AirWave Wireless Management Suite

airwave®

Configuration Guide

Copyright

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent a commitment on the part of AirWave Wireless.

AirWave Wireless is not connected, affiliated or related to Airwave O2 Limited in any manner.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS. Altering this device (such as painting it) voids the warranty.

ARUBA®
networks

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Preface

Document Audience and Organization

This configuration guide is intended for wireless network administrators and helpdesk personnel who deploy ArubaOS (AOS) on the network and wish to manage it with the AirWave Wireless Management Suite (AWMS). AWMS Versions 6.3 and later support Aruba Configuration. This document provides instructions for using Aruba Configuration and contains the following chapters:

Table 1 *Document Organization and Purposes*

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

Related Documents

The following documentation supports the AirWave Wireless Management Suite:

ArubaOS Documentation

- AOS User Guide

AirWave Wireless Management Suite / AirWave Management Platform

- Release Notes for the AirWave Wireless Management Suite
- AirWave Wireless Management Suite Knowledge Base
- AWMS Quick Start Guide
- AWMS User Guide
- Aruba Configuration Guide (this document)
- Supported APs/Devices
- Supported Firmware Versions

VisualRF

- Release Notes for the AirWave Wireless VisualRF Module
- Overview Page
- User Guide

RAPIDS

- Overview Page
- AirWave Management Client User Guide
- Download AirWave Management Client

Best Practice Guides

- Aruba and AirWave Best Practices Guide
- Choosing the Right Server Hardware
- Helpdesk Guide: Troubleshooting WLAN Issues
- Converting Cisco IOS APs to LWAPP

Interfacing With AWMS

- AWMS Integration Matrix
- State and Statistical XML API Documentation
- Location XML API Documentation

NMS Integration

- See AMP Setup NMS
- Download AWMS Trap MIB
- AWMS/NMS Integration Guide

AMPWatch Widget

- AMPWatch is a widget for the Yahoo! Widget Engine
- Download AMPWatch

Text Conventions

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

Table 2 *Text Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
GUI components	**Bold, sans-serif font** indicates that the AWMS GUI displays this item exactly as cited in body text.
`System items`	This fixed-width font depicts the following: ● Sample screen output ● System prompts ● Filenames, software devices, and specific commands when mentioned in the text
`Commands`	In the command examples, this bold font depicts text that you must type exactly as shown.

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

NOTE

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

CAUTION

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

Contacting AirWave Wireless and Aruba Networks

Online Contact and Support	
Main Website	http://www.airwave.com
Email Contact	
● AirWave Wireless Sales	sales@airwave.com
● AirWave Wireless Technical Support	support@airwave.com
● Aruba Networks general information	info@arubanetworks.com
● Aruba Networks Sales	sales@arubanetworks.com
● Aruba Networks Technical Support in the Americas and APAC	support@arubanetworks.com
● Aruba Networks Technical Support in the EMEA	emea_support@arubanetworks.com
● WSIRT Email—Please email details of any security problem found in an AirWave or Aruba product.	wsirt@arubanetworks.com

Telephone Contact and Support	
AirWave Wireless Corporate Headquarters	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
● United States	800-WI-FI-LAN (800-943-4526)
● Universal Free Phone Service Number (UIFN): Australia, Canada, China, France, Germany, Hong Kong, Ireland, Israel, Japan, Korea, Singapore, South Africa, Taiwan, and the UK.	+800-4WIFI-LAN (+800-49434-526)
● All Other Countries	+1 (408) 754-1200

Chapter 1

Aruba Configuration in AWMS

Introduction

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

The Aruba Configuration feature in the AirWave Wireless Management Suite consolidates AOS configuration and pushes global Aruba configurations from one utility. This chapter introduces the components and initial setup of Aruba Configuration with the following topics:

NOTE

AWMS supports ***Aruba AP Groups,*** and these are distinct and must not be confused with standard AWMS Device ***Groups***. This document provides information about the configuration and use of ***Aruba AP Groups***, and describes how ***Aruba AP Groups*** interoperate with standard AWMS Device ***Groups***.

Requirements, Restrictions, and AOS Support in AWMS

Requirements

Aruba Configuration has the following ***requirements*** in AWMS:

- AWMS 6.3 or a later AWMS version must be installed and operational on the network.
- Aruba Controllers on the network must have AOS installed and operational.
- Ensure you have Telnet/SSH credentials (configuration only) and the “enable” password (configuration only). Without proper Telnet/SSH credentials a user is not able to fetch the running configuration, nor acquire license and serial information from controllers.

Restrictions

Aruba Configuration has the following ***restrictions*** in AWMS:

- At the present time, Aruba Configuration in AWMS does not support every AOS Network component. AWMS supports only **IP Mobility** and **VLANs** in the **Advanced Services** section, for example.
- Future versions of AWMS will support additional AOS features, to include **Aruba AP Group** and **Profile** distribution from the Master Console.

AOS Support in AWMS

NOTE

Refer also to “Using AWMS to Deploy Aruba APs for the First Time” on page 39.

AWMS users can choose between the existing template-based configuration and new GUI-based configuration for Aruba devices on firmware 3.3.2.10 and greater. Upon upgrading to AWMS, groups with all devices in monitor-only mode will automatically use the GUI-based configuration.

- Only global configuration is supported; AWMS can work in a master-local or an all-master configuration.
- Configuration changes are pushed to the controller via SSH with no reboot required.
- All settings for Profiles, Aruba AP Groups, Servers and Roles are supported, as is the AOS WLAN Wizard (basic view). Controller IP addresses, VLANs and interfaces are not supported, nor are Advanced Services with the exception of VPN and IP Mobility.
- AWMS now understands AOS license dependencies.
- You can provision thin APs from the **AP/Devices > Manage** page. You can move APs into **Aruba AP Groups** from the **Modify These Devices** option on the **APs/Devices > List** page.
- You can configure AP names as **AP Overrides** on the **Device Setup > Aruba Configuration** page.
- Support for AOS GUI configuration via global groups and the AWMS Master Console will be added in a future release.

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

For more detailed information about this feature, as well as steps for 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 version supported by each release, refer to the *AWMS Release Notes*.

Overview of Aruba Configuration in AWMS

This section describes the **Device Setup > Aruba Configuration** page and all additional pages in AWMS that support Aruba Configuration.

The Primary Pages of Aruba Configuration

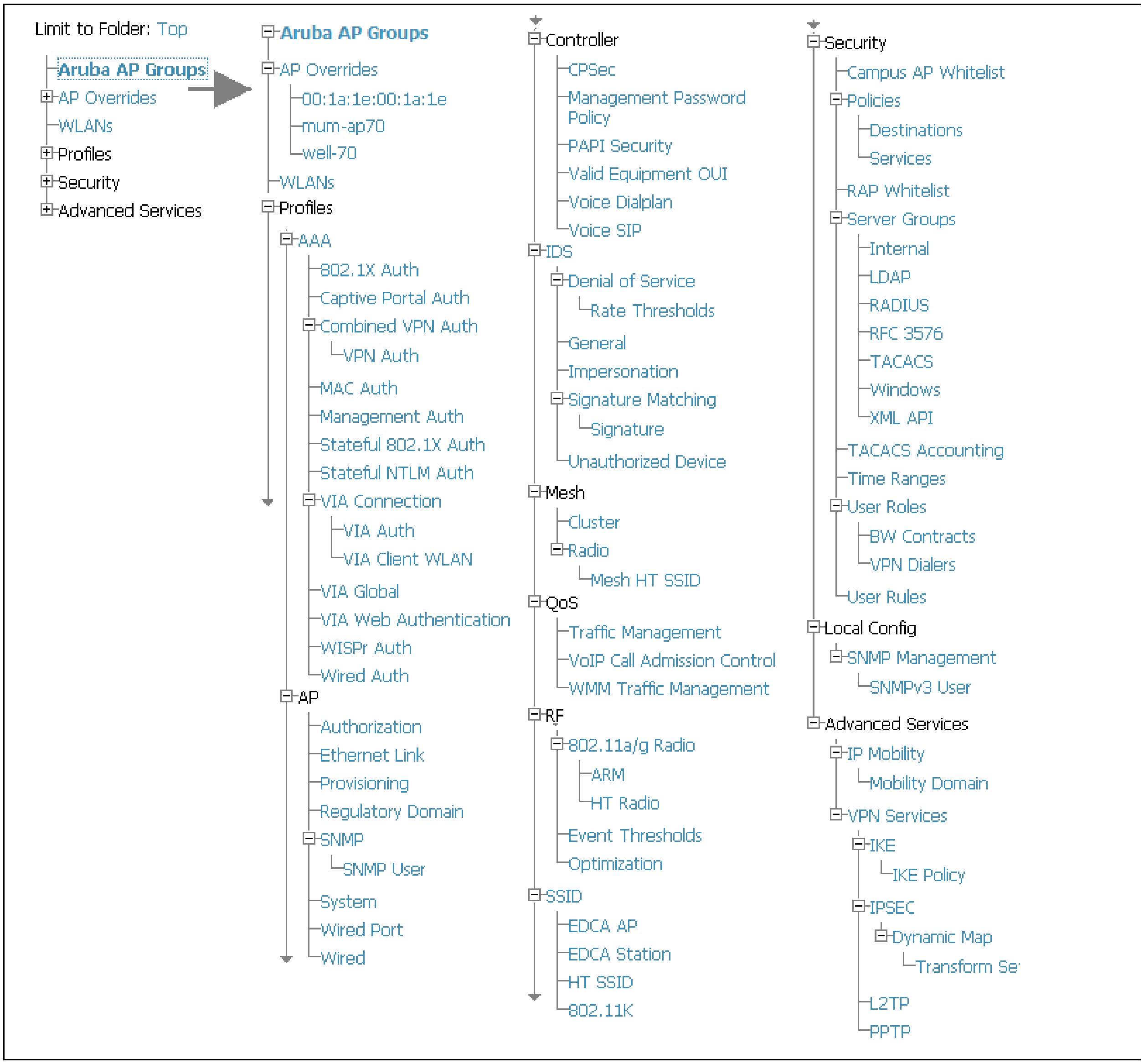
AWMS supports Aruba Configuration with the following pages:

- Device Setup > Aruba Configuration Page—deploys and maintains Aruba Configuration in AWMS. This page supports several sections, as follows:
  - Aruba AP Groups Section
  - AP Overrides Section
  - WLANs Section
  - Profiles Section
  - Security Section
  - Advanced Services Section
- Groups > Aruba Config Page—manages Aruba AP group and other controller-wide settings defined on the **Device Setup > Aruba Configuration** page.
- APs/Devices > List Page—modifies or reboots all devices, including Aruba devices deployed with Aruba Configuration.
- APs/Devices > Manage Page—supports device-level settings and changes in AWMS as a whole.
- APs/Devices > Monitor Page—supports device-level monitoring in AWMS as a whole.
- Groups > Basic Page—enables Aruba Configuration in the AWMS GUI and displays preferences for Aruba and other devices.

Device Setup > Aruba Configuration Page

This page, shown in Figure 1, uses an expandable navigation pane to support Aruba AP Groups, AP Overrides, WLANs, Profiles, Security, and Advanced Services.

Figure 1 ***Device Setup* > *Aruba Configuration*** *Navigation Pane (Contracted and Expanded)*



NOTE

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

The navigation pane can be used as follows:

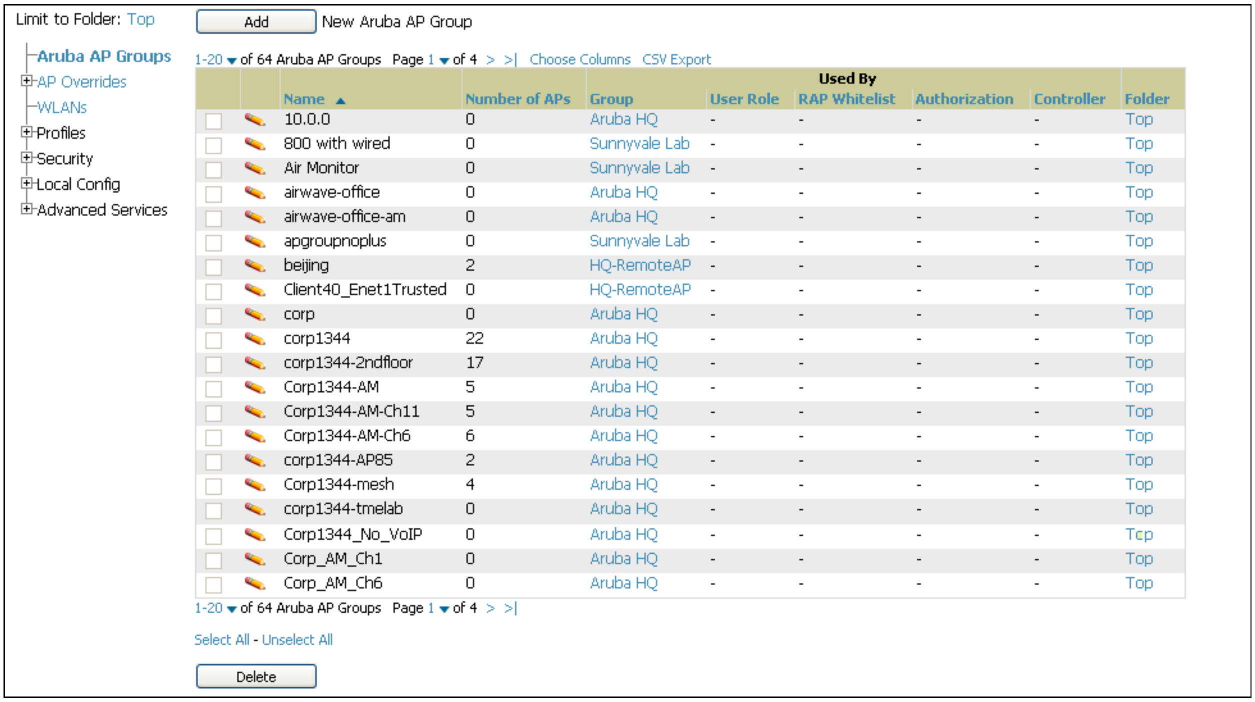
- Any portion with a plus sign (**+**) expands with a click to display additional contents.
- Any portion of the navigation tree can be contracted by clicking the contract sign (**-**).
- You can display the **Edit** or **Details** page for any component with a single click.

Aruba AP Groups Section

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

Navigate to the **Device Setup > Aruba Configuration > Aruba AP Groups** page. Figure 2 illustrates one example of this page.

Figure 2 *Device Setup* > *Aruba Configuration* > *Aruba AP Groups* Navigation



1-20 ▾ of 64 Aruba AP Groups Page 1 ▾ of 4 > >| Choose Columns CSV Export

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

1-20 ▾ of 64 Aruba AP Groups Page 1 ▾ of 4 > >|

Select All - Unselect All

Delete

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

Aruba AP Groups have the following characteristics:

- Aruba AP Groups are global, and any Aruba controller can support multiple Aruba AP Groups.
- Aruba AP Groups are assigned to folders, and folders define visibility. Using conventional AWMS folders to define visibility, Aruba 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 Aruba Configuration" on page 41.
- You can import a controller configuration file from ArubaOS for Aruba AP Group deployment in AWMS.

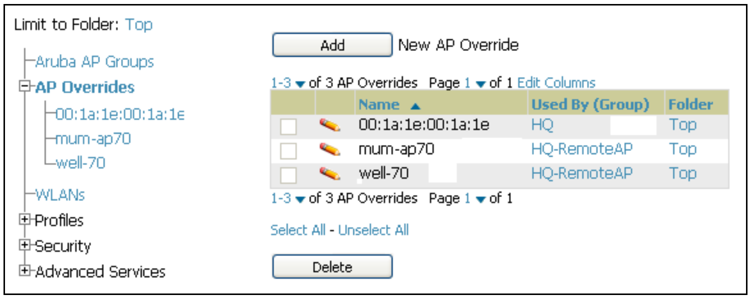
For additional information, refer to the following sections in this document:

- "Setting Up Initial Aruba Configuration" on page 24
- "General Aruba AP Groups Procedures and Guidelines" on page 30

AP Overrides Section

The second major component of Aruba Configuration is the **AP Overrides** page, appearing immediately below **Aruba AP Groups** in the Navigation Pane. Figure 3 illustrates this location and access:

Figure 3 *Device Setup* > *Aruba Configuration* > *AP Overrides* Navigation



1-3 ▾ of 3 AP Overrides Page 1 ▾ of 1 Edit Columns

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

1-3 ▾ of 3 AP Overrides Page 1 ▾ of 1

Select All - Unselect All

Delete

AP Overrides operate as follows in Aruba Configuration:

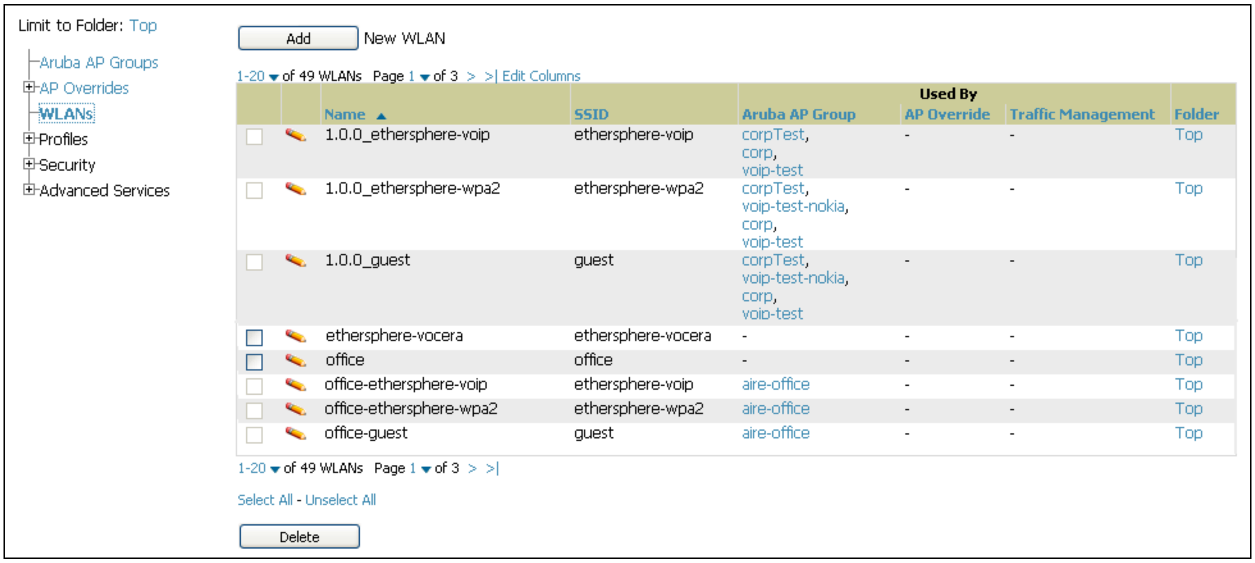
- Custom-created AP Overrides appear in the Aruba Configuration navigation pane, as illustrated in Figure 3.

- Aruba controllers and AP devices operate in Aruba AP Groups that define shared parameters for all devices in those groups. The **Device Setup > Aruba Configuration > Aruba AP Groups** page displays all current Aruba AP groups.
- **AP Override** allows you to change some parameters for any specific device without having to create an Aruba 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 37
  - "Configuring or Editing AP Overrides" on page 37
  - "AP Overrides Pages and Field Descriptions" on page 52

WLANs Section

Access WLANs with **Device Setup > Aruba Configuration > WLANs**, illustrated in Figure 4.

Figure 4 ***Device Setup > Aruba Configuration > WLANs*** *Navigation*


Limit to Folder: Top
Aruba AP Groups
⊞AP Overrides
WLANs
⊞Profiles
⊞Security
⊞Advanced Services
Add
New WLAN
1-20 ▾ of 49 WLANs Page 1 ▾ of 3 > >| Edit Columns
1-20 ▾ of 49 WLANs Page 1 ▾ of 3 > >|
Select All - Unselect All
Delete

				Used By			
		Name ▲	SSID	Aruba AP Group	AP Override	Traffic Management	Folder
☐	✎	1.0.0_ethersphere-voip	ethersphere-voip	corpTest, corp, voip-test	-	-	Top
☐	✎	1.0.0_ethersphere-wpa2	ethersphere-wpa2	corpTest, voip-test-nokia, corp, voip-test	-	-	Top
☐	✎	1.0.0_guest	guest	corpTest, voip-test-nokia, corp, voip-test	-	-	Top
☐	✎	ethersphere-vocera	ethersphere-vocera	-	-	-	Top
☐	✎	office	office	-	-	-	Top
☐	✎	office-ethersphere-voip	ethersphere-voip	aire-office	-	-	Top
☐	✎	office-ethersphere-wpa2	ethersphere-wpa2	aire-office	-	-	Top
☐	✎	office-guest	guest	aire-office	-	-	Top

The following concepts govern the use of WLANs in Aruba Configuration:

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

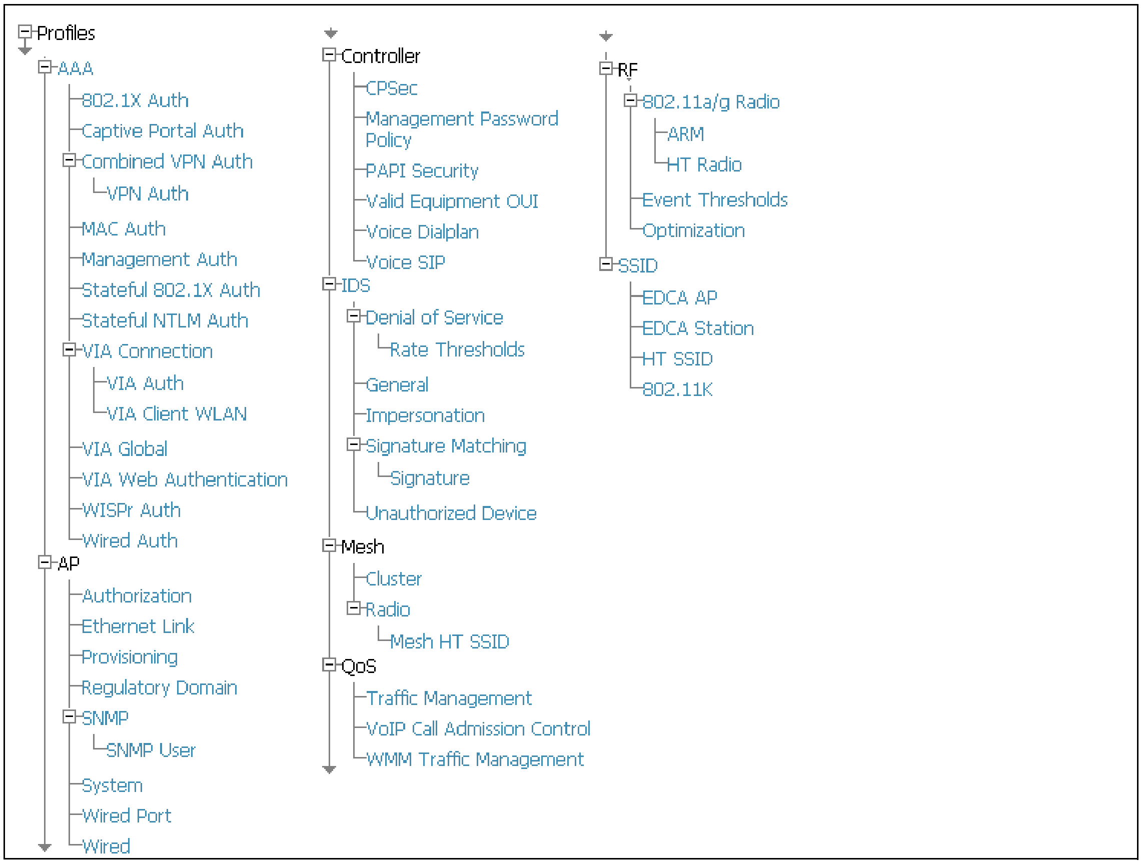
This document describes WLAN configuration in the following section and chapter:

- "Setting Up Initial Aruba Configuration" on page 24
- "General WLAN Procedures and Guidelines" on page 33
- "WLAN Pages and Field Descriptions" on page 56

Profiles Section

Profiles provide a way to organize and deploy groups of configurations for Aruba AP Groups, WLANs, and other profiles. Profiles are assigned to folders; this establishes visibility to Aruba AP Groups and WLAN settings. Access **Profiles** with **Device Setup > Aruba Configuration > Profiles**, illustrated in Figure 5.

Figure 5 ***Device Setup* > *Aruba Configuration* > *Profiles*** *Navigation*



- Profiles
  - AAA
    - 802.1X Auth
    - Captive Portal Auth
    - Combined VPN Auth
      - VPN Auth
    - MAC Auth
    - Management Auth
    - Stateful 802.1X Auth
    - Stateful NTLM Auth
    - VIA Connection
      - VIA Auth
      - VIA Client WLAN
    - VIA Global
    - VIA Web Authentication
    - WISPr Auth
    - Wired Auth
  - AP
    - Authorization
    - Ethernet Link
    - Provisioning
    - Regulatory Domain
    - SNMP
      - SNMP User
    - System
    - Wired Port
    - Wired
  - Controller
    - CPSec
    - Management Password Policy
    - PAPI Security
    - Valid Equipment OUI
    - Voice Dialplan
    - Voice SIP
  - IDS
    - Denial of Service
      - Rate Thresholds
    - General
    - Impersonation
    - Signature Matching
      - Signature
    - Unauthorized Device
  - Mesh
    - Cluster
    - Radio
      - Mesh HT SSID
  - QoS
    - Traffic Management
    - VoIP Call Admission Control
    - WMM Traffic Management
  - RF
    - 802.11a/g Radio
      - ARM
      - HT Radio
    - Event Thresholds
    - Optimization
  - SSID
    - EDCA AP
    - EDCA Station
    - HT SSID
    - 802.11K

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

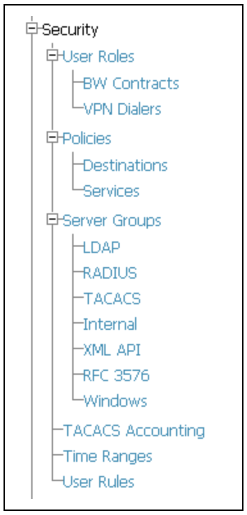
For additional information about profile procedures and guidelines, refer to the following sections in this document:

- "Setting Up Initial Aruba Configuration" on page 24
- "General Profiles Guidelines" on page 35
- "Profiles Pages and Field Descriptions" on page 62

Security Section

The **Security** section displays, adds, edits, or deletes security profiles in multiple categories, to include user roles, policies, rules, and servers such as RADIUS, TACACS+, and LDAP servers. Navigate to Security with the **Device Setup > Aruba Configuration > Security** path, illustrated in Figure 6.

Figure 6 ***Device Setup** > **Aruba Configuration** > **Security** Navigation*



The following general guidelines apply to **Security** profiles in Aruba configuration:

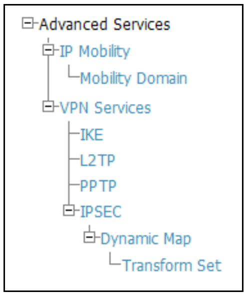
- Roles can have multiple policies; each policy can have numerous roles.
- Server groups are comprised of servers and rules. Security rules apply in Aruba Configuration in the same way as deployed in AOS.

For additional information about Security, refer to "Security Pages and Field Descriptions" on page 138.

Advanced Services Section

Navigate to Advanced Services with the **Device Setup > Aruba Configuration > Advanced Services** path. The **Advanced Services** section includes IP Mobility and VPN Services. Figure 7 illustrates this navigation and the components.

Figure 7 ***Device Setup** > **Aruba Configuration** > **Advanced Services** Navigation*



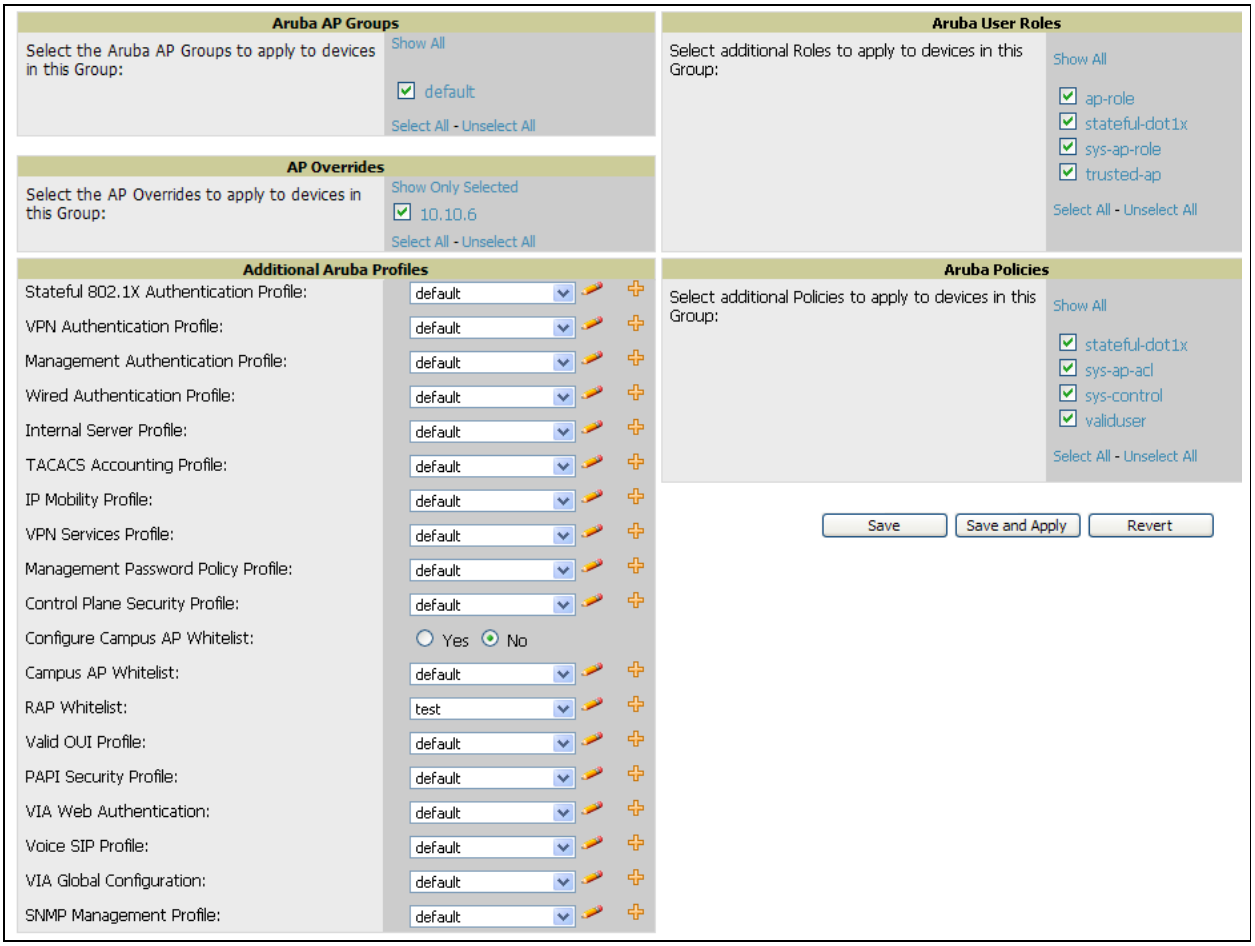
For additional information about IP Mobility and VPN Services, refer to "Advanced Services Pages and Field Descriptions" on page 157.

Groups > Aruba Config Page

This focused submenu page displays and edits all configured Aruba AP groups, with the following factors:

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

Figure 8 ***Groups > Aruba Config*** *Page Illustration*



Aruba AP Groups

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

Show All

☑ default

Select All - Unselect All

AP Overrides

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

Show Only Selected

☑ 10.10.6

Select All - Unselect All

Additional Aruba Profiles

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

Aruba User Roles

Select additional Roles to apply to devices in this Group:

Show All

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

Select All - Unselect All

Aruba Policies

Select additional Policies to apply to devices in this Group:

Show All

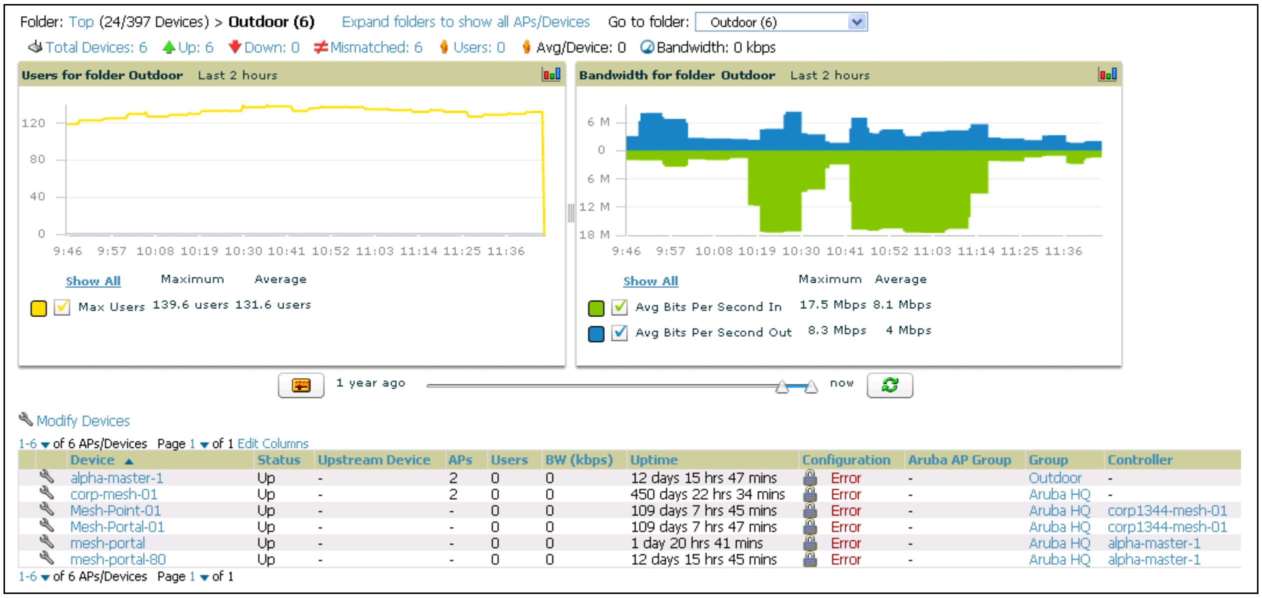
☑ stateful-dot1x
☑ sys-ap-acl
☑ sys-control
☑ validuser

Select All - Unselect All

APs/Devices > List Page

This page supports devices in all of AWMS. This page supports controller reboot, controller re-provisioning, and changing Aruba AP groups. Select **Modify Devices** to configure thin AP settings.

Figure 9 ***APs/Devices List*** *Page Illustration (Partial Display)*



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

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

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

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

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

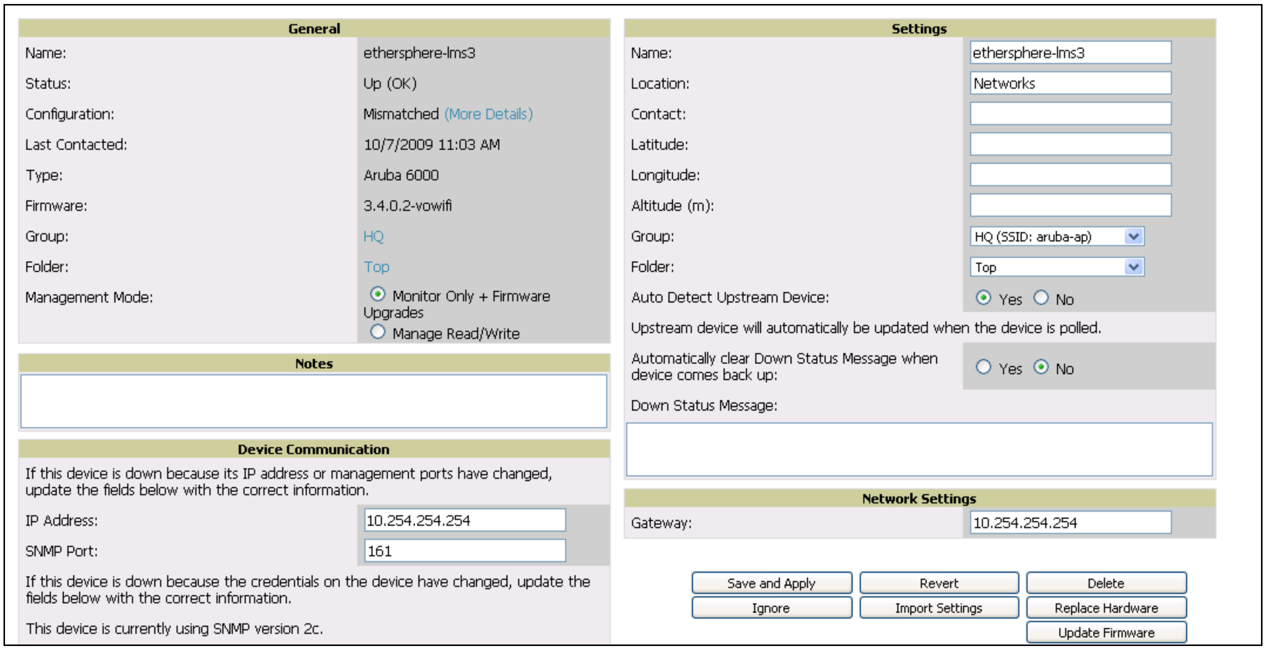
Device ▲	Status	Upstream Device	APs	Users	BW (kbps)	Uptime	Configuration	Aruba AP Group	Group	Controller
alpha-master-1	Up	-	2	0	0	12 days 15 hrs 47 mins	Error	-	Outdoor	-
corp-mesh-01	Up	-	2	0	0	450 days 22 hrs 34 mins	Error	-	Aruba HQ	-
Mesh-Point-01	Up	-	-	0	0	109 days 7 hrs 45 mins	Error	-	Aruba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

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

APs/Devices > Manage Page

This page configures device-level settings, including **Manage** mode that enables pushing configurations to controllers. For additional information, refer to "Pushing Device Configurations to Controllers" on page 36.

Figure 10 ***APs/Devices > Manage*** *Page Illustration (Partial Display)*



General

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

Notes

Device Communication

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

IP Address:	10.254.254.254
SNMP Port:	161

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

This device is currently using SNMP version 2c.

Settings

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

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

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

Down Status Message:

Network Settings

Gateway:	10.254.254.254

APs/Devices > Monitor Page

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

- **Status** information
- **User** and **Bandwidth** flash graphs
- **CPU Utilization** and **Memory Utilization** flash graphs
- **APs Managed by this Controller** (when viewing a controller)

- **Alert Summary**
- **Recent Events**
- **Audit Log**

For additional information, refer to "Pushing Device Configurations to Controllers" on page 36.

Groups > Basic Page

The **Groups > Basic** page deploys the following aspects of Aruba Configuration:

- This page contains a new **Aruba GUI Config** field. Use this page and field to make the **Device Setup > Aruba Config** page visible. This page is enabled by default in AWMS.
- Use this page to control which device settings appear on the **Groups** pages.
- If you are using Aruba firmware prior to version 3.0, you should disable Aruba GUI configuration from the **Groups > Basic** page and use template-based configuration.

Refer to Figure 14 for an illustration of this page.

Additional Concepts and Components of Aruba Configuration

Aruba Configuration emphasizes the following components and network management concepts:

- Global Configuration and Scope
- Embedded Profile Setup in Aruba Configuration
- Controller Overrides
- Save, Save and Apply, and Revert Buttons
- Folders, Users, and Visibility
- Additional Concepts and Benefits

Global Configuration and Scope

Aruba Configuration supports AOS as follows:

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

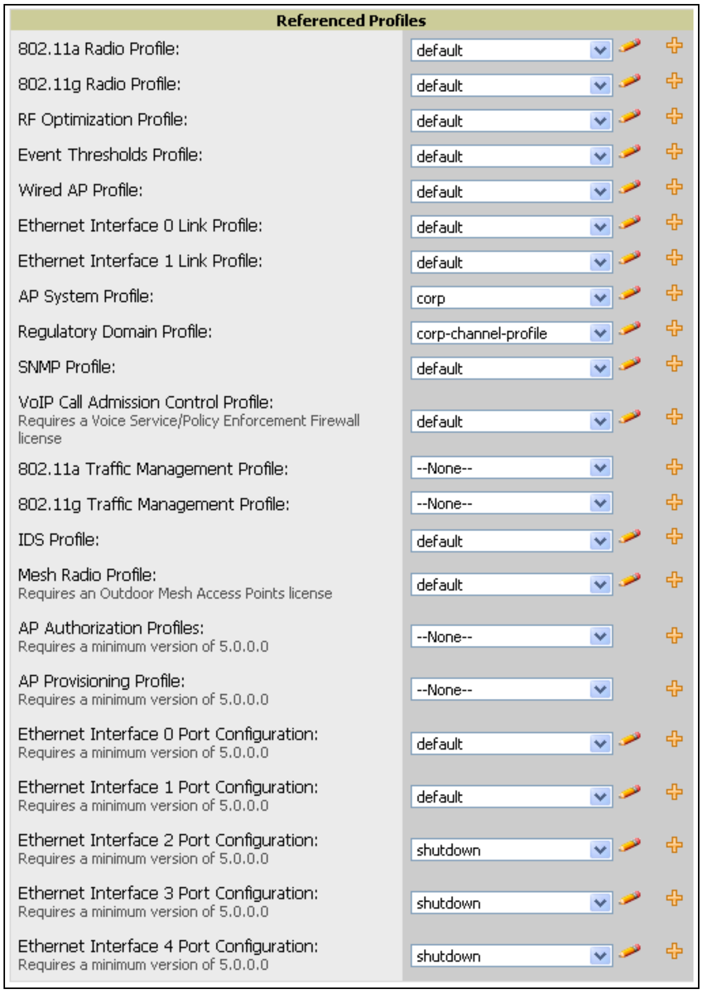
For additional information about these and additional functions, refer to "General Controller Procedures and Guidelines" on page 36.

Embedded Profile Setup in Aruba Configuration

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

- When you create a new Aruba AP Group from the **Device Setup > Aruba Configuration** page, the **Referenced Profile** section appears as shown in Figure 11:

Figure 11 *Embedded Profile Configuration for an Aruba AP Group*



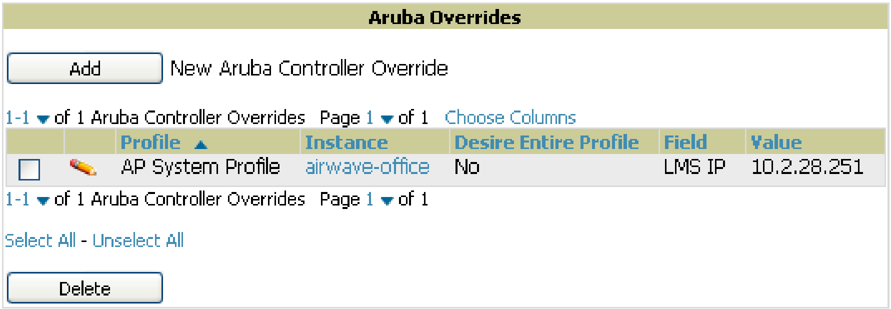
Referenced Profiles	
802.11a Radio Profile:	default
802.11g Radio Profile:	default
RF Optimization Profile:	default
Event Thresholds Profile:	default
Wired AP Profile:	default
Ethernet Interface 0 Link Profile:	default
Ethernet Interface 1 Link Profile:	default
AP System Profile:	corp
Regulatory Domain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

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

Controller Overrides

You can create controller overrides for entire profiles or a specific profile setting per profile. This allows you to avoid creating new profiles or Aruba AP Groups that differ by one more settings. Controller overrides can be added from the controller's Manage page.

Figure 12 *Overriding a Controller Profile*


Aruba Overrides
Add
New Aruba Controller Override
1-1 ▾ of 1 Aruba Controller Overrides Page 1 ▾ of 1
Choose Columns

		Profile ▲	Instance	Desire Entire Profile	Field	Value
□	✎	AP System Profile	airwave-office	No	LMS IP	10.2.28.251

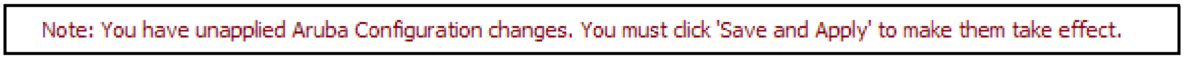
1-1 ▾ of 1 Aruba Controller Overrides Page 1 ▾ of 1
Select All - Unselect All
Delete

Save, Save and Apply, and Revert Buttons

Several **Add** or **Detail** pages in Aruba 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 Aruba Configuration pages. You can apply the configuration when all changes are complete at a later time.

Figure 13 *Unapplied Aruba Configuration Changes Message*



Note: You have unapplied Aruba 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 devices immediately if the controller is in **Manage** mode. If you have devices in **Monitor** mode, AWMS compares the current device configuration with the new desired configuration. For additional information and instructions about using **Manage** and **Monitor** modes, refer to "Pushing Device Configurations to Controllers" on page 36.
- **Revert**—This button cancels out of a new configuration or reverts back to the last saved configuration.

Folders, Users, and Visibility

Access and edit folders and visibility using the **Folder** column on the **Groups > Aruba Config** page. Profiles and Aruba AP Groups are assigned to folders. Folders allow you to set the visibility for controller information, and to set read/write privileges as required.

- As one example, it may be necessary to provide AWMS users with RF radio parameters while restricting access to SSID profiles.

Additional Concepts and Benefits

Scheduling Configuration Changes

You can schedule deployment of Aruba 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** mode, then pushing all configuration changes at one time by putting devices in **Manage** mode. Refer to "Pushing Device Configurations to Controllers" on page 36.

AWMS pushes configuration settings that are defined in the GUI to the Aruba Controllers as a set of CLI commands using Secure Shell (SSH). No controller reboot is required.

Auditing and Reviewing Configurations

AWMS supports auditing or reviewing in these ways.

1. You can review the AOS running configuration file. This is configuration information that AWMS reads from the device. In template-based configuration, you can review the running configuration file when working on a related template.
2. You can use the **APs/Devices > Audit** page for device-specific auditing.
3. Once you audit your controller, you can click **Import** from the **APs/Devices > Audit** page to reverse all of the profiles on the controller.

Licensing and Dependencies in Aruba Configuration

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

AWMS requires that you have a policy enforcement firewall license always installed on all Aruba controllers. If you push a policy to a controller without this license, a **Good** configuration will not result, and the controller will show as **Mismatched** on AWMS pages that reflect device configuration status.

Aruba 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. AWMS 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 ArubaOS, refer to the ArubaOS User Guide for that release.

Setting Up Initial Aruba Configuration

This section describes how to deploy an initial setup of Aruba Configuration in AWMS 6.4 or later versions.

Prerequisites

- Complete the AWMS upgrade to AWMS 6.4 or later. Refer to "Related Documents" on page 7 for installation or upgrade documents. Upon upgrade to AWMS Version 6.4 or later, Aruba Configuration is enabled by default in groups with devices in monitor-only mode and AOS firmware of 3.3.2.10 or greater.
- Back up your ArubaOS controller configuration file. Information about backing AWMS is available in the *AWMS User Guide* in the "Performing Daily Operations in AWMS" chapter.

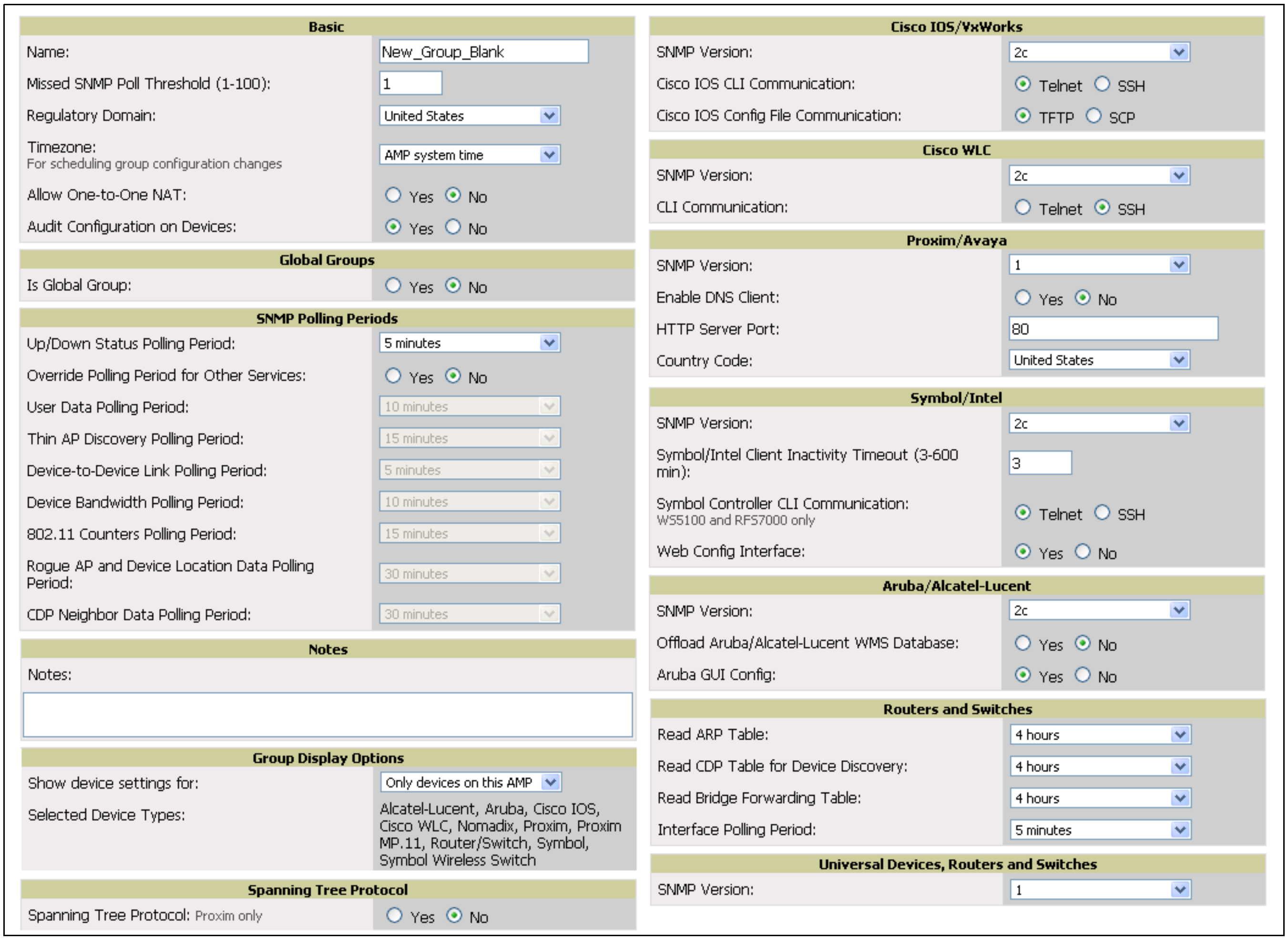
Procedure

Perform the following steps to deploy Aruba Configuration when at least one Aruba AP Group currently exists on at least one Aruba controller on the network:

1. On the **Groups > Basic** page, enable device preferences for Aruba devices. Figure 14 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 Aruba Configuration. One important setting on this page is the **Aruba GUI Config** option. Ensure that setting is **Yes**, which is the default setting.

Figure 14 ***Groups* > *Basic*** *Page Illustration (Partial Display)*



Basic

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

Global Groups

Is Global Group:	○ Yes ● No

SNMP Polling Periods

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

Notes

Notes:

Group Display Options

Show device settings for:	Only devices on this AMP
Selected Device Types:	Alcatel-Lucent, Aruba, Cisco IOS, Cisco WLC, Nomadix, Proxim, Proxim MP.11, Router/Switch, Symbol, Symbol Wireless Switch

Spanning Tree Protocol

Spanning Tree Protocol: Proxim only	○ Yes ● No

Cisco IOS/VxWorks

SNMP Version:	2c
Cisco IOS CLI Communication:	● Telnet ○ SSH
Cisco IOS Config File Communication:	● TFTP ○ SCP

Cisco WLC

SNMP Version:	2c
CLI Communication:	○ Telnet ● SSH

Proxim/Avaya

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

Symbol/Intel

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

Aruba/Alcatel-Lucent

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

Routers and Switches

Read ARP Table:	4 hours
Read CDP Table for Device Discovery:	4 hours
Read Bridge Forwarding Table:	4 hours
Interface Polling Period:	5 minutes

Universal Devices, Routers and Switches

SNMP Version:	1

2. Authorize Aruba controllers into the AMP Group.

CAUTION

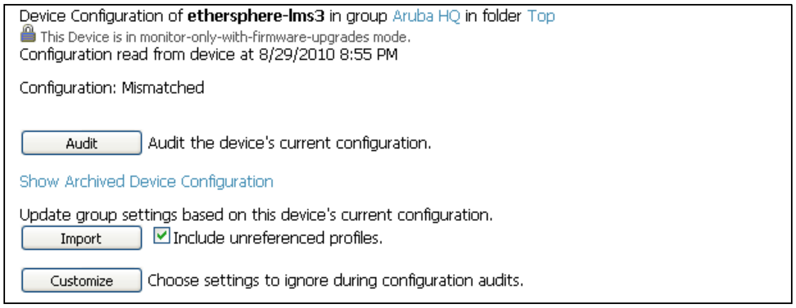
When authorizing the first controller onto a group, you must add the device in monitor-only mode. Otherwise, AWMS removes the configuration of the controller before you have a chance to import the configuration, and this would remove critical network configuration and status.

NOTE

Aruba Configuration is enabled by default in AWMS.

3. Navigate to the **AP/s/Devices > Audit** page for the first controller to prepare for importing an existing Aruba controller configuration file. Figure 15 illustrates the information available on this page if the device is mismatched.

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



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

This Device is in monitor-only-with-firmware-upgrades mode.

Configuration read from device at 8/29/2010 8:55 PM

Configuration: Mismatched

Audit the device's current configuration.

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

☑ Include unreferenced profiles.

Choose settings to ignore during configuration audits.

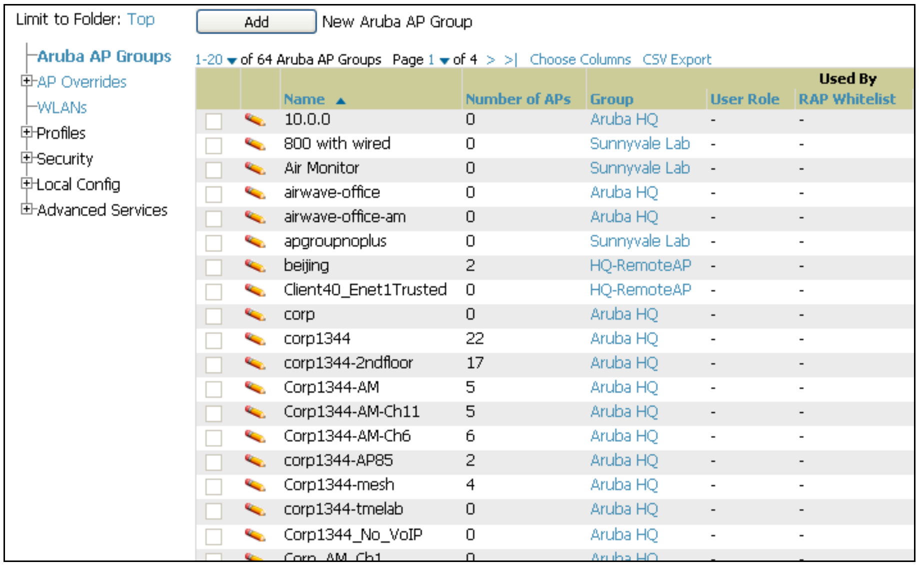
If the page reports a device mismatch, the page will display an **Import** button that allows you to import the Aruba controller settings from an Aruba Controller that has already been configured. To import the complete configuration from the controller (including any unreferenced profiles) select the **Include unreferenced profiles** checkbox. If you unselect the checkbox, AMP will delete the unreferenced profiles/AP Groups on the controller when it imports that configuration.

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

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

4. After configuration file import is complete, navigate to the **Device Setup > Aruba Configuration** page.
   - This page displays a list of APs authorized on the AMP that are using the Aruba AP Group.
   - The **User Role** is the Aruba User Role used in firewall settings. For additional information, refer to "Security > User Roles" on page 139.
   - The **Folder** column cites the visibility level to devices in each Aruba AP Group. For additional information, refer to "Visibility in Aruba Configuration" on page 41.
5. Add or modify **Aruba AP Groups** as required.
   a. Navigate to the **Device Setup > Aruba Configuration > Aruba AP Groups** page, illustrated in Figure 16.

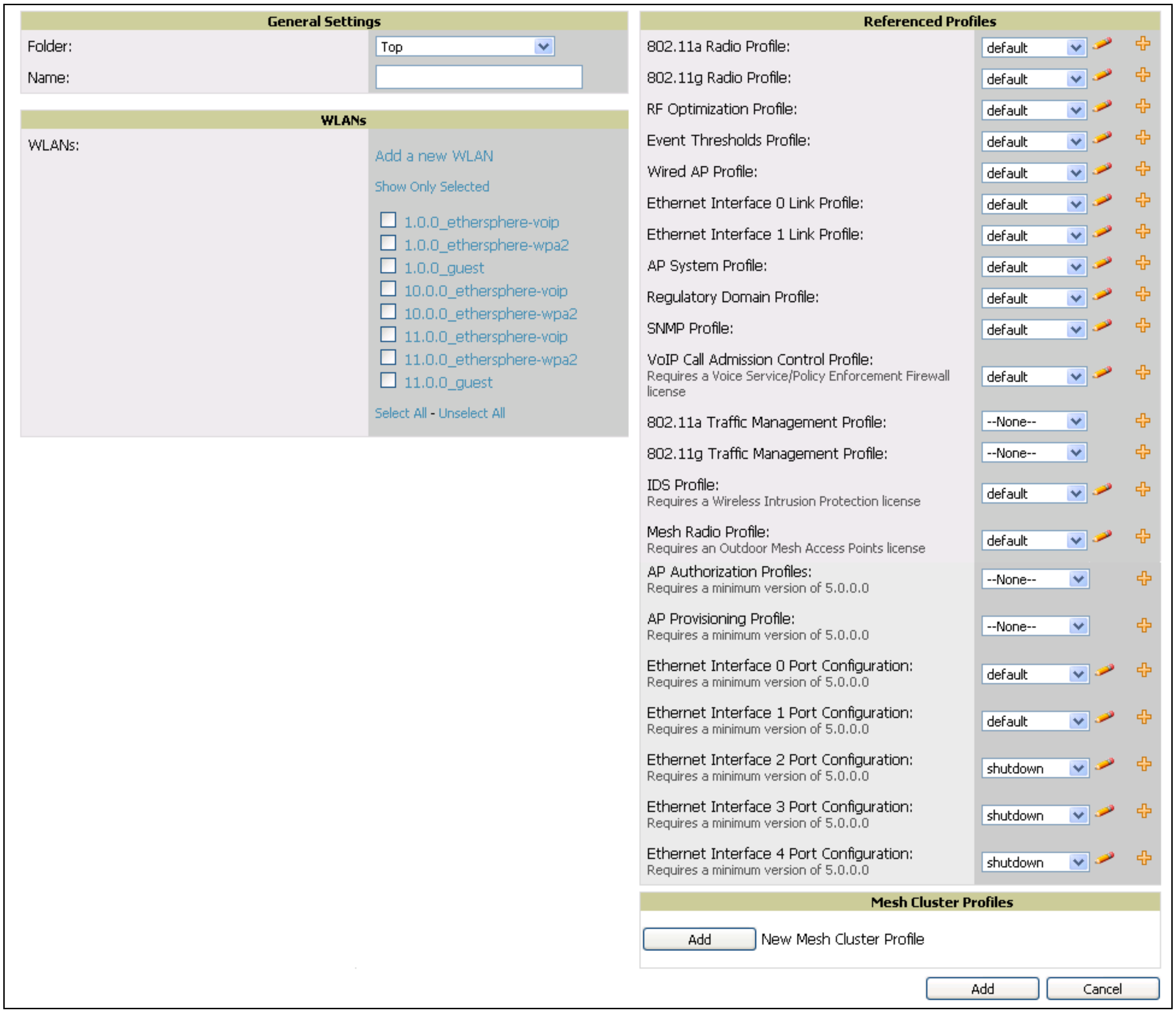
Figure 16 ***Device Setup* > *Aruba Configuration* > *Aruba AP Groups* Page**



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

   a. Click **Add** from the **Aruba AP Groups** page to create a new Aruba AP Group. To edit an Aruba AP Group, click the pencil icon next to the group. The **Details** page for the Aruba AP Group group appears. This page allows you to select the profiles to apply to the Aruba AP Group, and to select one or more WLANs that support that Aruba AP Group. Figure 17 illustrates this page.

Figure 17 ***Device Setup > Aruba Configuration > Aruba AP Groups > Add/Edit*** *Details Page*



General Settings

Folder:	Top
Name:	

WLANs

WLANs:

Add a new WLAN

Show Only Selected

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

Select All - Unselect All

Referenced Profiles

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

Mesh Cluster Profiles

Add New Mesh Cluster Profile

Add Cancel

The following section of this configuration guide provide additional information about configuring Aruba AP Groups:

- "General Aruba AP Groups Procedures and Guidelines" on page 30

6. Add or edit WLANs in Aruba Configuration as required.

   a. Navigate to **Device Setup > Aruba 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 Wizard View on the Aruba controller. This page does not require in-depth knowledge of the profiles that define the Aruba AP Group.
   - **Advanced**—This display allows you to select individual profiles that define the WLAN and associated Aruba 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 Procedures and Guidelines" on page 33
   - "WLAN Pages and Field Descriptions" on page 56

7. Add or edit Aruba Configuration **Profiles** as required.

   a. Navigate to **Device Setup > Aruba Configuration > Profiles** section of the navigation pane.

   b. You must select the type of profile 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 AWMS are similar to the **All Profiles** display in the Aruba Controller WebUI. The primary difference in AWMS is that **AAA** and **SSID** profiles are not listed under the **Wireless LAN** column as the controller.

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

   All other settings supported on Aruba controllers can be defined on the **Device Setup > Aruba Configuration** page. The following section in this document provides additional information about configuring profiles:

   - "General Profiles Guidelines" on page 35

8. Provision multiple Aruba AP Groups on one or more controllers by putting the controllers into an AMP group and configuring that group to use the selected Aruba AP Groups. Configure such Aruba AP Groups settings on the **Group > Aruba Config** page. The following section of this document provides additional information:

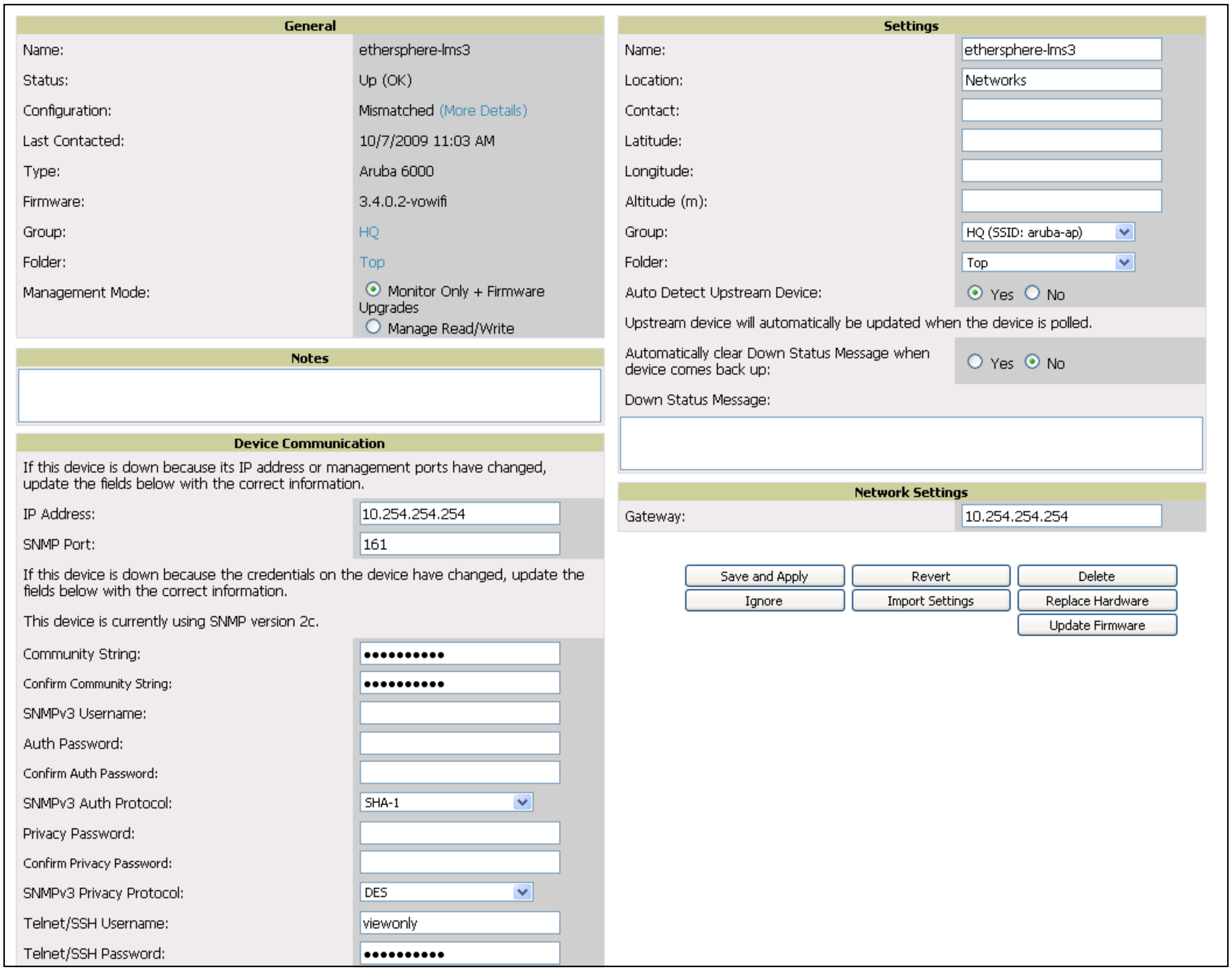
   - "General Aruba AP Groups Procedures and Guidelines" on page 30

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

   - "Supporting APs with Aruba Configuration" on page 37

10. Each AP can be assigned to a single Aruba AP Group. Make sure to choose an AP Group that has been configured on that controller using that controller's AMP 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 Aruba Configuration" on page 37.

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



General

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

Notes

Device Communication

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

IP Address:	10.254.254.254
SNMP Port:	161

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

This device is currently using SNMP version 2c.

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

Settings

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

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

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

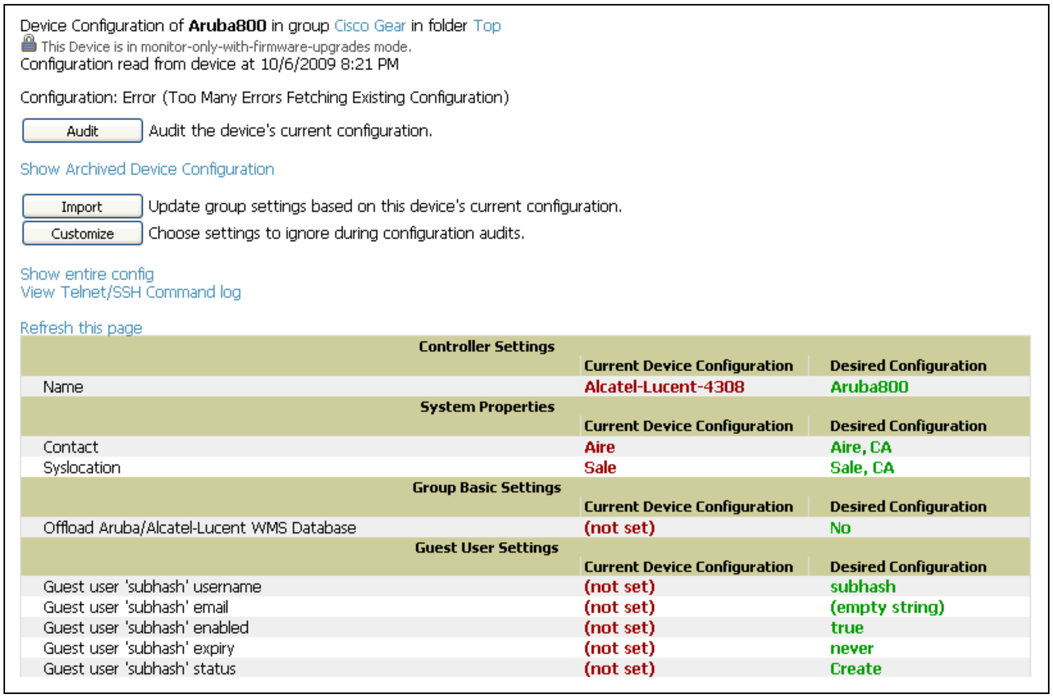
Down Status Message:

Network Settings

Gateway:	10.254.254.254

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

Figure 19 *APs/Devices > Audit* Page Illustration (Partial Display)



Device Configuration of **Aruba800** in group Cisco Gear in folder Top
This Device is in monitor-only-with-firmware-upgrades mode.
Configuration read from device at 10/6/2009 8:21 PM

Configuration: Error (Too Many Errors Fetching Existing Configuration)

Audit the device's current configuration.

Show Archived Device Configuration

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

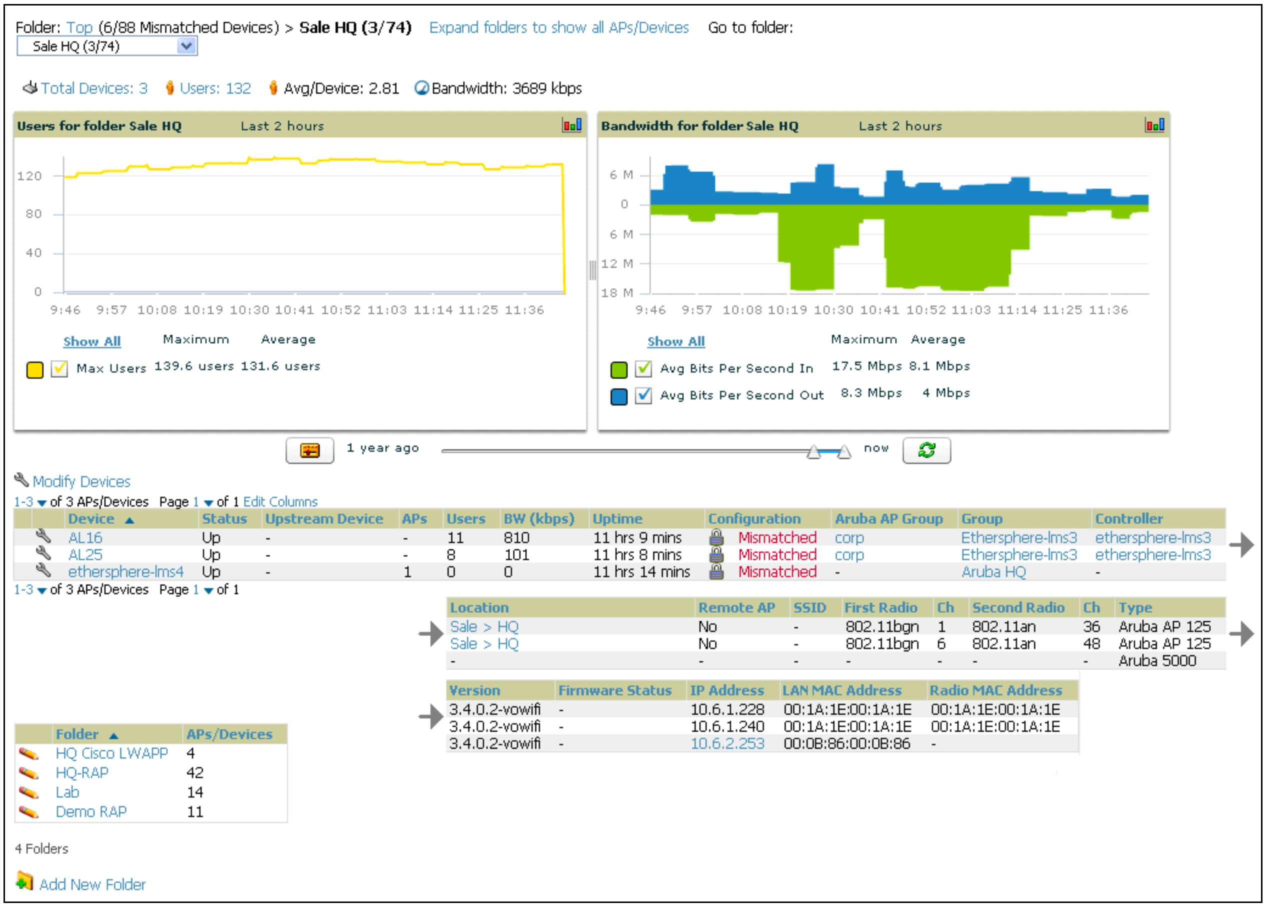
Choose settings to ignore during configuration audits.

Show entire config
View Telnet/SSH Command log

Refresh this page

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

Figure 20 *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:

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	00:0B:86:00:0B:86	-

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

4 Folders

Add New Folder

What Next?

After initial AOS deployment with the Aruba Configuration feature, you can make many additional configurations or continue with maintenance tasks, such as with the following examples:

- Once Aruba Configuration is deployed in AWMS, 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. Such configurations are supported on the **Groups > Basic** and **Device Setup > Communications** pages of AWMS. Refer to the *AWMS User Guide* for additional information.
- To resolve communication issues, review the credentials on the **AP Manage** page.
- Mismatches can occur when importing profiles because AWMS deletes orphaned profiles, even if following a new import.

Additional Capabilities of Aruba Configuration

AWMS supports many additional AOS configurations and settings. Refer to these additional resources for more information:

- *AOS User Guide*
- *AWMS User Guide*
- *AirWave and Aruba Best Practices Guide*

Chapter 2

Using Aruba Configuration in Daily Operations

Introduction

This chapter presents the more common tasks or concepts after initial setup of Aruba Configuration is complete, as described in the section "Setting Up Initial Aruba Configuration" on page 24. This chapter emphasizes frequent procedures as follows:

General Aruba AP Groups Procedures and Guidelines

- Guidelines and Pages for Aruba AP Groups in Aruba Configuration
- Selecting Aruba Controller Groups
- Configuring Aruba AP Groups

General WLAN Procedures and Guidelines

- Guidelines and Pages for WLANs in Aruba Configuration
- Configuring or Editing WLANs with Basic View
- Configuring or Editing WLANs with Advanced View

General Controller Procedures and Guidelines

- Using Master, Standby Master, and Local Controllers in Aruba Configuration
- Pushing Device Configurations to Controllers

Supporting APs with Aruba Configuration

- AP Overrides Guidelines
- Configuring or Editing AP Overrides
- Changing the Aruba AP Group for an AP Device
- Changing Adaptive Radio Management (ARM) Settings
- Changing SSID and Encryption Settings

Visibility in Aruba Configuration

- Visibility Overview
- Defining Visibility for Aruba Configuration

Using AWMS to Deploy Aruba APs for the First Time

NOTE

For a complete reference on all Aruba Configuration pages, field descriptions, and certain additional procedures that are more specialized, refer to Appendix A, "Aruba Configuration Reference" on page 49.

General Aruba AP Groups Procedures and Guidelines

Guidelines and Pages for Aruba AP Groups in Aruba Configuration

The fields and default settings for Aruba AP Groups are described in "Aruba AP Groups" on page 53. The following ***guidelines*** govern the configuration and use of Aruba AP Groups across AWMS:

- Aruba AP Groups function with standard AWMS groups that contain them. Add Aruba AP Groups to standard AWMS groups. Additional procedures in this document explain their interoperability.
- APs can belong to a controller's AWMS group or to an AWMS group by themselves.
- All configurations of Aruba AP Groups must be pushed to Aruba controllers to become active on the network.
- Additional dynamics between master, standby master, and local controllers still apply. In this case, refer to "Using Master, Standby Master, and Local Controllers in Aruba Configuration" on page 40.

The following ***pages*** in AWMS govern the configuration and use of Aruba AP Groups or standard device groups across AWMS:

- The **Device Setup > Aruba Configuration** navigation pane displays standard AOS components and your custom-configured Aruba AP Groups, WLANs, and AP Overrides.
- You define or modify Aruba AP Groups on the **Device Setup > Aruba Configuration** page. Click **Aruba AP Groups** from the navigation pane.
- You select Aruba AP Groups to associate with AMP (AWMS) Groups with the **Groups > Aruba Config** page.
- You modify devices in Aruba AP Groups with the **APs/Devices > List** page, clicking **Modify These Devices**. This is the page at which you assign devices to a given group and Aruba AP Group.

Selecting Aruba Controller Groups

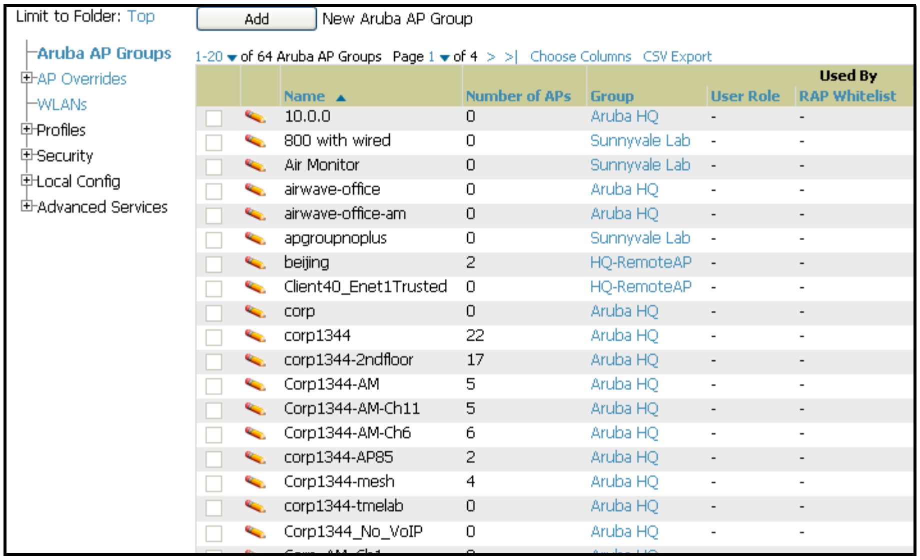
To select Aruba AP Groups, navigate to the **Device Setup > Aruba AP Groups** page. This page is central to defining Aruba AP Groups, to viewing the AMP groups with which an Aruba AP Group is associated, changing or deleting Aruba AP Groups, and assigning AP devices to an Aruba AP Group.

Configuring Aruba AP Groups

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

1. Browse to the **Device Setup > Aruba Configuration** page, and click the **AP Groups** heading in the navigation pane on the left. The **Groups Summary** page appears and displays all current Aruba AP Groups, as illustrated in Figure 21 and described in Table 3 of the *Appendix*.

Figure 21 ***Device Setup > Aruba Configuration > AP Groups*** *Page Illustration*



1-20 of 64 Aruba AP Groups Page 1 of 4 > >| Choose Columns CSV Export

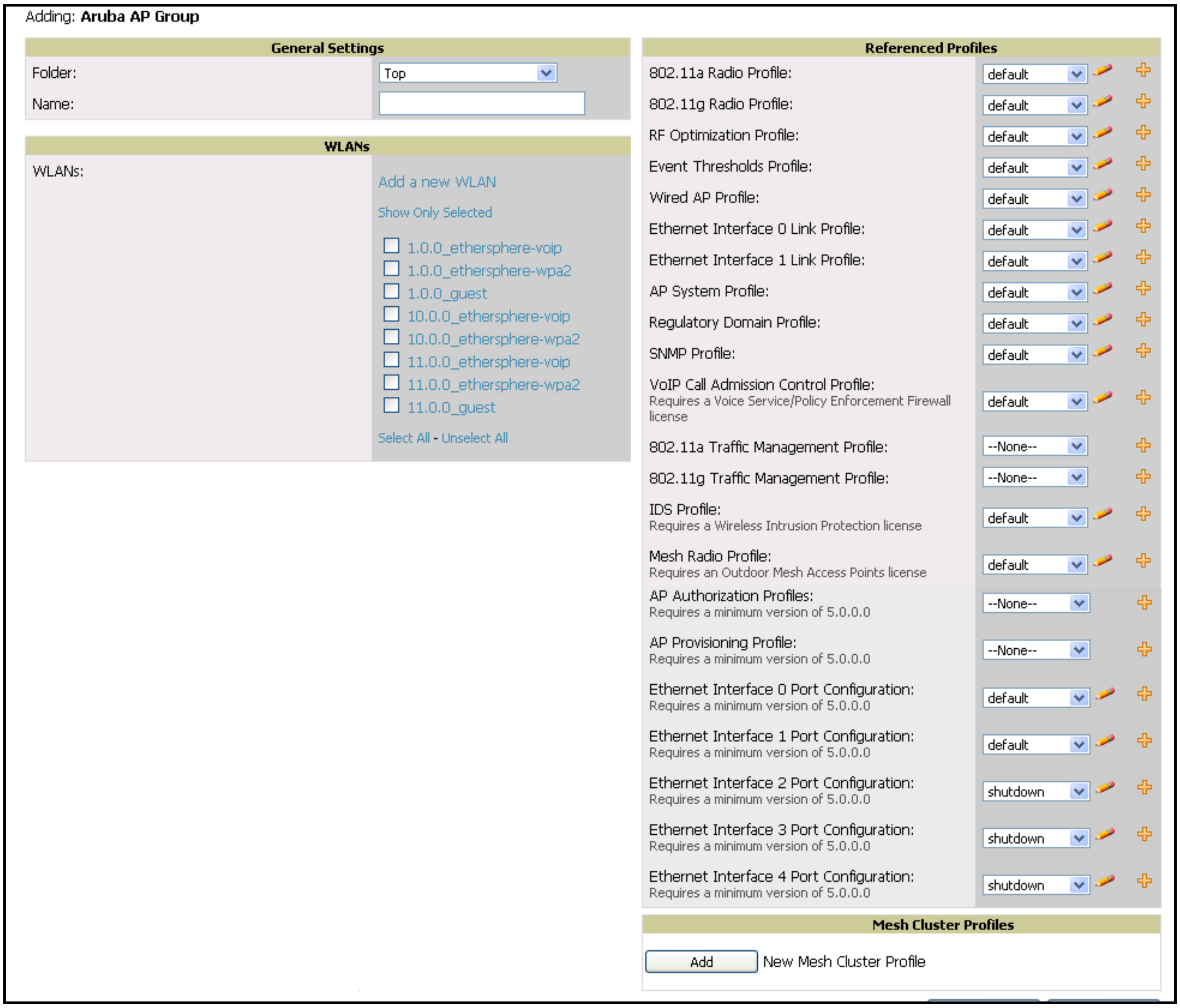
					Used By	
		Name ▲	Number of APs	Group	User Role	RAP Whitelist
□	✎	10.0.0	0	Aruba HQ	-	-
□	✎	800 with wired	0	Sunnyvale Lab	-	-
□	✎	Air Monitor	0	Sunnyvale Lab	-	-
□	✎	airwave-office	0	Aruba HQ	-	-
□	✎	airwave-office-am	0	Aruba HQ	-	-
□	✎	apgroupnoplus	0	Sunnyvale Lab	-	-
□	✎	beijing	2	HQ-RemoteAP	-	-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

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 **Group Details** page appears with current or default configurations. Figure 22 illustrates the **Details** page for a new group to be defined. The settings on this page are described in Table 4 of the *Appendix*.

Figure 22 *Device Setup > Aruba Configuration > Add/Edit Group Details Page Illustration*



Adding: **Aruba AP Group**

General Settings

Folder:	Top
Name:	

WLANs

WLANs:

Add a new WLAN

Show Only Selected

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

Select All - Unselect All

Referenced Profiles

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

Mesh Cluster Profiles

New Mesh Cluster Profile

3. Click **Add** or **Save** to finish creating or editing the Aruba 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 Aruba 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 Aruba controllers by clicking **Save and Apply**. The principles of Monitor and Manage mode still apply. For additional information, refer to "Pushing Device Configurations to Controllers" on page 40.

What Next?

Once Aruba AP groups are defined, ensure that all desired WLANs are referenced in Aruba AP Groups, as required. Repeat the above procedure to revise WLANs as required. You can add or edit AP devices in Aruba 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 Procedures and Guidelines

Guidelines and Pages for WLANs in Aruba Configuration

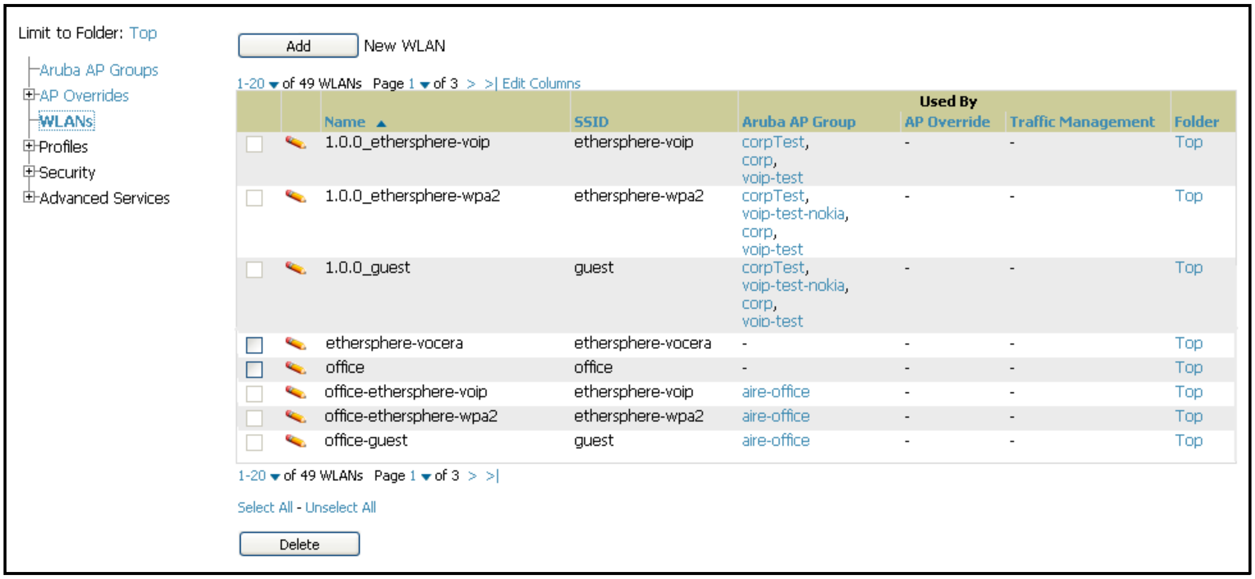
- The **Device Setup > Aruba Configuration** navigation pane displays custom-configured WLANs and Aruba AP Groups. You define or modify WLANs on the **Device Setup > Aruba Configuration** page. Click **WLANs** from the navigation pane.
- You can create or edit any profile in an WLAN as you define or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

Configuring or Editing WLANs with Basic View

Perform the following steps to create or configure a basic WLAN in Aruba Configuration.

1. Navigate to the **Aruba Configuration > WLANs** page. This page displays currently configured WLANs. Figure 23 illustrates this page.

Figure 23 ***Device Setup* > *Aruba Configuration* > *WLANs*** *Page Illustration*



Limit to Folder: Top

- Aruba AP Groups
- AP Overrides
- WLANs
- Profiles
- Security
- Advanced Services

New WLAN

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

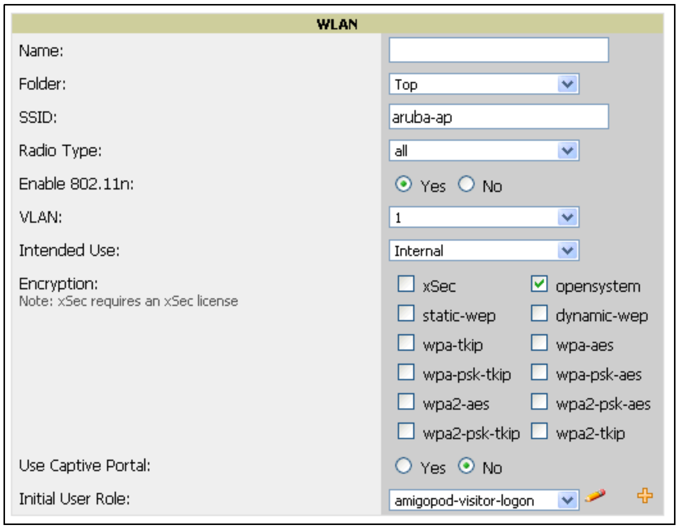
				Used By			
		Name ▲	SSID	Aruba AP Group	AP Override	Traffic Management	Folder
□	✎	1.0.0_ethersphere-voip	ethersphere-voip	corpTest, corp, voip-test	-	-	Top
□	✎	1.0.0_ethersphere-wpa2	ethersphere-wpa2	corpTest, voip-test-nokia, corp, voip-test	-	-	Top
□	✎	1.0.0_guest	guest	corpTest, voip-test-nokia, corp, voip-test	-	-	Top
□	✎	ethersphere-vocera	ethersphere-vocera	-	-	-	Top
□	✎	office	office	-	-	-	Top
□	✎	office-ethersphere-voip	ethersphere-voip	aire-office	-	-	Top
□	✎	office-ethersphere-wpa2	ethersphere-wpa2	aire-office	-	-	Top
□	✎	office-guest	guest	aire-office	-	-	Top

1-20 ▾ of 49 WLANs Page 1 ▾ of 3 > >|

Select All - Unselect All

2. To add a new WLAN, click the **Add WLAN** button. To edit an existing WLAN, click the **pencil** icon next to the WLAN name. Select **Basic** to define or modify the settings. Otherwise, refer to the "Configuring or Editing WLANs with Advanced View" on page 38 for additional information. Figure 27 illustrates the **Basic** view. For a detailed explanation of all fields, refer to Table 8 in the *Appendix*.

Figure 24 ***Device Setup > WLANs > Add > Basic*** *Page Illustration*



WLAN

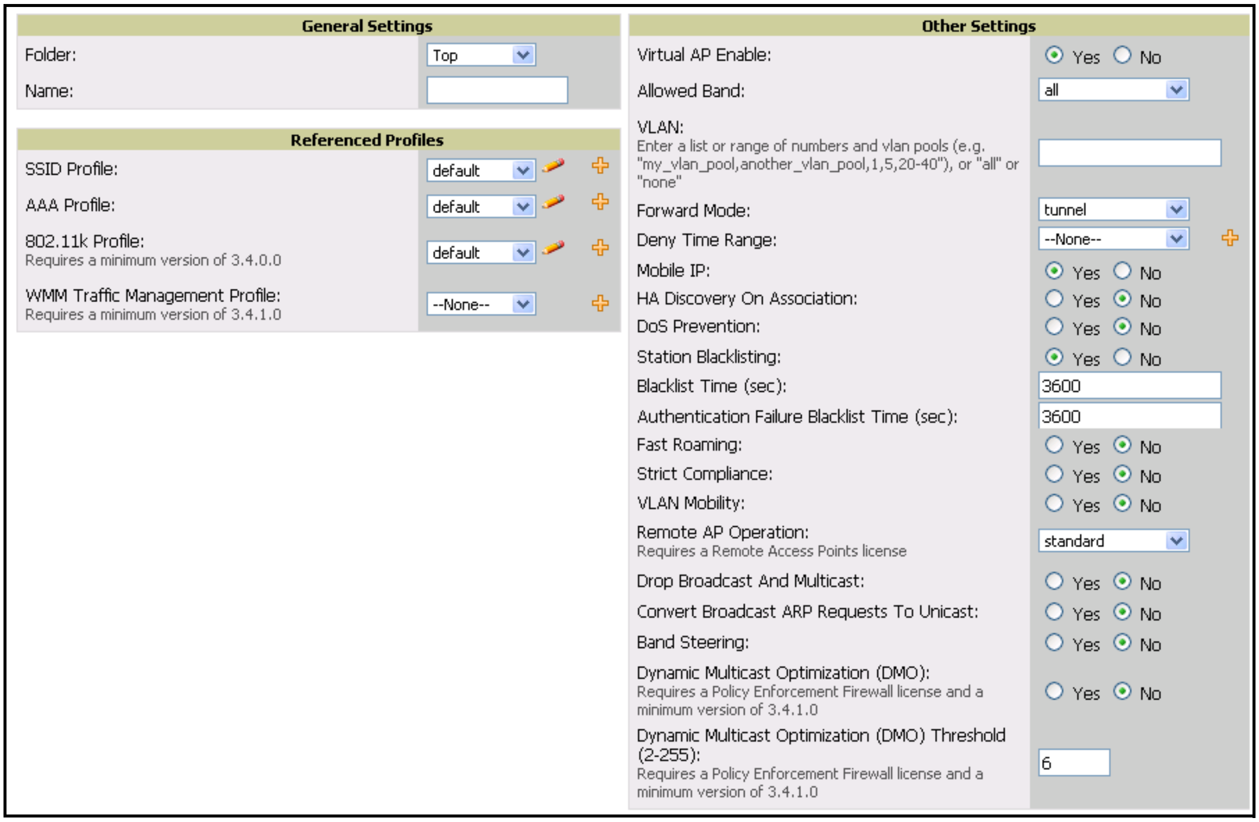
Name:	
Folder:	Top
SSID:	aruba-ap
Radio Type:	all
Enable 802.11n:	● Yes ○ No
VLAN:	1
Intended Use:	Internal
Encryption: Note: xSec requires an xSec license	□ xSec ☑ opensystem □ static-wep □ dynamic-wep □ wpa-tkip □ wpa-aes □ wpa-psk-tkip □ wpa-psk-aes □ wpa2-aes □ wpa2-psk-aes □ wpa2-psk-tkip □ wpa2-tkip
Use Captive Portal:	○ Yes ● No
Initial User Role:	amigopod-visitor-logon

3. Click **Add** or **Save**. The added or edited WLAN appears on the **WLANs** page. You can now use this WLAN with one or more Aruba AP Groups.
4. Repeat this procedure or continue to additional procedures to complete WLAN, Profile, Aruba AP Group or other configurations.
5. Push the newly added or edited WLAN to the desired Aruba Controllers. Refer to "Pushing Device Configurations to Controllers" on page 40.

Configuring or Editing WLANs with Advanced View

1. Navigate to the **Aruba Configuration > WLANs** page. This page displays currently configured WLANs. Figure 23 illustrates this page.
2. To add a new WLAN, click the **Add WLAN** button. To edit an existing WLAN, click the **pencil** icon next to the WLAN name. Select **Advanced** to define or modify the settings that pertain to advanced WLAN configuration. Figure 25 illustrates the **Advanced** view. For complete description of all fields on this page, refer to Table 9 in the *Appendix*.

Figure 25 ***Device Setup > Aruba Configuration > WLANs > Add > Advanced*** *Page Illustration*



General Settings	
Folder:	Top
Name:	

Referenced Profiles	
SSID Profile:	default
AAA Profile:	default
802.11k Profile: Requires a minimum version of 3.4.0.0	default
WMM Traffic Management Profile: Requires a minimum version of 3.4.1.0	--None--

Other Settings	
Virtual AP Enable:	● Yes ○ No
Allowed Band:	all
VLAN: Enter a list or range of numbers and vlan pools (e.g. "my_vlan_pool,another_vlan_pool,1,5,20-40"), or "all" or "none"	
Forward Mode:	tunnel
Deny Time Range:	--None--
Mobile IP:	● Yes ○ No
HA Discovery On Association:	○ Yes ● No
DoS Prevention:	○ Yes ● No
Station Blacklisting:	● Yes ○ No
Blacklist Time (sec):	3600
Authentication Failure Blacklist Time (sec):	3600
Fast Roaming:	○ Yes ● No
Strict Compliance:	○ Yes ● No
VLAN Mobility:	○ Yes ● No
Remote AP Operation: Requires a Remote Access Points license	standard
Drop Broadcast And Multicast:	○ Yes ● No
Convert Broadcast ARP Requests To Unicast:	○ Yes ● No
Band Steering:	○ Yes ● No
Dynamic Multicast Optimization (DMO): Requires a Policy Enforcement Firewall license and a minimum version of 3.4.1.0	○ Yes ● No
Dynamic Multicast Optimization (DMO) Threshold (2-255): Requires a Policy Enforcement Firewall license and a minimum version of 3.4.1.0	6

3. Click **Add** or **Save**. The added or edited WLAN appears on the **WLANs** page. You can now use this WLAN with one or more Aruba AP Groups.
4. Repeat this procedure or continue to additional procedures to complete WLAN, Profile, Aruba AP Group or other configurations.
5. Push the newly added or edited WLAN to the desired Aruba Controllers. For additional information, refer to "Pushing Device Configurations to Controllers" on page 40.

General Profiles Guidelines

AOS elements can be added or edited after an AOS configuration file is imported to AWMS and pushed to controllers with the steps described in "Setting Up Initial Aruba Configuration" on page 24.

Profiles in Aruba configuration entail the following concepts or dynamics:

- Profiles define nearly all parameters for Aruba AP Groups and WLANs, and Aruba 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 Aruba AP Group or WLAN setup. In the latter case, AWMS takes you to profile setup on separate pages, then returns you to your place in Aruba AP Group or WLAN setup.

For complete Profiles inventory and field descriptions, refer to "Profiles Pages and Field Descriptions" on page 68.

General Controller Procedures and Guidelines

Using Master, Standby Master, and Local Controllers in Aruba Configuration

AWMS implements the following general approaches in relation to controllers.

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

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

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

Pushing Device Configurations to Controllers

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

- Make device changes on the **Device Setup > Aruba Configuration** page and click **Save and Apply**.
- Make devices changes on the **Groups > Aruba Config** page and click **Save and Apply**.

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

NOTE

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

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

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

Supporting APs with Aruba Configuration

AP Overrides Guidelines

The **AP Override** component of Aruba Configuration appears in the navigation pane of the **Device Setup > Aruba Configuration** page. This component operates with the following principles:

- AP devices function within groups that define operational parameters for groups of APs. This is standard across all of AWMS.
- **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**.

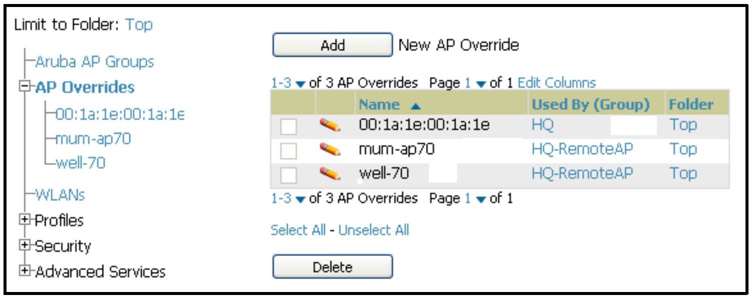
In summary, the **AP Override** feature prevents you from having to create a new AP group for customized APs that otherwise share parameters with other APs in a group. **AP Override** allows you to have less total AP groups than you might otherwise require.

Configuring or Editing AP Overrides

Perform the following steps to create or edit AP Overrides.

1. Navigate to the **Aruba Configuration > AP Overrides** page. This page displays currently configured AP overrides. Figure 26 illustrates this page.

Figure 26 ***Device Setup > Aruba Configuration > AP Overrides** Page Illustration*



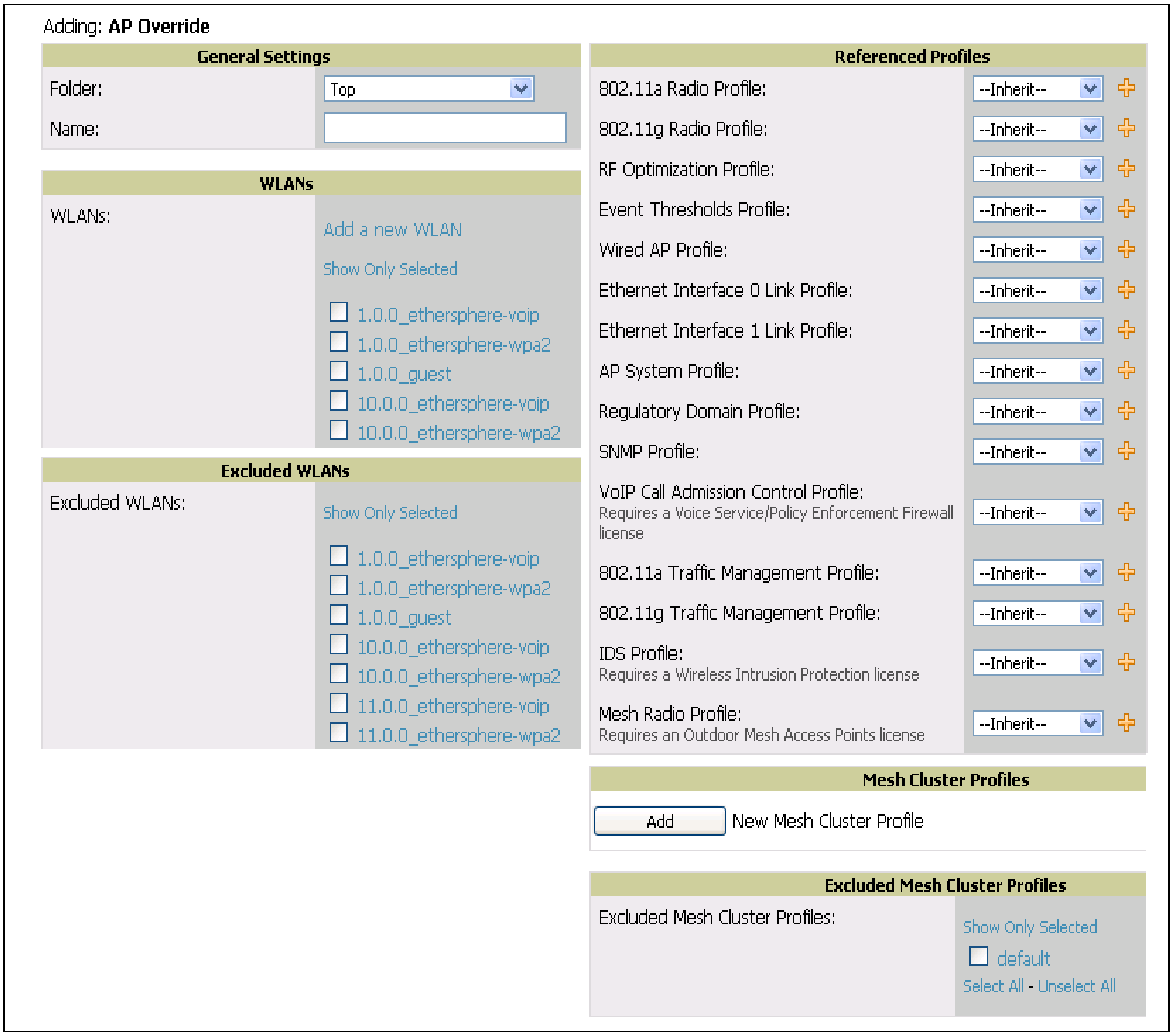
		Name ▲	Used By (Group)	Folder
□	✎	00:1a:1e:00:1a:1e	HQ	Top
□	✎	mum-ap70	HQ-RemoteAP	Top
□	✎	well-70	HQ-RemoteAP	Top

2. To add a new AP Override, click the **Add New AP Override** button.

   To edit an existing AP Override, click the **pencil** icon next to the **AP Override** name.

   The details page appears. Figure 27 illustrates the **AP Overrides** detail view.

Figure 27 ***AP Overrides Add*** *or* ***Edit*** *Page Illustration (Non-scrolling View)*



Adding: **AP Override**

General Settings

Folder:	Top
Name:	

WLANs

WLANs:

Add a new WLAN

Show Only Selected

- ☐ 1.0.0_ethersphere-voip
- ☐ 1.0.0_ethersphere-wpa2
- ☐ 1.0.0_guest
- ☐ 10.0.0_ethersphere-voip
- ☐ 10.0.0_ethersphere-wpa2

Excluded WLANs

Excluded WLANs:

Show Only Selected

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

Referenced Profiles

802.11a Radio Profile:	--Inherit--
802.11g Radio Profile:	--Inherit--
RF Optimization Profile:	--Inherit--
Event Thresholds Profile:	--Inherit--
Wired AP Profile:	--Inherit--
Ethernet Interface 0 Link Profile:	--Inherit--
Ethernet Interface 1 Link Profile:	--Inherit--
AP System Profile:	--Inherit--
Regulatory Domain Profile:	--Inherit--
SNMP Profile:	--Inherit--
VoIP Call Admission Control Profile: Requires a Voice Service/Policy Enforcement Firewall license	--Inherit--
802.11a Traffic Management Profile:	--Inherit--
802.11g Traffic Management Profile:	--Inherit--
IDS Profile: Requires a Wireless Intrusion Protection license	--Inherit--
Mesh Radio Profile: Requires an Outdoor Mesh Access Points license	--Inherit--

Mesh Cluster Profiles

Add New Mesh Cluster Profile

Excluded Mesh Cluster Profiles

Excluded Mesh Cluster Profiles:

Show Only Selected

- ☐ default

Select All - Unselect All

For a description of all fields on this page, refer to Table 5 in the *Appendix*.

3. Click **Add** or **Save**. The added or edited **AP Override** appears on the **AP Overrides** page.
4. Push the newly added or edited AP Override configuration to the desired Aruba Controllers. Refer to "Pushing Device Configurations to Controllers" on page 40.
5. Repeat this procedure or continue to additional procedures to complete WLAN, Profile, Aruba AP Group or other configurations.

Changing Adaptive Radio Management (ARM) Settings

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

- "Configuring Aruba AP Groups" on page 34
- "Aruba AP Groups" on page 53
- "Profiles > RF > 802.11a/g Radio > ARM" on page 124

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 Aruba AP Groups and WLANs that support them. To do so, refer to the following topics that describe relevant steps and configuration pages:

- "Configuring Aruba AP Groups" on page 34
- "Guidelines and Pages for WLANs in Aruba Configuration" on page 37
- "Profiles > SSID" on page 132 and related profiles.

Changing the Aruba AP Group for an AP Device

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

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

   To discover additional devices, ensure that the controller is set to perform a thin AP poll period.
4. On the **APs/Devices > List** page, you can specify the **Group** and **Folder** to which a device belongs. Click **Modify Devices** to change more than one device, or click the **Wrench** icon associated with any specific device to make changes. The **APs/Devices > Manage** page appears.
5. In the **Settings** section of the **APs/Devices > Manage** page, select the new Aruba 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 AWMS, 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 AWMS.
   - Click **Ignore** to keep the device in AWMS 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 controller that is to support this AP device. For additional information, refer to "Pushing Device Configurations to Controllers" on page 40.

Using AWMS to Deploy Aruba APs for the First Time

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

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

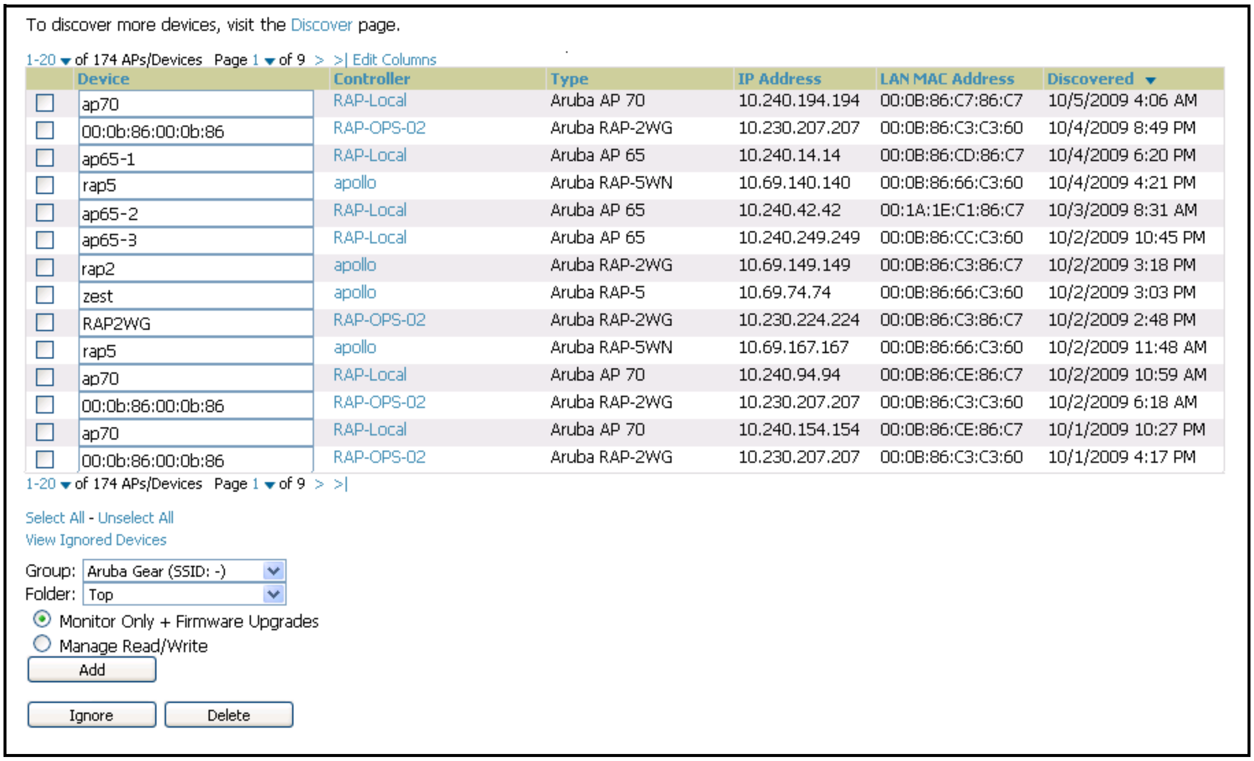
One possible workaround to update an Aruba AP device name in AWMS would be as follows, and this is not the most efficient approach:

1. Configure and deploy the AP from AOS (separate from AWMS).
2. Delete the AP from AWMS.
3. Have AWMS rediscover the device.

A more efficient and robust approach is to deploy Aruba APs in AWMS with the following steps:

1. Define communication settings for Aruba APs pending discovery. Use 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 Aruba APs with AWMS. You can do so with the **Device Setup > Discover** page
3. Click **New Devices** In the **Status** section at the top of any AWMS page, or navigate to the **APs/Devices > New** page, illustrated in Figure 28.

Figure 28 ***APs/ Devices*** **>** ***New*** *Page Illustration*



To discover more devices, visit the Discover page.

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

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

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

Select All - Unselect All
View Ignored Devices

Group: Aruba Gear (SSID: -)
Folder: Top

● Monitor Only + Firmware Upgrades
○ Manage Read/Write

4. Select (check) the box next to any AP you want to provision.
5. Rename all new APs. Type in the new device name in the **Device** column.
6. Scroll the bottom of the page and put APs in the appropriate AWMS 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 AMP but also on the Aruba AP Group and Aruba controller with the `show ap database` AOS command.
8. To set the appropriate Aruba AP Group, select the **AP/Devices** or **Groups** page and locate your APs.
9. Click **Modify Devices** under the **User** and **Bandwidth** flash graphics.
10. Select the APs you want to re-group.
11. In the field that states **Move to Aruba AP Group**, below the list of the APs, select the appropriate group, and click **Move**.

NOTE

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

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

Using General AWMS Device Groups and Folders

AWMS only allows any given AP to belong to one AWMS device group at a time. Supporting one AP in two or more AWMS device groups would create at least two possible issues, to include 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 AWMS graphs.

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

NOTE

Aruba APs can also belong to Aruba AP Groups, but each AP is still limited to one general AWMS 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 AWMS group level.
- AWMS folders support multiple sublevels.
- Therefore, unless there is a compelling reason to use the folders-by-device-type approach, AirWave generally recommends the first approach where you use groups for AP type and folders strictly for AP location.

Visibility in Aruba Configuration

Visibility Overview

Aruba Configuration supports device configuration and user information in the following ways;

- user roles
- AP/Device access level
- folders.

These and additional factors for visibility are as follows:

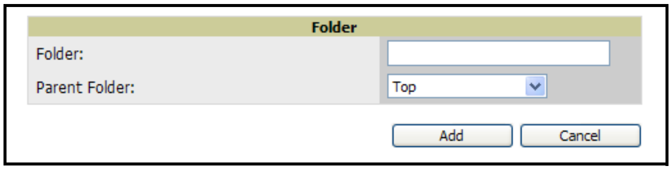
- Administrative and Management users in AWMS can view the **Device Setup > Aruba Configuration** page and the **APs/Devices > Aruba Config** pages.
  - Administrative users are enabled to view all configurations.
  - Management users have access to all profiles and Aruba AP groups for their respective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

Defining Visibility for Aruba Configuration

Perform these steps to define or adjust visibility for users to manage and support Aruba Configuration:

1. As required, create a new AWMS device folder with management access.
   a. Navigate to the **APs/Device > List** page, scroll to the bottom of the page. (An alternate page supporting new folders is **Users > Connected** page).
   b. Click the **Add New Folder** link. The **Folder** detail page appears, as illustrated in Figure 29:

Figure 29 ***APs/Devices*** **>** ***Add New Folder*** **>** ***Folders*** *Page Illustration*

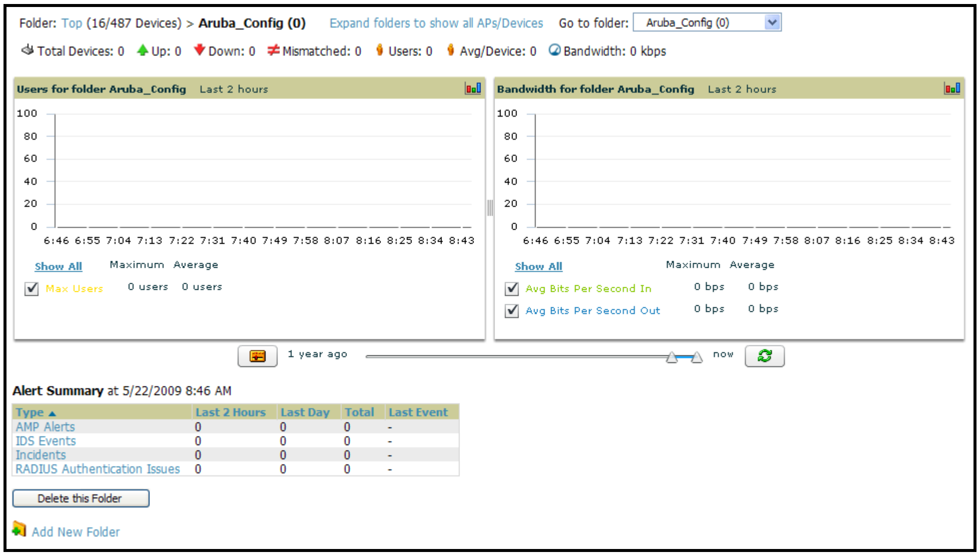


Folder

Folder:	
Parent Folder:	Top

   c. Click **Add**. The **APs/Devices > List** page reappears. You can view your new folder by selecting it from the **Go to folder** drop-down list at the top right of this page. Figure 30 illustrates an unpopulated device page for an example folder.

Figure 30 ***APs/Devices*** **>** ***List*** *Page With No Devices*



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

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

Show All	Maximum	Average
☑ Max Users	0 users	0 users

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

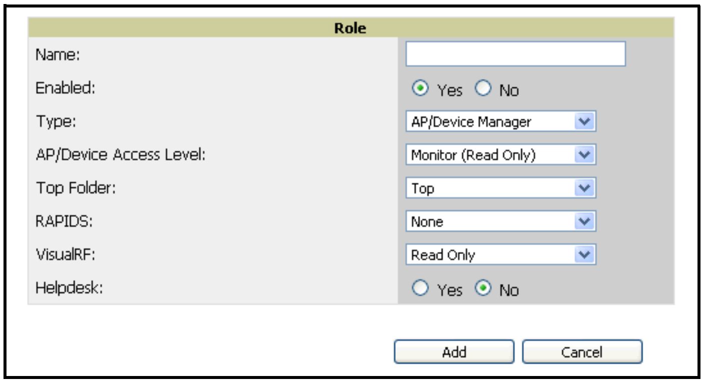
Alert Summary at 5/22/2009 8:46 AM

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

2. Add Aruba controller devices to that folder as required. Use the **Device Setup > Add** page following instructions available in the *AWMS User Guide*.

3. As required, create or edit a user role that is to have rights and manage privileges required to support their function in Aruba Configuration.
   a. At least one user must have administrative privileges, but several additional users may be required, with less rights and visibility, to support Aruba Configuration without access to the most sensitive information, such as SSIDs or other security related data.
   b. Navigate to the **AMP Setup > Roles** page, and click **Add New Role** to create a new role with appropriate rights, or click the **pencil** (manage) icon next to an existing role to adjust rights as required. The Role page appears, illustrated in Figure 31.

Figure 31 ***AMP Setup** > **Roles** > **Add/Edit** Role Page Illustration*



Role

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

   c. As per standard AWMS configuration, complete the settings on this page. The most important fields with regard to Aruba 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 Aruba controllers, devices, and general Aruba Configuration operations.
      - **Top Folder**—Specify the folder created earlier in this procedure, or specify the Top folder for an administrative user.
   d. Click **Add** to complete the role creation, or click **Save** to retain changes to an existing role. The **AMP > Setup** page now displays the new or revised role.
4. As required, add or edit one or more users to manage and support Aruba Configuration. This step creates or edits users to have rights appropriate to Aruba Configuration. This user inherits visibility to Aruba controllers and Aruba Configuration data based on the role and device folder created earlier in this procedure.
   a. Navigate to the **AMP 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 AWMS configuration. Refer to the *AWMS 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 Aruba 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 AWMS pages in this procedure.
6. Add or discover devices for the device folder defined during step 1 of this procedure. Information about devices is available in the *AWMS User Guide*.
7. Continue to other elements of Aruba Configuration, described in this document. Early emphasis entails creation or editing of Aruba AP Groups and WLANs with which they are associated.

Appendix A

Aruba Configuration Reference

Introduction

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

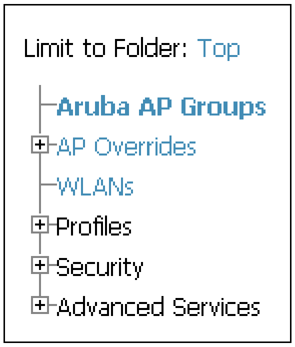
- Aruba Configuration components are summarized in "Additional Concepts and Components of Aruba Configuration" on page 21.
- For procedures that use several of these components, refer to earlier chapters in this document.
- For architectural information about ArubaOS (AOS), refer to the *AOS User Guide*.

NOTE

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

Access all pages and field descriptions in this appendix from the **Device Setup > Aruba Configuration** page, illustrated in Figure 32. The one exception is the additional **Groups > Aruba Config** page that you access from the standard AWMS navigation menu.

Figure 32 *Aruba Configuration Components*



This appendix describes Aruba Configuration components with the following organization and topics:

Aruba AP Groups Pages and Field Descriptions

- Aruba AP Groups

AP Overrides Pages and Field Descriptions

- AP Overrides

WLAN Pages and Field Descriptions

- Overview of WLANs in Aruba Configuration
- WLANs
- WLANs > Basic
- WLANs > Advanced

Profiles Pages and Field Descriptions

- Understanding Aruba Configuration Profiles
- Profiles > AAA
  - Profiles > AAA > Captive Portal Auth

  - Profiles > AAA > Mac Auth
  - Profiles > AAA > Stateful 802.1X Auth
  - Profiles > AAA > Wired Auth
  - Profiles > AAA > VPN Auth
  - Profiles > AAA > Management Auth
  - Profiles > AAA > 802.1x Auth
  - Profiles > AAA > Stateful NTLM Auth
  - Profiles > AAA > WISPr Auth
- Profiles > AP
  - Profiles > AP > System
  - Profiles > AP > Regulatory Domain
  - Profiles > AP > AP Wired
  - Profiles > AP > AP Ethernet Link
  - Profiles > AP > SNMP
    - Profiles > AP > SNMP > SNMP User
- Profiles > IDS
  - Profiles > IDS > General
  - Profiles > IDS > Signature Matching
    - Profiles > IDS > Signature Matching > Signatures
  - Profiles > IDS > Denial of Service
    - Profiles > IDS > Denial of Service > Rate Threshold
  - Profiles > IDS > Impersonation
  - Profiles > IDS > Unauthorized Device
- Profiles > Mesh
  - Profiles > Mesh > Radio
  - Profiles > Mesh > Radio > Mesh HT SSID
  - Profiles > Mesh > Cluster
- Profiles > QoS
  - Profiles > QoS > Traffic Management
  - Profiles > QoS > VoIP Call Admission Control
  - Profiles > QoS > WMM Traffic Management
- Profiles > RF
  - Profiles > RF > 802.11a/g Radio
    - Profiles > RF > 802.11a/g Radio > ARM
    - Profiles > RF > 802.11a/g Radio > High-Throughput (HT) Radio
  - Profiles > RF > Event Thresholds
  - Profiles > RF > Optimization
- Profiles > SSID
  - Profiles > SSID > EDCA AP
  - Profiles > SSID > EDCA Station
  - Profiles > SSID > HT SSID
  - Profiles > SSID > 802.11K

Security Pages and Field Descriptions

Advanced Services Pages and Field Descriptions

Groups > Aruba Config Page and Section Information

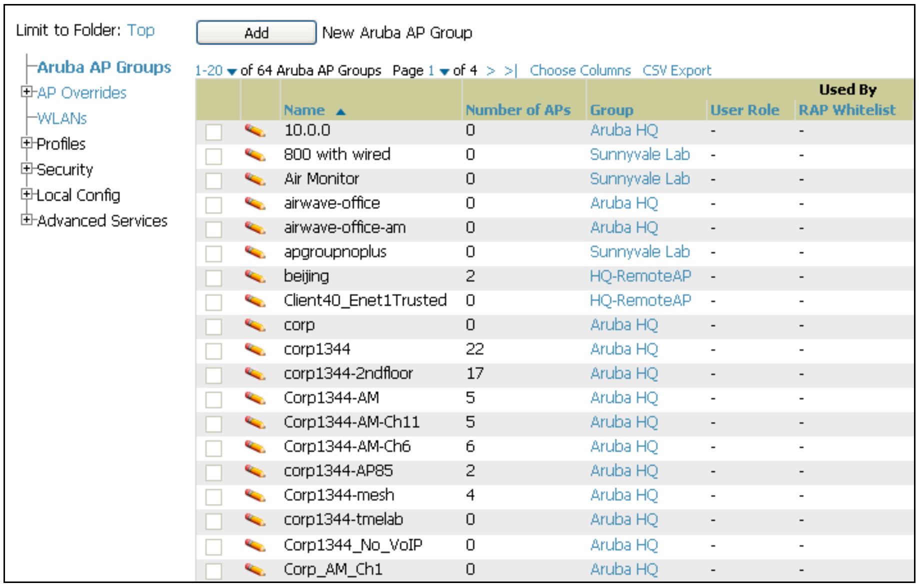
Aruba AP Groups Pages and Field Descriptions

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

Aruba AP Groups

The **Aruba AP Groups** page displays all configured Aruba AP Groups and enables you to add or edit Aruba AP Groups. For additional information about using this page, refer to "General Aruba AP Groups Procedures and Guidelines" on page 34. Figure 33 illustrates this page and location.

Figure 33 ***Aruba AP Groups*** *Navigation and Page*



Limit to Folder: Top

Add New Aruba AP Group

- Aruba AP Groups
- ⊞ AP Overrides
- WLANs
- ⊞ Profiles
- ⊞ Security
- ⊞ Local Config
- ⊞ Advanced Services

1-20 ▾ of 64 Aruba AP Groups Page 1 ▾ of 4 > >| Choose Columns CSV Export

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

The **Aruba AP Groups** page displays the following information for every group currently configured:

Table 3 ***Device Setup > Aruba Configuration > Aruba AP Groups*** *Page*

Column	Description
Name	Displays the name of the Aruba AP Group. Click the pencil icon next to any group to edit.
(Used by) Group	Displays the AWMS device groups that define this Aruba AP Group. Click the name of any group in this column to display the detailed **Groups > Aruba Config** page. The device groups in this column receive the profile configurations from the associated Aruba AP Group. Any Aruba AP Group profiles can define device groups.
(Used by) Number of AP	Displays the number of APs in this Aruba 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 Aruba AP Group, when defined.
Folder	Displays the folder that is associated with this Aruba 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 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.

Click **Add** to create a new Aruba AP Group, or click the pencil icon next to an existing Aruba AP Group to edit that group. The **Add/Edit Aruba AP Group** page contains the following fields, describes in Table 4.

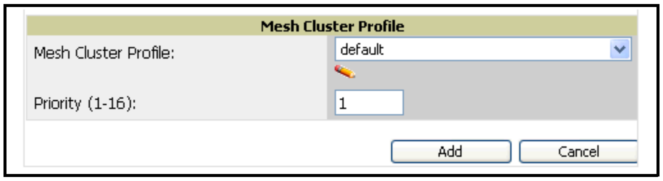
Table 4 ***Device Setup > Aruba Configuration > Aruba AP Groups*** *Details, Settings and Default Values*

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	N/A	Click this link to create a new WLAN to support Aruba Configuration. Once created, that new WLAN will appear with others on this page.
Show only selected	N/A	To set the WLANs that appear on this page, select (check) the desired WLANs, then click **Show Only Selected**.
Select WLANs	No WLANs selected by default	Displays the WLANs currently present in Aruba Configuration. 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 of the **Aruba Configuration** tool.
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. Click the **pencil** icon next to this field to edit or create additional profile settings in the **RF > 802.11a/g Radio** page of **Aruba Configuration**. Click **Save** on this page to return to the **Add AP Group** page.
802.11g Radio Profile	2.4_am	Defines AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Each 802.11a and 802.11b radio profile includes a reference to an Adaptive Radio Management (ARM) profile. If you would like the ARM feature to select dynamically the best channel and transmission power for the radio, verify that the 802.11a/802.11g radio profile references an active and enabled ARM profile. If you want to manually select a channel for each AP group, create separate 802.11a and 802.11g profiles for each AP group and assign a different transmission channel for each profile. The drop-down menu displays these options: ● **default** ● **nchannel too high** ● **nchannel too low** Click the **pencil** icon next to this field to edit profile settings in the **RF > 802.11a/g Radio** page of **Aruba Configuration**. Click **Save** on this page to return to the **Add AP Group** 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. Click the **pencil** icon next to this field to display the **Profiles > RF** section of **Aruba Configuration**, and edit these settings as desired. Click **Save** on this page to return to the **Add AP Group** page.
Event Thresholds Profile	default	Defines error event conditions, based on a customizable percentage of low-speed frames, non-unicast frames, or fragmented, retry or error frames. The drop-down menu displays these options: ● **default** ● all additional RF profiles currently configured in Aruba Configuration Click the **pencil** icon next to this field to display the **Profiles > RF > Events Threshold** section of **Aruba Configuration**, and edit these settings as desired. Click **Save** on this page to return to the **Add AP Group** page.

Table 4 ***Device Setup > Aruba Configuration > Aruba AP Groups*** *Details, Settings and Default Values (Continued)*

Field	Default	Description
Wired AP Profile	default	Controls whether 802.11 frames are tunneled to the controller using Generic Routing Encapsulation (GRE) tunnels, bridged into the local Ethernet LAN (for remote APs), or a configured for combination of the two (split-mode). This profile also configures the switching mode characteristics for the port, and sets the port as either trusted or untrusted. Click the **pencil** icon next to this field to display the **Profiles > AP > Wired** page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page.
Ethernet Interface 0 Link Profile	default	Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 0. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link. Click the **pencil** icon next to this field to display the **Profiles > AP > Ethernet Link** details page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page.
Ethernet Interface 1 Link Profile	default	Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 1. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link. Click the **pencil** icon next to this field to display the **Profiles > AP > Ethernet Link** details page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page.
AP System Profile	default	Defines administrative options for the controller, including the IP addresses of the local, backup, and master controllers, Real-time Locating Systems (RTLS) server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps. This field is a drop-down menu with the following options: ● **Non-integer RTLS Server Station Message Frequency** ● **Too-high RTLS Server Port** ● **Too-low AeroScout RTLS Server Port** ● **Too-low RTLS Server Port** Click the **pencil** icon next to this field to display the **Profiles > AP > System** details page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page.
Regulatory Domain Profile	default	Defines an AP's country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios. Click the **pencil** icon next to this field to display the **Profiles > AP > Regulatory Domain** page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page.
SNMP Profile	default	Selects the SNMP profile to associate with this AP group. The drop-down menu lists all SNMP profiles currently enabled in AWMS. Click the **pencil** icon next to this field to display the **Profiles > AP > SNMP** page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page.
VoIP Call Admission Control Profile	default	Aruba'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. Click the **pencil** icon next to this field to display the **Profiles > AP > Regulatory Domain** page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page.
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.

Table 4 ***Device Setup > Aruba Configuration > Aruba AP Groups*** *Details, Settings and Default Values (Continued)*

Field	Default	Description
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	Selects the IDS profile to be associated with the new AP Group. The drop-down menu contains these options: ● **ids-disabled** ● **ids-high-setting** ● **ids -low-setting** ● **ids-medium-setting** The IDS profiles configure the AP's Intrusion Detection System features, which detect and disable rogue APs and other devices that can potentially disrupt network operations. An AP is considered to be a rogue AP if it is both unauthorized and plugged into the wired side of the network. An AP is considered to be an interfering AP if it is seen in the RF environment but is not connected to the wired network. Click the **pencil** icon next to this field to display the **Profiles > IDS** page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page.
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	N/A	Click to display a new **Mesh Cluster Profile** section to this page, as illustrated in Figure 36. **Figure 34** ***Add New Mesh Cluster Profile*** *Illustration*  Mesh Cluster Profile Mesh Cluster Profile: default Priority (1-16): 1 This section has two fields, as follows: ● **Mesh Cluster Profile**—Drop-down menu displays all supported profiles. Select one from the menu. ● **Priority (1-16)**—Type in the priority number for this profile. The priority may be any integer between 1 to 16. Complete these fields, click the **Add** button, and the profile displays as an option in the **Mesh Cluster Profile** section, which may be selected for the AP Group to be added or edited.

Click **Add** to complete the creation or click **Save** to complete the editing of the Aruba AP Group. This group now appears in the navigation pane of the Aruba Configuration page.

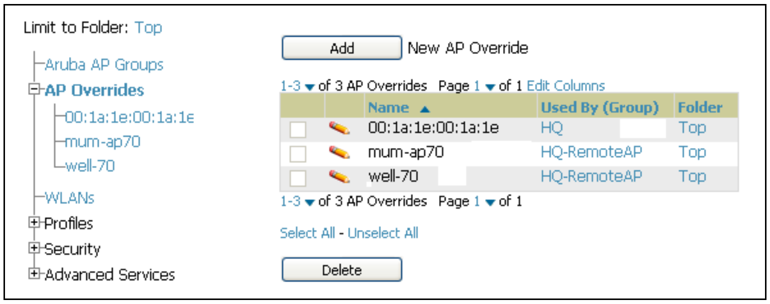
AP Overrides Pages and Field Descriptions

The **AP Overrides** component of Aruba Configuration allow you to define device-specific settings for an AP device without having to remove that device from an existing Aruba AP Group or create a new Aruba AP Group specifically for that device. The **AP Overrides** page is for custom AP devices that otherwise comply with most settings in the Aruba 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 35 AP Overrides *Page*



Limit to Folder: Top

- Aruba AP Groups
- AP Overrides
  - 00:1a:1e:00:1a:1e
  - mum-ap70
  - well-70
- WLANs
- Profiles
- Security
- Advanced Services

Add New AP Override

1-3 ▾ of 3 AP Overrides Page 1 ▾ of 1 Edit Columns

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

1-3 ▾ of 3 AP Overrides Page 1 ▾ of 1

Select All - Unselect All

Delete

Table 5 describes the fields on this page.

Table 5 ***AP Overrides*** *Field 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 Aruba AP Group in which this AP Override applies. Additional details about the Aruba AP Group appear on the **Groups > Aruba 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.

Click **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 6 describes the fields on the **AP Overrides > Add/Edit Details** page.

Table 6 ***Aruba Configuration*** *>* ***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. 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.
WLANs		
WLANs	N/A	This section lists the WLANs currently defined in Aruba Configuration by default. You can display selected WLANs or all WLANs. Select one or more WLANs for which AP Override is to apply.

Table 6 ***Aruba Configuration > AP Overrides Add*** *or* ***Edit*** *Page Fields*

Field	Default	Description
Excluded WLANs		
Excluded WLANs	N/A	This section displays WLANs currently defined in Aruba Configuration by default. This section can display selected WLANs or all WLANs. Use this section to specify which WLANs are ***not*** to support **AP Override**.
Referenced Profiles		
802.11a Radio Profile	5_am	Defines AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Click the **pencil** icon next to this field to edit or create additional profile settings in the **RF > 802.11a/g Radio** page of **Aruba Configuration**. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > RF > 802.11a/g Radio" on page 116.
802.11g Radio Profile	2.4_am	Defines AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Each 802.11a and 802.11b radio profile includes a reference to an Adaptive Radio Management (ARM) profile. If you would like the ARM feature to select dynamically the best channel and transmission power for the radio, verify that the 802.11a/802.11g radio profile references an active and enabled ARM profile. If you want to manually select a channel for each AP group, create separate 802.11a and 802.11g profiles for each AP group and assign a different transmission channel for each profile. The drop-down menu displays these options: ● **default** ● **nchannel too high** ● **nchannel too low** Click the **pencil** icon next to this field to edit or create additional profile settings in the **RF > 802.11a/g Radio** page of **Aruba Configuration**. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > RF > 802.11a/g Radio" on page 116.
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. Click the **pencil** icon next to this field to display the **Profiles > RF** section of **Aruba Configuration**, and edit these settings as desired. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > RF > 802.11a/g Radio" on page 116.
Event Thresholds Profile	default	Defines error event conditions, based on a customizable percentage of low-speed frames, non-unicast frames, or fragmented, retry or error frames. The drop-down menu displays these options: ● **default** ● all additional RF profiles currently configured in Aruba Configuration Click the **pencil** icon next to this field to display the **Profiles > RF > Events Threshold** section of **Aruba Configuration**, and edit these settings as desired. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > RF > Event Thresholds" on page 123.

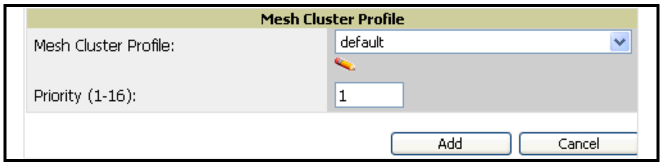
Table 6 ***Aruba Configuration > AP Overrides Add** or **Edit** Page Fields*

Field	Default	Description
Wired AP Profile	default	Controls whether 802.11 frames are tunneled to the controller using Generic Routing Encapsulation (GRE) tunnels, bridged into the local Ethernet LAN (for remote APs), or a configured for combination of the two (split-mode). This profile also configures the switching mode characteristics for the port, and sets the port as either trusted or untrusted. Click the **pencil** icon next to this field to display the **Profiles > AP > Wired** page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > AP > AP Wired" on page 88.
Ethernet Interface 0 Link Profile	default	Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 0. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link. Click the **pencil** icon next to this field to display the **Profiles > AP > Ethernet Link** details page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > AP > AP Ethernet Link" on page 90.
Ethernet Interface 1 Link Profile	default	Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 1. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link. Click the **pencil** icon next to this field to display the **Profiles > AP > Ethernet Link** details page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > AP > AP Ethernet Link" on page 90.
AP System Profile	default	Defines administrative options for the controller, including the IP addresses of the local, backup, and master controllers, Real-time Locating Systems (RTLS) server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps. This field is a drop-down menu with the following options: ● **Non-integer RTLS Server Station Message Frequency** ● **Too-high RTLS Server Port** ● **Too-low AeroScout RTLS Server Port** ● **Too-low RTLS Server Port** Click the **pencil** icon next to this field to display the **Profiles > AP > System** details page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > AP > System" on page 83.
Regulatory Domain Profile	default	Defines an AP's country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios. Click the **pencil** icon next to this field to display the **Profiles > AP > Regulatory Domain** page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > AP > Regulatory Domain" on page 87.

Table 6 ***Aruba Configuration > AP Overrides Add** or **Edit** Page Fields*

Field	Default	Description
SNMP Profile	default	Selects the SNMP profile to associate with this AP group. The drop-down menu lists all SNMP profiles currently enabled in AWMS. Click the **pencil** icon next to this field to display the **Profiles > AP > SNMP** page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > AP > SNMP" on page 90.
VoIP Call Admission Control Profile	default	Aruba'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. Click the **pencil** icon next to this field to display the **Profiles > AP > Regulatory Domain** page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > AP > SNMP" on page 90.
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. For additional information, refer to "Profiles > QoS > Traffic Management" on page 112
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. For additional information, refer to "Profiles > QoS > Traffic Management" on page 112
IDS Profile	default	Selects the IDS profile to be associated with the new AP Group. The drop-down menu contains these options: ● **ids-disabled** ● **ids-high-setting** ● **ids -low-setting** ● **ids-medium-setting** The IDS profiles configure the AP's Intrusion Detection System features, which detect and disable rogue APs and other devices that can potentially disrupt network operations. An AP is considered to be a rogue AP if it is both unauthorized and plugged into the wired side of the network. An AP is considered to be an interfering AP if it is seen in the RF environment but is not connected to the wired network. Click the **pencil** icon next to this field to display the **Profiles > IDS** page of **Aruba Configuration**, and adjust these settings as desired. Click **Save** on this page to return to the **Add AP Group** page. For additional information, refer to "Profiles > IDS" on page 94
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. For additional information, refer to "Profiles > Mesh" on page 107.

Table 6 ***Aruba Configuration* > *AP Overrides Add* or *Edit* Page Fields**

Field	Default	Description
Mesh Cluster Profiles		
Add New Mesh Cluster Profile	The **Add Mesh Cluster Profile** section is hidden by default, until the **Add** button is clicked.	Clicking this **Add** button displays a new **Mesh Cluster Profile** section to this page, as illustrated in Figure 36. **Figure 36 *Add New Mesh Cluster Profile* Illustration**  Mesh Cluster Profile Mesh Cluster Profile: default Priority (1-16): 1 This section has two fields, as follows: - **Mesh Cluster Profile**—Drop-down menu displays all supported profiles. Select one from the menu. - **Priority (1-16)**—Type in the priority number for this profile. The priority may be any integer between 1 to 16. Complete these fields, click the **Add** button, and the profile displays as an option in the **Mesh Cluster Profile** section, which may be selected for the AP Group to be added or edited. For additional information about Mesh Cluster profiles, refer to these sections: - "Profiles > Mesh" on page 107 - "Profiles > Mesh > Cluster" on page 111.
Excluded Mesh Cluster Profiles		
Excluded Mesh Cluster Profiles		If required, select one or more Mesh Cluster profiles from this field. This field can display all Mesh Cluster profiles or can display only selected Mesh Cluster profiles. For additional information about Mesh Cluster profiles, refer to "Profiles > Mesh > Cluster" on page 111.

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

WLAN Pages and Field Descriptions

Overview of WLANs in Aruba 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 User Guide* for additional information.

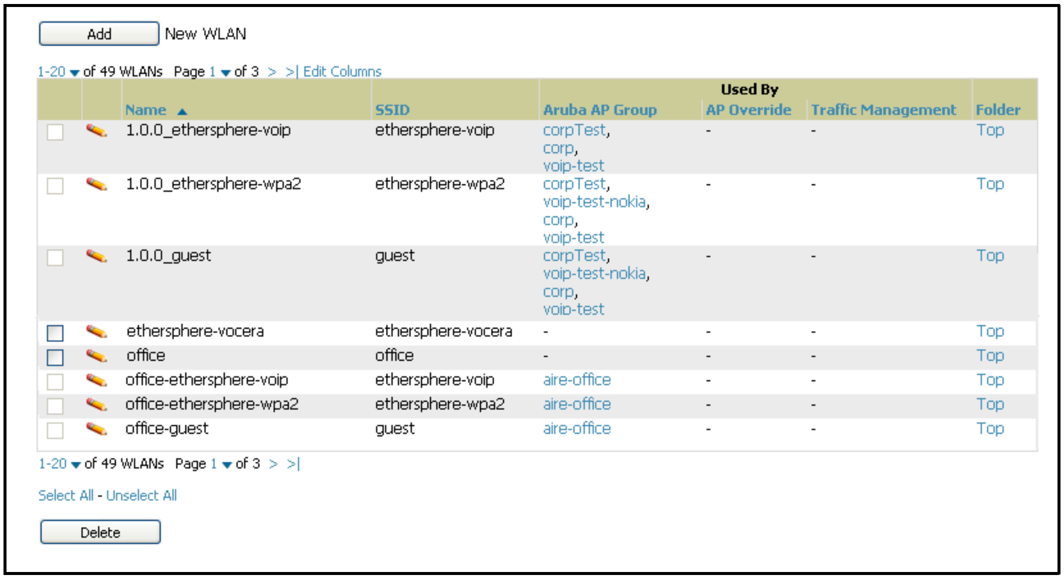
Use the following guidelines when configuring and using WLANs in Aruba Configuration:

- The **Device Setup > Aruba Configuration** navigation pane displays custom-configured WLANs and Aruba AP Groups. All other components of the navigation pane are standard across all deployments of Aruba Configuration.
- You define or modify WLANs on the **Device Setup > Aruba 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, AWMS 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 Aruba Configuration and enables you to add or edit WLANs. For additional information about using this page, refer to "General WLAN Procedures and Guidelines" on page 37. Figure 33 illustrates this page and location.

Figure 37 ***WLANs** Navigation and Page*



Add New WLAN

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

				Used By		
		Name ▲	SSID	Aruba AP Group	AP Override	Traffic Management	Folder
□	✎	1.0.0_ethersphere-voip	ethersphere-voip	corpTest, corp, voip-test	-	-	Top
□	✎	1.0.0_ethersphere-wpa2	ethersphere-wpa2	corpTest, voip-test-nokia, corp, voip-test	-	-	Top
□	✎	1.0.0_guest	guest	corpTest, voip-test-nokia, corp, voip-test	-	-	Top
□	✎	ethersphere-vocera	ethersphere-vocera	-	-	-	Top
□	✎	office	office	-	-	-	Top
□	✎	office-ethersphere-voip	ethersphere-voip	aire-office	-	-	Top
□	✎	office-ethersphere-wpa2	ethersphere-wpa2	aire-office	-	-	Top
□	✎	office-guest	guest	aire-office	-	-	Top

1-20 ▾ of 49 WLANs Page 1 ▾ of 3 > >|

Select All - Unselect All

Delete

The **Aruba Configuration > WLANs** page contains additional information as described in Table 7:

Table 7 ***Aruba Configuration** > **WLANs** Page Field Descriptions*

Field	Description
Name	Lists the name of the WLAN.
SSID	Lists the SSID currently defined for the WLAN.
Aruba AP Group	Lists the Aruba 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 Aruba 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 Aruba 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 8 describes the fields for this page.

Table 8 ***Aruba Configuration* > *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. 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.
SSID	N/A	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 > EDCA AP" on page 127.
Radio Type	N/A	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 69.
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 141.

Click **Add** to create the WLAN, or click **Save** to finish reconfiguring an existing WLAN. The WLAN appears on the **WLANs** page in the Aruba 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 63.

WLANs > Advanced

From the **Aruba 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 9 describes the fields for this page.

Table 9 ***Aruba Configuration > 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. 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	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 > EDCA AP" on page 127.
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" on page 67.
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	N/A	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 controller 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 9 *Aruba Configuration > WLANs > Advanced Page Fields* (Continued)

Field	Default	Description
HA Discovery on Association	No	Enable or disable HA discovery on Association. In normal circumstances a controller performs an HA discovery only when it is aware of the client's IP address which it learns through the ARP or any L3 packet from the client. This limitation of learning the client's IP and then performing the HA discovery is not effective when the client performs an inter switch move silently (does not send any data packet when in power save mode). This behavior is commonly seen with various handheld devices, Wi-Fi phones, etc. This delays HA discovery and eventually resulting in loss of downstream traffic if any meant for the mobile client. With HA discovery on association, a controller can perform a HA discovery as soon as the client is associated. This feature can be enabled using the `ha-disc-on assoc` parameter in the WLAN `virtual <ap-profile>` command. By default, this feature is disabled. You can enable this on virtual APs with devices in power-save mode and requiring mobility. This option will also poll for all potential HAs.
DoS Prevention	No	Enable or disable DoS prevention functions, as defined in virtual AP profiles.
Station Blacklisting	Yes	Enable or disable DoS prevention functions, as defined in virtual AP profiles. The blacklisting option can be used to prevent access to clients that are attempting to breach the security. When a client is blacklisted in the Aruba system, the client is not allowed to associate with any AP in the network for a specified amount of time. If a client is connected to the network when it is blacklisted, a de-authentication message is sent to force the client to disconnect. While blacklisted, the client cannot associate with another SSID in the network.
Blacklist Time	3600	If station blacklisting is enabled, specify the time in seconds for which blacklisting is enabled. When a client is blacklisted in the Aruba system, the client is not allowed to associate with any AP in the network for a specified amount of time.
Authentication Failure Blacklist Time	3600	You can configure a maximum authentication failure threshold in seconds for each of the following authentication methods: ● 802.1x ● MAC ● Captive portal ● VPN When a client exceeds the configured threshold for one of the above methods, the client is automatically blacklisted by the controller, an event is logged, and an SNMP trap is sent. By default, the maximum authentication failure threshold is set to 0 for the above authentication methods, which means that there is no limit to the number of times a client can attempt to authenticate. With 802.1x authentication, you can also configure blacklisting of clients who fail machine authentication. **NOTE:** This requires that the External Services Interface (ESI) license be installed in the controller. **NOTE:** When clients are blacklisted because they exceed the authentication failure threshold, they are blacklisted indefinitely by default. You can configure the duration of the blacklisting;
Fast Roaming	No	Fast roaming is a component of virtual AP profiles in which client devices are allowed to roam from one access point to another without requiring reauthentication by the main RADIUS server.
Strict Compliance	No	Define whether clients should have strict adherence to settings on this page for network access.
VLAN Mobility	No	Define whether clients in the WLAN and VLAN should have mobility or roaming privileges.

Table 9 ***Aruba Configuration*** **>** ***WLANs*** **>** ***Advanced*** *Page Fields (Continued)*

Field	Default	Description
Remote AP Operation	standard	Define the rights for remote APs in this WLAN. Options are as follows: - standard - persistent - backup - always Remote APs connect to a controller 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. For example, voice over IP (VoIP) applications can be extended to remote sites while the servers and the PBX remain secure in the corporate office. Secure Remote Access Point Service can also be used to secure control traffic between an AP and the controller in a corporate environment. In this case, both the AP and controller are in the company's private address space.
Drop Broadcast and Multicast	No	Specify whether the WLAN should drop broadcast and multicast mesh network advertising on the WLAN.
Convert Broadcast ARP Requests to Unicast	No	Specify whether ARP table information should be distributed in broadcast (default) or unicast fashion.
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.

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

The alternate way to create or edit WLANs is from the **Basic** page.

Profiles Pages and Field Descriptions

Understanding Aruba Configuration Profiles

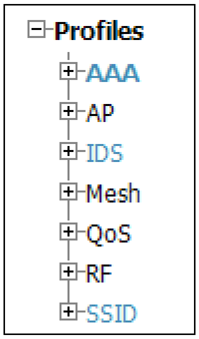
In ArubaOS, related configuration parameters are grouped into a profile that you can apply as needed to an AP group or to individual APs. This section lists each category of AP profiles that you can configure and then apply to an AP group or to an individual AP. Note that some profiles reference other 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. See Figure 39. For additional details and configuration instructions, continue to the related procedures in this section.

Perform the following initial steps to configure profiles.

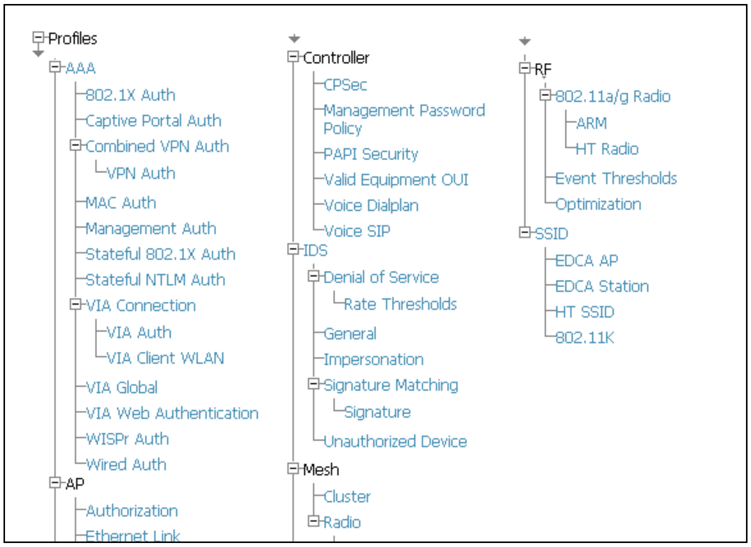
1. Browse to the **Device Setup > Aruba Configuration** page, and click the **Profiles** heading in the navigation pane on the left. Figure 38 illustrates general profile categories.

Figure 38 ***Profiles*** *in the* ***Aruba Configuration*** *Navigation Pane*



2. Expand the **Profiles** menu by clicking the plus sign (**+**) next to it. Several profile options appear, as illustrated in Figure 39.

Figure 39 ***Profile*** *Navigation Pane of AWMS* ***Aruba Configuration***



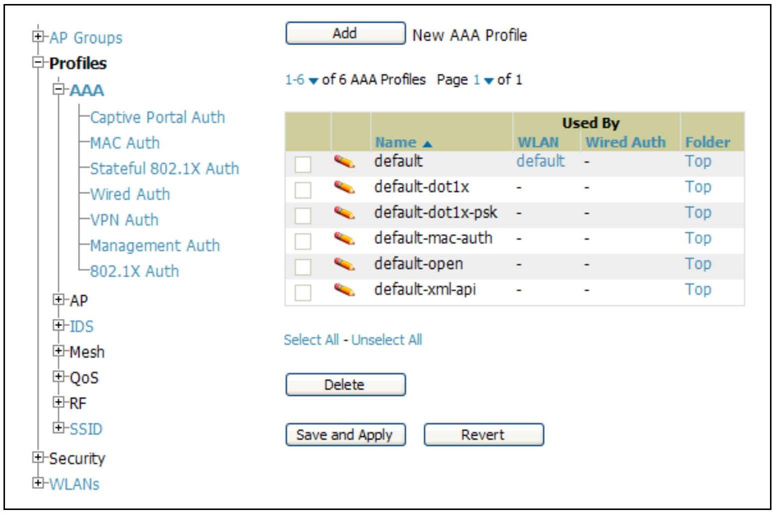
This document section describes the profiles and settings supported in Aruba Configuration.

Profiles > AAA

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. To view and configure AAA profiles, click the **AAA** profile heading in the navigation pane. The **AAA Profiles** page appears and lists the current profiles. Figure 40 illustrates this page.

Figure 40 ***AAA Profiles*** *Page of* ***Aruba Configuration***



			Used By		
		Name ▲	WLAN	Wired Auth	Folder
□	✎	default	default	-	Top
□	✎	default-dot1x	-	-	Top
□	✎	default-dot1x-psk	-	-	Top
□	✎	default-mac-auth	-	-	Top
□	✎	default-open	-	-	Top
□	✎	default-xml-api	-	-	Top

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 68.
- ***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 69.
- ***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 71.
- ***Stateful 802.11 Auth***—Enables or disables 802.1x authentication for clients on non-Aruba 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 72.
- ***Wired Auth***—This profile merely references an AAA profile to be used for wired authentication. Refer to "Profiles > AAA > Wired Auth" on page 73.
- ***VPN Auth***—Identifies the default role for authenticated VPN clients. This profile also references a server group. Refer to "Profiles > AAA > VPN Auth" on page 73.
- ***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 74.
- ***802.1x Auth***—Manages settings for the 802.11k protocol. In a 802.1k network, if the AP with the strongest signal is reaches its maximum capacity, clients may connect to an under utilized AP with a weaker signal under utilized APs. Refer to "Profiles > AAA > 802.1x Auth" on page 75.
- ***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 80.

- ***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 81.

Profiles > AAA

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

1. Click **Profiles > AAA** in the **Aruba Configuration Navigation** pane.
2. Click the **Add** button to create a new **AAA** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 11.

Table 10 ***Captive Portal Auth*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the AAA profile.
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 71 if required.
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 > 802.1x Auth" on page 75.
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. Click the add icon to create a new RADIUS server group.
Other Settings		
Initial Role	ap-role	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	ap-role	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.

Table 10 ***Captive Portal Auth*** *Profile Settings*

Field	Default	Description
802.1X Authentication Default Role	ap-role	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 controller 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. Click 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.
XML API Servers		
XML API Servers	N/A	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	N/A	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. Click **Add** or **Save.** The added or edited **AAA** profile appears on the **AAA Profiles** 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. Click **Profiles > AAA > Captive Portal Auth** in the **Aruba Configuration Navigation** pane.
2. Click the **Add** button to create a new **Captive Portal Auth** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 11.

Table 11 ***Captive Portal Auth*** *Profile Settings*

Field	Default	Description
General Settings		

Table 11 ***Captive Portal Auth*** *Profile Settings*

Field	Default	Description
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the Captive Port 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.
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 sec)	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.
Show FQDN	No	Allows the user to see and select the fully-qualified domain name (FQDN) on the login page.
Use CHAP (Non-standard)	No	Use CHAP protocol. You should not use this option unless instructed to do so by an Aruba representative.
Sygate-on-demand-agent	No	Enables client remediation with Sygate-on-demand-agent (SODA).
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.

Table 11 ***Captive Portal Auth*** *Profile Settings*

Field	Default	Description
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.
Adding Switch IP Address in Redirection URL	No	Select this option to send the controller's IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the controller from which a request originated by parsing the 'switchip' variable in the URL.

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

Modifying the Initial User Role

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 > 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 controller 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. Click **Profiles > AAA > Mac Auth** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Mac Auth** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 12:

Table 12 ***Aruba Configuration > Profiles > AAA > MAC Auth*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the MAC Auth profile.
Other Settings		
Delimiter	none	Delimiter used in the MAC string: ● 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
Case	lower	The case (upper or lower) used in the MAC string.

Table 12 *Aruba Configuration > Profiles > AAA > MAC Auth Profile Settings*

Field	Default	Description
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. Click **Add** or **Save.** The added or edited **Mac Auth** profile appears on the **AAA Profiles** 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-Aruba 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. Click **Profiles > AAA > Stateful 802.11 Auth** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Stateful 802.11 Auth** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings described in Table 13:

Table 13 *Aruba Configuration > Profiles > AAA > Stateful 802.1X Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
Referenced Profiles		
Server Group	N/A	Select the AAA authentication server group. Click 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. Click **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 merely references an AAA profile to be used for wired authentication.

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

1. Click **Profiles > AAA > Wired Auth** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Wired Auth** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 14:

Table 14 ***Aruba Configuration > Profiles > AAA > Wired Auth*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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. Click the pencil icon to edit an existing profile or click the add icon to create a new profile.

3. Click **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 > 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 controller 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 controller. The authentication server can be any type of server supported by the controller, including the controller's internal database.

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

1. Click **Profiles > AAA > VPN Auth** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **VPN Auth** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 15:

Table 15 ***Aruba Configuration > Profiles > AAA > VPN Auth*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
Referenced Profiles		
Server Group	N/A	Select the AAA authentication server group. Click 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	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.

3. Click **Add** or **Save**. The added or edited **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 controller to monitor, manage, or configure the Aruba 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. Click **Profiles > AAA > Management Auth** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Management Auth** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 16:

Table 16 ***Aruba Configuration > Profiles > AAA > Management Auth*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.

Table 16 ***Aruba Configuration > Profiles > AAA > Management Auth*** *Profile Settings*

Field	Default	Description
Referenced Profiles		
Server Group	N/A	Select the AAA authentication server group. Click 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 role to be associated with this authentication profile.
Enable	No	When enabled with **Yes**, this setting activates the authentication server.

3. Click **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 > 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 Aruba 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 Aruba controller 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 controller.
- 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 Aruba user-centric networks, you can terminate the 802.1x authentication on the controller. The controller 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. Click **Profiles > AAA > 802.1x Auth** in the **Aruba Navigation** pane. The details page summarizes the current profiles of this type.
2. Click the **Add** button to create a new **802.1x Auth** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 17:

Table 17 ***Aruba Configuration > Profiles > AAA > 802.1x Auth*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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. Role Assignment with Machine Authentication Enabled When you enable machine authentication, there are two additional roles you can define in the 802.1x authentication profile: • 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 polices 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 controller. This setting requires a policy enforcement firewall license.
Blacklist on Machine Authentication Failure	No	Define whether the user is blacklisted upon authentication failure. This setting requires a policy enforcement firewall license.

Table 17 ***Aruba Configuration > Profiles > AAA > 802.1x Auth*** *Profile Settings (Continued)*

Field	Default	Description
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.
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.

Table 17 *Aruba Configuration > Profiles > AAA > 802.1x Auth* Profile Settings (Continued)

Field	Default	Description
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	Full field name is **Delay between EAP-Success and WPA2 Unicast Key Exchange**. 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 t his 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.
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.

Table 17 *Aruba Configuration > Profiles > AAA > 802.1x Auth* Profile Settings (Continued)

Field	Default	Description
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 controller.
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 controller 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 controller 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	N/A	Type the CA certificate imported into the controller.
Server-Certificate	N/A	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 controller 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 17 ***Aruba Configuration* > *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.

3. Click **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 > 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 156.

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

1. Click **Profiles > AAA > Stateful NTLM Auth** in the **Aruba Navigation** pane. The details page summarizes the current profiles of this type.
2. Click the **Add** button to create a new **Stateful NTLM Auth** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 18:

Table 18 ***Aruba Configuration > Profiles > AAA > Stateful NTLM Auth*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
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	guess	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.

3. Click **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.

ArubaOS 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 controller 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 User Guide* for additional information about stateful NTLM and WISPr authentication.

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

1. Click **Profiles > AAA > WISPr Auth** in the **Aruba Navigation** pane. The details page summarizes the current profiles of this type.
2. Click the **Add** button to create a new **Stateful NTLM Auth** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 18:

Table 19 ***Aruba Configuration > Profiles > AAA > WISPr Auth*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
Other Settings		
Server Group	default	Select the AAA authentication server group. Click 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.
Logon Wait Minimum Wait	5	Define the minimum wait time for additional logon attempts. If the controller'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 controller'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	N/A	Enter the ISO Country Code section of the WISPr Location ID.
WISPr Location-ID E.164 Area Code	N/A	Enter the E.164 Area Code section of the WISPr Location ID.
WISPr Location-ID SSID/zone	N/A	Enter the SSID/Zone section of the WISPr Location ID.
WISPr Operator Name	N/A	Enter a name identifying the hotspot operator.
WISPr Location Name	N/A	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. Click **Add** or **Save**. The added or edited profile appears on the **Stateful NTLM Auth** page, and on the details page.

Profiles > AP

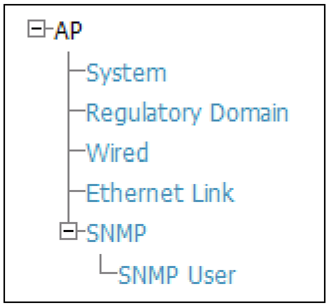
Display the currently configured AP profiles by navigating to **Device Setup > Profiles > AP**.

In AOS, 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. To view and configure AP profiles, click the **AP** profile heading in the navigation pane.

Figure 41 ***AP Profiles** in **Aruba 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:
   - ***System***—Defines administrative options for the controller, including the IP addresses of the local, backup, and master controllers, Real-time Locating Systems (RTLS) server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps. Refer to "Profiles > AP > System" on page 83
   - ***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 87.
   - ***Wired***—Controls whether 802.11 frames are tunneled to the controller using Generic Routing Encapsulation (GRE) tunnels, bridged into the local Ethernet LAN (for remote APs), or a configured for combination of the two (split-mode). This profile also configures the switching mode characteristics for the port, and sets the port as either trusted or untrusted. Refer to "Profiles > AP > AP Wired" on page 88.
   - ***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 > AP Ethernet Link" on page 90.
   - ***SNMP***—Defines and enables SNMP settings, to include community string and SNMP user profiles. "Profiles > AP > SNMP" on page 90.
   - ***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 91.

Profiles > AP > System

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

If the remote AP loses connectivity on the IPSec tunnel to the controller, the remote AP establishes connectivity with a backup controller 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 controller 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. Click **Profiles > AP > System** in the **Aruba Navigation** pane. This page summarizes the current profiles of this type.
2. Click the **Add** button to create a new **System** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 20:

Table 20 ***Aruba Configuration > Profiles > AP > System*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
Other Settings		
LMS IP	N/A	Enter an IP address. For those APs that need to boot off the local controller, configure the LMS IP address to point to the new local controller.
Backup LMS IP	N/A	Enter the IP address of the backup LMS controller.
LMS Preemption	No	The AP fallback feature allows an AP associated with the backup controller (backup LMS) to fail back to the primary controller (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 controller.
Master Controller IP Address	N/A	Enter the IP address of the master controller.
LED Operating Mode	normal	Specify the LED operating mode for AP-12X controllers. 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.
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 controller and the AP (wired traffic and traffic from a split-tunneled SSID) are always encrypted in the IPSec tunnel.
Native VLAN ID (0-4094)	1	Enter the ID of the native VLAN. The supported range is from 0 to 4094.
SAP MTU	N/A	Specify the Service Access Point (SAP) maximum transmission unit (MTU) in bytes. The range is 1024 to 1578 bytes.

Table 20 ***Aruba Configuration* > *Profiles* > *AP* > *System*** *Profile Settings (Continued)*

Field	Default	Description
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. Aruba recommends the default maximum request retries and bootstrap threshold settings for most mesh networks; 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 controller.
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, Aruba recommends a value of 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	N/A	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	N/A	Enter the IP address of the RFProtect server.
RFprotect Backup Server IP	N/A	Enter an IP address. When an Aruba controller is present in an Aruba RFprotect system, an Aruba AP that is acting as an RFprotect sensor can be configured and managed from the controller. As a Managed Sensor, the Aruba AP is managed by the controller 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 Aruba controller uses an Ortonics walljack. Ortronics® Wi-Jack™ and Wi-Jack Duo™ thin client access points are centrally configured and managed by the Aruba Networks wireless controllers 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 20 ***Aruba Configuration > Profiles > AP > System*** *Profile Settings (Continued)*

Field	Default	Description
Remote-AP DHCP Server VLAN (1-4094)	N/A	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	N/A	Specify the IP address of the remote-AP DHCP server.
Remote-AP DHCP Default Router	N/A	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	N/A	Enter the IP address or addresses of one or more remote-AP DHCP DNS servers.
Remote-AP DHCP Pool Start	N/A	Specify the DHCP IP address pool. This configures the pool of IP addresses from which the remote AP uses to assign IP addresses. 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 End	N/A	
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. Options are as follows: ● none ● stateful-dot11x ● stateful kerbos ● valid user
Corporate DNS Domain	N/A	Enter the domain name service (DNS) domain or domains, one per line.
Image URL	N/A	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, when used.
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 controller 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.

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

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 ArubaOS:

- 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. Click **Profiles > AP > Regulatory Domain** in the **Aruba Navigation** pane. This page summarizes the current profiles of this type.
2. Click the **Add** button to create a new **Regulatory Domain** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 21:

Table 21 ***Aruba Configuration* > *Profiles* > *AP* > *Regulatory Domain*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
Other Settings		
Country Code		Designate the country with the 802.1X regulatory standard relevant to this WLAN.
Valid 802.11a 40MHz Channel pairs	N/A	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.

Table 21 ***Aruba Configuration* > *Profiles* > *AP* > *Regulatory Domain*** *Profile Settings*

Field	Default	Description
Valid 802.11g 40 MHz Channel Pairs	N/A	Select a 40MHz channel pair for 802.11ag 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 802.11a 40MHz Channels	N/A	Specify the valid channels for 40MHz channel pairing in 802.11a.
Valid 802.11g 40 MHz Channels	N/A	Specify the valid channels for 40MHz channel pairing in 802.11g.

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

Profiles > AP > 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** AP profile.

1. Click **Profiles > AP > Wired** in the **Aruba Navigation** pane. This page summarizes the current profiles of this type.
2. Click the **Add** button to create a new **Wired** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 22:

Table 22 ***Aruba Configuration* > *Profiles* > *AP* > *Wired*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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.

Table 22 ***Aruba Configuration** > **Profiles** > **AP** > **Wired** Profile Settings*

Field	Default	Description
Switchport Mode	Access	Select **access** or **trunk**. These options only apply to bridge mode configurations. ● **Access mode** forwards untagged packets received on the port to the controller and they appear on the configured access mode VLAN. Tagged packets are dropped. All packets received from the controller 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 controller. Untagged packets are forwarded to the controller on the configured Native VLAN. Packets received from the controller 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 controller and they appear on the configured access mode VLAN. Tagged packets are dropped. All packets received from the controller 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.
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 controller. Untagged packets are forwarded to the controller on the configured Native VLAN. Packets received from the controller 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. Click **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 > AP > 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. Click **Profiles > AP > Ethernet Link** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **System** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 23:

Table 23 ***Aruba Configuration > Profiles > AP > Ethernet Link*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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. Click **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 > SNMP

Aruba controllers 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 Aruba system in the current ArubaOS version. Perform these steps to configure a **SNMP** profile.

1. Click **Profiles > AP > SNMP** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **SNMP** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 24:

Table 24 ***Aruba Configuration > Profiles > AP > SNMP*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.

Table 24 ***Aruba Configuration* > *Profiles* > *AP* > *SNMP*** *Profile Settings*

Field	Default	Description
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. Click **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. Click **Profiles > AP > SNMP > SNMP User** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **SNMP** user, or click the **pencil** icon next to an existing user to edit that user. The **Details** page appears. Complete the settings as described in Table 24:

Table 25 ***Aruba Configuration* > *Profiles* > *AP* > *SNMP* > *SNMP User*** *Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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 Aruba Configuration
Authentication Profile	none	Select a protocol from the drop-down menu. Options are as follows: ● **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. Click **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 following topics for additional information about SNMP profiles:

- "Aruba Controller Traps" on page 92
- "Access Point/Air Monitor Traps" on page 93

Aruba Controller Traps

Table 26 provides a list of key traps generated by the Aruba controller.

Table 26 *Key SNMP Traps of the Aruba Controller*

Trap	Description	Priority Level
Mobility controller IP changed	This indicates the controller IP has been changed. The controller IP is either the loopback IP address or the IP address of the VLAN 1 interface (if no loopback IP address is configured).	Critical
Mobility controller role changed	This indicates that the controller has transitioned from being a master controller to a local controller or vice versa.	Critical
User entry created/ deleted/authenticated/de-authenticated/ authentication failed.	Each of these traps are triggered by an event related to a user event. The event can be a new user entry being created in the user table, deletion of a user entry, a user getting authenticated successfully, a user getting de-authenticated, or a failed authentication attempt. Each of these traps will be generated by the controller on which the user event occurs. In other words this is a local event to the controller where the user is visible.	Medium
Authentication server request timed out.	This trap indicates that a request to a authentication server did not receive a response from the server within a specified amount of time and therefore the request timed out. This usually indicates a connectivity problem from the Aruba controller to the authentication server or some other problem related to the authentication server.	High
Authentication server timed out	**NOTE:** Earlier versions of ArubaOS supported SNMP on individual APs. This feature is not supported by this version of ArubaOS. This trap indicates that an authentication server has been taken out of service. This is almost always same as **AuthServerReqTimedOut** except when there is only one authentication server in which case the server will never be taken out of service. In that case the **AuthServerReqTimedOut** will continue to be raised but not then **AuthServerTimedOut**.	High
Authentication server up	This trap indicates that an authentication server that was previously not responding has started responding to authentication requests. This will be triggered by a user event that causes the controller to send an authentication request to the authentication server.	Low.
Authentication user table full	This trap indicates that the authentication user table has reached its limit with the number of user entries it can hold. This event is local to the controller that generates the traps. The maximum number of user entries that can be present at the same time in the user table is 4096.	Critical
Authentication Bandwidth contracts table full	This trap indicates that the maximum number of configured bandwidth contracts on the controller has been exceeded. The threshold for this is 4096	High
Authentication ACL table full	This trap indicates that the maximum number of ACL entries in the ACL table has been exceeded. The limit for this is 2048 entries on a controller.	High
Power supply failure	As the name indicates, this trap indicates the failure of one of the two possible power supplies in the controller.	Critical
Fan failure	As the name indicates, this trap indicates a failure of the fan in the controller.	Critical
Out of Range Voltage	This trap indicates an out of range voltage being supplied to the controller.	Critical
Out of Range temperature	This trap indicates an out of range operating temperature being supplied to the controller.	Critical
Line card inserted/ removed	These traps indicate that a Line Card has been inserted or removed from the controller.	Critical.
Supervisor card inserted/ removed	These traps indicate that a Supervisor card has been inserted or removed from the controller	Critical
Power supply missing	This trap indicates that one of the power supplies is missing.	Critical

Access Point/Air Monitor Traps

Table 27 describes the key traps that can be generated by an Aruba access point or an air monitor:

Table 27 *Key SNMP Traps from Aruba Access Points or Air Monitors*

Trap	Description	Priority
Unsecure AP Detected	This trap indicates that an air monitor has detected and classified an access point as unsecure. It will indicate the location of the air monitor that has detected the unsecure AP, the channel on which the AP was detected as well as the BSSID and SSID of the detected AP.	Critical
Station impersonation	This trap indicates an air monitor has detected a station impersonation event. The trap will provide the location of the air monitor that has detected the event and the MAC address of the station.	Critical
Reserved channel impersonation	This trap indicates an access point is being detected is violating the reserved channels. The location of the AP/AM that detects the event is provided in the trap. In addition to this, the BSSID and SSID of the detected AP is also included.	High
Valid SSID violation	This indicates a configuration in the configuration of the SSID of the AP. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap.	High
Channel misconfiguration	This trap indicates an error in channel configuration of an AP. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap	High
OUI misconfiguration	This trap indicates an error in the OUI configuration of an Access Point. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap	High
SSID misconfiguration	This trap indicates an error in the SSID configuration of an Access Point. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap	High
Short Preamble misconfiguration	This trap indicates an error in the Short Preamble configuration of an AP. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap. This check will be done only if the short-preamble option is selected for the AP from the CLI or the WebUI. For a complete list of traps, refer to the Aruba MIB Reference.	High
AM misconfiguration	This trap indicates an error in the Short Preamble configuration of an AP. The AP generates the trap and includes its BSSID, the configured SSID and the location of the AP in the trap	High
Repeat WEP-IV violation	This trap indicates that the AM has detected a valid station or a valid AP sending consecutive frames that has the same IV (initialization vector). This usually means that entity has a “flawed” WEP implementation and is therefore a potential security risk.	High
Weak WEP-IV violation	This trap indicates that the AM has detected a valid station or a valid AP sending frames with an IV that is in the range of IV that are known to be cryptographically weak and therefore are a potential security risk.	High
Adhoc networks detected	This trap indicates that the AM has detected Adhoc networks	High
Valid station policy violation	This trap indicates that a valid station policy is being violated.	High
AP interference	This trap indicates that the indicated AM (identified by the BSSID/ SSID) is detecting AP interference on the indicated channel.	Medium

Table 27 *Key SNMP Traps from Aruba Access Points or Air Monitors (Continued)*

Trap	Description	Priority
Frame Retry rate exceeded	This trap refers to the event when the percentage of received and transmitted frames with the retry bit crosses the High watermark. This event can be triggered for an AP, a station or a channel. The two values that should be configured related to this event are Frame Retry Rate – High Watermark and Frame Retry Rate –Low watermark. The High Watermark refers to the percentage threshold which if surpassed triggers the event that causes the trap to be sent. The Low Watermark refers to the percentage threshold such that if the retry rate reaches a value lower than this value the event is reset. What this means is that the trap will be triggered the first time the Frame Retry rate crosses the High Watermark and then will only be triggered if the Frame Retry Rate goes under the Low Watermark and then crosses the High Watermark again. This holds true for all the thresholds explained below as well.	Medium
Frame Bandwidth rate exceeded	This trap refers to the event of the bandwidth rate for a station exceeding a configured threshold (High watermark). The terms High Watermark and Low Watermark hold the same meaning as explained above.	Medium
Frame low speed rate exceeded	This trap refers to the event when the percentage of received and transmitted frames at low speed (less that 5.5Mbps for 802.11b and less that 24 Mbps for 802.11a) exceeds the configured High Watermark. The terms High Watermark and Low Watermark hold the same meaning as explained above.	Medium

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.

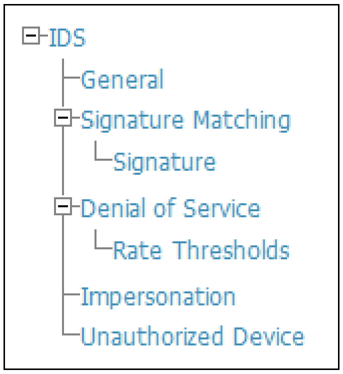
The top-level IDS profile, assigned to an Aruba AP group or AP name, references additional IDS profiles that are also described in this section. ArubaOS includes predefined top-level IDS profiles that provide different levels of sensitivity. The following are predefined IDS profiles:

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

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

To view IDS profiles, click **Profiles > IDS** in the Aruba Configuration navigation pane.

Figure 42 ***IDS Profiles** in **Aruba Configuration***



NOTE

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.

Click the **Add** button to create a new **IDS** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 29:

Table 28 ***Aruba Configuration > Profiles > IDS > General*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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 104.
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 97.
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 96.
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 103.
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 98.

4. Select the profile type to view or configure:

- ***General***—Configures general AP attributes. Refer to "Profiles > IDS > General" on page 96.
- ***Signature Matching***—Configures signatures and signature matching for intrusion detection. Refer to "Profiles > IDS > Signature Matching" on page 97.
  - ***Signature***—Defines a predefined signature. Refer to "Profiles > IDS > Signature Matching > Signatures" on page 98.
- ***Denial of Service***—Configures traffic anomaly settings for Denial of Service (DoS) attacks. Refer to "Profiles > IDS > Impersonation" on page 103.
  - ***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 101.
- ***Impersonation***—Configures anomaly settings for impersonation attacks. Refer to "Profiles > IDS > Impersonation" on page 103.
- ***Unauthorized Device***—Configures detection for unauthorized devices. Also configures rogue AP detection and containment. Refer to "Profiles > IDS > Unauthorized Device" on page 104.

5. Click **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. Click **Profiles > IDS > General** in the **Aruba Navigation** pane. The list of current IDS profiles appears on this page.
2. Click the **Add** button to create a new **General** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 29:

Table 29 ***Aruba Configuration > Profiles > IDS > General*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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 controller with statistics. **NOTE:** This setting takes effect only if the Aruba Mobility Manager is configured. Otherwise, statistics update to the controller is disabled.
AP Inactivity Timeout (5-36000 sec)	5	Set the time, in seconds, after which an AP is aged out.
STA Inactivity Timeout (30-36000 sec)	60	Set the time, in seconds, after which a STA 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.

Table 29 ***Aruba Configuration* > *Profiles* > *IDS* > *General*** *Profile Settings*

Field	Default	Description
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.
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	Yes	Enable or disable containment from the wireless side.
Debug Wireless Containment	No	Enable or disable debugging of containment from the wireless side. Enabling this debug option causes containment to function improperly.
Wired Containment	No	Enable or disable containment from the wireless side.

3. Click **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 30 describes the predefined signatures that you can add to the profile.

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

1. Click **Profiles > IDS > Signature Matching** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Signature Matching** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 30 ***Aruba Configuration* > *Profiles* > *IDS* > *Signature Matching*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
Signature Profiles		
Select Signature Profiles	N/A	Select from signature options as follows: ● AirJack ● ASLEAP ● Deauth-Broadcast ● Default ● Netstumbler Generic ● Netstrumbler Version 3.3.0x ● Null-Probe-Response

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

Profiles > IDS > Signature Matching > Signatures

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

1. Click **Profiles > IDS > Signature Matching > Signature** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Signature**, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 31:

Table 31 ***Aruba Configuration > Profiles > IDS > Signature*** *Creation Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the signature.
Add		Click this button to add a new IDS signature. Complete the settings as follows: ● Parameter, which can be one of the following: ■ bssid ■ dst-mac ■ frame-type ■ payload ■ seq-num ■ src-mac ● BSSID Click **Add** when these signature settings are defined.

3. Click **Add** 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 Aruba system. When a client is blacklisted in the Aruba 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 32 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 32 *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
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. Click **Profiles > IDS > Denial of Service** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Signature Matching** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 33:

Table 33 ***Aruba Configuration** > **Profiles** > **IDS** > **Denial of Service*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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.
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.

Table 33 *Aruba Configuration > Profiles > IDS > Denial of Service* Profile Settings (Continued)

Field	Default	Description
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 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.
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. Click **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. Aruba 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. Click **Profiles > IDS > Denial of Service > Rate Thresholds** in the **Aruba Navigation** pane. This page summarizes the current thresholds available.
2. Click the **Add** button to create a new **Rate Threshold**, or click the **pencil** icon next to an existing threshold to edit. The **Details** page appears. Complete the settings as described in Table 34:

Table 34 ***Aruba Configuration* > *Profiles* > *IDS* > *Denial of Service, Rate Threshold*** *Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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.
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. Click **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. Click **Profiles > IDS > Impersonation** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Impersonation** profile, or click the **pencil** icon next to an existing profile to edit. The **Details** page appears. Complete the settings as described in Table 35:

Table 35 ***Aruba Configuration > Profiles > IDS > Impersonation*** *Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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 event.
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.
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.

3. Click **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 Aruba 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.

NOTE

Rogue device classification for Aruba WMS Offload infrastructure is also described in the *AWMS User Guide*.

You can enable a policy to automatically disable APs that are classified as a rogue APs by the Aruba 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. Click **Profiles > IDS > Unauthorized Devices** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Unauthorized Devices** profile, or click the **pencil** icon next to an existing profile to edit. The **Details** page appears. Complete the settings as described in Table 36:

Table 36 ***Aruba Configuration > Profiles > IDS > Unauthorized Devices*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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.

Table 36 ***Aruba Configuration* > *Profiles* > *IDS* > *Unauthorized Devices*** *Profile Settings (Continued)*

Field	Default	Description
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 controller 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	Blank Text Field	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.
Allow Well Known MAC	N/A	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: ● **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. If you modify an existing configuration, the new configuration overrides the original configuration. For example, if you configure `allow-well-known-mac hsrp` and then configure `allow-well-known-mac iana`, the original configuration is lost.
Suspected Rogue Containment	No	Use this setting to treat suspected rogue APs as interfering APs; thereby the controller attempts to reclassify them as rogue APs. By default, suspected rogue APs are not automatically contained. 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.

Table 36 *Aruba Configuration > Profiles > IDS > Unauthorized Devices Profile Settings (Continued)*

Field	Default	Description
Suspected Rogue Containment Confidence Level (50-100)	60	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%. 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.
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	Enable or disable detection of misconfigured APs. An AP is classified as misconfigured if it does not meet any of the following configurable parameters: ● 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.
Protect SSID	No	Enable or disable use of SSID by only valid APs.
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.
Valid 802.11g Channel for Policy Enforcement	N/A	Enter the list of valid 802.11g channels that third-party APs are allowed to use.
Valid 802.11a Channel for Policy Enforcement	N/A	Enter the list of valid 802.11a channels that third-party APs are allowed to use.
Valid MAC OUIs	N/A	Enter the list of MAC OUIs of wired devices in the network, typically gateways or servers.
Valid and Protected SSIDs	N/A	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. Click **Add** or **Save**. The added or edited **Unauthorized Devices** 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.

- ***Radio****—Aruba 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 107.*
- ***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 109.
- ***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 > Mesh > Cluster" on page 111*.

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. Click **Profiles > Mesh > Radio** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Radio** profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 37 ***Aruba Configuration > Profiles > Mesh > Radio*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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.

Table 37 ***Aruba Configuration* > *Profiles* > *Mesh* > *Radio*** *Profile Settings (Continued)*

Field	Default	Description
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: ● **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:** AirWave recommends using the default value.
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: ● **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:** AirWave recommends using the default value.
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. Aruba recommends creating a new mesh cluster profile if needed.
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.

Table 37 *Aruba Configuration > Profiles > Mesh > Radio Profile Settings (Continued)*

Field	Default	Description
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:** AirWave recommends using the default value.

3. Click **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. Click **Profiles > Mesh > Radio > Mesh HT SSID** in the **Aruba Navigation** pane. The details page summarizes the current profiles of this type.
2. Click the **Add** button to create a new **Mesh HT SSID** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 18:

Table 38 *Aruba Configuration > Mesh > Radio > Mesh HT SSID Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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.

Table 38 ***Aruba Configuration* > *Mesh* > *Radio* > *Mesh HT SSID*** *Profile Settings (Continued)*

Field	Default	Description
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.
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 3.4 are 8191, 16383, 32767, or 65535 bytes. AWMS 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 MDPU 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: ● 2-10 ● 1,3,6,9,12
Short Guard Interval in 40 MHz Mode	Yes	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. 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. This parameter is enabled by default.
Legacy Stations	Yes	Allow or disallow associations from legacy (non-HT) stations. This parameter is enabled by default (legacy stations are allowed).
Max Transmitted A-MPDU Size	65535	Sets maximum size of a transmitted aggregate MPDU, in bytes. Specify size in the supported range of 1576 to 65535 bytes.
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.

3. Click **Add** or **Save**. The added or edited profile appears on the **Mesh HT SSID** page, and on the details page.

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. Click **Profiles > Mesh > Cluster** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Cluster** profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 39 ***Aruba Configuration > Profiles > Mesh > Cluster*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
Other Settings		
Cluster Name	aruba-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 “Aruba-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). AirWave recommends selecting WPA2-PSK-AES and entering a passphrase (see WPA Passphrase). Keep the passphrase in a safe place.

3. Click **Add** or **Save**. The added or edited **Cluster** profile appears on the **Profiles > Mesh > Cluster** 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 112.
- ***VoIP Call Admission Control***—Aruba’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 112.

- ***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 115.

Profiles > QoS > Traffic Management

Perform these steps to create or edit Traffic Management profiles.

1. Click **Profiles > QoS > Traffic Management** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Traffic Management** profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 40 ***Aruba Configuration > Profiles > QoS > Traffic Management*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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: ● default-access ● fair access ● preferred access
WLAN Bandwidths		
WLAN	N/A	Click the **Add** button to specify, edit, or add a WLAN bandwidth allocation, and the associated WLAN.
Bandwidth Allocation	N/A	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. Click **Add** or **Save**. The added or edited profile appears on the **Profiles > QoS > Traffic Management** page.

Profiles > QoS > VoIP Call Admission Control

Aruba'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. Click **Profiles > QoS > *VoIP Call Admission Control*** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **VoIP Call Admission Control** profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 41 ***Aruba Configuration > Profiles > QoS > VoIP Call Admission Control*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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	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 controller 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 specifies the bandwidth allocation to T-Spec voice calls when Admission Control is enabled.
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.

Table 41 ***Aruba Configuration > Profiles > QoS > VoIP Call Admission Control*** *Profile Settings*

Field	Default	Description
VoIP High-capacity Threshold (0-100%)	20	Specifies the threshold that defines high-capacity VoIP. This field is a percentage of entire bandwidth.
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 controller 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 controller. 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 controller 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 controller 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 controller. 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 controller 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 controller. Use this field to enable or disable SIP call setup keepalive in the VoIP Call Admission Control profile for the server.

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

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.

NOTE

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. Click **Profiles > QoS > WMM Traffic Management** in the **Aruba Navigation** pane. The details page summarizes the current profiles of this type.
2. Click the **Add** button to create a new **WMM Traffic Management** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 18:

Table 42 ***Aruba Configuration* > *Profiles* > *QoS* > *WMM Traffic Management*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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%.

Click **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 116.
- ***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 116.
- ***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 118.
- ***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 > High-Throughput (HT) Radio" on page 122.
- ***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 123
- ***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 124

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. Click **Profiles > RF > 802.11a/g** in the **Aruba Configuration** navigation pane.
2. Click the appropriate **Add** button to create a new **802.11a** or **g** profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 43 ***Aruba Configuration > Profiles > RF > 802.11a/g** Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the threshold profile.
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. Click 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, AWMS 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 118.
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. Click 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, AWMS returns you to the 802.11a/g Profile page. For additional HT radio profile information, refer to "Profiles > RF > 802.11a/g Radio > High-Throughput (HT) Radio" on page 122.
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: ● **am-mode**—Air Monitor mode ● **ap-mode**—Access Point mode ● **apm-mode**—Access Point Monitor mode ● **sensor-mode**—RFprotect sensor mode
High Throughput Enable (Radio)	Yes	Enable or disable high-throughput (802.11n) features on the radio.
Channel (34-165)	N/A	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: ● **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.
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.

Table 43 ***Aruba Configuration* > *Profiles* > *RF* > *802.11a/g*** *Profile Settings (Continued)*

Field	Default	Description
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.
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.
Protection for 802.11b Clients	Yes	Supported for 802.11g only, use this field to enable protection for 802.11b clients. Disabling this protection violates the 802.11b standard and may cause interoperability issues.

3. Click **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 > 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.

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. Aruba recommends creating a new mesh cluster profile if needed.

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

1. Click **Profiles > RF > 802.11a/g Radio > ARM** in the **Aruba Navigation** pane.

2. Click the **Add** button to create a new **ARM** profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 44 ***Aruba Configuration > Profiles > RF > 802.11a/g Radio > ARM*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
Other Settings		
Assignment	single-band	Activates one of four ARM channel/power assignment modes. ● **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	Set the 802.11 radio bands to be supported by this ARM profile. The drop-down menu supports the following options: ● **a-only**—802.11a radio bands ● **g-only**—802.11g radio bands ● **all**—both 802.11a and g bands
Client Aware	Yes	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.
Max Tx Power (dBm)	30	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. **NOTE:** Power settings will not change if the **Assignment** option is set to disabled or maintain.
Min Tx Power (dBm)	0	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**. **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.
Multi Band Scan	Yes	If enabled, single radio channel APs scans for rogue APs across multiple channels. This option requires that **Scanning** is also enabled. The **Multi Band Scan** option does not apply to APs that have two radios, such as an Aruba 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.

Table 44 ***Aruba Configuration*** **>** ***Profiles*** **>** ***RF*** **>** ***802.11a/g Radio*** **>** ***ARM*** *Profile Settings (Continued)*

Field	Default	Description
Rogue AP Aware	No	If you have enabled both the **Scanning** and **Rogue AP** options, Aruba 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. 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.
Scan Interval (sec)	10	If **Scanning** is enabled, the **Scan Interval** defines how often the AP will leave its current channel to scan other channels in the band. 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. The supported range for this setting is 0 to 2,147,483,647 seconds.
Active Scan	No	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. **Active Scan** is disabled by default, and should not be enabled except under the direct supervision of AirWave or Aruba Support.
Scanning	Yes	The **Scanning** field enables or disables AP scanning across multiple channels. Disabling this option also disables the following scanning features: ● Multi Band Scan ● Rogue AP Aware ● Voip Aware Scan ● Power Save Scan Do not disable **Scanning** unless you want to disable ARM and manually configure AP channel and transmission power.
Scan Time	110 msec	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. Aruba recommends a scan time between 50 to 200 msec.
VoIP Aware Scan	No	Aruba's **VoIP** Call Admission Control (CAC) prevents any single AP from becoming congested with voice calls. When you enable CAC, you should also enable **VoIP Aware Scan** in the ARM profile, 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.
Power Save Aware Scan	Yes	If enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode.
Ideal Coverage Index	10	The Aruba coverage index metric is a weighted calculation based on the RF coverage for all Aruba 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.
Acceptable Coverage Index	4	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.

Table 44 ***Aruba Configuration > Profiles > RF > 802.11a/g Radio > ARM** Profile Settings (Continued)*

Field	Default	Description
Free Channel Index	25	The Aruba 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. **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.
Backoff Time	240	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.
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. Aruba recommends a Minimum Scan Time between 1 to 20 scans.
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).

3. Click **Add** or **Save**. The added or edited **ARM** 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 > High-Throughput (HT) Radio

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

1. Click **Profiles > RF > HT Radio** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **HT Radio** profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 45 ***Aruba Configuration > Profiles > RF > HT Radio*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
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. Click **Add** or **Save**. The added or edited **HT Radio** profile appears on the **Profiles > RF > HT Radio** page.

Profiles > RF > Event Thresholds

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

1. Click **Profiles > RF > Event Thresholds** in the **Aruba Navigation** pane.
2. Click the **Add** button to create a new **Event Thresholds** profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 46 ***Aruba Configuration > Profiles > RF > Event Thresholds** Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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.
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 that 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 that 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.

Table 46 ***Aruba Configuration* > *Profiles* > *RF* > *Event Thresholds*** *Profile Settings (Continued)*

Field	Default	Description
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. Click **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. Click **Profiles > RF > Optimization** in the **Aruba Navigation** pane. This page summarizes the current cluster profiles.
2. Click the **Add** button to create a new **Optimization** profile**,** or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 47 ***Aruba Configuration* > *Profiles* > *RF* > *Optimization*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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.

Table 47 ***Aruba Configuration > Profiles > RF > Optimization*** *Profile Settings (Continued)*

Field	Default	Description
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.
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. 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. 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. 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. 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. 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.

Table 47 ***Aruba Configuration* > *Profiles* > *RF* > *Optimization*** *Profile Settings (Continued)*

Field	Default	Description
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. Click **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 9HT) SSID profile.

- ***SSID***—The SSID profile defines SSID settings and references additional EDCA and HT profiles. Refer to "Profiles > SSID > EDCA AP" on page 127.
- ***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 131.
- ***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 134.
- ***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 controller or the AP. Refer to "Profiles > SSID > HT SSID" on page 137.
- ***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. Refer to "Profiles > SSID > 802.11K" on page 138.

Profiles > SSID > EDCA AP

Perform these steps to create or edit EDCA AP profiles.

1. Click **Profiles > SSID > EDCA AP** in the **Aruba Navigation** pane. This page summarizes the SSID profiles currently configured.
2. Click the **Add** button to create a new EDCA AP profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 48 ***Aruba Configuration* > *Profiles* > *EDCA AP*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Displays the name of the profile.
Referenced Profiles		
EDCA Parameters Station Profile	None	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. Click the Plus sign to create a new EDCA Station profile, as required. For additional information about this profile type, refer to "Profiles > SSID > EDCA Station" on page 134. Referencing an EDCA Station profile requires a Voice Service license.
EDCA Parameters AP Profile	None	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. Click the Plus sign to create a new EDCA AP profile, as required. For additional information about this profile type, refer to "Profiles > SSID > EDCA AP" on page 131. Referencing an EDCA Station profile requires a Voice Service license.
High-throughput SSID Profile	default	The drop-down menu allows you to select any High-throughput SSID profile profile that has already been configured. The referenced HT profile defines several settings that are used in the SSID profile. Click the Plus sign to create a new HT SSID profile, as required. For additional information about this profile type, refer to "Profiles > SSID > HT SSID" on page 137.
Security Settings		

Table 48 ***Aruba Configuration* > *Profiles* > *EDCA AP*** *Profile Settings (Continued)*

Field	Default	Description
Encryption	opensystem	Select any encryption type to be supported in this SSID profile. The supported encryption types are as follows: ● **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.
WEP Key 1	N/A	Enter WEP Key 1, and confirm the key in the **Confirm** field.
WEP Key 2	N/A	Enter WEP Key 2, and confirm the key in the **Confirm** field.
WEP Key 3	N/A	Enter WEP Key 3, and confirm the key in the **Confirm** field.
WEP Key 4	N/A	Enter WEP Key 4, and confirm the key in the **Confirm** field.
WPA Hexkey	N/A	Enter the hex key to be used with Wi-Fi Protected Access.
WPA Passphrase	N/A	Enter a difficult-to-guess passphrase between eight and 63 characters.
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.

Table 48 ***Aruba Configuration* > *Profiles* > *EDCA AP*** *Profile Settings (Continued)*

Field	Default	Description
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.
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 controller 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	N/A	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 Differentiated Services Codepoint (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.

Table 48 ***Aruba Configuration* > *Profiles* > *EDCA AP*** *Profile Settings (Continued)*

Field	Default	Description
DSCP Mapping for WMM Video AC	N/A	Specify Differentiated Services Code Point (DSCP) mapping for wireless multimedia video admission control. The supported range is 0 to 63.
DSCP Mapping for WMM Best-Effort AC	N/A	Specify Differentiated Services Code Point (DSCP) mapping for wireless multimedia best effort admission control. The supported range is 0 to 63.
DSCP Mapping for WMM Background AC	N/A	Specify Differentiated Services Code Point (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 controller and APs (for example, in a remote location where an AP is not in range of another Aruba AP), Aruba recommends that you enable the “local probe response” option in the SSID profile. (Generating probe responses on the Aruba controller is an optimization that allows ArubaOS to make better decisions.) This option is enabled by default in the SSID profile. You can also increase the value for the bootstrap threshold in the AP System profile to minimize the chance of the AP rebooting due to temporary loss of connectivity with the Aruba controller.
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.
Battery Boost	No	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. **NOTE:** This setting requires a voice service license. **NOTE:** Although you can enable battery boost on a per-virtual AP basis, it must be enabled for any SSIDs that support voice traffic. 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.
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.

Table 48 ***Aruba Configuration* > *Profiles* > *EDCA AP*** *Profile Settings (Continued)*

Field	Default	Description
BC/MC Rate Optimization	No	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. **NOTE:** Aruba recommends using the default value.
Strict Spectralink Voice Protocol (SVP)	No	Use this setting for Spectralink VoIP devices. This setting automatically permits and prioritizes the Spectralink Voice Protocol (SVP).

3. Click **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 49.

Table 49 *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 controller, 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. Click **Profiles > SSID > EDCA AP** in the **Aruba Navigation** pane. This page summarizes the current profiles of this type.
2. Click the **Add** button to create a new EDCA AP profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 50:

Table 50 ***Aruba Configuration* > *Profiles* > *SSID* > *EDCA*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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: ● 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: ● arbitrary inter-frame space number (AIFSN) ● minimum and maximum contention window (CW) size
Minimum Contention Window (Exponent)	4	
Maximum Contention Window (Exponent)	10	

Table 50 ***Aruba Configuration > Profiles > SSID > EDCA** 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: ● 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.
Other Settings		
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: ● 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.

Table 50 ***Aruba Configuration* > *Profiles* > *SSID* > *EDCA*** *Profile Settings (Continued)*

Field	Default	Description
ACM	No	Define whether or not admission control mandatory (ACM) is to be supported on APs configured with this EDCA profile.

3. Click **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 49.

Table 51 *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 controller, 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. Click **Profiles > SSID > EDCA Station** in the **Aruba Navigation** pane. This page summarizes the current cluster profiles.
2. Click the **Add** button to create a new **EDCA Station** profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 52 ***Aruba Configuration > Profiles > SSID > EDCA Station** Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Name of the EDCA STA 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: ● 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	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: ● 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	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.

Table 52 ***Aruba Configuration > Profiles > SSID > EDCA Station*** *Profile Settings (Continued)*

Field	Default	Description
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	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: ● 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.
Other Settings		
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: ● 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. Click **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.

Aruba 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 affect immediately. You do not reboot the controller or the AP.

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

1. Click **Profiles > SSID > HT SSID** in the **Aruba Navigation** pane. This page summarizes the current cluster profiles.
2. Click the **Add** button to create a new **HT SSID** profile, or click the **pencil** icon to edit an existing profile. The **Details** page appears. Complete the settings as described in Table 30:

Table 53 ***Aruba Configuration > Profiles > SSID > HT SSID*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	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.

Table 53 ***Aruba Configuration** > **Profiles** > **SSID** > **HT SSID*** *Profile Settings (Continued)*

Field	Default	Description
Min MPDU Start Spacing (usec)	0	Set the minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds. Allowed values: 0 (No restriction on MDPU start spacing), 0.25 usec, 0.5 usec, 1 usec, 2 usec, 4 usec.
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. Examples: ● 2-10 ● 1,3,6,9,12 Range: 0-15
Short Guard Interval in 40 MHz Mode	Yes	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. 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. This parameter is enabled by default.
Legacy Stations	Yes	Allow or disallow associations from legacy (non-HT) stations. By default, this parameter is enabled (legacy stations are allowed).
Allow Weak Encryption	No	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

3. Click **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. Click **Profiles > SSID > 802.11K** in the **Aruba Navigation** pane. The details page summarizes the current profiles of this type.
2. Click the **Add** button to create a new **802.11K** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 18:

Table 54 ***Aruba Configuration > Profiles > SSID > 802.11K*** *Profile Settings*

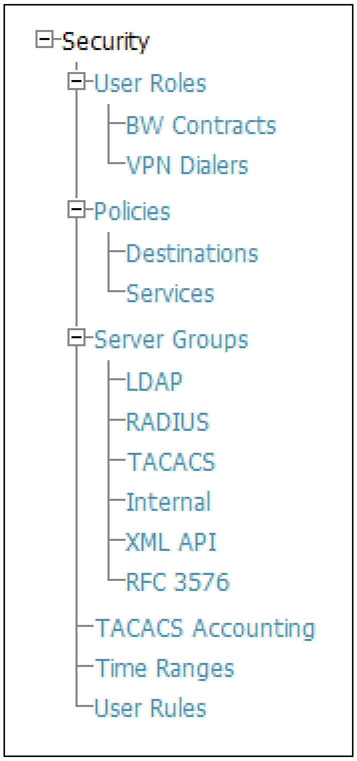
Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. Folders provide a way to organize the visibility of device parameters that is 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	Blank	Enter the name of the profile.
Other Settings		
Measurement Mode for Beacon Reports	beacon-table	Click the Measurement Mode for **Beacon Reports** drop-down menu and specify one of the following measurement modes: ● **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. **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.
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. Click **Add** or **Save**. The added or edited profile appears on the **802.11K** page, and on the details page.

Security Pages and Field Descriptions

Aruba 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 **Aruba Configuration** page, as illustrated in Figure 43:

Figure 43 *Security Components in Aruba Configuration*



This section describes the profiles, pages, parameters and default settings for all **Security** components in **Aruba 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 Aruba Vendor-Specific Attributes (VSA) for RADIUS server authentication. A role derived from an Aruba VSA takes precedence over any other user roles.

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

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

This page displays the current user roles in Aruba Configuration and where they are used. This page contains the columns described in Table 55:

Table 55 ***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 68.
Captive Portal Auth	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 69.
802.1X Auth	Displays the 802.1X Auth profiles that are referenced by the user role. For additional information, refer to "Profiles > AAA > 802.1x Auth" on page 75.
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 72.
VPN Auth	Displays the VPN Auth profiles that are referenced by the user role. For additional information, refer to "Profiles > AAA > VPN Auth" on page 73.

Table 55 ***Security* > *User Roles*** *Page Contents (Continued)*

Column	Description
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 56:

Table 56 ***Security* > *User Roles* > *Add New User Role*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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 Auth		(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 69. Click 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 143.
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 143.
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.
ID of 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 controller. Use this field to override this assignment and configure the VLAN ID that is to be assigned to the user role.

Table 56 ***Security > User Roles > Add New User Role*** *Field Descriptions*

Field	Default	Description
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 144.
Policies		
Add New Policy	N/A	Click this button to add a new policy to the user role. The following two fields appear with respective drop-down menus: ● Policy ● Aruba 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 146.
Aruba AP Group	None	Select the **Aruba AP group** in which this policy and user role will apply. For additional information, refer to "General Aruba AP Groups Procedures and Guidelines" on page 34.

Click **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 controller ("upstream" traffic)
- from the controller to the client ("downstream" traffic)

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

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

The **Details** page for **Security > User Roles > Add New Bandwidth Contract** page contains the following fields, as described in Table 57:

Table 57 ***Security > User Roles > Add New BW Contract*** *Page Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the Bandwidth Contract is associated. The drop-down menu displays all folders available for association with the profile.

Table 57 ***Security** > **User Roles** > **Add New BW Contract** Page Field Descriptions (Continued)*

Field	Default	Description
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: - from the client to the controller ("upstream" traffic) - from the controller to the client ("downstream" traffic)
Bandwidth	N/A	Specify whether this bandwidth contract is upstream or downstream by typing one of the following terms in lower case: - `upstream` - `downstream` Click **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.

Click **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 58:

Table 58 ***Security** > **User Roles** > **Add VPN Dialer** Field Descriptions*

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

Table 58 ***Security > User Roles > Add VPN Dialer*** *Field Descriptions (Continued)*

Field	Default	Description
Enable L2TP	Yes	Enable L2TP with this setting as desired. The combination of Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec) is a highly secure technology that enables VPN connections across public networks such as the Internet. L2TP/IPSec provides both a logical transport mechanism on which to transmit PPP frames as well as tunneling or encapsulation so that the PPP frames can be sent across an IP network. L2TP/IPSec relies on the PPP connection process to perform user authentication and protocol configuration. With L2TP/IPSec, the user authentication process is encrypted using the Data Encryption Standard (DES) or Triple DES (3DES) algorithm. L2TP/IPSec requires two levels of authentication: ● Computer-level authentication with a preshared key to create the IPSec security associations (SAs) to protect the L2TP-encapsulated data. ● User-level authentication through a PPP-based authentication protocol using passwords, SecureID, digital certificates, or smart cards after successful creation of the SAs.
Send traffic to the direct network in clear	No	Use this setting if no encryption is to be used and packets passing between the wireless client and controller are to be in clear text.
Disable wireless devices when client is wired	No	Use this setting to disable wireless clients when a wired device is known to be on the VPN.
Enable SecurID New and Next Pin Mode	No	Use this setting to enable or disable SecurID PIN modes. The SecurID authentication scheme authenticates the user on a RSA ACE/Server. When challenged, the user has to enter a password that is a combination of two numbers: a personal identification number (PIN), supplied by RSA, combined with a token code, which is the number displayed on the RSA SecurID authenticator. New PIN mode is applied in cases where the authentication process requires additional verification of the PIN. In this case, the user is required to use a new PIN. The new PIN is derived from one of the following two sources, depending on the configuration of the RSA ACE/Server: ● The user is prompted to select and enter a new PIN. ● The server supplies the user with a new PIN. The user is then required to re-authenticate with the new PIN. The use of the New PIN mode is optional and can be enabled or disabled.
PPP Authentication Modes	CHAP MSCHAP MSCHAPv2 PAP	Use this section to select the authentication modes to be supported for PPP in the VPN. The following options are available: ● CHAP ● Cache SecurID Token ● MSCHAP ● MSCHAPv2 ● PAP
IKE Lifetime (300-85400 secs)	28800	Specify the Internet Key Exchange (IKE) Lifetime in seconds. When this period of time expires, the IKE SA is replaced by a new SA or is terminated. The IKE SA specifies values for the IKE exchange: the authentication method used, the encryption and hash algorithms, the Diffie-Hellman group used, the lifetime of the IKE SA in seconds, and the shared secret key values for the encryption algorithms. The IKE SA in each peer is bi-directional.
IKE Encryption	168-bit 3DES-CBC	Select the Internet Key Exchange (IKE) encryption method from the following two options: ● 168-bit 3DES-CBC ● 56-bit DES-CBC

Table 58 ***Security > User Roles > Add VPN Dialer*** *Field Descriptions (Continued)*

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

Click **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 > Policy > Add New Policy** page contains the following fields, as described in Table 59:

Table 59 *Security > Policy > Add New Policy Field Descriptions*

Field		Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the policy is associated. The drop-down menu displays all folders available for association with the policy.

Table 59 *Security > Policy > Add New Policy Field Descriptions (Continued)*

Field		Description
Name	Blank	Enter the name of the policy.
Other Settings		
Policy Type	IPv4 Session	Specify the type of policy. The options are as follows: - IPv4 - IPv6

Click **Add** to complete the configuration of the **Policies** profile. The new policy appears on the **Security > Policies > 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 60:

Table 60 ***Security > Policies > Net Destinations*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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.
Other Settings		
Invert	No	Use this field to invert the destination from one end of the VPN connection to the other.
Add New Net Destination Rule	N/A	Click this button to create a new rule for this destination profile. Clicking this button displays the **Net Destination Rule** section, which is comprised of two settings: - **Rule Type**—Specify whether the rule applies to **Host**, **Network**, or **Range**. - **IP Address**—Enter the IP address for the net destination rule.

Click **Add** to complete the configuration of the **Destination** policy profile, or click **Save** to complete the editing of an existing server. 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.

Click **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 61:

Table 61 ***Security > Policies > Services** Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the security policy service is associated. The drop-down menu displays all folders available for association with the service.
Name	Blank	Enter the name of the destination.
Other Settings		
Protocol	TCP	Specify the protocol that is to support the security policy service being configured. The service options are as follows: ● **TCP** ● **UDP** ● **IP** The remaining fields on this page change according to which protocol you have selected.
TCP/UDP Port	N/A	Specify the TCP/UDP port or range of ports to support the service being configured.
TCP/UDP Max Port	N/A	Specify the highest port that will support the TCP/UDP service being configured.
IP Protocol Number (0-255)	N/A	Specify the numeric identifier of the upper layer IP protocol that an IP packet should use.
Configure Application Level Gateway	No	Specify whether to create an application level gateway, which filters incoming and outgoing information packets before copying and forwarding across the gateway. If you select **Yes** in this field, you are prompted with a new drop-down menu in which to select the Application Level Gateway type.
Application Level Gateway	dhcp	If you select **Yes** for **Configure Application Level Gateway**, then specify the gateway type from this drop-down menu. The following application level gateway types are supported: ● **dhcp** ● **dns** ● **ftp** ● **h323** ● **noe** ● **rtsp** ● **sccp** ● **sip** ● **sips** ● **svp** ● **tftp** ● **vocera**

Security > Server Groups

Server Groups Page Overview

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

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

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

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

Before enabling fail-through authentication, note the following:

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

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

Supported Servers

ArubaOS 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 controller's internal database to authenticate users. You create entries in the database for users and their passwords and default role.

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

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

Adding a New Server Group

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

To create a new server group, click the **Add** button, or to edit an existing group, click the pencil icon next to that group. The **Add New Server Group** page appears, and contains the following fields, as described in Table 62:

Table 62 ***Security > Server Groups > Add or Edit Server Group*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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	Enable or disable a fail through server. When fail-through authentication is enabled, users that fail authentication on the first server in the server list should be authenticated with the second server. The controller attempts authentication with each server in the list until either there is a successful authentication or the list of servers in the group is exhausted. This feature is useful in environments where there are multiple, independent authentication servers; users may fail authentication on one server but can be authenticated on another server.
Add New Server	N/A	Click this button to add a new server to the Server Group being configured. A new **Server** section and Server Group Server Rules section appear with the following settings to be defined: **Server Section** ● **Trim FQDN**—Default setting is **No**. Change to **Yes** to enable. You can use the “match FQDN” option for a server match rule. With a match FQDN rule, the server is selected if the <domain> portion of the user information in the formats <domain>\<user> or <user>@<domain> exactly matches a specified string. Note the following caveats when using a match FQDN rule: ● 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. **Server Group Server Rules Section** Click the **Add** button to add a new rules section. The page that appears contains the following settings to define: ● **Match Type**—From the drop-down menu, select **Authstring** or **FQDN**. The following settings complete the configuration. ● **Operator**—For **Authstring** only, specify how to process the string (**contains, equals, starts with**). ● **Match String**—Enter the string or string fragment. Finish by clicking the **Add New Server Group Server Rules** button.

Table 62 *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	N/A	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.

Click **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. Click **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 63:

Table 63 *Security > Server Groups > Add LDAP Server Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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	N/A	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	N/A	Enter the password for the admin user.
Allow Clear-text	No	Enable this setting to allows clear-text (unencrypted) communication with the LDAP server.
Auth Port	389	Enter the port number used for authentication on the LDAP server.

Table 63 ***Security > Server Groups > Add LDAP Server** Field Descriptions (Continued)*

Field	Default	Description
Base-DN	N/A	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: ● **clear-text**—No encryption is used. ● **ldap-s**—Uses SSL encryption. ● **start-tls**—Uses TLS encryption.

Click **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. Click **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 64:

Table 64 *Security > Server Groups > RADIUS*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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	N/A	Set the IP address of the authentication server.
Key (Confirm Key)	N/A	Set the shared secret between the controller and the authentication server. The maximum length is 48 bytes.
Auth Port	1812	Set the authentication port on the server.

Table 64 *Security > Server Groups > RADIUS (Continued)*

Field	Default	Description
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 controller before the server is marked as down.
Timeout	(1-30 sec)	Set the maximum time, in seconds, that the controller waits before timing out the request and resending it.
NAS ID	N/A	Set the Network Access Server (NAS) identifier to use in RADIUS packets.
NAS IP	N/A	Set the NAS IP address to send in RADIUS packets. You can configure a "global" NAS IP address that the controller 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.

Click **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. Click **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 65:

Table 65 *Security > Server Groups > TACACS*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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)	N/A	Set the shared secret to authenticate communication between the TACACS+ client and server.
TCP Port	49	Set the TCP port to be used by the server.
Retransmits (0-3)	3	Set the maximum number of times a request is retried.

Table 65 *Security > Server Groups > TACACS (Continued)*

Field	Default	Description
Tmout (1-30 sec)	20	Set the timeout period for TACACS+ requests, in seconds.
Enable	Yes	Enable or disable the TACACS server.

Click **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 66:

Table 66 ***Security > Server Groups > Add Internal Server*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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		
Maximum Expiration (mins)	N/A	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	N/A	This section displays internal server users currently configured for use on the Internal Server. Click this button to add a new user. The **Internal Server User** section appears with the following settings.
Internal Server User		
User Name	N/A	Enter the name of a user, or click **Generate** to create an anonymous ID for this user.
Password	N/A	Enter the password in plain text, or click **Generate** to create a random password for this user.

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

Field	Default	Description
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.
E-Mail	N/A	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.

Click **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

Aruba 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 67:

Table 67 ***Security > Server Groups > Add New XML API Server** Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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.

Click **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). Aruba 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.

Click **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 68.

Table 68 ***Security > Server Groups > Add RFC 3576 Server*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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.

Click **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. Click **Security > Server Groups > Windows** in the **Aruba Navigation** pane. The details page summarizes the current profiles of this type.
2. Click the **Add** button to create a new **Windows** profile, or click the **pencil** icon next to an existing profile to edit that profile. The **Details** page appears. Complete the settings as described in Table 18:

Table 69 ***Aruba Configuration > Security > Server Groups > Windows*** *Profile Settings*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile. 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	Blank	Enter the name of the profile.
Other Settings		
Host	N/A	Enter the IP address of the Windows server.
Enable	No	Enable or disable the Windows server.

3. Click **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 controller to be reported to TACACS+ servers. You can specify the types of commands that are reported, and these are action, configuration, or show commands. You can have all commands reported as desired. Aruba 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. Click **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 70:

Table 70 ***Security > Server Groups > Add/Edit TACACS Accounting Profile*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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 AWMS 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.

Click **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 Aruba 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 71:

Table 71 ***Security > Time Range > Add/Edit Time Range** Field Descriptions*

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

Click **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 Aruba 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. The Details page appears. Table 72 describes the contents of this page.

Table 72 ***Security > User Rules > Add/Edit User Rules** Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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	N/A	Click this button to create a new rule. Additional fields appear that require configuration, as follows.

Table 72 ***Security* > *User Rules* > *Add/Edit User Rules*** *Field Descriptions (Continued)*

Field	Default	Description
Set Type	role	Select whether the rule is based on role or VLAN.
Rule Type	bssid	Select one of the following options from the drop-down menu. Your selection in this field changes an ensuing field that must be completed, as follows: • **bssid**—Selecting this option displays the **BSSID** field below. Specify the BSSID in text. • **dhcp-option-77**—Selecting this option displays the **DHCP Option 77** field below. Enter this information in text. • **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	If you selected **role** for the **Set Type** field above, then select the specific user role from this drop-down menu. If you selected **VLAN** for the **Set Type** field above, then select the specific VLAN from this drop-down menu.

Advanced Services Pages and Field Descriptions

This document section describes the contents, parameters, and default settings for all **Advanced Services** components in **Aruba Configuration**. Aruba Configuration in AWMS 6.3 supports advanced services such as IP Mobility and VPN services. Future AWMS 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 *ArubaOS User Guide*.

Overview of IP Mobility Domains

Aruba'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 Aruba mobility solution does not require that you install mobility software or perform additional configuration on wireless clients. The Aruba controllers 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 Aruba controller in the foreign network with which the mobile client is associated.

The *home agent* for the client is the controller 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 controller 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 Aruba controllers among which a wireless user can roam without losing their IP address. Mobility domains are not tied with the master controller, thus it is possible for a user to roam between controllers managed by different master controllers as long as all of the controllers belong to the same mobility domain.

You enable and configure mobility domains only on Aruba controllers. 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 controllers that support the VLANs into which employee users can be placed should be part of the same mobility domain.

A controller can be part of multiple mobility domains, although Aruba recommends that a controller belong to only one domain. The controllers in a mobility domain do not need to be managed by the same master controller.

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

Although you configure a mobility domain on a master controller, the master controller does not need to be a member of the mobility domain. For example, you could set up a mobility domain that contains only local controllers; you still need to configure the mobility domain on the master controller that manages the local controllers. You can also configure a mobility domain that contains multiple master controllers; you need to configure the mobility domain on each master controller.

Table 73 *Controllers in a Mobility Domain*

On a master controller:	On all controllers in the mobility domain:
● Configure the mobility domain, including the entries in the home agent table (HAT).	● 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 **Aruba 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.

Click **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 74:

Table 74 ***Advanced Services > IP Mobility, Add/Edit*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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.
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.

Table 74 ***Advanced Services > IP Mobility, Add/Edit*** *Field Descriptions (Continued)*

Field	Default	Description
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 controller detects when a mobile client has moved to a foreign network and determines the home agent for a roaming client. The proxy mobile IP module performs the following functions: ● Derives the address of the home agent for a mobile client from the HAT using the mobile client's IP address. If there is more than one possible home agent for a mobile client in the HAT, the proxy mobile IP module uses a discovery mechanism to find the current home agent for the client. ● Detects when a mobile client has moved. Client moves are detected based on ingress port and VLAN changes and mobility is triggered accordingly. For faster roaming convergence between AP(s) on the same controller, 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.

Table 74 ***Advanced Services > IP Mobility, Add/Edit*** *Field Descriptions (Continued)*

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

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

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

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

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

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

Navigate to **Advanced Services > IP Mobility > Mobility Domain** from the Ar**uba Configuration** navigation pane. This page displays all currently configured IP Mobility domains. Click **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 75:

Table 75 ***Advanced Services > IP Mobility > Add/Edit IP Mobility Domain*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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.
Mobile IP Home Agents		
Add	N/A	Use this button to create new home agents. Once you click **Add**, the following additional fields appear in the Mobile IP Home Agent section. Complete these settings. ● **Subnet**—Define the subnet mask for the IP Mobility Domain. ● **Netmask**—Define the net mas for the IP Mobility Domain. ● **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. Click **Add** to create the home agent.

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

Advanced Services > VPN Services

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

You can configure the controller 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 controller 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 controller 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.

Click 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 76.

Table 76 ***Advanced Services > VPN Services > Add/Edit VPN Service Profiles*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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	N/A	Select an IKE profile from the drop-down menu. Click 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 166.

Table 76 ***Advanced Services > VPN Services > Add/Edit VPN Service Profiles*** *Field Descriptions*

Field	Default	Description
PPTP Profile	N/A	Select a PPTK profile from the drop-down menu. Click 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 167.
L2TP Profile	N/A	Select an L2TP profile from the drop-down menu. Click 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 167.
IPSEC Profile	N/A	Select an IPSEC profile from the drop-down menu. Click 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 169.

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

NOTE

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

Click **Add** to create a new IKE profile, or click the pencil icon next to an existing profile to edit that profile. Table 77 describes the fields on the **Advanced Services > VPN Services > IKE Add/Edit Detail** page.

Table 77 ***Advanced Services > VPN Services > IKE Add/Edit Detail*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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	N/A	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.

Table 77 ***Advanced Services > VPN Services > IKE Add/Edit Detail*** *Field Descriptions (Continued)*

Field	Default	Description
IKE Shared Secrets		
Add	N/A	Click this button to add an IKE shared secret. The following settings appear. Complete these settings and click **Add** in this section. ● **Subnet**—Enter the subnet for the shared secret. ● **Subnet Mask**—Enter the subnet mask for the shared secret. ● **IKE Shared Secret**—Type the shared secret, and confirm.
IKE Policies		
Add	N/A	Click this button to add a new IKE policy. The following settings appear. Complete these settings and click **Add** in this section. ● **Priority**—Type the priority number of this IKE policy. ● **Encryption**—From the drop-down menu, select the encryption type to be supported in the IKE policy. ● **Hash Algorithm**—Select the hash algorithm for this IKE policy. ● **Authentication**—Select the authentication type to be supported in this IKE policy. ● **Diffie-Hellman Group**—Select the bit-level to be supported. ● **Lifetime** (300-86400 sec)—Define the lifetime, in seconds, for the IKE policy. Once one or more policies are added, select the policy to apply to the **VPN Services > IKE** profile being configured.

Click **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 > 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 **Aruba Configuration** navigation pane. This page lists all L2TP profiles that are currently available. Click **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 79.

Table 78 ***Advanced Services > VPN Services > L2TP*** *Add/Edit Details Field Descriptions*

Field	Default	Description
General Settings		

Table 78 ***Advanced Services > VPN Services > L2TP** Add/Edit Details Field Descriptions*

Field	Default	Description
Folder	Top	Use this field to set and display 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	N/A	Enter the IP address of the primary DNS server.
Secondary DNS Server	N/A	Enter the IP address of the secondary DNS server.
Primary WINS Server	N/A	Enter the IP address of the primary Windows Internet Naming Service (WINS) server.
Secondary WINS Server	N/A	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.

Click **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. Click Add to create a new PPTP profile, or click the pencil icon next to an existing profile to edit that profile. The Add/Edit Details page appears.

The **Advanced Services > VPN Services > PPTP Add/Edit Details** page contains the following fields, as described in Table 79:

Table 79 ***Advanced Services > VPN Services > PPTP Add/Edit Details** Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the PPTP profile is associated. The drop-down 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	N/A	Enter the IP address of the primary DNS server.
Secondary DNS Server	N/A	Enter the IP address of the secondary DNS server.
Primary WINS Server	N/A	Enter the IP address of the primary Windows Internet Naming Service (WINS) server.
Secondary WINS Server	N/A	Enter the IP address of the secondary WINS server.

Click **Add** to create the PPTP profile, or click **Save** to preserve changes to an existing PPTP 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 **Aruba 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.

Click **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 80:

Table 80 ***Advanced Services > VPN Services > IPSEC Add/Edit*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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	N/A	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 170.

Click **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 > Aruba 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.

Click **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 81:

Table 81 ***Advanced Services > VPN Services > IPSEC > Dynamic Map Add/Edit*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display the folder with which the Dynamic Map is associated. The drop-down menu displays all folders available for association with the Dynamic Map.

Table 81 ***Advanced Services > VPN Services > IPSEC > Dynamic Map Add/Edit*** *Field Descriptions*

Field	Default	Description
Name	Blank	Enter the name of the Dynamic Map.
Other Settings		
Priority	N/A	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.
Perfect Forward Secrecy Mode	None	From the drop-down menu, select the Diffie-Hellman group to be used by this dynamic map.
Lifetime (300-86400 sec)	N/A	Define the lifetime in seconds for the dynamic map, when deployed in IPSEC profiles.
Transform Set 1-4	N/A	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 171.

Click **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 **Aruba Configuration** navigation pane. This page displays all currently configured Transform Sets, and which Dynamic Maps reference them.

Click **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 82:

Table 82 ***Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set Add/Edit Details*** *Field Descriptions*

Field	Default	Description
General Settings		
Folder	Top	Use this field to set and display 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.

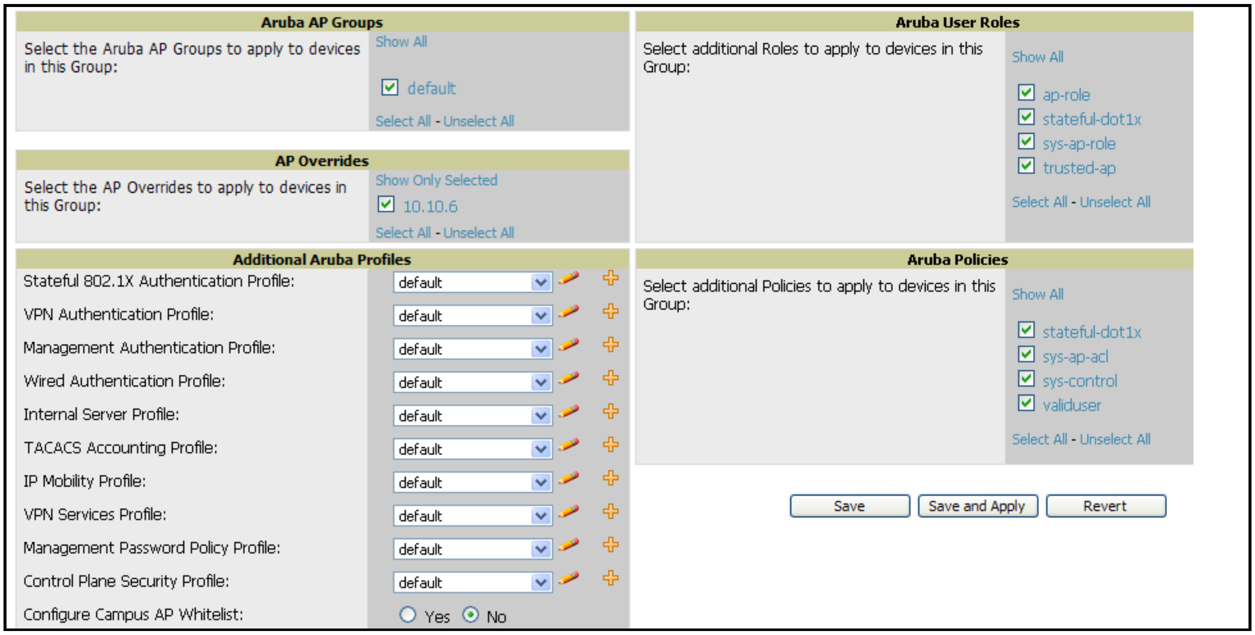
Click **Add** to create the new Transform Set, or click **Save** if editing an existing Transform Set. The Transform Set is available for reference by Dynamic Maps in support of IPSEC profiles and VPN services.

Groups > Aruba Config Page and Section Information

Create Aruba AP Groups with the **Device Setup > Aruba Configuration** page, as described in earlier in this document. To view and edit profile assignments for Aruba AP Groups, perform these steps.

1. Navigate to the **Groups > List** page.
2. Click the name of the Aruba AP Group to view and edit, and navigate to the **Aruba Config** page, illustrated in Figure 44:

Figure 44 ***Groups* > *List* > *Aruba Config*** *Page Illustration for an Aruba AP Group*



Aruba AP Groups

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

☑ default

Select All - Unselect All

AP Overrides

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

☑ 10.10.6

Select All - Unselect All

Additional Aruba Profiles

Stateful 802.1X Authentication Profile:	default
VPN Authentication Profile:	default
Management Authentication Profile:	default
Wired Authentication Profile:	default
Internal Server Profile:	default
TACACS Accounting Profile:	default
IP Mobility Profile:	default
VPN Services Profile:	default
Management Password Policy Profile:	default
Control Plane Security Profile:	default
Configure Campus AP Whitelist:	○ Yes ● No

Aruba User Roles

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

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

Select All - Unselect All

Aruba Policies

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

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

Select All - Unselect All

3. Complete the profile assignments on this page, referring to additional topics in this appendix for additional infomration. Table 83 provides a summary of topics supporting these settings.

Table 83 *Information Resources for the* ***Groups* > *List* > *Aruba Config*** *Page*

Section	Additional Information Available In These Locations
Aruba AP Groups Section	● "Aruba AP Groups Pages and Field Descriptions" on page 52 ● "General Aruba AP Groups Procedures and Guidelines" on page 34 ● "Setting Up Initial Aruba Configuration" on page 24 ● "Aruba AP Groups Section" on page 14
AP Overrides	● "AP Overrides Pages and Field Descriptions" on page 56 ● "AP Overrides Guidelines" on page 41 ● "Configuring or Editing AP Overrides" on page 41 ● "AP Overrides Section" on page 15
Additional Aruba Profiles	● Appendix A, "Aruba Configuration Reference" on page 49
Aruba User Roles	● "Security > User Roles" on page 141 ● "Visibility in Aruba Configuration" on page 45
Aruba Policies	● "Security > Policies" on page 146 ● "Visibility in Aruba Configuration" on page 45

Index