
EDCA Parameters Station Profile	None	<p>The drop-down menu allows you to select any EDCA Station profile that has already been configured. The referenced EDCA Station profile defines several settings that are used in the SSID profile. Select the Plus sign to create a new EDCA Station profile, as required.</p> <p>For additional information about this profile type, refer to “Profiles > SSID > EDCA Station” on page 125.</p> <p>Referencing an EDCA Station profile requires a Voice Service license.</p>
EDCA Parameters AP Profile	None	<p>The drop-down menu allows you to select any EDCA AP profile that has already been configured. The referenced EDCA AP profile defines several settings that are used in the SSID profile. Select the Plus sign to create a new EDCA AP profile, as required.</p> <p>For additional information about this profile type, refer to “Profiles > SSID > EDCA AP” on page 122.</p> <p>Referencing an EDCA Station profile requires a Voice Service license.</p>
High-throughput SSID Profile	default	<p>The drop-down menu allows you to select any High-throughput SSID profile that has already been configured. The referenced HT profile defines several settings that are used in the SSID profile. Select the Plus sign to create a new HT SSID profile, as required.</p> <p>For additional information about this profile type, refer to “Profiles > SSID > HT SSID” on page 128.</p>
Security Settings		
Encryption	opensystem	<p>Select any encryption type to be supported in this SSID profile. The supported encryption types are as follows:</p> <ul style="list-style-type: none"> • xSec—Encrypts an original Layer-2 data frame inside a Layer-2 xSec frame, the contents of which are defined by the protocol. xSec relies on 256-bit Advanced Encryption Standard (AES) encryption. • opensystem—No information sent to the client in plain text • static-wep—Static Wired Equivalent Privacy • dynamic-wep—Dynamic WEP with a key management service • wpa-tkip—Wi-Fi Protected Access with Temporal Key Integrity Protocol • wpa-aes—Wi-Fi-Protected-Access-Advanced Encryption Standard • wpa-psk-tkip—Wi-Fi-Protected-Access-Preshared Key-Temporal Key Integrity Protocol • wpa-psk-aes—Wi-Fi Protected Access-Preshared Key-Advanced Encryption Standard • wpa2-aes—Wi-Fi-Protected Access that adds AES and CCMP • wpa2-psk-aes—Wi-Fi Protected Access that adds Preshared Key and Advanced Encryption Standard • wpa2-psk-tkip—Wi-Fi Protected Access that adds Preshared Key and Temporal Key Integrity Protocol • wpa2-tkip—Wi-Fi Protected Access that adds Temporary Key Integrity Protocol
WEP Transmit Key Index	1	Drop-down menu allows you to specify the key index for Wired Equivalent Privacy. Range: 1-4
WEP Key 1		Enter WEP Key 1, and confirm the key in the Confirm field.
WEP Key 2		Enter WEP Key 2, and confirm the key in the Confirm field.
WEP Key 3		Enter WEP Key 3, and confirm the key in the Confirm field.
WEP Key 4		Enter WEP Key 4, and confirm the key in the Confirm field.

Table 51 Profiles > SSID Profile Settings (Continued)

Field	Default	Description
WPA Hexkey		Enter the hex key to be used with Wi-Fi Protected Access.
WPA Passphrase		Enter a difficult-to-guess passphrase between eight and 63 characters. NOTE: WPA Hexkey overrides WPA passphrase when both are set.
Other Settings		
DTIM Interval (1-255 beacon periods)	1	Enter the Delivery Traffic Indication Message that informs wireless clients about the presence of buffered, multicast, or broadcast data on the AP. The DTIM interval specifies the beacon frequency that synchronizes the AP to the network. This setting supports 1 to 255 milliseconds.
Station Ageout Time	1000	Enter the amount of time, in minutes, that a client is unseen by any probes before it is deleted from the database. Enter 0 to disable ageout.
802.11g Transmit Rates	All selected	Specify the total transmit rates for the 802.11g radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate. All transmission rates are selected and used. If you do not select 802.11a or 802.11g transmit rates, all rates are selected by default when you click Apply.
802.11g Basic Rates	1 and 2 selected	Specify the basic rates for the 802.11g radio.
802.11a Transmit Rates	All selected	Specify the transmit rates for the 802.11a radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate. All transmission rates are selected and used by default. If you do not select 802.11a or 802.11g transmit rates, all rates are selected by default when you click Apply.
802.11a Basic Rates	6, 12, and 24 selected	Specify the basic rates for the 802.11a radio.
Max Transmit Attempts	8	Specify the maximum number of transmit attempts. The supported range is 1 to 15.
RTS Threshold (bytes)	2333	Specify the Request to Send parameter that defines the packet size sent by mesh nodes. Mesh nodes transmitting frames larger than this threshold must issue request to send (RTS) and wait for other mesh nodes to respond with clear to send (CTS) to begin transmission. This helps prevent mid-air collisions. A smaller value causes more RTS packets to be sent more often, possibly impacting bandwidth. However, a smaller value may help the system recover more quickly from interference or data packet collisions. Specify the size in bytes.
Short Preamble	Yes	Instructs the AP to use short preambles in packets. Short preambles are often standard in AP configuration.
Max Associations	64	Define the maximum associations to be supported by devices configured with this SSID profile. The range is from 0 to 255.
Wireless Multimedia (WMM)	No	Specify whether the devices are to support wireless multimedia (WMM): voice, video, best effort (BE), or background.
Wireless Multimedia U-ASPD Powersave	Yes	Enable or disable unscheduled-automatic power save delivery. U-ASPD allows the saving of WLAN client power. The WLAN client transmits frames that trigger the forwarding of data frames for a client that has been buffered at the AP for power saving purposes.

Table 51 Profiles > SSID Profile Settings (Continued)

Field	Default	Description
WMM TSPEC Min Inactivity Interval	0	A WMM client can send a Traffic Specification (TSPEC) signaling request to the AP before sending traffic of a specific AC type, such as voice. You can configure the switch so that the TSPEC signaling request from a client is ignored if the underlying voice call is not active; this feature is disabled by default. If you enable this feature, you can also configure the number of seconds that a client must wait to start the call after sending the TSPEC request (the default is one second). You enable TSPEC signaling enforcement in the VoIP Call Admission Control profile. The supported range is 0 to 3,600,000 milliseconds.
DSCP Mapping for WMM Voice AC		Specify Differentiated Services Code Point (DSCP) mapping for wireless multimedia voice admission control. The supported range is 0 to 63. The IEEE 802.11e standard defines the mapping between WMM ACs and DSCP tags. The WMM AC mapping setting allows you to customize the mapping between WMM ACs and DSCP tags to prioritize various traffic types: voice, video, best effort, and background.
DSCP Mapping for WMM Video AC		Specify DSCP mapping for wireless multimedia video admission control. The supported range is 0 to 63.
DSCP Mapping for WMM Best-Effort AC		Specify DSCP mapping for wireless multimedia best effort admission control. The supported range is 0 to 63.
DSCP Mapping for WMM Background AC		Specify DSCP mapping for wireless multimedia background admission control. The supported range is 0 to 63.
902il Compatibility Mode	No	Enable or disable support for NEC 902il compatibility.
Deny Broadcast Probes	No	Deny or accept broadcast probes. This setting is used in conjunction with Local Probe Response. An AP broadcasts its configured service set identifier (SSID), which corresponds to a specific wireless local area network (WLAN). Wireless clients discover APs by listening for broadcast beacons or by sending active probes to search for APs with a specific SSID.
Local Probe Response	Yes	For deployments where there are expected to be considerable delays between the switch and APs (for example, in a remote location where an AP is not in range of another Alcatel-Lucent AP), enable the this option in the SSID profile. (Generating probe responses on the Alcatel-Lucent switch is an optimization that allows AOS-W to make better decisions.) This option is enabled by default.
Local Probe Request Threshold	0	The threshold, in dBm, for the bootstrap threshold to minimize the chance of the AP rebooting due to temporary loss of connectivity with the Alcatel-Lucent switch.
Disable Probe Retry	Yes	Prevent (disable Yes) or accept (disable No) the resending of packets in local probe operations. NOTE: This setting requires a voice service license.

Table 51 Profiles > SSID Profile Settings (Continued)

Field	Default	Description
Battery Boost	No	<p>Battery boost converts all multicast traffic to unicast before delivery to the client. This feature is disabled by default. Enabling this feature on an SSID allows you to set the DTIM interval from 10 - 100 (the previous allowed values were 1 or 2), equating to 1,000 - 10,000 milliseconds. This longer interval keeps associated wireless clients from activating their radios for multicast indication and delivery, leaving them in powersave mode longer, and thus lengthening battery life. The DTIM configuration is performed on the WLAN, so no configuration is necessary on the client.</p> <p>NOTE: This setting requires a voice service license.</p> <p>NOTE: Although you can enable battery boost on a per-virtual AP basis, it must be enabled for any SSIDs that support voice traffic.</p> <p>Although the multicast to unicast conversion generates more traffic, that traffic is buffered by the AP and delivered to the client when the client emerges from power-save mode. An associated parameter available on some clients is the Listening Interval (LI). This defines the interval (in number of beacons) after which the client must wake to read the Traffic Indication Map (TIM). The TIM indicates whether there is buffered unicast traffic for each sleeping client. With battery boost enabled, the DTIM is increased but multicast traffic is buffered and delivered as unicast. Increasing the LI can further increase battery life, but can also decrease client responsiveness.</p>
Maximum Transmit Failures	0	Specify the maximum number of transmit failures to be supported before a radio is considered to be down. A setting of 0 disables this feature.
BC/MC Rate Optimization	No	<p>Enables or disables scanning of all active stations currently associated to a mesh point to select the lowest transmission rate based on the slowest connected mesh child. When enabled, this setting dynamically adjusts the multicast rate to that of the slowest connected mesh child. Multicast frames are not sent if there are no mesh children.</p> <p>NOTE: The default value is recommended.</p>
Strict Spectralink Voice Protocol (SVP)	No	Use this setting for SpectraLink VoIP devices. This setting automatically permits and prioritizes the SpectraLink Voice Protocol (SVP).
802.11g Beacon Rate		<p>Sets the beacon rate for 802.11a (use for Distributed Antenna System (DAS) only).</p> <p>CAUTION: Using this parameter in normal operation may cause connectivity problems.</p>
802.11a Beacon Rate		<p>Sets the beacon rate for 802.11g (use for Distributed Antenna System (DAS) only).</p> <p>CAUTION: Using this parameter in normal operation may cause connectivity problems.</p>

Table 51 Profiles > SSID Profile Settings (Continued)

Field	Default	Description
Rate Optimization for Delivering EAPOL Frames		Enable rate optimization for delivering EAPOL frames.Requires a minimum version of 6.1.0.0.
Advertise QBSS Load IE		<p>Enabled the advertising of Quality-of-service BSS in the load element. The element includes the following parameters that provide information on the traffic situation:</p> <ul style="list-style-type: none"> • Station count: The total number of stations associated to the QBSS. • Channel utilization: The percentage of time (normalized to 255) the channel is sensed to be busy. The access point uses either the physical or the virtual carrier sense mechanism to sense a busy channel. • Available admission capacity: The remaining amount of medium time (measured as number of 32us/s) available for a station via explicit admission control. <p>The QAP uses these parameters to decide whether to accept an admission control request. A wireless station uses these parameters to choose the appropriate access points.</p> <p>NOTE: Ensure that wmm is enabled for legacy APs to advertise the QBSS load element. For 802.11n APs, ensure that either wmm or high throughput is enabled. Requires a minimum version of 6.1.0.0.</p>

3. Select **Add** or **Save**. The added or edited profile appears on the **Profiles > SSID** page.

Profiles > SSID > EDCA AP

Wireless Multimedia (WMM) provides media access prioritization through Enhanced Distributed Channel Access (EDCA). EDCA defines four access categories (ACs) to prioritize traffic: voice, video, best effort, and background. These ACs correspond to 802.1d priority tags, as shown in [Table 52](#).

Table 52 WMM Access Categories and 802.1d Tags

WMM Access Category	Description	802.1d Tag
Voice	Highest priority	7, 6
Video	Prioritize video traffic above other data traffic	5, 4
Best Effort	Traffic from legacy devices or traffic from applications or devices that do not support QoS	0, 3
Background	Low priority traffic (file downloads, print jobs)	2, 1

While the WMM ACs designate specific types of traffic, you can determine the priority of the ACs. For example, you can choose to give video traffic the highest priority. With WMM, applications assign data packets to an AC. In the client, the data packets are then added to one of the transmit queues for voice, video, best effort, or background.

WMM is an extension to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol's Distributed Coordination Function (DCF). The collision resolution algorithm responsible for traffic prioritization depends on the following configurable parameters for each AC:

- arbitrary inter-frame space number (AIFSN)
- minimum and maximum contention window (CW) size

For each AC, the backoff time is the sum of the AIFSN and a random value between 0 and the CW value. The AC with the lowest backoff time is granted the opportunity to transmit (TXOP). Frames with the highest priority AC are more likely to get TXOP as they tend to have the lowest backoff times (a result of having

smaller AIFSN and CW parameter values). The value of the CW varies through time as the CW doubles after each collision up to the maximum CW. The CW is reset to the minimum value after successful transmission.

In addition, you can configure the TXOP duration for each AC. On the switch, you configure the AC priorities in the WLAN EDCA parameters profile. There are two sets of EDCA profiles you can configure:

- AP parameters affect traffic from the AP to the client
- STA parameters affect traffic from the client to the AP

Perform these steps to create or edit EDCA AP profiles.

1. Select **Profiles > SSID > EDCA AP** in the **Alcatel-Lucent Navigation** pane. This page summarizes the current profiles of this type.
2. Select the **Add** button to create a new EDCA AP profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 53](#):

Table 53 Alcatel-Lucent Configuration > Profiles > SSID > EDCA AP Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Name of the EADC AP profile.
Best Effort		
Arbitrary Inter-frame Space Number (1-15)	3	WMM is an extension to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol's Distributed Coordination Function (DCF). The collision resolution algorithm responsible for traffic prioritization depends on the following configurable parameters for each AC: <ul style="list-style-type: none"> • arbitrary inter-frame space number (AIFSN) • minimum and maximum contention window (CW) size
Minimum Contention Window (Exponent) (0-15)	4	
Maximum Contention Window (Exponent) (1-15)	6	
Transmission Opportunity Slots in 32 usec Units	0	For each AC, the backoff time is the sum of the AIFSN and a random value between 0 and the CW value. The AC with the lowest backoff time is granted the opportunity to transmit (TXOP). Frames with the highest priority AC are more likely to get TXOP as they tend to have the lowest backoff times (a result of having smaller AIFSN and CW parameter values). The value of the CW varies through time as the CW doubles after each collision up to the maximum CW. The CW is reset to the minimum value after successful transmission. In addition, you can configure the TXOP duration for each AC.
Background		
Arbitrary Inter-frame Space Number	7	WMM is an extension to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol's Distributed Coordination Function (DCF). The collision resolution algorithm responsible for traffic prioritization depends on the following configurable parameters for each AC: <ul style="list-style-type: none"> • arbitrary inter-frame space number (AIFSN) • minimum and maximum contention window (CW) size
Minimum Contention Window (Exponent)	4	
Maximum Contention Window (Exponent)	10	

Table 53 Alcatel-Lucent Configuration > Profiles > SSID > EDCA AP Profile Settings (Continued)

Field	Default	Description
Transmission Opportunity Slots in 32 usec Units	0	Set the transmission opportunity slots in 32-micro-second intervals. For each AC, the backoff time is the sum of the AIFSN and a random value between 0 and the CW value. The AC with the lowest backoff time is granted the opportunity to transmit (TXOP). Frames with the highest priority AC are more likely to get TXOP as they tend to have the lowest backoff times (a result of having smaller AIFSN and CW parameter values). The value of the CW varies through time as the CW doubles after each collision up to the maximum CW. The CW is reset to the minimum value after successful transmission. In addition, you can configure the TXOP duration for each AC.
ACM	No	Define whether or not admission control mandatory (ACM) is to be supported on APs configured with this EDCA profile.
Video		
Arbitrary Inter-frame Space Number	1	WMM is an extension to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol's Distributed Coordination Function (DCF). The collision resolution algorithm responsible for traffic prioritization depends on the following configurable parameters for each AC: <ul style="list-style-type: none"> arbitrary inter-frame space number (AIFSN) minimum and maximum contention window (CW) size
Minimum Contention Window (Exponent)	3	
Maximum Contention Window (Exponent)	4	
Transmission Opportunity Slots in 32 usec Units	94	For each AC, the backoff time is the sum of the AIFSN and a random value between 0 and the CW value. The AC with the lowest backoff time is granted the opportunity to transmit (TXOP). Frames with the highest priority AC are more likely to get TXOP as they tend to have the lowest backoff times (a result of having smaller AIFSN and CW parameter values). The value of the CW varies through time as the CW doubles after each collision up to the maximum CW. The CW is reset to the minimum value after successful transmission. In addition, you can configure the TXOP duration for each AC.
ACM	No	Define whether or not admission control mandatory (ACM) is to be supported on APs configured with this EDCA profile.
Voice		
Arbitrary Inter-frame Space Number	1	WMM is an extension to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol's Distributed Coordination Function (DCF). The collision resolution algorithm responsible for traffic prioritization depends on the following configurable parameters for each AC: <ul style="list-style-type: none"> arbitrary inter-frame space number (AIFSN) minimum and maximum contention window (CW) size
Minimum Contention Window (Exponent)	2	
Maximum Contention Window (Exponent)	3	

Table 53 Alcatel-Lucent Configuration > Profiles > SSID > EDCA AP Profile Settings (Continued)

Field	Default	Description
Transmission Opportunity Slots in 32 usec Units	47	For each AC, the backoff time is the sum of the AIFSN and a random value between 0 and the CW value. The AC with the lowest backoff time is granted the opportunity to transmit (TXOP). Frames with the highest priority AC are more likely to get TXOP as they tend to have the lowest backoff times (a result of having smaller AIFSN and CW parameter values). The value of the CW varies through time as the CW doubles after each collision up to the maximum CW. The CW is reset to the minimum value after successful transmission. In addition, you can configure the TXOP duration for each AC.
ACM	No	Define whether or not admission control mandatory (ACM) is to be supported on APs configured with this EDCA profile.

3. Select **Add** or **Save**. The added or edited profile appears on the **Profiles > SSID > EDCA AP** page.

Profiles > SSID > EDCA Station

Wireless Multimedia (WMM) provides media access prioritization through Enhanced Distributed Channel Access (EDCA). EDCA defines four access categories (ACs) to prioritize traffic: voice, video, best effort, and background. These ACs correspond to 802.1d priority tags, as shown in [Table 54](#).

Table 54 WMM Access Categories and 802.1d Tags

WMM Access Category	Description	802.1d Tag
Voice	Highest priority	7, 6
Video	Prioritize video traffic above other data traffic	5, 4
Best Effort	Traffic from legacy devices or traffic from applications or devices that do not support QoS	0, 3
Background	Low priority traffic (file downloads, print jobs)	2, 1

While the WMM ACs designate specific types of traffic, you can determine the priority of the ACs. For example, you can choose to give video traffic the highest priority. With WMM, applications assign data packets to an AC. In the client, the data packets are then added to one of the transmit queues for voice, video, best effort, or background.

WMM is an extension to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol's Distributed Coordination Function (DCF). The collision resolution algorithm responsible for traffic prioritization depends on the following configurable parameters for each AC:

- arbitrary inter-frame space number (AIFSN)
- minimum and maximum contention window (CW) size

For each AC, the backoff time is the sum of the AIFSN and a random value between 0 and the CW value. The AC with the lowest backoff time is granted the opportunity to transmit (TXOP). Frames with the highest priority AC are more likely to get TXOP as they tend to have the lowest backoff times (a result of having smaller AIFSN and CW parameter values). The value of the CW varies through time as the CW doubles after each collision up to the maximum CW. The CW is reset to the minimum value after successful transmission.

In addition, you can configure the TXOP duration for each AC. On the switch, you configure the AC priorities in the WLAN EDCA parameters profile. There are two sets of EDCA profiles you can configure:

- AP parameters affect traffic from the AP to the client
- STA parameters affect traffic from the client to the AP

Perform these steps to create or edit **Event Station** profiles.

1. Select **Profiles > SSID > EDCA Station** in the **Alcatel-Lucent Navigation** pane. This page summarizes the current cluster profiles.
2. Select the **Add** button to create a new **EDCA Station** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 55](#):

Table 55 Profiles > SSID > EDCA Station Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Name of the EDCA STA profile.
Best Effort		
Arbitrary Inter-frame Space Number (1-15)	3	<p>WMM is an extension to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol's Distributed Coordination Function (DCF). The collision resolution algorithm responsible for traffic prioritization depends on the following configurable parameters for each AC:</p> <ul style="list-style-type: none"> • arbitrary inter-frame space number (AIFSN) • minimum and maximum contention window (CW) size
Minimum Contention Window (Exponent) (0-15)	4	
Maximum Contention Window (Exponent) (1-15)	10	
Transmission Opportunity Slots in 32 usec Units	0	<p>For each AC, the backoff time is the sum of the AIFSN and a random value between 0 and the CW value. The AC with the lowest backoff time is granted the opportunity to transmit (TXOP). Frames with the highest priority AC are more likely to get TXOP as they tend to have the lowest backoff times (a result of having smaller AIFSN and CW parameter values). The value of the CW varies through time as the CW doubles after each collision up to the maximum CW. The CW is reset to the minimum value after successful transmission.</p> <p>In addition, you can configure the TXOP duration for each AC.</p>
Background		
Arbitrary Inter-frame Space Number	7	<p>WMM is an extension to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol's Distributed Coordination Function (DCF). The collision resolution algorithm responsible for traffic prioritization depends on the following configurable parameters for each AC:</p> <ul style="list-style-type: none"> • arbitrary inter-frame space number (AIFSN) • minimum and maximum contention window (CW) size
Minimum Contention Window (Exponent)	4	
Maximum Contention Window (Exponent)	10	
Transmission Opportunity Slots in 32 usec Units	0	<p>For each AC, the backoff time is the sum of the AIFSN and a random value between 0 and the CW value. The AC with the lowest backoff time is granted the opportunity to transmit (TXOP). Frames with the highest priority AC are more likely to get TXOP as they tend to have the lowest backoff times (a result of having smaller AIFSN and CW parameter values). The value of the CW varies through time as the CW doubles after each collision up to the maximum CW. The CW is reset to the minimum value after successful transmission.</p> <p>In addition, you can configure the TXOP duration for each AC.</p>
ACM	No	Define whether or not admission control mandatory (ACM) is to be supported on APs configured with this EDCA profile.

Table 55 Profiles > SSID > EDCA Station Profile Settings (Continued)

Field	Default	Description
Video		
Arbitrary Inter-frame Space Number	2	WMM is an extension to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol's Distributed Coordination Function (DCF). The collision resolution algorithm responsible for traffic prioritization depends on the following configurable parameters for each AC: <ul style="list-style-type: none"> arbitrary inter-frame space number (AIFSN) minimum and maximum contention window (CW) size
Minimum Contention Window (Exponent)	3	
Maximum Contention Window (Exponent)	4	
Transmission Opportunity Slots in 32 usec Units	94	For each AC, the backoff time is the sum of the AIFSN and a random value between 0 and the CW value. The AC with the lowest backoff time is granted the opportunity to transmit (TXOP). Frames with the highest priority AC are more likely to get TXOP as they tend to have the lowest backoff times (a result of having smaller AIFSN and CW parameter values). The value of the CW varies through time as the CW doubles after each collision up to the maximum CW. The CW is reset to the minimum value after successful transmission. In addition, you can configure the TXOP duration for each AC.
ACM	No	Define whether or not admission control mandatory (ACM) is to be supported on APs configured with this EDCA profile.
Voice		
Arbitrary Inter-frame Space Number	2	WMM is an extension to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol's Distributed Coordination Function (DCF). The collision resolution algorithm responsible for traffic prioritization depends on the following configurable parameters for each AC: <ul style="list-style-type: none"> arbitrary inter-frame space number (AIFSN) minimum and maximum contention window (CW) size
Minimum Contention Window (Exponent)	2	
Maximum Contention Window (Exponent)	3	
Transmission Opportunity Slots in 32 usec Units	47	For each AC, the backoff time is the sum of the AIFSN and a random value between 0 and the CW value. The AC with the lowest backoff time is granted the opportunity to transmit (TXOP). Frames with the highest priority AC are more likely to get TXOP as they tend to have the lowest backoff times (a result of having smaller AIFSN and CW parameter values). The value of the CW varies through time as the CW doubles after each collision up to the maximum CW. The CW is reset to the minimum value after successful transmission. In addition, you can configure the TXOP duration for each AC.
ACM	No	Define whether or not admission control mandatory (ACM) is to be supported on APs configured with this EDCA profile.

3. Select **Add** or **Save**. The added or edited profile appears on the **Profiles > SSID > EDCA Station** page.

Profiles > SSID > HT SSID

High-throughput (HT) APs support additional settings not available in legacy APs. A mesh high-throughput SSID profile can enable or disable high-throughput (802.11n) features and 40 MHz channel usage, and define values for aggregated MAC protocol data units (MDPUs) and Modulation and Coding Scheme (MCS) ranges.

Alcatel-Lucent provides a “default” version of the mesh high-throughput SSID profile. You can use the “default” version or create a new instance of a profile which you can then edit as you need. High-throughput Mesh nodes operating in different cluster profiles can share the same high-throughput SSID radio profile.

The mesh high-throughput SSID profile defines settings unique to 802.11n-capable, high-throughput APs. If none of the APs in your mesh deployment are 802.11n-capable APs, you do not need to configure a high-throughput SSID profile.

If you modify a currently provisioned and running high-throughput SSID profile, your changes take effect immediately. You do not reboot the switch or the AP.

Perform these steps to create or edit **HT SSID** profiles.

1. Select **Profiles > SSID > HT SSID** in the **Alcatel-Lucent Navigation** pane. This page summarizes the current cluster profiles.
2. Select the **Add** button to create a new **HT SSID** profile, or click the **pencil** icon to edit an existing profile. Complete the settings as described in [Table 56](#):

Table 56 Profiles > SSID > HT SSID Profile Settings

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Name of the HT SSID profile.
Other Settings		
High Throughput Enable (SSID)	Yes	Enable or disable high-throughput (802.11n) features on this SSID. This parameter is enabled by default.
40 MHz Channel Usage	Yes	Enable or disable the use of 40 MHz channels. This parameter is enabled by default.
MPDU Aggregation	Yes	Enable or disable MAC protocol data unit (MPDU) aggregation. High-throughput mesh APs are able to send aggregated MAC protocol data units (MDPUs), which allow an AP to receive a single block acknowledgment instead of multiple ACK signals. This option, which is enabled by default, reduces network traffic overhead by effectively eliminating the need to initiate a new transfer for every MPDU.
Max Transmitted A-MPCU Size	65535	Set the maximum size of a transmitted aggregate MPDU, in bytes. Range: 1576 -65535
Max Received A-MPDU Size (bytes)	65535	Set the maximum size of a received aggregate MPDU, in bytes. Allowed values: 8191, 16383, 32767, 65535.
Min MPDU Start Spacing (usec)	0	Set the minimum time between the start of adjacent MDPUs within an aggregate MPDU, in microseconds. Allowed values: 0 (No restriction on MPDU start spacing), 0.25 usec, 0.5 usec, 1 usec, 2 usec, 4 usec.

Table 56 Profiles > SSID > HT SSID Profile Settings (Continued)

Field	Default	Description
Supported MCS Set	0-15	<p>Set a list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this SSID.</p> <p>The MCS you choose determines the channel width (20MHz vs. 40MHz) and the number of spatial streams used by the mesh node.</p> <p>The default value is 1-15; the complete set of supported values. To specify a smaller range of values, enter a hyphen between the lower and upper values. To specify a series of different values, separate each value with a comma.</p> <p>Examples:</p> <ul style="list-style-type: none"> • 2-10 • 1,3,6,9,12 <p>Range: 0-15</p>
Short Guard Interval in 40 MHz Mode	Yes	<p>Enable or disable use of short (400ns) guard interval in 40 MHz mode.</p> <p>A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data.</p> <p>The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput.</p> <p>This parameter is enabled by default.</p>
Legacy Stations	Yes	<p>Allow or disallow associations from legacy (non-HT) stations. By default, this parameter is enabled (legacy stations are allowed).</p>
Allow Weak Encryption	No	<p>Use this setting to define TKIP or WEP encryption for unicast traffic, which forces legacy transmission rates on high-throughput APs. This option is disabled by default, preventing clients using TKIP or WEP for unicast traffic from associating with the mesh node</p>

3. Select **Add** or **Save**. The added or edited profile appears on the **Profiles > SSID > HT SSID** page.

Profiles > SSID > 802.11K

The 802.11k protocol provides mechanisms to APs and clients to dynamically measure the available radio resources. In a 802.11k enabled network, APs and clients can send neighbor reports, beacon reports, and link measurement reports to each other. This allows the APs and clients to take appropriate connection actions. This profile is disabled by default.

Perform these steps to configure an **802.11K** profile.

1. Select **Profiles > SSID > 802.11K** in the **Alcatel-Lucent Navigation** pane. The details page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **802.11K** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 57](#):

Table 57 Profiles > SSID > 802.11K Profile Settings

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

Table 57 Profiles > SSID > 802.11K Profile Settings (Continued)

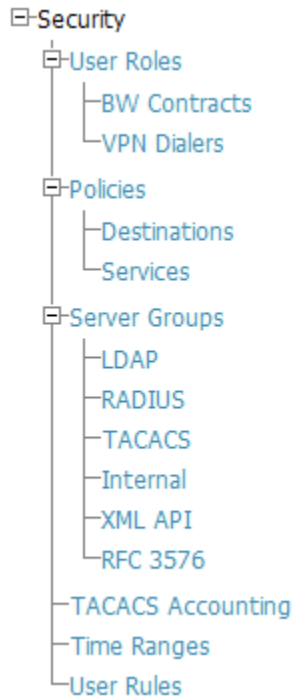
Field	Default	Description
Name	Blank	Enter the name of the profile.
Other Settings		
Measurement Mode for Beacon Reports	beacon-table	<p>Select the Measurement Mode for Beacon Reports drop-down menu and specify one of the following measurement modes:</p> <ul style="list-style-type: none"> ● active—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. ● beacon-table—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. ● passive—Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. <p>NOTE: If a station does not support the selected measurement mode, it returns a Beacon Measurement Report with the Incapable bit set in the Measurement Report Mode field.</p>
Advertise 802.11K Capability	No	Select this option to allow Virtual APs using this profile to advertise 802.11K capability. This feature is disabled by default.
Forcefully Disassociate On-hook Voice Clients	No	Select this option to allow the AP to forcefully disassociate on-hook voice clients (clients that are not on a call) after period of inactivity. Without the forced disassociation feature, if an AP has reached its call admission control limits and an on-hook voice client wants to start a new call, that client may be denied. If forced disassociation is enabled, those clients can associate to a neighboring AP that can fulfil their QoS requirements. This feature is disabled by default.

3. Select **Add** or **Save**. The added or edited profile appears on the **802.11K** page, and on the details page.

Security

Alcatel-Lucent Configuration supports user roles, policies, server groups, and additional security parameters with profiles that are listed in the **Security** portion of the navigation pane on the **Alcatel-Lucent Configuration** page, as illustrated in [Figure 6](#):

Figure 6 Security Components in Alcatel-Lucent Configuration



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

- Security > User Roles
 - Security > User Roles > BW Contracts
 - Security > User Roles > VPN Dialers
- Security > Policies
 - Security > Policies > Destinations
 - Security > Policies > Services
- Security > Server Groups
 - Security > Server Groups > LDAP
 - Security > Server Groups > RADIUS
 - Security > Server Groups > TACACS
 - Security > Server Groups > Internal
 - Security > Server Groups > XML API
 - Security > Server Groups > RFC 3576
- Security > TACACS Accounting
- Security > Time Ranges
- Security > User Rules

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 switch.

This page displays the current user roles in Alcatel-Lucent Configuration and where they are used. This page contains the columns described in [Table 58](#):

Table 58 *Security > User Roles* Page Contents

Column	Description
Name	Name of the user role.
AAA	Displays the AAA profile or profiles that are referenced by the user role. For additional information, refer to " Profiles > AAA " on page 51.
Captive Portal Profile	Displays the Captive Portal Auth profiles, if any, that are referenced by the user role. For additional information, refer to " Profiles > AAA > Captive Portal Auth " on page 60.
802.1X Auth	Displays the 802.1X Auth profiles that are referenced by the user role. For additional information, refer to " Profiles > AAA > Advanced Authentication " on page 58.

Table 58 Security > User Roles Page Contents (Continued)

Column	Description
Stateful 802.1X Auth	Displays the Stateful 802.1X Auth profiles that are referenced by the user role. For additional information, refer to “Profiles > AAA > Stateful 802.1X Auth” on page 63.
VPN Auth	Displays the VPN Auth profiles that are referenced by the user role. For additional information, refer to “Profiles > AAA > Combined VPN Auth” on page 64.
Folder	Displays the folder that is associated with this User Role. A Top viewable folder for the role is able to view all devices and groups contained by the top folder. The top folder and its subfolders must contain all of the devices in any of the groups it can view. Clicking any folder name takes you to the APs/Devices > List page for folder inventory and configuration.

The **Security > User Roles > Add New User Role** page contains the following fields, as described in [Table 59](#):

Table 59 Security > User Roles > Add New User Role Field Descriptions

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the User Role is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the user role.
Other Settings		
Captive Portal Profile	None	(Optional) Select the Captive Portal Auth profile, if any, that is to be referenced by the user role. For additional information, refer to “Profiles > AAA > Captive Portal Auth” on page 60. Select the add icon to create a new profile, or click the pencil icon to edit an existing profile.
Downstream Bandwidth Contract	None	(Optional) You can assign a bandwidth contract to provide an upper limit to upstream or downstream bandwidth utilized by clients in this role. You can select the Per User option to apply the bandwidth contracts on a per-user basis instead of to all clients in the role. For additional information, refer to “Security > User Roles > BW Contracts” on page 134.
Downstream Contract Applies Per User	No	If you selected a DS BW contract in the prior field, this gray field becomes active. Select Yes or No .
Upstream Bandwidth Contract	None	(Optional) You can assign a bandwidth contract to provide an upper limit to upstream or downstream bandwidth utilized by clients in this role. You can select the Per User option to apply the bandwidth contracts on a per-user basis instead of to all clients in the role. For additional information, refer to “Security > User Roles > BW Contracts” on page 134.
Upstream Contract Applies Per User	No	If you selected an US BW contract in the prior field, this gray field becomes active. Select Yes or No .
Maximum Number of Datapath Sessions Allowed	None	Use this field to configure a maximum number of sessions per user in this role. You can configure any value between 0-65535.
Reauthentication Interval Time	0	(Optional) Set the time, in minutes, after which the client is required to re-authenticate. Enter a value between 0-4096. 0 disables reauthentication.

Table 59 Security > User Roles > Add New User Role Field Descriptions (Continued)

Field	Default	Description
VLAN To Be Assigned	Blank	(Optional) By default, a client is assigned a VLAN on the basis of the ingress VLAN for the client to the switch. Use this field to override this assignment and configure the VLAN ID that is to be assigned to the user role.
VPN Dialer Profile	None	(Optional) Use this field to assign a VPN dialer to a user role. Select a dialer from the drop-down list and assign it to the user role. This dialer will be available for download when a client logs in using captive portal and is assigned this role. For additional VPN information, refer to “Security > User Roles > VPN Dialers” on page 135.
Policies		
Add New Policy		Select this button to add a new policy to the user role. The following two fields appear with respective drop-down menus: <ul style="list-style-type: none"> • Policy • Alcatel-Lucent AP Group
Policy	dhcp-acl	Select the policy to apply to this user role. Once any policy is selected, you can edit the policy by clicking the pencil icon. You can create a new policy by clicking the add icon. For additional information, refer to “Security > Policies” on page 138.
Alcatel-Lucent AP Group	None	Select the Alcatel-Lucent AP group in which this policy and user role will apply. For additional information, refer to “General Alcatel-Lucent AP Groups Procedures and Guidelines” on page 27.

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

Security > User Roles > BW Contracts

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

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

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

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

The Details page for **Security > User Roles > Add New Bandwidth Contract** contains the following fields, as described in [Table 60](#):

Table 60 *Security > User Roles > Add New BW Contract Page Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the Bandwidth Contract is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Other Settings		
Units	kbits	Configure bandwidth contracts, in kilobits per second (Kbps) or megabits per second (Mbps), for the following types of traffic: <ul style="list-style-type: none"> from the client to the switch (“upstream” traffic) from the switch to the client (“downstream” traffic)
Bandwidth		Specify whether this bandwidth contract is upstream or downstream by typing one of the following terms in lower case: <ul style="list-style-type: none"> upstream downstream Select Add to finish the new BW Contract and to return to the BW Contract page. The new contact appears below the Add New BW Contract button.

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

Security > User Roles > VPN Dialers

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

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

The **Security > User Roles > Add New VPN Dialer** page contains the following fields, as described in [Table 61](#):

Table 61 *Security > User Roles > Add VPN Dialer Field Descriptions*

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

Table 61 Security > User Roles > Add VPN Dialer Field Descriptions (Continued)

Field	Default	Description
Other Settings		
Enable PPTP	No	<p>Enable PPTP with this setting as desired.</p> <p>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.</p> <p>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).</p>
Enable L2TP	Yes	<p>Enable L2TP with this setting as desired.</p> <p>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.</p> <p>L2TP/IPSec requires two levels of authentication:</p> <ul style="list-style-type: none"> • 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, SecurID, digital certificates, or smart cards after successful creation of the SAs.
Send traffic to the direct network in clear	No	Use this setting if no encryption is to be used and packets passing between the wireless client and switch are to be in clear text.
Disable wireless devices when client is wired	No	Use this setting to disable wireless clients when a wired device is known to be on the VPN.
Enable SecurID New and Next Pin Mode	No	<p>Use this setting to enable or disable SecurID PIN modes.</p> <p>The SecurID authentication scheme authenticates the user on a RSA ACE/Server. When challenged, the user has to enter a password that is a combination of two numbers: a personal identification number (PIN), supplied by RSA, combined with a token code, which is the number displayed on the RSA SecurID authenticator.</p> <p>New PIN mode is applied in cases where the authentication process requires additional verification of the PIN. In this case, the user is required to use a new PIN. The new PIN is derived from one of the following two sources, depending on the configuration of the RSA ACE/Server:</p> <ul style="list-style-type: none"> • The user is prompted to select and enter a new PIN. • The server supplies the user with a new PIN. <p>The user is then required to re-authenticate with the new PIN. The use of the New PIN mode is optional and can be enabled or disabled.</p>

Table 61 Security > User Roles > Add VPN Dialer Field Descriptions (Continued)

Field	Default	Description
PPP Authentication Modes	CHAP MSCHAP MSCHAPv2 PAP	Use this section to select the authentication modes to be supported for PPP in the VPN. The following options are available: <ul style="list-style-type: none"> • CHAP • Cache SecurID Token • MSCHAP • MSCHAPv2 • PAP
IKE Lifetime (300-85400 secs)	28800	Specify the Internet Key Exchange (IKE) Lifetime in seconds. When this period of time expires, the IKE SA is replaced by a new SA or is terminated. The IKE SA specifies values for the IKE exchange: the authentication method used, the encryption and hash algorithms, the Diffie-Hellman group used, the lifetime of the IKE SA in seconds, and the shared secret key values for the encryption algorithms. The IKE SA in each peer is bi-directional.
IKE Encryption	168-bit 3DES-CBC	Select the Internet Key Exchange (IKE) encryption method from the following two options: <ul style="list-style-type: none"> • 168-bit 3DES-CBC • 56-bit DES-CBC
IKE Diffie-Hellman Group	1024-bit (1)	Select the IPSEC Mode Group that matches the Diffie Hellman Group configured for the IPSEC policy. The two options are as follows: <ul style="list-style-type: none"> • 1024-bit • 768-bit <p>The IKE policy selections, along with the preshared key, need to be reflected in the VPN configuration. Set the VPN configuration on clients to match the choices made above. In case the Alcatel-Lucent dialer is used, these configuration need to be made on the dialer prior to downloading the dialer onto the local client.</p>
IKE Hash Algorithm	SHA	Set the IKE Hash Algorithm to either SHA or MD5, to match the IKE policy for IPSEC.
IKE Authentication	Pre-Shared	IKE Phase 1 authentication can be done with either an IKE preshared key or digital certificates. This establishes how the client is authenticated with the internal database on the switch. The options are Pre-Shared Keys or RSA Signatures .
IPSEC Lifetime	7200	Define the IPSEC lifetime in seconds, after which a new IPSEC key is required.
IPSEC Diffie Hellman Group	1024-bit (1)	Select the IPSEC Mode Group that matches the Diffie Hellman Group configured for the IKE policy. The two options are as follows: <ul style="list-style-type: none"> • 1024-bit • 768-bit <p>The IPSEC policy selections, along with the preshared key, need to be reflected in the VPN configuration. Set the VPN configuration on clients to match the choices made above. In case the Alcatel-Lucent dialer is used, these configuration need to be made on the dialer prior to downloading the dialer onto the local client.</p>
IPSEC Encryption	168-bit 3DES	Specify the type of IPSEC encryption to support for the VPN. Options are as follows: <ul style="list-style-type: none"> • Encapsulating Security Payload (ESP) with 168-bit 3DES • ESP with 56-bit DES
IPSEC Hash Algorithm	SHA	Set the IKE Hash Algorithm to either SHA or MD5, to match the IKE policy for IKE Hash Algorithm.

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

Security > Policies

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

The **Security > Policies > Add New Policy** page contains the following fields, as described in [Table 62](#):

Table 62 *Security > Policies > Add New Policy Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the policy is associated. The drop-down menu displays all folders available for association with the policy.
Name	Blank	Enter the name of the policy.
Rules		
IPv6	No	Select whether to use the IPv6 protocol. If you select No, OV3600 displays options for the IPv4 protocol instead. NOTE: As of AOS-W 6.0, you can mix IPv4 and IPv6 rules on one policy.
Source Traffic Match	any	The traffic source, which can be one of the following: <ul style="list-style-type: none"> • alias: After choosing this option, specify the network resource from the Source Alias drop-down menu that appears. Select the pencil icon to edit, or the plus icon to add a new alias. • any: match any traffic (wildcard) • host: This refers to traffic from a specific host. When this option is chosen, you must configure the source IP address of the host. For example, 2002:d81f:f9f0:1000:c7e:5d61:585c:3ab • localip: (IPv4 only) specify the local IP address to match traffic • network: This refers to a traffic that has a source IP from a subnet of IP addresses. When this option is chosen, you must configure the source address and network mask of the subnet. For example, 2002:ac10:fe::ffff:ffff:: • user: This refers to traffic from the wireless client.
Destination Traffic Match	any	The traffic destination, which can be any of the same types as the Source Traffic Match options.
Service Type	any	Type of traffic, which can be one of the following: <ul style="list-style-type: none"> • any: This option specifies that this rule applies to any type of traffic. • tcp: Using this option, configure a range of TCP port(s) to match for the rule to be applied. • udp: Using this option, configure a range of UDP port(s) to match for the rule to be applied. • service: Selecting this option creates a new field called Service underneath Service Type with a drop-down list of pre-defined services (common protocols such as HTTPS, HTTP, and others) as the protocol to match for the rule to be applied. Select the pencil icon to edit the Netservice Profile (refer to “Security > Policies > Services” on page 140), or the plus sign to create a new Netservice profile. • protocol: Using this option, specify a different layer 4 protocol (other than TCP/UDP) by configuring the IP protocol value. • icmpv6: Use this option to configure ICMPv6. Requires IPv6 enabled.

Table 62 Security > Policies > Add New Policy Field Descriptions (Continued)

Field	Default	Description
Action	permit	Action if rule is applied, which can be one of the following: reject: deny packets. A new field will appear where you can Send Deny Response dst-nat: perform destination NAT on packets. New fields appear to specify the Dual NAT Pool and Dual NAT Port. dual-nat: perform both source and destination NAT on packets permit: forward packets redirect: specify the location to which packets are redirected, which can be one of the following: <ul style="list-style-type: none"> • Datapath Destination ID (0-65535) • ESI Server Group: specify the ESI server group configured with the esi group command. • Tunnel: specify the ID of the tunnel configured with the interface tunnel command src-nat: perform source NAT on packets
ICMPv6 Message Type		Choose from the informational or error message types. This field appears if IPv6 is enabled and ICMPv6 is selected in the Service Type field.
Log if ACL is applied	No	Whether to generate a log message when the rule is applied.
Mirror all session packets	No	Whether to mirror all session packets to datapath or remote destination.
Queue Priority	low	Assigns a matching flow to a priority queue (high/low).
Time Range	None	Define a time range for this rule.
Pause ARM Scanning	No	Whether to pause Adaptive Radio Management scan activity when traffic is present. Note that the Scanning setting in the ARM profile should be activated in order to be paused. Refer to “Profiles > RF > 802.11a/g Radio > ARM Profile Settings” on page 108 for this setting.
Blacklist user if ACL is applied	No	Whether to blacklist any user.
TOS Value	None	Value of type of service (TOS) bits to be marked in the IP header of a packet matching this rule when it leaves the switch.
802.1p Priority	None	Specify 802.1p priority (0-7).

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

Security > Policies > Destinations

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

The **Security > Policies > Add New Destinations** page contains the following fields, as described in [Table 63](#):

Table 63 *Security > Policies > Destinations Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the security policy is associated. The drop-down menu displays all folders available for association with the policy.
Name	Blank	Enter the name of the destination.
Rules		
Invert	No	Use this field to invert the destination from one end of the VPN connection to the other.
IPv6	No	Select this button to create a new rule for this destination profile. Clicking this button displays the Net Destination Rule section for the selected protocol, which is comprised of two settings: <ul style="list-style-type: none">● Rule Type—Specify whether the rule applies to Host, Network, or Range.● IP Address—Enter the IP address for the net destination rule.

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

Security > Policies > Services

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

Select **Add** to create a new Netservice profile, or click the pencil icon next to an existing Netservice profile to edit it. The **Security > Policies > Services** page contains the following fields, as described in [Table 64](#):

Table 64 *Security > Policies > Services Field Descriptions*

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

Table 64 Security > Policies > Services Field Descriptions (Continued)

Field	Default	Description
Other Settings		
Protocol	TCP	Specify the protocol that is to support the security policy service being configured. The service options are: <ul style="list-style-type: none"> ● TCP ● UDP ● IP The remaining fields on this page change according to which protocol you have selected.
Port Selection	Range	Choose whether to list ports by Range (which causes the Port and Max Port fields to appear below) or List (which introduces a Port List field and requires a minimum version of 6.0.0.0).
TCP/UDP Port		Appears if Range is specified in Port Selection. Specify the TCP/UDP port or range of ports to support the service being configured.
TCP/UDP Max Port		Appears if Range is specified in Port Selection. Specify the highest port that will support the TCP/UDP service being configured.
Port List		Appears if List is specified in Port Selection. Enter a comma separated list of ports. Requires a minimum version of 6.0.0.0.
IP Protocol Number (0-255)		Specify the numeric identifier of the upper layer IP protocol that an IP packet should use.
Configure Application Level Gateway	No	Specify whether to create an application level gateway, which filters incoming and outgoing information packets before copying and forwarding across the gateway. If you select Yes in this field, you are prompted with a new drop-down menu in which to select the Application Level Gateway type.
Application Level Gateway	dhcp	If you select Yes for Configure Application Level Gateway , then specify the gateway type from this drop-down menu. The following application level gateway types are supported: <ul style="list-style-type: none"> ● dhcp ● dns ● ftp ● h323 ● noe ● rtsp ● sccp ● sip ● sips ● svp ● tftp ● vocera

Security > Server Groups

Server Groups Page Overview

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

- **AAA**
- **Captive Portal Auth**
- **Management Auth**

- **Stateful 802.1X Auth**
- **TACACS Accounting**
- **VPN Auth**
- **Folder**

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

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

Before enabling fail-through authentication, note the following:

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

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

Supported Servers

AOS-W supports the following external authentication servers:

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

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

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

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

Adding a New Server Group

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

To create a new server group, click the **Add** button, or to edit an existing group, click the pencil icon next to that group. The **Add New Server Group** page appears, and contains the following fields, as described in Table 65:

Table 65 Security > Server Groups > Add or Edit Server Group Field Descriptions

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server group.
Other Settings		
Fail Through	No	<p>Enable or disable a fail through server.</p> <p>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. The switch attempts authentication with each server in the list until either there is a successful authentication or the list of servers in the group is exhausted.</p> <p>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.</p>
Add New Server		<p>Select this button to add a new server to the Server Group being configured. A new Server section and Server Group Server Rules section appear with the following settings to be defined:</p> <p>Server Section</p> <ul style="list-style-type: none"> • Trim FQDN—Default setting is No. Change to Yes to enable. You can use the “match FQDN” option for a server match rule. With a match FQDN rule, the server is selected if the <domain> portion of the user information in the formats <domain>\<user> or <user>@<domain> exactly matches a specified string. Note the following caveats when using a match FQDN rule: <ul style="list-style-type: none"> • This rule does not support client information in the host/<pc-name>.<domain> format, so it is not useful for 802.1x machine authentication. • The match FQDN option performs matches on only the <domain> portion of the user information sent in an authentication request. The match-authstring option (described previously) allows you to match all or a portion of the user information sent in an authentication request. • Server Type—Select the server type for the new server being added. Options are RADIUS (default), LDAP, TACACS, and Internal. • RADIUS Server—Select the RADIUS server from the drop-down menu that the new server is to use. You can edit an existing RADIUS server or create a new server. <p>Server Group Server Rules Section</p> <p>Select the Add button to add a new rules section. The page that appears contains the following settings to define:</p> <ul style="list-style-type: none"> • Match Type—From the drop-down menu, select Authstring or FQDN. The following settings complete the configuration. • Operator—For Authstring only, specify how to process the string (contains, equals, starts with). • Match String—Enter the string or string fragment. <p>Finish by clicking the Add New Server Group Server Rules button.</p>

Table 65 Security > Server Groups > Add or Edit Server Group Field Descriptions (Continued)

Field	Default	Description
Server Group Rule		
Field to set	role	Specify whether the server group rule is a role or a VLAN . The Role/VLAN field at the bottom of the page changes in response to your selection here.
Attribute	ARAP-Features	From the drop-down menu, click the attribute that defines the server group rule being configured. Many options are supported.
Operation	contains	Select the criteria by which to process the Operand , which you specify in the following field.
Operand		Enter a text string.
Role/VLAN	ap-role	Select the role or VLAN to associate with this new server group rule from the drop-down menu.

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

Security > Server Groups > LDAP

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

The **Security > Server Groups > Add LDAP Server** page contains the following fields, as described in [Table 66](#):

Table 66 Security > Server Groups > Add LDAP Server Field Descriptions

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server.
Other Settings		
Host IP Address	0.0.0.0	Enter the IP address of the LDAP server.
Admin-DN		Enter the distinguished name for the admin user who has read/search privileges across all the entries in the LDAP database. The user need not have write privileges but the user should be able to search the database, and read attributes of other users in the database.
Admin Password		Enter the password for the admin user.
Allow Clear-text	No	Enable this setting to allow clear-text (unencrypted) communication with the LDAP server.
Auth Port	389	Enter the port number used for authentication on the LDAP server.

Table 66 Security > Server Groups > Add LDAP Server Field Descriptions (Continued)

Field	Default	Description
Base-DN		Enter the distinguished name of the node which contains the entire user database to use.
Filter	(objectclass=*)	Select the filter that should be applied to any search of the user in the LDAP database.
Key Attribute	sAMAccountName	Enter the attribute that should be used as a key in search for the LDAP server. For Active Directory, the value is sAMAccountName.
Timeout (1030 sec)	20	Define the timeout period of a LDAP request, in seconds.
Enable	Yes	Use this field to enable or disable the LDAP server being configured. You can configure the LDAP server as disabled, but return later to enable it.
Preferred Connection Type	ldap-s	Select the connection type for the LDAP server from the drop-down menu. LDAP servers support the following connection types: <ul style="list-style-type: none"> ● clear-text—No encryption is used. ● ldap-s—Uses SSL encryption. ● start-tls—Uses TLS encryption.

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

Security > Server Groups > RADIUS

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

The **Security > Server Groups > Add New RADIUS Server** page contains the following fields, as described in [Table 67](#):

Table 67 Security > Server Groups > RADIUS

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server.
Other Settings		
Host IP Address		Set the IP address of the authentication server.
Key (Confirm Key)		Set the shared secret between the switch and the authentication server. The maximum length is 48 bytes.
Auth Port	1812	Set the authentication port on the server.
Acct Port	1813	Set the accounting port on the server.
Retransmits (0-3)	3	Set the Maximum number of retries sent to the server by the switch before the server is marked as down.

Table 67 Security > Server Groups > RADIUS (Continued)

Field	Default	Description
Timeout	(1-30 sec)	Set the maximum time, in seconds, that the switch waits before timing out the request and resending it.
NAS ID		Set the Network Access Server (NAS) identifier to use in RADIUS packets.
NAS IP		Set the NAS IP address to send in RADIUS packets. You can configure a “global” NAS IP address that the switch uses for communications with all RADIUS servers. If you do not configure a server-specific NAS IP, the global NAS IP is used.
Use MD5	No	Enable or disable the use of MD5 hashing for cleartext passwords.
Enable	Yes	Enable or disable the RADIUS server.
Source Interface		Enter a VLAN number ID between 1-4094. Allows you to use source IP addresses to differentiate RADIUS requests. Associates a VLAN interface with the RADIUS server to allow the server-specific source interface to override the global configuration. If you associate a Source Interface (by entering a VLAN number) with a configured server, then the source IP address of the packet will be that interface’s IP address. If you do not associate the Source Interface with a configured server (leave the field blank), the IP address of the global Source Interface will be used. Requires a minimum version of 6.1.0.0.

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

Security > Server Groups > TACACS

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

The **Security > Server Groups > Add New TACACS Server** page contains the following fields, as described in [Table 68](#):

Table 68 Security > Server Groups > TACACS

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

Table 68 Security > Server Groups > TACACS (Continued)

Field	Default	Description
Retransmits (0-3)	3	Set the maximum number of times a request is retried.
Tmeout (1-30 sec)	20	Set the timeout period for TACACS+ requests, in seconds.
Enable	Yes	Enable or disable the TACACS server.
Session Authorization	No	Enables or disables session authoriaztion.Session authorization turns on the optional authorization session for admin users.

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

Security > Server Groups > Internal

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

The **Security > Server Groups > Add New Internal Server** page contains the following fields, as described in [Table 69](#):

Table 69 Security > Server Groups > Add Internal Server Field Descriptions

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

Table 69 Security > Server Groups > Add Internal Server Field Descriptions (Continued)

Field	Default	Description
E-Mail		Enter the email address of the guest user.
Enabled	Yes	Specify whether this guest user is enabled or disabled on the internal server.
Expire User	No	Specify whether to expire the guest user after a period of time. If you click Yes , a new field appears with instructions about the date and time in which the guest user is expired from the internal server.

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

Security > Server Groups > XML API

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

The **Security > Server Groups > Server** page lists any XML API servers currently available for use by server groups. From this page, click **Add** to create a new XML API server, or click the pencil icon next to an existing server to edit. The **Security > Server Groups > Add New XML API Server** page contains the following fields, as described in [Table 70](#):

Table 70 Security > Server Groups > Add New XML API Server Field Descriptions

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

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

Security > Server Groups > RFC 3576

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

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

Select **Add** to create a new RFC3576 server, or click the pencil icon next to an existing server to edit it. The **Security > Server Groups > Add RFC 3576 Server** page contains the following fields, as described in [Table 71](#).

Table 71 *Security > Server Groups > Add RFC 3576 Server Field Descriptions*

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

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

Security > Server Groups > Windows

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

1. Select **Security > Server Groups > Windows** in the **Alcatel-Lucent Navigation** pane. The details page summarizes the current profiles of this type.
2. Select the **Add** button to create a new **Windows** profile, or click the **pencil** icon next to an existing profile to edit. Complete the settings as described in [Table 72](#):

Table 72 *Security > Server Groups > Windows Profile Settings*

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

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

Security > TACACS Accounting

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

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

The **Add/Edit TACACS Accounting Profile** page contains the following fields, as described in [Table 73](#):

Table 73 *Security > Server Groups > Add/Edit TACACS Accounting Profile Field Descriptions*

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

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

Security > Time Ranges

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

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

To create a new time range profile, click the **Add New Time Range** button, or click the pencil icon next to an existing time range profile to adjust settings. The **Security > Time Range > Add/Edit New Time Range** page contains the following fields, as described in [Table 74](#):

Table 74 *Security > Time Range > Add/Edit Time Range Field Descriptions*

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

Table 74 Security > Time Range > Add/Edit Time Range Field Descriptions (Continued)

Field	Default	Description
Other Settings		
Type	Absolute	<p>Specify whether the time range is Absolute, meaning a very specific range of time, or Periodic, meaning regularly occurring time ranges that occur repeatedly over time.</p> <p>If you select Absolutely, specify the Start Date and End Date and time as instructed.</p> <p>If you select Periodic, the Add New Time Period button appears. Select this button, then complete the three settings that follow:</p> <ul style="list-style-type: none"> • Period—Specify whether the time period is daily, weekday, weekend, or day. • Start Time—Specify the hour and minute that the time period is to be begin. • End Time—Specify the hour and minute that the time period is to end.

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

Security > User Rules

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

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

To add a new user rule, which is a derivation profile, click Add New User Derivation Profile. To edit an existing user rule, click the pencil icon next to an existing rule. [Table 75](#) describes the contents of this page.

Table 75 Security > User Rules > Add/Edit User Rules Field Descriptions

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

Table 75 Security > User Rules > Add/Edit User Rules Field Descriptions (Continued)

Field	Default	Description
Rule Type	bssid	<p>Select one of the following options from the drop-down menu. Your selection in this field changes an ensuing field that must be completed, as follows:</p> <ul style="list-style-type: none"> ● bssid—Selecting this option displays the BSSID field below. Specify the BSSID in text. ● dhcp-option-77—Selecting this option displays the DHCP Option 77 field below. Enter this information in text. ● encryption-type—Selecting this option displays the Encryption Type field below, in which you must select the encryption type from the drop-down menu. Select open, static-wep, or another other encryption type from the drop-down menu. ● essid—Selecting this option displays ESSID field below, in which you enter the ESSID in text. ● location—Selecting this option displays the Location field below, in which you enter the location in text. ● macaddr—Selecting this option displays the MAC Address field below, in which you must enter the MAC address.
Operator	contains	Select the matching operator.
User Role/VLAN	ap-role	<p>If you selected role for the Set Type field above, then select the specific user role from this drop-down menu.</p> <p>If you selected VLAN for the Set Type field above, then select the specific VLAN from this drop-down menu.</p>

Local Config of SNMP Management

The Local Config component, introduced in OV3600 7.2, is used for local configuration of Alcatel-Lucent controllers. Locally configured settings are not pushed to local controllers by master controllers.

SNMP trap settings for controllers are managed locally. Trap settings for the AP are managed by group or global configuration in **Profiles > AP > SNMP**. Refer to “[Profiles > AP > SNMP](#)” on page 73 if you want to manage AP settings.



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

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

Table 76 describes the fields that appear in the Details page for this profile:

Table 76 *Local Config > SNMP Management Profile Settings*

Field	Description
General Settings	
Folder	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Enter the name of the profile.
SNMP Settings	
Community Strings	Community strings used to authenticate requests for SNMP versions before version 3. NOTE: This is needed only if using SNMP v2c and is not needed if using version 3.
Enable Trap Generation	Enables generation of SNMP traps to configured SNMP trap receivers.
Engine ID	Sets the SNMP server engine ID as a hexadecimal number. 24 character maximum.
Inform Queue Length (100-350)	Specifies the length for the SNMP inform queue. Default is 250.
Always use the switch's IP address as source address	Set whether to use the IP address of the switch as the trap source.
Trap Source IP Address	Enter the source IP address for sending traps.
SNMP Trap Hosts	
IP Address	Enter the IP address of the trap host.
SNMP Version	Configures the SNMP version as 1, 2c, or 3. <ul style="list-style-type: none">• If 2c is selected, the Send Inform field appears at the bottom of this section.• If 3 is selected, the SNMP User field will appear as a drop-down menu containing any configured v3 users. Select the plus icon to add them via the SNMP Management > SNMPv3 User profile.

Table 76 Local Config > SNMP Management Profile Settings

Field	Description
Community String	Configure the security string for notification messages. Does not appear if SNMP Version is set to 3.
UDP Port (1-65535)	The port number to which trap notification messages are sent. Default is 162.
Send Informs	Whether to send SNMP inform messages to the configured host. Displays when 2c is selected in SNMP Version .
<p>SNMPv3 Users</p> <p>If you are using SNMPv3 to obtain values from the Alcatel-Lucent switch, navigate to Local Config > SNMP Management > SNMPv3 User to configure the following parameters:</p>	
User name	A string representing the name of the user.
Authentication protocol	<p>An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values:</p> <ul style="list-style-type: none"> • MD5: HMAC-MD5-96 Digest Authentication Protocol • SHA: HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption Protocol).
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol.

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

Advanced Services

This document section describes the contents, parameters, and default settings for all **Advanced Services** components in **Alcatel-Lucent Configuration**. Alcatel-Lucent Configuration in OV3600 6.3 supports advanced services such as IP Mobility and VPN services. Future OV3600 versions will support additional advanced services.

For additional information about IP Mobility domains, VPN services, and additional architecture or concepts, refer to your version of the *AOS-W User Guide*.

Overview of IP Mobility Domains

Alcatel-Lucent's layer-3 mobility solution is based on the Mobile IP protocol standard, as described in RFC 3344, "IP Mobility Support for IPv4". This standard addresses users who need both network connectivity and mobility within the work environment.

Unlike other layer-3 mobility solutions, an Alcatel-Lucent mobility solution does not require that you install mobility software or perform additional configuration on wireless clients. The Alcatel-Lucent switches perform all functions that enable clients to roam within the mobility domain.

In a mobility domain, a mobile client is a wireless client that can change its point of attachment from one network to another within the domain. A mobile client receives an IP address (a home address) on a home network. A mobile client can detach at any time from its home network and reconnect to a foreign network (any network other than the mobile client's home network) within the mobility domain. When a mobile client is connected to a foreign network, it is bound to a care-of address that reflects its current point of attachment. A care-of address is the IP address of the Alcatel-Lucent switch in the foreign network with which the mobile client is associated.

The *home agent* for the client is the switch where the client appears for the first time when it joins the mobility domain. The home agent is the single point of contact for the client when the client roams. The *foreign agent* for the client is the switch which handles all Mobile IP communication with the home agent on behalf of the client. Traffic sent to a client's home address is intercepted by the home agent and tunneled for delivery to the client on the foreign network. On the foreign network, the foreign agent delivers the tunneled data to the mobile client.

A mobility domain is a group of Alcatel-Lucent switches among which a wireless user can roam without losing their IP address. Mobility domains are not tied with the master switch, thus it is possible for a user to roam between switches managed by different master switches as long as all of the switches belong to the same mobility domain.

You enable and configure mobility domains only on Alcatel-Lucent switches. No additional software or configuration is required on wireless clients to allow roaming within the domain.

Before configuring a mobility domain, you should determine the user VLAN(s) for which mobility is required. For example, you may want to allow employees to be able to roam from one subnetwork to another. All switches that support the VLANs into which employee users can be placed should be part of the same mobility domain.

A switch can be part of multiple mobility domains, although it is best if a switch belong to only one domain. The switches in a mobility domain do not need to be managed by the same master switch.

You configure a mobility domain on a master switch; the mobility domain information is pushed to all local switches that are managed by the same master switch. On each switch, you must specify the active domain (the domain to which the switch belongs). If you do not specify the active domain, the switch will be assigned to a predefined "default" domain.

Although you configure a mobility domain on a master switch, the master switch does not need to be a member of the mobility domain. For example, you could set up a mobility domain that contains only local switches; you still need to configure the mobility domain on the master switch that manages the local

switches. You can also configure a mobility domain that contains multiple master switches; you need to configure the mobility domain on each master switch.

Table 77 *Switches in a Mobility Domain*

On a master switch:	On all switches in the mobility domain:
Configure the mobility domain, including the entries in the home agent table (HAT).	<ul style="list-style-type: none"> • Enable mobility (disabled by default). • Join a specified mobility domain (not required for “default” mobility domain).

You can enable or disable IP mobility in a virtual AP profile (IP mobility is enabled by default). When IP mobility is enabled in a virtual AP profile, the ESSID that is configured for the virtual AP supports layer-3 mobility. If you disable IP mobility for a virtual AP, any clients that associate to the virtual AP will not have mobility service.

Advanced Services > IP Mobility

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

Select **Add** to create a new **IP Mobility** profile, or click the pencil icon next to an existing profile to modify settings on an existing profile. The **Advanced Services > IP Mobility Profile Details** page contains the following fields, as described in [Table 78](#):

Table 78 *Advanced Services > IP Mobility, Add/Edit Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
Mobility Domains		
Mobility Domains	None selected	This section displays all domains that are available for association with this IP mobility profile. You can show all, or show only selected domains. Select one or more mobility domains to associate with this IP Mobility profile.
Foreign Agent		
Registration Lifetime Requested by Proxy (10-65,534 sec)	180	Specify the client registration time on the foreign network. A foreign agent receives traffic that is intercepted by the home agent on the home network, and forwards to the client on the foreign network. This setting defines the registration time of a client on the foreign network.
Maximum Number of Active Visitors (0-5000)	5000	Set the maximum number of users to be supported by the foreign network.
Maximum Number of Requests Retransmits (0-5)	3	Set the maximum number of times that a retransmit is to be supported on the foreign network by proxy.
Retransmit Interval (100-10000 msec)	1000	Set the foreign agent retransmit time in milliseconds. The retransmit interval defines retransmission between the home agent and the foreign agent.

Table 78 Advanced Services > IP Mobility, Add/Edit Field Descriptions (Continued)

Field	Default	Description
Home Agent		
Replay Protection Time Value (0-300 sec)	7	Define the time period over which message replay is to be detected. Message replay detects if a message that is intended for a client has been intercepted and replayed. This setting defines how long replay detection is to monitor for replay.
Maximum Number of Active Bindings (0-5000)	5000	Define the maximum number of bindings in which the home agent network is to support a client when the client is out of range of the network, or otherwise disconnected.
Proxy Mobile IP		
Trigger Mobility on Station Association	Yes	Enable this setting to trigger client mobility processing on the network once a client has associated to the network in mobile fashion. The proxy mobile IP module in a mobility-enabled switch detects when a mobile client has moved to a foreign network and determines the home agent for a roaming client. The proxy mobile IP module performs the following functions: <ul style="list-style-type: none"> Derives the address of the home agent for a mobile client from the HAT using the mobile client's IP address. If there is more than one possible home agent for a mobile client in the HAT, the proxy mobile IP module uses a discovery mechanism to find the current home agent for the client. Detects when a mobile client has moved. Client moves are detected based on ingress port and VLAN changes and mobility is triggered accordingly. For faster roaming convergence between AP(s) on the same switch, it is recommended that you keep the "on station association" option enabled. This helps trigger mobility as soon as 802.11 association packets are received from the mobile client.
Enable Support for Standalone APs	No	Select this option to support standalone APs on the IP Mobility domain.
Log User Moves	Yes	Enable this option to log client movement in the IP Mobility domain. This setting is derived from station association in a foreign network.
Allow Roaming for Authenticated Stations Only	Yes	Enable this setting to require authentication for roaming stations.
Filter out DHCP Release from Stations	No	Enable or disable the filtering of DHCP information when a client is released from a station.
Re-home Idle Voice Capable Client	No	Enable or disable re-homing for idle voice-capable clients. This setting reassigns the home network in relation to a voice-capable client that is idle (non-roaming).
Maximum Number of Station Mobility Events Per Second (1-65535)	10	Set the maximum number of events, per second, that station mobility events can be supported.
Maximum Interval Mobility Will Hold Inactive Host Trail (120-3600 sec)	600	Define how long inactive host trails are to be supported in IP mobility.
Maximum Entries in User Mobility Trail (1-30)	10	Define how many events are to be logged in IP mobility.
Mobility Host Entry Hold Time After Connectivity Loss (30-3600 sec)	60	Define how long IP mobility is to support hosts should there be a disconnection.

Table 78 Advanced Services > IP Mobility, Add/Edit Field Descriptions (Continued)

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

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

Advanced Services > IP Mobility > Mobility Domain

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

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

It is recommended that you configure the switch IP address to match the AP's local switch or define the Virtual Router Redundancy Protocol (VRRP) IP address to match the VRRP IP used for switch 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 switch.

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 switch in the mobility domain providing service for the same user VLAN, you must configure an entry for the VLAN for each switch. It is best to use the same VRRP IP used by the AP.

The mobility domain named “default” is the default active domain for all switches. If you need only one mobility domain, you can use this default domain. However, you also have the flexibility to create one or more user-defined domains to meet the unique needs of your network topology. Once you assign a switch to a user-defined domain, it automatically leaves the “default” mobility domain. If you want a switch 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 switch.

Navigate to **Advanced Services > IP Mobility > Mobility Domain** from the **Alcatel-Lucent Configuration** navigation pane. This page displays all currently configured IP Mobility domains. Select **Add** to create a new **IP Mobility Domain**, or click the pencil icon next to an existing profile to modify an existing domain. The **Advanced Services > IP Mobility > Add/Edit IP Mobility Domain** page contains the following fields, as described in [Table 79](#):

Table 79 *Advanced Services > IP Mobility > Add/Edit IP Mobility Domain Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the domain is associated. The drop-down menu displays all folders available for association with the domain.
Name	Blank	Enter the name of the domain.
Other Settings		
Active	No	Define whether the IP Mobility Domain is active or inactive.
Description		Add a description for the domain (requires AOS-W 6.0.0.0 or later)
Mobile IP Home Agents		
Add		Use this button to create new home agents. Once you click Add , the following additional fields appear in the Mobile IP Home Agent section. Complete these settings. <ul style="list-style-type: none"> • Subnet—Define the subnet mask for the IP Mobility Domain. • Netmask—Define the net mas for the IP Mobility Domain. • VLAN ID (1-4094)—Set the VLAN to be supported on the IP Mobility Domain. • Home Agent—Set the home agent for the IP Mobility Domain. When you enable IP mobility in a mobility domain, the proxy mobile IP module determines the home agent for a roaming client. Select Add to create the home agent.

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

Advanced Services > VPN Services

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

You can configure the switch 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 switch supports the following remote access VPN protocols:

- Layer-2 Tunneling Protocol over IPsec (L2TP/IPsec)
- Point-to-Point Tunneling Protocol (PPTP)
- Site-to-site VPNs allow networks such as a branch office network to connect to other networks such as a corporate network. Unlike a remote access VPN, hosts in a site-to-site VPN do not run VPN client software. All traffic for the other network is sent and received through a VPN gateway that encapsulates and encrypts the traffic.

Before enabling VPN authentication, you must configure the following:

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

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

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

Select the **Add** button to add a new VPN Service profile, or click the pencil icon next to an existing profile to change its configuration. The **VPN Services** detail page appears, with settings defined in [Table 80](#).

Table 80 *Advanced Services > VPN Services > Add/Edit VPN Service Profiles* Field Descriptions

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the VPN service profile is associated. The drop-down menu displays all folders available for association with the VPN services profile.
Name	Blank	Enter the name of the VPN services profile.
Other Settings		
IKE Profile		Select an IKE profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing IKE profile. For additional information, refer to “Advanced Services > VPN Services > IKE” on page 161.
PPTP Profile		Select a PPTK profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing PPTP profile. For additional information, refer to “Advanced Services > VPN Services > L2TP” on page 163.
L2TP Profile		Select an L2TP profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing L2TP profile. For additional information, refer to “Advanced Services > VPN Services > L2TP” on page 163.
IPSEC Profile		Select an IPSEC profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing IPSEC profile. For additional information, refer to “Advanced Services > VPN Services > IPSEC” on page 164.

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

Advanced Services > VPN Services > IKE

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



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

Select **Add** to create a new IKE profile, or click the pencil icon next to an existing profile to edit. [Table 81](#) describes the fields on the **Advanced Services > VPN Services > IKE Add/Edit Detail** page.

Table 81 *Advanced Services > VPN Services > IKE Add/Edit Detail Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the IKE profile is associated. The drop-down menu displays all folders available for association with the IKE services profile.
Name	Blank	Enter the name of the IKE profile.
Other Settings		
IKE Aggressive Group Name		Enter the authentication group name for aggressive mode. Make sure that the group name matches the group name configured in the VPN client software. Aggressive Mode condenses the IKE SA negotiations into three packets (versus six packets for Main Mode). A group associates the same set of attributes to multiple clients.
Enable IKE RAP PSKL Refresh/Caching	No	Use this setting to enable refresh and caching for IKE on remote APs.
IKE Shared Secrets		
Add		Select this button to add an IKE shared secret. The following settings appear. Complete these settings and click Add in this section. <ul style="list-style-type: none"> Subnet—Enter the subnet for the shared secret. Subnet Mask—Enter the subnet mask for the shared secret. IKE Shared Secret—Type the shared secret, and confirm.

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

Advanced Services > VPN Services > IKE > IKE Policy

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

Table 82 *Advanced Services > VPN Services > IKE > IKE Policy*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the IKE policy profile is associated. The drop-down menu displays all folders available for association with the IKE Policy profile.
Priority	Blank	Enter the priority number of this IKE policy.
Other Settings		
Encryption		From the drop-down menu, select the encryption type to be supported in the IKE policy. <ul style="list-style-type: none"> • DES • 3DES • AES128 • AES192 • AES256
Hash Algorithm		Select the hash algorithm for this IKE policy. <ul style="list-style-type: none"> • MD5 • SHA • SHA1-96 • SHA2-256-128 • SHA2-384-192 <p>NOTE: 'SHA2-256-128' and 'SHA2-384-192' require an Advanced Cryptography license and a minimum version of 6.1.0.0.</p>
Authentication		AOS-W VPNs support client authentication using pre-shared keys, RSA digital certificates, or Elliptic Curve Digital Signature Algorithm (ECDSA) certificates. To set the authentication type for the IKE rule, click the Authentication drop-down list and select one of the following types: <ul style="list-style-type: none"> • Pre-Share (for IKEv1 clients using pre-shared keys) • RSA (for clients using certificates) • ECDSA-256 (for clients using certificates) • ECDSA-384 (for clients using certificates) <p>NOTE: 'ECDSA-256' and 'ECDSA-384' require an Advanced Cryptography license and a minimum version of 6.1.0.0.</p>
Diffie-Hellman Group		Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie Hellman Group for the ISAKMP policy, click the Diffie Hellman Group drop-down list and select one of the following groups: <ul style="list-style-type: none"> • Group 1: 768-bit Diffie Hellman prime modulus group. • Group 2: 1024-bit Diffie Hellman prime modulus group. • Group 19: 256-bit random Diffie Hellman ECP modulus group. • Group 20: 384-bit random Diffie Hellman ECP modulus group. <p>NOTE: 'EC 256-bit (19)' and 'EC 384-bit (20)' require an Advanced Cryptography license and a minimum version of 6.1.0.0.</p>
Lifetime	empty	Set the Security Association Lifetime to define the lifetime of the security association, in seconds.
Version	1	Select 1 to configure the VPN for IKEv1, or 2 for IKEv2.

Advanced Services > VPN Services > L2TP

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

L2TP/IPSec requires two levels of authentication:

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

Navigate to **Advanced Services > VPN Services > L2TP** page from the **Alcatel-Lucent Configuration** navigation pane. This page lists all L2TP profiles that are currently available. Select **Add** to create a new **L2TP** profile, or click the pencil icon next to an existing profile to modify settings. The **Advanced Services > VPN Services > L2TP Add/Edit Details** page contains the following fields, as described in [Table 83](#).

Table 83 *Advanced Services > VPN Services > L2TP Add/Edit Details Field Descriptions*

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

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

Advanced Services > VPN Services > PPTP

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

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

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

The **Advanced Services > VPN Services > PPTP Add/Edit Details** page contains the following fields, as described in [Table 84](#):

Table 84 *Advanced Services > VPN Services > PPTP Add/Edit Details Field Descriptions*

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

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

Advanced Services > VPN Services > IPSEC

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

authentication process is encrypted using the Data Encryption Standard (DES) or Triple DES (3DES) algorithm.

L2TP/IPSec requires two levels of authentication:

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

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

Select **Add** to create a new **IPSEC** profile, or click the pencil icon next to an existing profile to modify settings. The **Add/Edit Details** page contains the following fields, as described in [Table 85](#):

Table 85 *Advanced Services > VPN Services > IPSEC Add/Edit Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the IPSEC profile is associated. The drop-down menu displays all folders available for association with the IPSEC profile.
Name	Blank	Enter the name of the IPSEC profile.
Other Settings		
Maximum MTU Size (1034-1500 bytes)	1500	Define the Maximum transmission unit (MTU) size in bytes.
Dynamic Maps		
Dynamic Maps		Select one or more dynamic maps that the IPSEC profile is to reference. You can add or edit dynamic maps as required. For additional information, refer to “Advanced Services > VPN Services > IPSEC > Dynamic Map” on page 165.

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

Advanced Services > VPN Services > IPSEC > Dynamic Map

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

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

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

Select **Add** to create a new **Dynamic Map**, or click the pencil icon next to an existing map to modify settings. The **Add/Edit Details** page contains the fields as described in [Table 86](#):

Table 86 *Advanced Services > VPN Services > IPSEC > Dynamic Map Add/Edit Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the Dynamic Map is associated. The drop-down menu displays all folders available for association with the Dynamic Map.
Name	Blank	Enter the name of the Dynamic Map.
Other Settings		
Priority		Specify the priority in which this Dynamic Map should be processed in relation to additional Dynamic Maps that may be configured and used by IPSEC profiles.
Diffie-Hellman Group		Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie Hellman Group for the ISAKMP policy, click the Diffie Hellman Group drop-down list and select one of the following groups: <ul style="list-style-type: none"> Group 1: 768-bit Diffie Hellman prime modulus group. Group 2: 1024-bit Diffie Hellman prime modulus group. Group 19: 256-bit random Diffie Hellman ECP modulus group. Group 20: 384-bit random Diffie Hellman ECP modulus group. NOTE: 'EC 256-bit (19)' and 'EC 384-bit (20)' require an Advanced Cryptography license and a minimum version of 6.1.0.0.
Lifetime (300-86400 sec)		Define the lifetime in seconds for the dynamic map, when deployed in IPSEC profiles.
Transform Set 1-4		From the drop-down menu, select up to four transform sets in the sequence in which they should be referenced by the Dynamic Map. You can add a new Transform Set by clicking the add icon, or you can edit an existing Transform Set by clicking the pencil icon. For additional information, refer to "Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set" on page 166.
Version	1	Select 1 to configure the VPN for IKEv1, or 2 for IKEv2.

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

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

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

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

Select **Add** to create a new **Transform Set**, or click the pencil icon next to an existing Transform Set to modify settings. The **Add/Edit Details** page contains the following fields, as described in [Table 87](#):

Table 87 *Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set Add/Edit Details Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Set the folder with which the Transform Set is associated. The drop-down menu displays all folders available for association with the Transform Set.
Name	Blank	Enter the name of the Transform Set.
Other Settings		
Encryption	168-bit 3DES-CBC	Select the encryption for the transform set from the drop-down menu.
Hash Algorithm	SHA (HMAC Variant)	Select the hash algorithm from the drop-down menu.

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

Groups > Alcatel-Lucent Config Page and Section Information

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

1. Navigate to the **Groups > List** page.
2. Select the name of the Alcatel-Lucent AP Group to view and edit, and navigate to the **Alcatel-Lucent Config** page, illustrated in [Figure 7](#):

Figure 7 Groups > List > Alcatel-Lucent Config Page Illustration for an Alcatel-Lucent AP Group

The screenshot displays the configuration page for an Alcatel-Lucent AP Group, organized into several sections:

- Alcatel-Lucent AP Groups:** A section for selecting Aruba AP Groups to apply to devices. It includes a 'Show All' link, a checked checkbox for 'default', and 'Select All - Unselect All' options.
- AP Overrides:** A section for selecting AP Overrides to apply to devices. It includes a 'Show Only Selected' link, a checked checkbox for '10.10.6', and 'Select All - Unselect All' options.
- Additional Alcatel-Lucent Profiles:** A list of profiles with dropdown menus and edit/delete icons. Profiles include: Stateful 802.1X Authentication Profile, VPN Authentication Profile, Management Authentication Profile, Wired Authentication Profile, Internal Server Profile, TACACS Accounting Profile, IP Mobility Profile, VPN Services Profile, Management Password Policy Profile, Control Plane Security Profile, and Configure Campus AP Whitelist (with Yes/No radio buttons).
- Alcatel-Lucent User Roles:** A section for selecting additional roles to apply to devices. It includes a 'Show All' link, checked checkboxes for 'ap-role', 'stateful-dot1x', 'sys-ap-role', and 'trusted-ap', and 'Select All - Unselect All' options.
- Alcatel-Lucent Policies:** A section for selecting additional policies to apply to devices. It includes a 'Show All' link, checked checkboxes for 'stateful-dot1x', 'sys-ap-acl', 'sys-control', and 'validuser', and 'Select All - Unselect All' options.

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

3. Complete the profile assignments on this page, referring to additional topics in this appendix for additional information. [Table 88](#) provides a summary of topics supporting these settings.

Table 88 Information Resources for the Groups > List > Alcatel-Lucent 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 36 • “General 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 40 • “AP Overrides Guidelines” on page 30
Alcatel-Lucent User Roles	<ul style="list-style-type: none"> • “Security > User Roles” on page 132 • “Visibility in Alcatel-Lucent Configuration” on page 33
Alcatel-Lucent Policies	<ul style="list-style-type: none"> • “Security > Policies” on page 138 • “Visibility in Alcatel-Lucent Configuration” on page 33

A		
Adaptive Radio Management (ARM)	32	
Advanced Services		
defined	17	
pages and field descriptions	155	
Advanced Services > IP Mobility	158	
Advanced Services > IP Mobility > Mobility Domain	160	
Advanced Services > IP Mobility page	158	
Advanced Services > VPN Services	161	
Advanced Services > VPN Services > IKE	163	
Advanced Services > VPN Services > IPSEC	166	
Advanced Services > VPN Services > IPSEC > Dynamic Map	167	
Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set	168	
Advanced Services > VPN Services > L2TP	165	
Advanced Services > VPN Services > PPTP	165	
AP Overrides	42	
guidelines	32	
pages and field descriptions	42	
APs		
deploying with OV3600 for the first time	33	
using in groups and folders	34	
APs/Devices > List	12	
APs/Devices > Manage	18	
APs/Devices > Monitor	19	
Alcatel-Lucent AP Groups		
general procedures and guidelines	29	
Alcatel-Lucent APs	33	
Alcatel-Lucent Configuration		
Advanced Services	17	
Folders, Users, and Visibility	21	
initial setup	22	
initial setup procedure	22	
navigating	10	
prerequisites	22	
Profiles	16	
Security	16	
WLANs	15	
D		
device groups		
using with APs	34	
Device Setup > Alcatel-Lucent Configuration	11	
E		
Encryption	32	
F		
folders		
using with APs	34	
G		
groups		
using with APs	34	
Groups > Basic	19	
I		
IP Mobility Domains	157	
P		
Profiles		
defined	16	
embedded configuration	20	
overview	52	
pages and field descriptions	52	
Profiles > AAA	52	
Profiles > AAA > 802.1x Auth	60	
Profiles > AAA > Captive Portal Auth	61	
Profiles > AAA > Mac Auth	63, 64	
Profiles > AAA > Management Auth	67	
Profiles > AAA > Stateful 802.1X Auth	65	
Profiles > AAA > Stateful NTLM Auth	68	
Profiles > AAA > VPN Auth	66	
Profiles > AAA > Wired Auth Profile	66	
Profiles > AAA > WISPr Auth	69	
Profiles > AP	70	
Profiles > AP > AP Ethernet Link	75	
Profiles > AP > AP Wired	76	
Profiles > AP > Regulatory Domain	74	
Profiles > AP > SNMP	75	
Profiles > AP > SNMP > SNMP User	76	
Profiles > AP > System	75, 76	
Profiles > IDS	82	
Profiles > IDS > Denial of Service	87	
Profiles > IDS > Denial of Service > Rate Threshold	90	
Profiles > IDS > General	84	
Profiles > IDS > Impersonation	91	
Profiles > IDS > Signature Matching	85	
Profiles > IDS > Signature Matching > Signatures	86	
Profiles > IDS > Unauthorized Device	92	
Profiles > Mesh	95	
Profiles > Mesh > Cluster	100	
Profiles > Mesh > Radio	96	
Profiles > Mesh > Radio > Mesh HT SSID	99	
Profiles > QoS	100	
Profiles > QoS > Traffic Management	101	
Profiles > QoS > VoIP Call Admission Control	101	
Profiles > QoS > WMM Traffic Management	103	
Profiles > RF	104	
Profiles > RF > 802.11a/g Radio	105	
Profiles > RF > 802.11a/g Radio > ARM	110	
Profiles > RF > 802.11a/g Radio > High-Throughput (HT) Radio	113	
Profiles > RF > Event Thresholds	115	
Profiles > RF > Optimization Profiles	117	
Profiles > SSID	119	
Profiles > SSID > 802.11K	131	
Profiles > SSID > EDCA AP	124	
Profiles > SSID > EDCA Station	127	
Profiles > SSID > HT SSID	130	
S		
Save, Save and Apply, and Revert buttons	21	
Security		
defined	16	
pages and field descriptions	133	
Security > Policies	140	
Security > Policies > Destinations	142	
Security > Policies > Services	142	
Security > Server Groups	143	
Security > Server Groups > Internal	149	
Security > Server Groups > LDAP	146	
Security > Server Groups > RADIUS	147	
Security > Server Groups > RFC 3576	150	

Security > Server Groups > TACACS	148
Security > Server Groups > Windows	151
Security > Server Groups > XML API	150
Security > TACACS Accounting	151
Security > Time Ranges	152
Security > User Roles	134
Security > User Roles > BW Contracts	136
Security > User Roles > VPN Dialers	137
Security > User Rules	153
SSIDs	14, 15, 24, 32, 40, 47, 48, 49, 119, 130

W

WLANs	47
defined	15
pages and field descriptions	47
WLANs > Advanced	48
WLANs > Basic	48

