

# Dell Networking W-AirWave 8.0



Controller Configuration Guide

## Copyright

© 2014 Aruba Networks, Inc. Aruba Networks trademarks include , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. All other trademarks are the property of their respective owners.

## 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. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011

Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg, et al. The Open Source code used can be found at this site:

[http://www.arubanetworks.com/open\\_source](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.

<b>Controller Configuration in AirWave .....</b>	<b>7</b>
Requirements, Restrictions, and AOS Support in AirWave .....	7
Requirements .....	7
Restrictions .....	7
AOS Support in AirWave .....	7
Overview of Dell Networking W Configuration in AirWave .....	8
Device Setup > Dell Networking W Configuration Page .....	9
Groups > Controller Config Page with Global Configuration Enabled .....	10
Groups > Controller Config when Global Configuration is Disabled .....	10
Support for Editing Multiple Device Settings .....	10
Controller Configuration Sections in the Tree View .....	11
Dell Networking W AP Groups Section .....	11
AP Overrides Section .....	12
WLANs Section .....	12
Profiles Section .....	13
Security Section .....	14
Local Config Section .....	14
Advanced Services Section .....	15
APs/Devices > List Page .....	15
APs/Devices > Manage Page .....	15
APs/Devices > Monitor Page .....	16
APs/Devices > Audit Page .....	17
Groups > Basic Page .....	17
Additional Concepts and Components .....	17
Global Configuration and Scope .....	17
Referenced Profile Setup .....	17
Save, Save and Apply, and Revert Buttons .....	19
Additional Concepts and Benefits .....	20
Scheduling Configuration Changes .....	20
Auditing and Reviewing Configurations .....	20
Licensing and Dependencies in Dell Networking W Configuration .....	20
Setting Up Initial Dell Networking W Configuration .....	20
Prerequisites .....	21
Procedure .....	21
Additional Capabilities .....	26
<b>Dell Networking W Configuration in Daily Operations .....</b>	<b>27</b>
Dell Networking W AP Groups Procedures and Guidelines .....	27
Guidelines and Pages for Dell Networking W AP Groups .....	27
Selecting Dell Networking W AP Groups .....	27
Configuring Dell Networking W AP Groups .....	28
General WLAN Guidelines .....	28
Guidelines and Pages for WLANs in Dell Networking W Configuration .....	28
General Profiles Guidelines .....	28
General Controller Procedures and Guidelines .....	29
Using Master, Standby Master, and Local Controllers .....	29

Pushing Device Configurations to Controllers .....	29
AP Overrides Guidelines .....	30
Supporting APs with Dell Networking W Configuration .....	30
Changing Adaptive Radio Management (ARM) Settings .....	30
Changing SSID and Encryption Settings .....	30
Changing the Dell Networking W AP Group for an AP Device .....	30
Using AirWave to Deploy Dell Networking W-Series APs .....	31
Using General AirWave Device Groups and Folders .....	32
Visibility in Dell Networking W Configuration .....	32
Visibility Overview .....	32
Defining Visibility for Dell Networking W Configuration .....	33
<b>Controller Configuration Reference .....</b>	<b>37</b>
Overview .....	37
Dell Networking W AP Groups .....	38
About Dell Networking W AP Groups .....	38
AP Overrides .....	41
WLANs .....	46
Overview of WLANs Configuration .....	46
WLANs .....	46
WLANs > Basic .....	47
WLANs > Advanced .....	47
Profiles .....	47
Understanding Dell Networking W Configuration Profiles .....	47
Security .....	48
Security > User Roles .....	50
Security > User Roles > BW Contracts .....	50
Security > User Roles > VPN Dialers .....	51
Security > Policies .....	51
Security > Policies > Destinations .....	51
Security > Policies > Services .....	51
Security > Server Groups .....	52
Server Groups Page Overview .....	52
Supported Servers .....	52
Adding a New Server Group .....	53
Security > Server Groups > LDAP .....	53
Security > Server Groups > RADIUS .....	53
Security > Server Groups > TACACS .....	53
Security > Server Groups > Internal .....	54
Security > Server Groups > XML API .....	54
Security > Server Groups > RFC 3576 .....	54
Security > Server Groups > Windows .....	54
Security > TACACS Accounting .....	54
Security > Time Ranges .....	55
Security > User Rules .....	55
Local Config .....	55
Local Config > Network .....	56
Local Config > Network > Controller .....	56
Local Config > Network > VLANs .....	56
Local Config > Network > Ports/Interfaces .....	57
Local Config > Network > IP .....	57

Local Config > Management .....	57
Local Config > Management >General .....	57
Local Config > Management >Administration .....	58
Local Config > Management >SNMP .....	58
Local Config > Management> Logging .....	58
Local Config > Management> Clock .....	58
Local Config > Advanced >Redundancy .....	58
Advanced Services .....	59
Advanced Services > AirGroup .....	59
Advanced Services > AirGroup > CPPM Server AAA .....	59
Advanced Services > AirGroup > Domain .....	60
Advanced Services > AirGroup > Service .....	60
Advanced Services > IP Mobility .....	61
Advanced Services > IP Mobility > Mobility Domain .....	61
Advanced Services > VPN Services .....	62
Advanced Services > VPN Services > IKE Profile .....	62
Advanced Services > VPN Services > IKE > IKE Policy .....	63
Advanced Services > VPN Services > IPSEC Profile .....	63
Advanced Services > VPN Services > IPSEC > Dynamic Map .....	63
Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set .....	64
Advanced Services > VPN Services > L2TP Profile .....	64
Advanced Services > VPN Services > PPTP Profile .....	64
Groups > Controller Config Page .....	65
<b>Index .....</b>	<b>67</b>



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



---

When configuring the controller, we recommend that you have access to the *Dell Networking W-Series ArubaOS User Guide* and the *Dell Networking W-Series ArubaOS CLI Guide* to use as a reference.

---

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

- "Requirements, Restrictions, and AOS Support in AirWave" on page 7
- "Additional Concepts and Components" on page 17
- "Setting Up Initial Dell Networking W Configuration" on page 20



---

AirWave supports Dell Networking W AP Groups, which should not be confused with standard Dell Networking W Device Groups. This document provides information about the configuration and use of Dell Networking W AP Groups and describes how Dell Networking W AP Groups inter-operate with standard Dell Networking W Device Groups.

---



---

Dell Networking W may be represented as Dell PowerConnect W in the AirWave WebUI.

---

## Requirements, Restrictions, and AOS Support in AirWave

### Requirements

Dell Networking W Configuration has the following requirements in AirWave:

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

### Restrictions

Dell Networking W configuration has the following restrictions in AirWave:

- At present, Dell Networking W Configuration in AirWave does not support every AOS network component. For example, AirWave supports only **AirGroup**, **IP Mobility** and **VLANs** in the **Advanced Services** section.
- AOS Configuration is not supported in either Global Groups or the Master Console. Appropriate options will be available in the Subscriber Groups containing the controllers.

### AOS Support in AirWave

AirWave provides the following options for configuring your devices:

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

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

AirWave only supports configuration of the settings that a master controller would push to the standby / local controllers (global features). AirWave supports all master, master-standby, and master-local deployments. AirWave supports all settings for Profiles, Dell Networking W AP Groups, Servers and Roles, and the WLAN Wizard. Controller IP addresses, VLANs, and interfaces are also supported, as are AirGroup, VPN and IP Mobility Advanced services.

Other features of Dell Networking W Configuration in AirWave include:

- AirWave understands AOS license dependencies.
- AirWave supports a variety of Dell Networking W-Series firmware versions. Profiles and fields that are not supported by an older version will not be configured on the controller running that version.
- You can provision thin APs from the **AP/Devices > Manage** page. You can move APs into Dell Networking W AP Groups from the **Modify Devices** option on the **APs/Devices > List** page.
- You can configure AP names in the **Settings section** of the **AP/Devices > Manage** page.
- Values for specific fields can be overwritten for individual controllers via overrides on the controller's **APs/Devices > Manage** page.

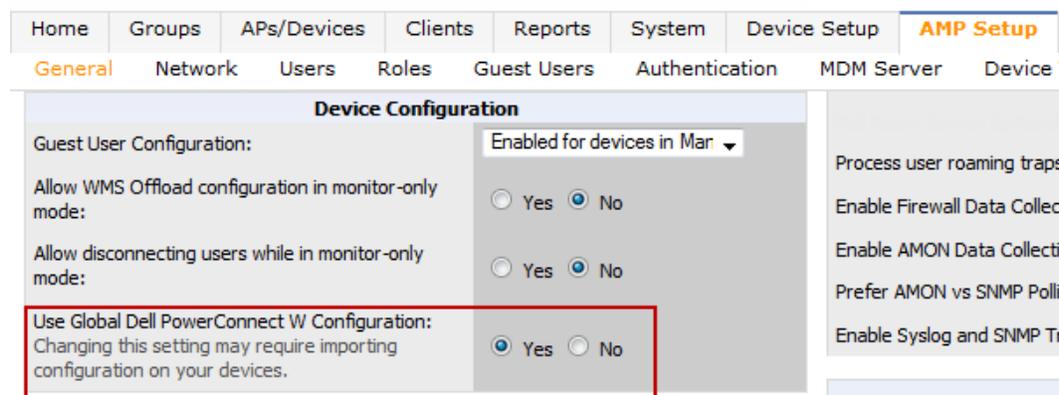
For more detailed information about this feature, as well as steps to transition from template-based configuration to web-based configuration, refer to additional chapters in this user guide. For known issues and details about the AOS version supported by each release, see the *Dell Networking W-AirWave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

## Overview of Dell Networking W Configuration in AirWave

This section describes the pages in AirWave that support Dell Networking W Configuration.

AirWave can be set up on **AMP Setup > General > Device Configuration** to configure Dell Networking W-Series devices globally (using the **Device Setup > Dell Networking W Configuration** page) or by Device Group (in the **Groups > Controller Config** page). By default, global Dell Networking W Configuration is enabled, as shown in the following image.

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



AirWave supports Dell Networking W Configuration with the following pages:

- "[Device Setup > Dell Networking W Configuration Page](#)" on [page 9](#)—Deploys and maintains *global* Dell Networking W Configuration in AirWave. You can limit the view to a folder.

- "Groups > Controller Config Page with Global Configuration Enabled" on page 10—the way this page displays depends on whether global or group configuration is enabled in **AMP Setup > General > Device Configuration**:
  - If global configuration is enabled, the **Groups > Controller Config** page manages Dell Networking W AP group and other controller-wide settings defined on the **Device Setup > Dell Networking W Configuration** page.
  - If global configuration is disabled, the **Groups > Controller Config** page resembles the **Device Setup > Dell Networking W Configuration** tree navigation (the same sections listed in the previous bullet are available), but the **Groups > Controller Config** pages do not display the **Folder** as a column in the list tables or as a field in the individual profiles.
- "Groups > Controller Config when Global Configuration is Disabled" on page 10— this page modifies or reboots all devices when Global Dell Networking W Configuration is disabled.
- "APs/Devices > Manage Page" on page 15—supports device-level settings and changes in AirWave.
- "APs/Devices > Monitor Page" on page 16—supports device-level monitoring in AirWave.
- "APs/Devices > Audit Page" on page 17—supports device level configuration importing in AirWave.
- "Groups > Basic Page" on page 17—For device groups containing Dell Networking W devices, basic information such as the group's name, regulatory domain, the use of Global Groups, SNMP Polling periods, and turning on the Dell Networking W GUI Config are managed here.

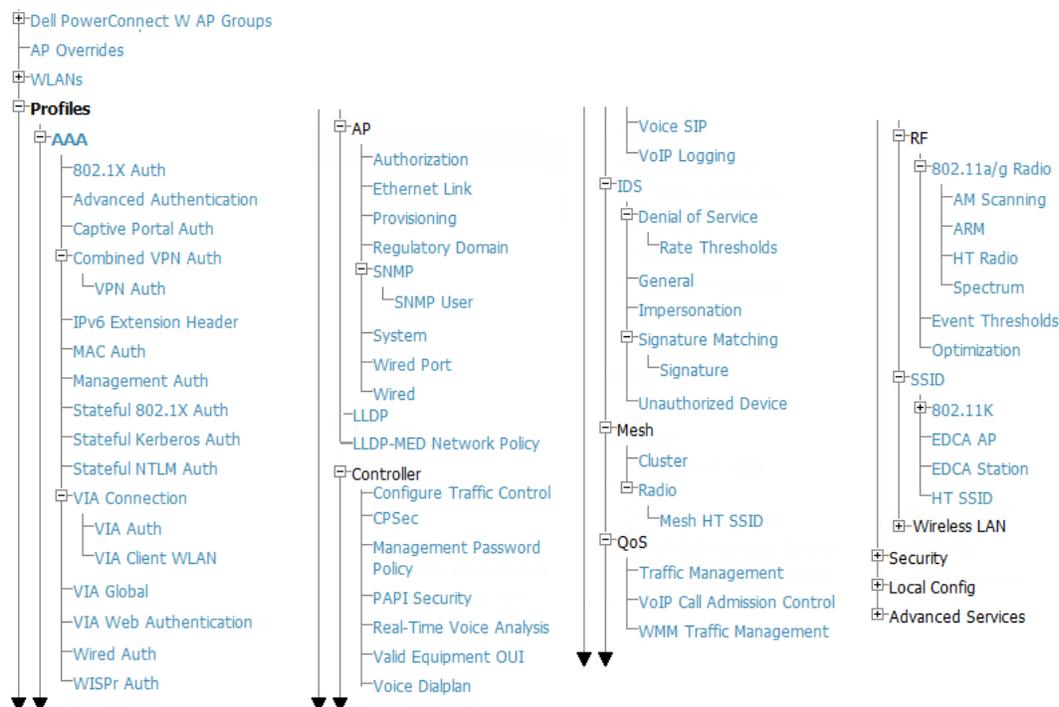
## Device Setup > Dell Networking W Configuration Page



This page is not available if **Use Global Dell Networking W Configuration** is disabled in **AMP Setup > General**.

The **Device Setup > Dell Networking W Configuration** page displays the expandable navigation pane shown in Figure 2, allowing you to monitor and configure Dell Networking W AP Groups, AP Overrides, WLANs, Profiles, Security, Local Config, and Advanced Services. Each of these sections is summarized in "Controller Configuration Sections in the Tree View" on page 11.

**Figure 2: Device Setup > Dell Networking W Configuration Navigation Illustration**



## Groups > Controller Config Page with Global Configuration Enabled

When **Use Global Dell Networking W Configuration** is enabled in the **AMP Setup > General** page, a focused sub-menu page displays allowing you to edit all configured Dell Networking W AP groups with the following factors:

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

**Figure 3:** *Groups > Controller Config > Dell Networking W AP Groups page illustration (partial display)*

## Groups > Controller Config when Global Configuration is Disabled

If **Use Global Dell Networking W Configuration** in **AMP Setup > General** is set to **No**, the **Groups > Controller Config** page can be used to manage two or more distinctive configuration strategies using the same tree navigation as the **Device Setup > Dell Networking W Configuration** page. Each of the sections is explained in "[Controller Configuration Sections in the Tree View](#)" on page 11.

## Support for Editing Multiple Device Settings

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

**Table 1:** *Editing Multiple Device Settings*

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

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

## Controller Configuration Sections in the Tree View

Whether you are using global or group configuration, the Dell Networking W Configuration tree view page supports several sections, as follows:

- "Dell Networking W AP Groups Section" on page 11
- "AP Overrides Section" on page 12
- "WLANs Section" on page 12
- "Profiles Section" on page 13
- "Security Section" on page 14
- "Local Config Section" on page 14
- "Advanced Services Section" on page 15




---

Only Dell Networking W AP Groups, AP Overrides, and WLANs contain custom-created items in the navigation pane.

---

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

## Dell Networking W AP Groups Section

A Dell Networking W AP Group is a collection of configuration profiles that define specific settings on Dell Networking W-Series controllers and the devices that they govern. A Dell Networking W AP Group references multiple configuration profiles, and in turn links to multiple WLANs. Navigate to the **Controller Config** > **Dell Networking W AP Groups** page (see Figure 4).

**Figure 4:** Controller Config > Dell Networking W AP Groups Navigation

Limit to Folder: Top

Add New Dell PowerConnect W AP Group

11-20 of 72 Dell PowerConnect W AP Groups | < < Page 2 of 8 > > | Choose Columns CSV Export

	Name ▲	APs	Used By			
			User Role	RAP Whitelist	Authorization	Controller
<input type="checkbox"/>	10.0.0	1	-	-	-	-
<input type="checkbox"/>	1341-AlphaNet-SM	0	-	-	-	-
<input type="checkbox"/>	1341-FiveNines-AP	0	-	-	-	-
<input type="checkbox"/>	1341-FiveNines-SM	0	-	-	-	-
<input type="checkbox"/>	1341-QA-LoadTest	0	-	-	-	-
<input type="checkbox"/>	1344	0	-	-	-	-
<input type="checkbox"/>	azalea-corp	0	-	-	-	-
<input type="checkbox"/>	Beijing-BSO	0	-	-	-	-
<input type="checkbox"/>	Beijing-ENG-10thFloor	0	-	-	-	-
<input type="checkbox"/>	Beijing-ENG-9thFloor	0	-	-	-	-

11-20 of 72 Dell PowerConnect W AP Groups | < < Page 2 of 8 > > |

Select All - Unselect All

Delete




---

Dell Networking W AP Groups are not to be confused with conventional AirWave device groups. AirWave supports both group types, and both are viewable on the **Groups** > **List** page when so configured.

---

Dell Networking W AP Groups share the following characteristics:

- Any Dell Networking W-Series controllers can support multiple Dell Networking W AP Groups.

- Dell Networking W AP Groups are assigned to folders, and folders define visibility. Using conventional AirWave folders to define visibility, Dell Networking W 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 Dell Networking W Configuration](#)" on page 32.
- You can import a controller configuration file from AOS for Dell Networking W AP Group deployment in AirWave.

For additional information, see:

- "[Setting Up Initial Dell Networking W Configuration](#)" on page 20
- "[Dell Networking W AP Groups Procedures and Guidelines](#)" on page 27

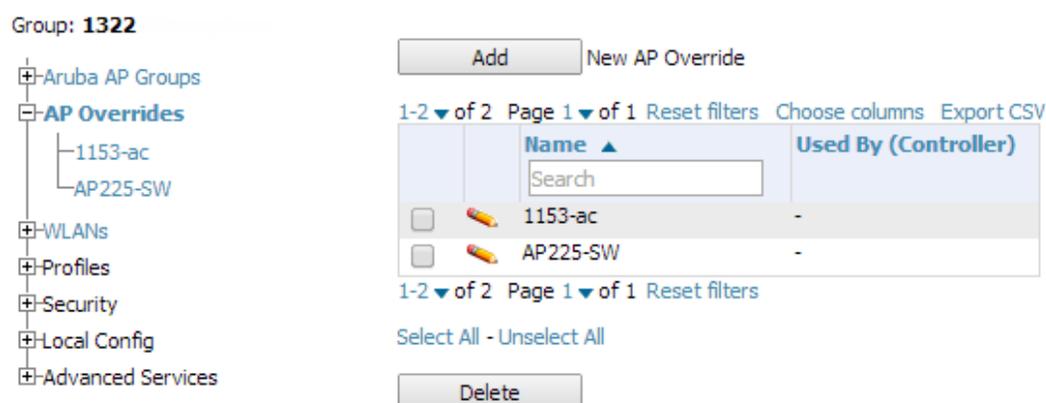
## AP Overrides Section

The second major component of Dell Networking W Configuration is the **AP Overrides** page, appearing immediately below **Dell Networking W AP Groups** in the Navigation Pane.

**AP Overrides** operate as follows in Dell Networking W Configuration:

- Custom-created AP Overrides appear in the Dell Networking W Configuration navigation pane, as illustrated in .
- Dell Networking W-Series controllers and AP devices operate in Dell Networking W AP Groups that define shared parameters for all devices in those groups. The **Dell Networking W Configuration > Dell Networking W AP Groups** page displays all current Dell Networking W AP groups.
- **AP Override** allows you to change some parameters for any specific device without having to create a Dell Networking W AP group per AP.
- The name of any **AP Override** should be the same as the name of the device to which it applies. This establishes the basis of all linking to that device.
- Once you have created an **AP Override** for a device in a group, you specify the **WLANs** to be included and excluded.
- For additional information about how to configure and use AP Overrides, refer to "[AP Overrides](#)" on page 41.

**Figure 5:** *AP Overrides*



## WLANs Section

Access WLANs with **Dell Networking W Configuration > WLANs**, (see [Figure 6](#)). The following concepts govern the use of WLANs in Dell Networking W configuration:

- WLANs are the same as virtual AP configuration profiles.
- WLAN profiles contain settings including SSIDs, referenced Dell Networking W AP Groups, Traffic Management profiles, and device folders.

WLAN configurations are described in:

- "Setting Up Initial Dell Networking W Configuration" on page 20
- "General WLAN Guidelines" on page 28
- "WLANs" on page 46

**Figure 6: Dell Networking W Configuration > WLANs Navigation**

Group: 1322

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

Add		New WLAN				
		1-15 of 15 Page 1 of 1 Reset filters Choose columns Export CSV				
	Name	SSID	Aruba AP Group	AP Override	Used By	
	Search				Traffic Management	Controller
<input type="checkbox"/>	1.0.0_ethersphere-voip	ethersphere-voip	corp-no-scanning, corp	-	g-band	-
<input type="checkbox"/>	1.0.0_ethersphere-voip-11ac	ethersphere-11ac-voip	-	-	-	-
<input type="checkbox"/>	1.0.0_ethersphere-voip-psk	ethersphere-psk	corp-no-scanning, corp	-	-	-
<input type="checkbox"/>	1.0.0_ethersphere-wpa2	ethersphere-wpa2	corp-no-scanning, corp	-	a-band	-
<input type="checkbox"/>	1.0.0_ethersphere-wpa2-11ac	ethersphere-11ac-test	-	-	-	-
<input type="checkbox"/>	1.0.0_ethersphere_guest	ethersphere-wpa2	-	-	-	-
<input type="checkbox"/>	1.0.0_guest_tunnel	ARUBA-VISITOR	corp-no-scanning, corp	-	g-band, a-band	-
<input type="checkbox"/>	1341-HD-Test	hd-wpa2-psk	-	-	-	-
<input type="checkbox"/>	default	ethersphere-wpa2	-	-	-	-
<input type="checkbox"/>	India-Guest	ARUBA-VISITOR	SA-india-default, SA-india-corp	-	-	-
<input type="checkbox"/>	indiaMDNS	indiamdns	SA-india-corp, SA-india-corp	-	-	-
<input type="checkbox"/>	SA-india-ethersphere-voip	ethersphere-voip	SA-india-default, SA-india-corp	-	-	-
<input type="checkbox"/>	SA-india-ethersphere-wpa2	ethersphere-wpa2	SA-india-default, SA-india-corp	-	-	-
<input type="checkbox"/>	SA-india-ethersphere-wpa2-G-radio	ethersphere-wpa2	-	-	-	-

1-15 of 15 Page 1 of 1 Reset filters

Select All - Unselect All

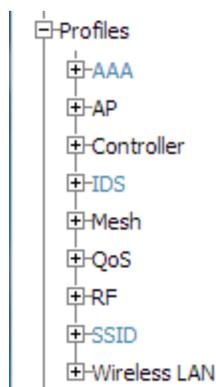
Delete

## Profiles Section

Use Profiles to organize and deploy groups of configurations for Dell Networking W AP Groups, WLANs, and other profiles. Profiles are assigned to folders, which establishes visibility to Dell Networking W AP Groups and WLAN settings. Access Profiles with **Dell Networking W Configuration > Profiles** (see Figure 7). Profiles are organized by type. Custom-named profiles do not appear in the navigation pane as do custom-named Dell Networking W AP Groups, WLANs, and AP Overrides. Profile procedures and guidelines are described in:

- "Setting Up Initial Dell Networking W Configuration" on page 20
- "General Profiles Guidelines" on page 28
- "Profiles" on page 47

**Figure 7: Dell Networking W Configuration > Profiles Navigation**

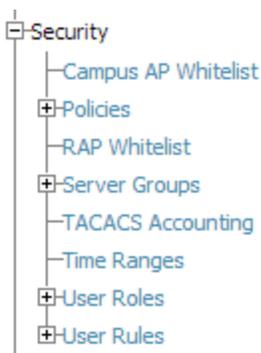


## Security Section

Use the **Security** section to add edits or delete security profiles in multiple categories, including user roles, policies, rules, and servers such as RADIUS, TACACS+, and LDAP servers. Navigate to Security with the **Dell Networking W Configuration > Security** path, (see [Figure 8](#)). The following general guidelines apply to **Security** profiles in Dell Networking W configuration:

- Roles can have multiple policies, and each policy can have numerous roles.
- Server groups are comprised of servers and rules. Security rules apply in Dell Networking W Configuration in the same way as the rules deployed in AOS. For additional information about Security, refer to "Security" on page 48 in the Appendix.

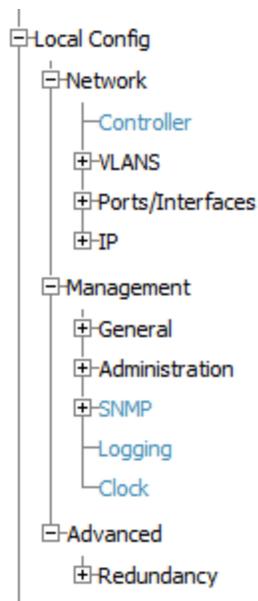
**Figure 8:** Dell Networking W Configuration > Security Navigation



## Local Config Section

Use the Local Config section for local configuration of Dell Networking W-Series controllers (see [Figure 4](#)). Locally configured settings are not pushed to local controllers by master controllers. SNMP trap settings for controllers are also managed locally. For additional information, refer to "Local Config " on page 55.

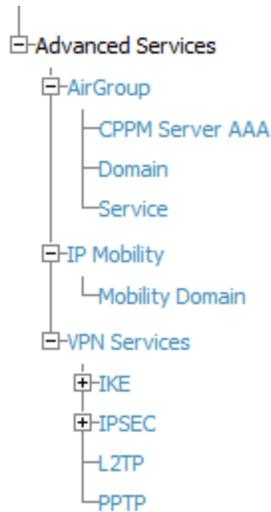
**Figure 9:** Dell Networking W Configuration > Local Config Navigation



## Advanced Services Section

Navigate to Advanced Services with the **Dell Networking W Configuration > Advanced Services** path. The **Advanced Services** section includes AirGroup, IP Mobility and VPN Services (see [Figure 10](#) For additional information about AirGroup, IP Mobility and VPN Services, refer to "Advanced Services" on page 59.

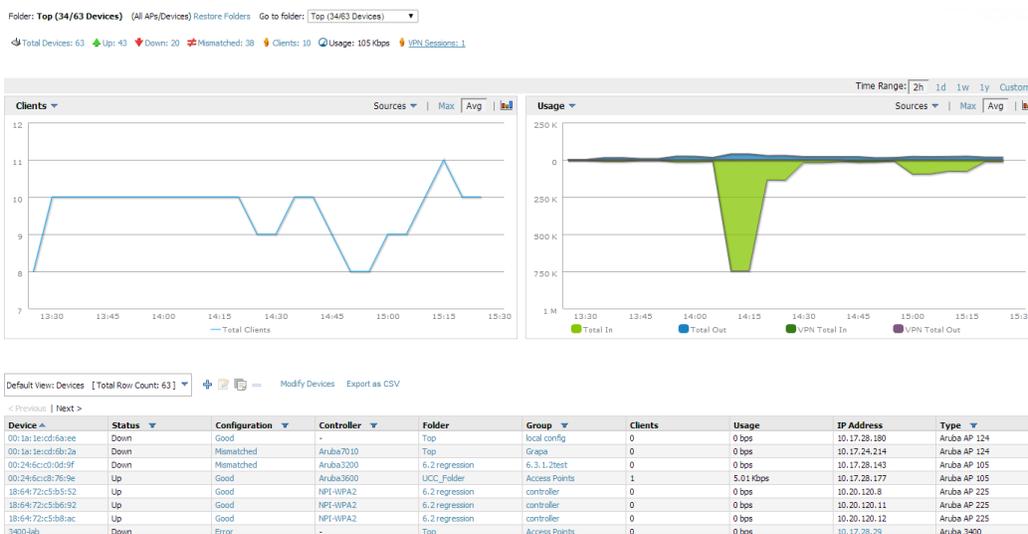
**Figure 10:** Dell Networking W Configuration > Advanced Services Navigation



## APs/Devices > List Page

This page supports all AirWave devices. This page supports controller reboot, re-provisioning, changing Dell Networking W AP groups, and updating thin AP settings (see [Figure 11](#)). Select **Modify Devices** below the graphs to perform these tasks and more. The Modify Devices field also includes an option to configure a custom view using search filters.

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



## APs/Devices > Manage Page

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

You can create controller overrides for entire profiles or a specific profile setting per profile. This allows you to avoid creating new profiles or Dell Networking W AP Groups that differ by one or more settings. Controller overrides can be added from the controller's **APs/Devices > Manage** page (see [Figure 12](#)).

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

The screenshot displays the configuration page for an Aruba 3600 controller. It is divided into several sections:

- General:** Name: Aruba3600, Status: Up (OK), Configuration: Mismatched (More Details), Last Contacted: 4/13/2014 7:34 PM, Type: Aruba 3600, Firmware: 6.3.1.2, Group: 10.17.24.28 Customer Issue, Folder: Top, Management Mode: Monitor Only + Firmware Upgrades, Enable Planned Downtime Mode: Yes.
- Settings:** Name: Aruba3600, Location, Contact, Latitude, Longitude, Altitude (m), Group: 10.17.24.28 Customer Iss, Folder: Top, Auto Detect Upstream Device: Yes, Upstream device will automatically be updated when the device is polled, Automatically clear Down Status Message when device comes back up: Yes, Down Status Message.
- Device Communication:** View Device Credentials, IP Address: 10.17.24.28, SNMP Port (1-65535): 161, SSH Port (1-65535): 22, 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.
- Aruba Overrides:** Add New Aruba Controller Override, Table with 4 columns: Profile, Instance, Field, Value.
 

Profile	Instance	Field	Value
Routed Virtual Interface	Routed Virtual Interface 1	IP Address	10.17.24.28
Routed Virtual Interface	Routed Virtual Interface 1	IP Netmask	255.255.255.0
Web SSH Management Profile	default	Captive Portal Certificate	-
Web SSH Management Profile	default	Web Server Certificate	-
- Network Settings:** Gateway.
- Maintenance Windows:** Add New AP Maintenance Window.

## APs/Devices > Monitor Page

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

- Status nfo
- Controller's License link
- Radio Statistics about some Dell Networking W thin APs
- **Clients** and **Usage** and interactive graphs showing the numbers of clients connected to the network, and upstream and downstream bandwidth usage over the selected period.
- CPU Utilization and Memory Utilization interactive graphs.
- APs Managed by this controller list (when viewing a controller)
- Alert Summary
- An option to poll the controller
- Recent AirWave Device Events
- Links to the **System Event** and **Audit Logs**
- Information about wired interfaces
- Information about RF Neighbors

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

## APs/Devices > Audit Page

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

- Audit a device's current configuration
- Update group settings based on the device's current configuration using the **Import** button
- Customize settings to include/ignore during configuration audits
- View configuration mismatches
- View archived device configurations
- Create and restore flash backups.

## Groups > Basic Page

The **Groups > Basic** page deploys the following aspects of Dell Networking W Configuration:

- Use this page to control which device settings appear on the **Groups** pages.
- If you want to configure your controllers using templates instead, disable Dell Networking W GUI configuration from the **Groups > Basic** page and use template-based configuration. See the *Dell Networking W-AirWave 8.0 User Guide* for more information about templates.

## Additional Concepts and Components

Dell Networking W Configuration emphasizes the following components and network management concepts.

- ["Global Configuration and Scope" on page 17](#)
- ["Referenced Profile Setup" on page 17](#)
- ["Save, Save and Apply, and Revert Buttons" on page 19](#)
- ["Additional Concepts and Benefits" on page 20](#)

## Global Configuration and Scope

AirWave 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 controller to local controllers. AirWave supports this AOS functionality.
- In an all-master-controller scenario, every master controller operates independently of other master controllers. AirWave provides the ability to push configurations to all master controllers in this scenario.
- Dell Networking W Configuration supports AOS profiles, Dell Networking W AP Profiles, Servers, and User Roles.

For additional information about these and additional functions, see ["General Controller Procedures and Guidelines" on page 29](#).

## Referenced Profile Setup

AirWave allows you to add or reconfigure many configuration profiles while guiding you through a larger configuration sequence for a Dell Networking W AP Group or WLAN. For example, after you create an Dell Networking W AP Group from the **Device Setup > Dell Networking W Configuration** page, the **Referenced Profile** section appears (see [Figure 13](#)).

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

This configuration is also supported on the **Additional Dell Networking W Profiles** section of the **Groups > Controller Config** page.

**Figure 13: Referenced Profile Configuration for a Dell Networking W 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: Requires version $\geq$ 3.3.0.0 and $<$ 5.0.0.0	default  
Ethernet Interface 0 Link Profile: Requires version $\geq$ 3.3.0.0 and $<$ 5.0.0.0	default  
Ethernet Interface 1 Link Profile: Requires version $\geq$ 3.3.0.0 and $<$ 5.0.0.0	default  
AP System Profile:	default  
Regulatory Domain Profile:	default  
SNMP Profile: Requires a version earlier than 3.4.0.0	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:	ids-low-setting  
Mesh Radio Profile: Requires an Outdoor Mesh Access Points license	default  
AP Authorization Profile: Requires a Remote Access Points license and version 5.0.0.0 and above, or RN 3.0	--None-- 
AP Provisioning Profile: Requires version 5.0.0.0 and above, or RN 3.0	--None-- 
Ethernet Interface 0 Port Configuration: Requires version 5.0.0.0 and above, or RN 3.0	default  
Ethernet Interface 1 Port Configuration: Requires version 5.0.0.0 and above, or RN 3.0	default  
Ethernet Interface 2 Port Configuration: Requires version 5.0.0.0 and above, or RN 3.0	shutdown  
Ethernet Interface 3 Port Configuration: Requires version 5.0.0.0 and above, or RN 3.0	shutdown  
Ethernet Interface 4 Port Configuration: Requires version 5.0.0.0 and above, or RN 3.0	shutdown  

## Save, Save and Apply, and Revert Buttons

Several **Add** or **Detail** pages in Dell Networking W Configuration include the **Save**, **Save and Apply**, and **Revert** buttons. These buttons function as follows:

- **Save** —This button saves a configuration but does not apply it, allowing you to return to complete or apply the configuration at a later time. If you use this button, you might see an alert on other Dell Networking W Configuration pages warning that you have unapplied Dell Networking W-Series Configuration Changes, and that

you must click **Save and Apply** to make the changes take effect. You can apply the configuration after all changes are complete.

- **Save and Apply**—This button saves and applies the configuration with reference to Manage and Monitor modes. For example, you must click **Save and Apply** for a configuration profile to propagate to all controllers in **Manage** mode. If you have controllers in **Monitor Only** mode, AirWave audits them, comparing their current configuration with the new desired configuration. For additional information and instructions about using **Manage** and **Monitor Only** modes, refer to "[Pushing Device Configurations to Controllers](#)" on page 29.
- **Revert**—This button cancels out of a new configuration or reverts back to the last saved configuration.

## Additional Concepts and Benefits

### Scheduling Configuration Changes

You can schedule deployment of Dell Networking W Configuration to minimize impact on network performance.

For example, configuration changes can be accumulated over time by using **Save and Apply** for devices in **Monitor Only** mode, then pushing all configuration changes at one time by putting devices in **Manage** mode. Refer to "[Pushing Device Configurations to Controllers](#)" on page 29.



---

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

---

AirWave pushes configuration settings that are defined in the GUI to the Dell Networking W-Series controllers as a set of CLI commands using Secure Shell (SSH). No controller reboot is required.

### Auditing and Reviewing Configurations

AirWave supports auditing or reviewing in these ways:

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

### Licensing and Dependencies in Dell Networking W Configuration

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

AirWave requires that you have a policy enforcement firewall license always installed on all Dell Networking W-Series 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 AirWave pages that reflect device configuration status.

Dell Networking W 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. AirWave does not push such configurations when a license related to those configurations is unavailable. For details on the licenses required by a specific version of AOS, refer to the *Dell Networking W-Series ArubaOS User Guide* for that release.

## Setting Up Initial Dell Networking W Configuration

This section describes how to deploy an initial setup of Dell Networking W Configuration.



---

Dell Networking W Configuration is enabled by default in AirWave.

---

## Prerequisites

- Complete the AirWave upgrade to AirWave 6.4 or later. Upon upgrade, global Dell Networking W Configuration is enabled by default in groups with devices in monitor-only mode that have AOS firmware of 3.3.2.10 or greater.
- Back up AOS controller configuration file. Information about backing up AirWave is available in the *Dell Networking W-AirWave 8.0 User Guide*.

## Procedure

Perform the following steps to deploy Dell Networking W Configuration when at least one Dell Networking W AP Group currently exists on at least one Dell Networking W-Series controller on the network:

1. Determine whether you are using global or group configuration, and set **AMP Setup > General > Device Configuration > Use Global Dell Networking W Configuration** accordingly.
2. On the **Groups > Basic** page, enable device preferences for Dell Networking W devices. This configuration defines optional group display options. This step is not critical to setup, and default settings will support groups appropriate for Dell Networking W Configuration. One important setting on this page is the **Dell Networking W GUI Config** option. Ensure that setting is **Yes**, which is the default setting. If this feature is disabled, the user will only be able to configure Aruba devices using templates.
3. Authorize Dell Networking W-Series controllers into the device group in **Monitor Only** mode, to prevent AirWave from changing the controllers' configurations.



---

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

---

4. Navigate to the **AP/s/Devices > Audit** page for the first controller to and select Import to importing an existing configuration file. [Figure 14](#) illustrates the information available on this page if the device is mismatched.

Figure 14: APs/Devices > Audit Page Illustration

Device Configuration of **Aruba650** in group **Access Points** in folder **Top**  
 This Device is in monitor-only mode.  
 Configuration read from device at 5/20/2014 4:16 AM

Configuration: Mismatched

**Audit** Audit the device's current configuration.

**Create Backup Now**

**Archived Backups & Configs**

1-1 of 1 Backups Page 1 of 1 [Choose columns](#) [Export CSV](#)

Archived Date	Type	Running Configuration	Backup	Firmware Version	Restore
5/18/2014 4:17 AM	Nightly	<a href="#">View</a>	<a href="#">Save</a>	6.1.3.2	<a href="#">Restore</a>

1-1 of 1 Backups Page 1 of 1  
[More Archived Configs](#)

Compare device configuration **Current Device Configuration** to device configuration

**Desired Configuration** **Compare**

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

**Import**  Include unreferenced profiles.

**Customize** Choose settings to ignore during configuration audits.

[Show entire config](#)  
[View Running Configuration](#)  
[View Telnet/SSH Command log](#)  
[Refresh this page](#)

Guest User Settings		
	Current Device Configuration	Desired Configuration
Guest user 'LTI-User' status	<b>Present</b>	<b>Destroy</b>
Guest user 'dcrsjraq' status	<b>Present</b>	<b>Destroy</b>
Guest user 'guestuser 1' status	<b>Present</b>	<b>Destroy</b>
Guest user 'wbrjptqd' status	<b>Present</b>	<b>Destroy</b>
Aruba AP Group Settings		
	Current Device Configuration	Desired Configuration
Aruba AP Group 'default' IDS Profile	<b>default</b>	<b>ids-low-setting</b>
Aruba AP Override Settings		
	Current Device Configuration	Desired Configuration
AP Override 'test' Status	<b>Present</b>	<b>Delete</b>
Aruba WLAN Settings		

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

*In Global Configuration:*

Importing a global configuration creates all the Profiles and Dell Networking W AP Groups on the **Device Setup > Dell Networking W Configuration** page. This action also adds and selects the Dell Networking W AP Groups that appear on the **Groups > Dell Networking W Config** page.

The folder that contains all of the Profiles and Dell Networking W AP Groups is set to the top folder of the AirWave user who imports the configuration. This folder is named **Top** in the case of managing administrators with read/write privileges.

*In Group Configuration:*

Importing the group configuration creates Profiles and Dell Networking W AP Groups in the controller's **Groups > Controller Config** page.

5. After configuration file import is complete, refresh the page to verify the results of the import and add or edit the imported parameters as required.
6. Navigate to the **Controller Configuration** page.
  - This page displays a list of APs authorized on AirWave that are using the Dell Networking W AP Group.
  - The **User Role** is the Dell Networking W User Role used in firewall settings. For additional information, refer to "[Security > User Roles](#)" on page 50.
  - *Global Configuration only:* The **Folder** column cites the visibility level to devices in each Dell Networking W AP Group. For additional information, refer to "[Visibility in Dell Networking W Configuration](#)" on page 32.
7. Add or modify Dell Networking W AP Groups as required.
  - a. Navigate to the **Dell Networking W Configuration > Dell Networking W AP Groups** page.
  - b. Click **Add New Dell Networking W AP Group** to create a new Dell Networking W AP Group. To edit an AP Group, click the pencil icon next to the group. The **Details** page for the AP Group appears. This page allows you to select the profiles to apply to the AP Group, and to select one or more WLANs that support that AP Group (see [Figure 15](#)).

**Figure 15:** Dell Networking W Configuration > Dell Networking W AP Groups > Add/Edit Details Page (Partial View)

Folder: Top

Name:

**WLANs**

WLANs: Show All

default

Select All - Unselect All

**Referenced Profiles**

802.11a Radio Profile:	default		
802.11g Radio Profile:	default		
RF Optimization Profile:	default		
Event Thresholds Profile:	default		
Wired AP Profile: Requires version ≥ 3.3.0.0 and < 5.0.0.0	default		
Ethernet Interface 0 Link Profile: Requires version ≥ 3.3.0.0 and < 5.0.0.0	default		
Ethernet Interface 1 Link Profile: Requires version ≥ 3.3.0.0 and < 5.0.0.0	default		
AP System Profile:	default		
Regulatory Domain Profile:	default		
SNMP Profile: Requires a version earlier than 3.4.0.0	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:	ids-low-setting		
Mesh Radio Profile: Requires an Outdoor Mesh Access Points license	default		
AP Authorization Profile: Requires a Remote Access Points license and version 5.0.0.0 and above, or RN 3.0	--None--		
AP Provisioning Profile: Requires version 5.0.0.0 and above, or RN 3.0	--None--		

For additional information about configuring Dell Networking W AP Groups, see "[Dell Networking W AP Groups Procedures and Guidelines](#)" on page 27.

8. Add or edit WLANs in Dell Networking W Configuration as required.
  - a. Navigate to the **Dell Networking W Configuration > WLANs** page. This page can display all WLANs currently configured, or it can display only selected WLANs.
  - b. Click **Add** to create a WLAN, or click the pencil icon to edit a WLAN.

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

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

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

- ["General WLAN Guidelines" on page 28](#)
- ["WLANs" on page 46](#) for details on all WLAN settings

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

Most profiles in AirWave are similar to the **All Profiles** display in the Dell Networking W-Series controller WebUI. The primary difference in AirWave is that **AAA** and **SSID** profiles are not listed under the **WLAN** column, but under **Profiles**.

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

All other settings supported on Dell Networking W-Series controllers can be defined on the **Dell Networking W Configuration** page. The following section in this document provides additional information about configuring profiles:

["General Profiles Guidelines" on page 28](#)

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

["Dell Networking W AP Groups Procedures and Guidelines" on page 27](#)

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

["Selecting Dell Networking W AP Groups" on page 27](#)

12. Each AP can be assigned to a single Dell Networking W AP Group. Make sure to choose an AP Group that has been configured on that controller using that controller's AirWave 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 Dell Networking W Configuration" on page 30](#).
13. Navigate to the **APs/Devices > Audit** page for the controller to view mismatched settings. This page provides links to display additional and current configurations. You can display all mismatched devices by navigating to the **APs/Devices > Mismatched** page.

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

- Once Dell Networking W Configuration is deployed in AirWave, you can perform debugging with Telnet/SSH. Review the `telnet_cmds` file in the `/var/log` folder from the command line interface, or access this file from the **System > Status** page. For additional information, refer to the *Dell Networking W-AirWave 8.0 User Guide*.
- To resolve communication issues, review the credentials on the **APs/Devices > Manage** page.
- Mismatches can occur when importing profiles because AirWave deletes orphaned profiles, even if following a new import.

## **Additional Capabilities**

AirWave supports many additional AOS configurations and settings. Refer to the following additional resources on [dell.com/support/manuals](http://dell.com/support/manuals) for more information:

- *Dell Networking W-Series ArubaOS User Guide*
- *Dell Networking W-AirWave 8.0 User Guide*
- *Dell Networking W-AirWave 8.0 Best Practices Guide*

This section presents common tasks or concepts after initial setup of Dell Networking W Configuration is complete, as described in the section ["Setting Up Initial Dell Networking W Configuration"](#) on page 20. This chapter emphasizes frequent procedures as follows:

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



---

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

---

## Dell Networking W AP Groups Procedures and Guidelines

### Guidelines and Pages for Dell Networking W AP Groups

The fields and default settings for Dell Networking W AP Groups are described in ["Dell Networking W AP Groups"](#) on page 38. The following guidelines govern the configuration and use of Dell Networking W AP Groups across AirWave:

- Dell Networking W AP Groups function with standard AirWave groups that contain them. Add Dell Networking W AP Groups to standard AirWave groups. Additional procedures in this document explain their interoperability.
- APs can belong to a controller's AirWave group or to an AirWave group by themselves.
- All configurations of Dell Networking W AP Groups must be pushed to Dell Networking W-Series controllers to become active on the network.
- Additional dynamics between master, standby master, and local controllers still apply. In this case, refer to ["Using Master, Standby Master, and Local Controllers"](#) on page 29.

The following pages in AirWave govern the configuration and use of Dell Networking W AP Groups or standard device groups across AirWave:

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

### Selecting Dell Networking W AP Groups

To select Dell Networking W AP Groups, navigate to the **Dell Networking W Configuration > Dell Networking W AP Groups** page. This page is central to defining Dell Networking W AP Groups, viewing the AirWave groups with which an AP Group is associated, changing or deleting AP Groups, and assigning AP devices to an AP Group.

## Configuring Dell Networking W AP Groups

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

1. Browse to the **Dell Networking W Configuration** page, and click the **AP Groups** heading in the navigation pane on the left. The **Groups Summary** page appears and displays all current Dell Networking W AP Groups.
2. To add a new group, click the **Add AP Group** button. To edit an existing group, click the **pencil** icon next to the group name. The **Details** page appears with current or default configurations. The settings on this page are described in ["Dell Networking W AP Groups Procedures and Guidelines"](#) on page 27.
3. Click **Add** or **Save** to finish creating or editing the Dell Networking W AP Group. Click **Cancel** to exit this screen and to cancel the AP Group configurations.
4. New AP groups appear in the **AP Groups** section of the Dell Networking W 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 Dell Networking W-Series controllers by clicking **Save and Apply**. The principles of Monitor and Manage mode still apply. For additional information, refer to ["Pushing Device Configurations to Controllers"](#) on page 29.

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

## General WLAN Guidelines

### Guidelines and Pages for WLANs in Dell Networking W Configuration

- The **Dell Networking W Configuration** navigation pane displays custom-configured WLANs and Dell Networking W AP Groups. You define or modify WLANs on the **Dell Networking W 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, AirWave returns you to your place on the **WLAN** setup page once you are done with profile setup.
- All configurations must be pushed to Dell Networking W-Series controllers to become active on the network.

## General Profiles Guidelines

AOS elements can be added or edited after an AOS configuration file is imported to AirWave and pushed to controllers with the steps described in ["Setting Up Initial Dell Networking W Configuration"](#) on page 20.

Profiles in Dell Networking W configuration entail the following concepts or dynamics:

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

For additional information about Profiles, refer to ["Profiles"](#) on page 47.

# General Controller Procedures and Guidelines

## Using Master, Standby Master, and Local Controllers

AirWave implements the following general approaches to controllers:

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

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

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

## Pushing Device Configurations to Controllers

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

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

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



---

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

---

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

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

## AP Overrides Guidelines

The **AP Override** component of Dell Networking W Configuration operates with the following principles:

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

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

## Changing Adaptive Radio Management (ARM) Settings

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

- ["Configuring Dell Networking W AP Groups" on page 28](#)
- ["Dell Networking W AP Groups Procedures and Guidelines" on page 27](#)
- ["Profiles" on page 47](#)

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

- ["Configuring Dell Networking W AP Groups" on page 28](#)
- ["Guidelines and Pages for WLANs in Dell Networking W Configuration" on page 28](#)
- ["Profiles" on page 47](#)

## Changing the Dell Networking W AP Group for an AP Device

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

1. As required, review the Dell Networking W AP Groups currently configured in AirWave. Navigate to the **Dell Networking W Configuration** page, and click **Dell Networking W AP Groups** from the navigation pane. This page displays and allows editing for all AP Groups that are currently configured in AirWave.
2. Navigate to the **APs/Devices > List** page to view all devices currently seen by AirWave.
3. If necessary, add the device to AirWave 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 Dell Networking W 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 AirWave, 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 AirWave.
  - Click **Ignore** to keep the device in AirWave but to ignore it.
  - Click **Import Settings** to define device settings from previously created configurations.
  - Click **Replace Hardware** to replace the AP device with a new AP device.
  - Click **Update Firmware** to update the Firmware that operates this device.
7. Push this configuration change to the controller that is to support this AP device. For additional information, refer to ["Pushing Device Configurations to Controllers" on page 29](#).

## Using AirWave to Deploy Dell Networking W-Series APs

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

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

An efficient and robust approach to update a Dell Networking W-Series AP device name is to deploy Dell Networking W-Series APs in AirWave with the following steps:

1. Define communication settings for Dell Networking W-Series APs pending discovery in the **Device Setup > Communication** page. This assigns communication settings to multiple devices at the time of discovery, and prevents having to define such settings manually for each device after discovery.
2. Discover new Dell Networking W-Series APs with AirWave. You can do so with the **Device Setup > Discover** page.
3. Click **New Devices** In the **Status** section at the top of any AirWave page, or navigate to the **APs/Devices > New** page.
4. Select (check) the box next to any AP you want to provision.
5. Rename all new APs. Type in the new device name in the **Device** column.
6. Scroll to the bottom of the page and put APs in the appropriate AirWave 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 AirWave but also on the Dell Networking W AP Group and the Dell Networking W-Series controller with the `show ap databaseaos` command.
8. To set the appropriate Dell Networking W AP Group, select the **AP/Devices** or **Groups** page and locate your APs.
9. Click **Modify Devices**.

10. Select the APs you want to re-group.

11. In the field that states **Move to Dell Networking W Group** below the list of the devices, select the appropriate group, and the click **Move**.



---

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

---

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

## Using General AirWave Device Groups and Folders

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

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

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



---

Dell Networking W APs can also belong to Dell Networking W AP Groups, but each AP is still limited to one general AirWave 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 AirWave group level.
- AirWave folders support multiple sublevels.

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

## Visibility in Dell Networking W Configuration

### Visibility Overview

Dell Networking W Configuration supports device configuration and user information in the following ways:

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

Additional factors for visibility are as follows:

- Administrative and Management users in AirWave can view the **Dell Networking W Configuration** page and the **APs/Devices > Manage** pages.
  - Administrative users are enabled to view all configurations.
  - Management users have access to all profiles and Dell Networking W AP groups for their respective folders.
- The **Device Setup > Dell Networking W Configuration** page has a limit to folder drop-down options for customers that manage different accounts and different types of users.
- Dell Networking W Configuration entails specific user role and security profiles that define some components of visibility, as follows:
  - "Security > User Roles" on page 50
  - "Security > Policies" on page 51
- AirWave continues to support the standard operation of folders, users, and user roles as described in the *Dell Networking W-AirWave 8.0 User Guide*.

## Defining Visibility for Dell Networking W Configuration

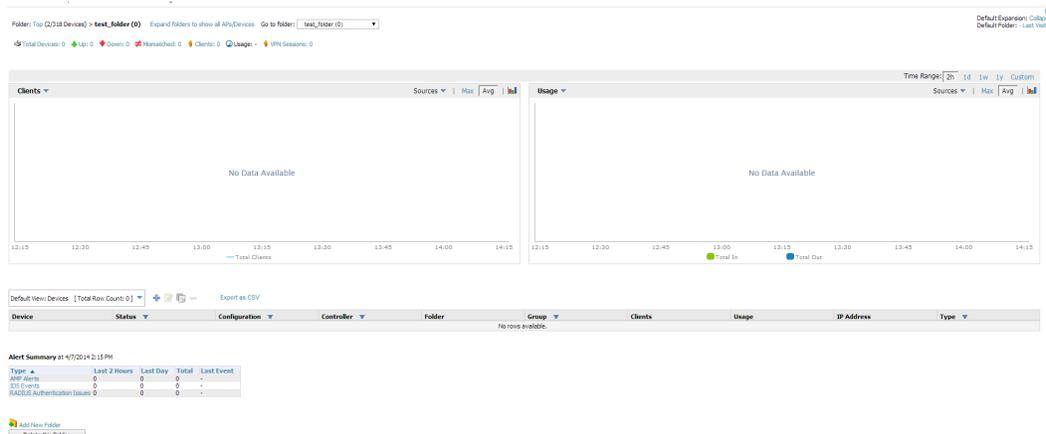
Perform these steps to define or adjust visibility for users to manage and support Dell Networking W Configuration:

1. As required, create a new AirWave 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 16](#):

**Figure 16:** APs/Devices > Add New Folder > Folders page illustration

- 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 17](#) illustrates an unpopulated device page for an example folder.

**Figure 17:** APs/Devices > List Page with no devices



2. Add Dell Networking W-Series controller devices to that folder as required. Use the **Device Setup > Add** page following instructions available in the *Dell Networking W-AirWave 8.0 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 Dell Networking W Configuration.
  - a. At least one user must have administrative privileges, but several additional users may be required with less rights and visibility to support Dell Networking W 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 18](#).

**Figure 18:** AMP Setup > Roles > Add/Edit Role Page Illustration

- c. As per standard AirWave configuration, complete the settings on this page. The most important fields with regard to Dell Networking W 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 Dell Networking W-Series controller, devices, and general Dell Networking W 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 Dell Networking W Configuration. This step creates or edits users to have rights appropriate to Dell Networking W Configuration. This user inherits visibility to Dell Networking W-Series controllers and Dell Networking W Configuration data based on the role and device folder created earlier in this procedure.
  - a. Navigate to the **AMP Setup > User** page.
  - b. Click **Add New User**, or click the **pencil** (manage) icon next to an existing user to edit that user.
  - c. Select the user role created with the prior step, and complete the remainder of this page as per standard AirWave configuration. Refer to the *Dell Networking W-AirWave 8.0 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 Dell Networking W 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 AirWave 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 *Dell Networking W-AirWave 8.0 User Guide*.
7. Continue to other elements of Dell Networking W Configuration described in the Reference section of this document.



## Overview

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

- Controller Configuration components are summarized in ["Additional Concepts and Components" on page 17](#).
- For procedures that use several of these components, refer to earlier chapters in this document.
- For architectural information about AOS, refer to the *Dell Networking W-Series ArubaOS User Guide*.




---

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 > Controller Configuration** page, illustrated in [Figure 19](#). The one exception is the additional **Groups > Controller Config** page that you access from the standard AirWave navigation menu.

**Figure 19:** *Controller Configuration Components*



This section describes Dell Networking W Configuration components with the following organization and topics:

- ["Groups > Controller Config Page" on page 65](#)
- ["Dell Networking W AP Groups" on page 38](#)
- ["AP Overrides" on page 41](#)
- ["WLANs" on page 46](#)
- ["Profiles" on page 47](#)
- ["Security" on page 48](#)
- ["Local Config " on page 55](#)
- ["Advanced Services" on page 59](#)

## Dell Networking W AP Groups

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

### About Dell Networking W AP Groups

The **Dell Networking W AP Groups** page displays all configured Dell Networking W AP Groups and enables you to add or edit Dell Networking W AP Groups. For additional information about using this page, refer to ["Dell Networking W AP Groups Procedures and Guidelines" on page 27](#).

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

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

**Table 2:** *Dell Networking W Configuration > Dell Networking W AP Groups Details, Settings and Default Values*

Field	Default	Description
<b>General Settings</b>		
Name	Default	Enter the name of the AP Group.
<b>WLANs</b>		
Add a new WLAN		Select this link to create a new WLAN to support Dell Networking W Configuration. Once created, that new WLAN will appear with others on this page.
Show only selected/Show All		To set the WLANs that appear on this page, select (check) the desired WLANs, then click <b>Show Only Selected</b> .
WLANs	None selected	Displays the WLANs currently present in Dell Networking W Configuration with checkboxes. You may select as few or as many WLANs as desired for which this AP Group is active.  To configure additional WLANs that appear in this section, click <b>Add a new WLAN</b> or navigate to the <b>WLANs</b> section in the navigation pane on the left.
<b>Referenced Profiles</b>		

**Table 2: Dell Networking W Configuration > Dell Networking W AP Groups Details, Settings and Default Values (Continued)**

Field	Default	Description
802.11a Radio Profile	5_am	<p>Defines AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.</p> <p>Select the <b>pencil</b> icon next to this field to edit or create additional profile settings in the <b>RF &gt; 802.11a/g Radio</b> page of Dell Networking W Configuration.</p>
802.11g Radio Profile	2.4_am	<p>Defines AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Each 802.11a and 802.11b radio profile includes a reference to an Adaptive Radio Management (ARM) profile.</p> <p>If you would like the ARM feature to select dynamically the best channel and transmission power for the radio, verify that the 802.11a/802.11g radio profile references an active and enabled ARM profile. If you want to manually select a channel for each AP group, create separate 802.11a and 802.11g profiles for each AP group and assign a different transmission channel for each profile. The drop-down menu displays these options:</p> <ul style="list-style-type: none"> <li>● default</li> <li>● nchannel too high</li> <li>● nchannel too low</li> </ul> <p>Select the <b>pencil</b> icon next to this field to edit profile settings in the <b>RF &gt; 802.11a/g Radio</b> page.</p>
RF Optimization Profile	default	<p>Enables or disables load balancing based on a user-defined number of clients or degree of AP utilization on an AP. Use this profile to detect coverage holes, radio interference and STA association failures and configure Received signal strength indication (RSSI) metrics.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; RF</b> section and edit these settings as desired.</p>
Event Thresholds Profile	default	<p>Defines error event conditions, based on a customizable percentage of low-speed frames, non-unicast frames, or fragmented, retry or error frames. The drop-down menu displays these options:</p> <ul style="list-style-type: none"> <li>● default</li> <li>● all additional RF profiles currently configured in Dell Networking W Configuration</li> </ul> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; RF &gt; Events Threshold</b> section and edit these settings as desired.</p>
Wired AP Profile	default	<p>Controls whether 802.11 frames are tunneled to the controller using Generic Routing Encapsulation (GRE) tunnels, bridged into the local Ethernet LAN (for remote APs), or are configured for combination of the two (split-mode). This profile also configures the switching mode characteristics for the port, and sets the port as either trusted or untrusted.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; Wired</b> page and adjust these settings as desired.</p>

**Table 2: Dell Networking W Configuration > Dell Networking W AP Groups Details, Settings and Default Values (Continued)**

Field	Default	Description
Ethernet Interface 0 Link Profile	default	<p>Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 0. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; Ethernet Link</b> details page and adjust these settings as desired.</p>
Ethernet Interface 1 Link Profile	default	<p>Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 1. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; Ethernet Link</b> details page and adjust these settings as desired.</p>
AP System Profile	default	<p>Defines administrative options for the controller, including the IP addresses of the local, backup, and master controllers, Real-Time Locating Systems (RTLS) server values, and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps.</p> <p>This field is a drop-down menu with the following options:</p> <ul style="list-style-type: none"> <li>● Non-integer RTLS Server Station Message Frequency</li> <li>● Too-high RTLS Server Port</li> <li>● Too-low AeroScout RTLS Server Port</li> <li>● Too-low RTLS Server Port</li> </ul> <p>Select the <b>pencil</b> icon next to this field to display the <b>Profiles &gt; AP &gt; System</b> details page and adjust these settings as desired.</p>
Regulatory Domain Profile	default	<p>Defines an AP's country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; Regulatory Domain</b> page and adjust these settings as desired.</p>
SNMP Profile	default	<p>Selects the SNMP profile to associate with this AP group. The drop-down menu lists all SNMP profiles currently enabled in AirWave.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; SNMP</b> page and adjust these settings as desired.</p>
VoIP Call Admission Control Profile	default	<p>Voice Call Admission Control limits the number of active voice calls per AP by load-balancing or ignoring excess call requests. This profile enables active load balancing and call admission controls, and sets limits for the numbers of simultaneous Session Initiated Protocol (SIP), SpectraLink Voice Priority (SVP), Cisco Skinny Client Control Protocol (SCCP), Vocera or New Office Environment (NOE) calls that can be handled by a single radio.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; Regulatory Domain</b> page and adjust these settings as desired.</p>
802.11g Traffic Management Profile	default	<p>Specify the minimum percentage of available bandwidth to be allocated to a specific SSID when there is congestion on the wireless network, and sets the interval between bandwidth usage reports. This setting pertains specifically to 802.11g.</p>

**Table 2: Dell Networking W Configuration > Dell Networking W AP Groups Details, Settings and Default Values (Continued)**

Field	Default	Description
802.11a Traffic Management Profile	default	Specify the minimum percentage of available bandwidth to be allocated to a specific SSID when there is congestion on the wireless network, and sets the interval between bandwidth usage reports. This setting pertains specifically to 802.11a.
IDS Profile	default	<p>Selects the IDS profile to be associated with the new AP Group. The drop-down menu contains these options:</p> <ul style="list-style-type: none"> <li>• ids-disabled</li> <li>• ids-high-setting</li> <li>• ids-low-setting</li> <li>• ids-medium-setting</li> </ul> <p>The IDS profiles configure the AP's Intrusion Detection System features, which detect and disable rogue APs and other devices that can potentially disrupt network operations. An AP is considered to be a rogue AP if it is both unauthorized and plugged into the wired side of the network. An AP is considered to be an interfering AP if it is seen in the RF environment but is not connected to the wired network.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; IDS</b> page and adjust these settings as desired.</p>
Mesh Radio Profile	default	Determines many of the settings used by mesh nodes to establish mesh links and the path to the mesh portal, including the maximum number of children a mesh node can accept, and transmit rates for the 802.11a and 802.11g radios.
<b>Mesh Cluster Profiles</b>		
Add New Mesh Cluster Profile		<p>Select to display a new <b>Mesh Cluster Profile</b> section to this page. This section has two fields, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Mesh Cluster Profile</b>—Drop-down menu displays all supported profiles. Select one from the menu.</li> <li>• <b>Priority (1-16)</b>—Type in the priority number for this profile. The priority may be any integer between 1 and 16.</li> </ul> <p>Complete these fields, click the <b>Add</b> button, and the profile displays as an option in the <b>Mesh Cluster Profile</b> section, which may be selected for the AP Group to be added or edited.</p>

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

## AP Overrides

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

The **AP Overrides** page displays all AP overrides that are currently configured. These overrides also appear in the navigation pane at left. The name of any override matches the AP device name. Select **Add** on the **AP Overrides** page to create a new AP Override, or click the pencil icon next to an existing override to edit that override.

**Figure 20:** AP Overrides page illustration (partial view)

Adding: **AP Override**

Folder:	Top ▼
Name:	<input type="text"/>

WLANs	
WLANs:	Show All <input type="checkbox"/> default Select All - Unselect All <span style="float: right;">+</span>

Excluded WLANs	
Excluded WLANs:	Show All <input type="checkbox"/> default Select All - Unselect All <span style="float: right;">+</span>

Referenced Profiles	
802.11a Radio Profile:	--Inherit-- ▼ <span style="float: right;">+</span>
802.11g Radio Profile:	--Inherit-- ▼ <span style="float: right;">+</span>
RF Optimization Profile:	--Inherit-- ▼ <span style="float: right;">+</span>
Event Thresholds Profile:	--Inherit-- ▼ <span style="float: right;">+</span>
Wired AP Profile: Requires version ≥ 3.3.0.0 and < 5.0.0.0	--Inherit-- ▼ <span style="float: right;">+</span>
Ethernet Interface 0 Link Profile: Requires version ≥ 3.3.0.0 and < 5.0.0.0	--Inherit-- ▼ <span style="float: right;">+</span>
Ethernet Interface 1 Link Profile: Requires version ≥ 3.3.0.0 and < 5.0.0.0	--Inherit-- ▼ <span style="float: right;">+</span>
AP System Profile:	--Inherit-- ▼ <span style="float: right;">+</span>
Regulatory Domain Profile:	--Inherit-- ▼ <span style="float: right;">+</span>
SNMP Profile: Requires a version earlier than 3.4.0.0	--Inherit-- ▼ <span style="float: right;">+</span>

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

**Table 3:** AP Overrides Add or Edit page fields

Field	Default	Description
Name	Blank	Name of the AP Override. Use the name of the AP device to which it applies.
<b>WLANs</b>		

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

Field	Default	Description
WLANs		<p>This section lists the WLANs currently defined in Dell Networking W Configuration by default. You can display selected WLANs or all WLANs.</p> <p>Select one or more WLANs for which AP Override is to apply.</p>
<b>Excluded WLANs</b>		
Excluded WLANs		<p>This section displays WLANs currently defined in Dell Networking W Configuration by default. This section can display selected WLANs or all WLANs. Use this section to specify which WLANs are <i>not</i> to support <b>AP Override</b>.</p>
<b>Referenced Profiles</b>		
802.11a Radio Profile	5_am	<p>Defines AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.</p> <p>Select the <b>pencil</b> icon next to this field to edit or create additional profile settings in the <b>RF &gt; 802.11a/g Radio</b> page.</p>
802.11g Radio Profile	2.4_am	<p>Defines AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Each 802.11a and 802.11b radio profile includes a reference to an Adaptive Radio Management (ARM) profile.</p> <p>If you would like the ARM feature to select dynamically the best channel and transmission power for the radio, verify that the 802.11a/802.11g radio profile references an active and enabled ARM profile. If you want to manually select a channel for each AP group, create separate 802.11a and 802.11g profiles for each AP group and assign a different transmission channel for each profile.</p> <p>The drop-down menu displays these options:</p> <ul style="list-style-type: none"> <li>• default</li> <li>• nchannel too high</li> <li>• nchannel too low</li> </ul> <p>Select the <b>pencil</b> icon next to this field to edit or create additional profile settings in the <b>RF &gt; 802.11a/g Radio</b> page of <b>Dell Networking W Configuration</b>.</p>
RF Optimization Profile	default	<p>Enables or disables load balancing based on a user-defined number of clients or degree of AP utilization on an AP. Use this profile to detect coverage holes, radio interference and STA association failures and configure Received signal strength indication (RSSI) metrics.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; RF</b> section and edit these settings as desired.</p>

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

Field	Default	Description
Event Thresholds Profile	default	<p>Defines error event conditions, based on a customizable percentage of low-speed frames, non-unicast frames, or fragmented, retry or error frames. The drop-down menu displays these options:</p> <ul style="list-style-type: none"> <li>• default</li> <li>• all additional RF profiles currently configured in Dell Networking W Configuration</li> </ul> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; RF &gt; Events Threshold</b> section and edit these settings as desired.</p>
Wired AP Profile	default	<p>Controls whether 802.11 frames are tunneled to the controller using Generic Routing Encapsulation (GRE) tunnels, bridged into the local Ethernet LAN (for remote APs), or a configured for combination of the two (split-mode). This profile also configures the switching mode characteristics for the port, and sets the port as either trusted or untrusted.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; Wired</b> page and adjust these settings as desired.</p>
Ethernet Interface 0 Link Profile	default	<p>Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 0. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; Ethernet Link</b> details page and adjust these settings as desired.</p>
Ethernet Interface 1 Link Profile	default	<p>Sets the duplex mode and speed of AP's Ethernet link for ethernet interface 1. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; Ethernet Link</b> details page and adjust these settings as desired.</p>
AP System Profile	default	<p>Defines administrative options for the controller, including the IP addresses of the local, backup, and master controllers, Real-time Locating Systems (RTLS) server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots traps.</p> <p>This field is a drop-down menu with the following options:</p> <ul style="list-style-type: none"> <li>• Non-integer RTLS Server Station Message Frequency</li> <li>• Too-high RTLS Server Port</li> <li>• Too-low AeroScout RTLS Server Port</li> <li>• Too-low RTLS Server Port</li> </ul> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; System</b> details page and adjust these settings as desired.</p>
Regulatory Domain Profile	default	<p>Defines an AP's country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; Regulatory Domain</b> page and adjust these settings as desired.</p>
SNMP Profile	default	<p>Selects the SNMP profile to associate with this AP group. The drop-down menu lists all SNMP profiles currently enabled in AirWave.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; SNMP</b> page and adjust these settings as desired.</p>

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

Field	Default	Description
VoIP Call Admission Control Profile	default	<p>Voice Call Admission Control limits the number of active voice calls per AP by load-balancing or ignoring excess call requests. This profile enables active load balancing and call admission controls, and sets limits for the numbers of simultaneous Session Initiated Protocol (SIP), SpectraLink Voice Priority (SVP), Cisco Skinny Client Control Protocol (SCCP), Vocera or New Office Environment (NOE) calls that can be handled by a single radio.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; AP &gt; Regulatory Domain</b> page and adjust these settings as desired.</p>
802.11g Traffic Management Profile	default	Specify the minimum percentage of available bandwidth to be allocated to a specific SSID when there is congestion on the wireless network, and sets the interval between bandwidth usage reports. This setting pertains specifically to 802.11g.
802.11a Traffic Management Profile	default	Specify the minimum percentage of available bandwidth to be allocated to a specific SSID when there is congestion on the wireless network, and sets the interval between bandwidth usage reports. This setting pertains specifically to 802.11a.
IDS Profile	default	<p>Selects the IDS profile to be associated with the new AP Group. The drop-down menu contains these options:</p> <ul style="list-style-type: none"> <li>● ids-disabled</li> <li>● ids-high-setting</li> <li>● ids -low-setting (the default)</li> <li>● ids-medium-setting</li> </ul> <p>The IDS profiles configure the AP's Intrusion Detection System features, which detect and disable rogue APs and other devices that can potentially disrupt network operations. An AP is considered to be a rogue AP if it is both unauthorized and plugged into the wired side of the network. An AP is considered to be an interfering AP if it is seen in the RF environment but is not connected to the wired network.</p> <p>Select the pencil icon next to this field to display the <b>Profiles &gt; IDS</b> page and adjust these settings as desired.</p>
Mesh Radio Profile	default	Determines many of the settings used by mesh nodes to establish mesh links and the path to the mesh portal, including the maximum number of children a mesh node can accept, and transmit rates for the 802.11a and 802.11g radios.
AP Authorization Profile		Selects the AP Authorization profile to be associated with the new AP Group. This profile requires a Remote Access Points license.
AP Provisioning Profile		Selects the AP Provisioning profile to be associated with the new AP Group.
Ethernet Interface 0-4 Port Configuration		<p>Selects the Ethernet port configuration to be associated with the new AP Group. This profile allows you to configure all AP wired port profiles and their status. The drop-down menu contains these options:</p> <ul style="list-style-type: none"> <li>● default</li> <li>● NoWiredAuthPort</li> <li>● shutdown</li> </ul>

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

Field	Default	Description
<b>Mesh Cluster Profiles</b>		
Add New Mesh Cluster Profile	Hidden by default until the <b>Add</b> button is clicked	Clicking this <b>Add</b> button displays a new <b>Mesh Cluster Profile</b> field. The drop-down menu displays all supported profiles. Select one from the menu.  Complete this field, click the <b>Add</b> button, and the profile displays as an option in the <b>Mesh Cluster Profile</b> section, which may be selected for the AP Group to be added or edited.
<b>Excluded Mesh Cluster Profiles</b>		
Excluded Mesh Cluster Profiles		If required, select one or more Mesh Cluster profiles from this field. This field can display all Mesh Cluster profiles or can display only selected Mesh Cluster profiles.

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

## WLANs

### Overview of WLANs Configuration

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

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

Refer to the *Dell Networking W-AirWave 8.0 User Guide* for additional information.

Use the following guidelines when configuring and using WLANs in Dell Networking W Configuration:

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

### WLANs

The **WLANs** page displays all configured WLANs in Dell Networking W Configuration and enables you to add or edit WLANs. For additional information about using this page, refer to "[General WLAN Guidelines](#)" on page 28.

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

**Table 4: Dell Networking W Configuration > WLANs Page Fields and Descriptions**

Field	Description
Name	Lists the name of the WLAN.
SSID	Lists the SSID currently defined for the WLAN.
Dell Networking W AP Group	Lists the Dell Networking W 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 Dell Networking W AP Groups.
Traffic Management	Lists Traffic Management profiles that are currently configured and deployed on the WLAN.
Controller	Lists the controller for the WLAN.
Folder	Name of the folder in which the configuration resides.

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

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

## WLANs > Basic

From the **Dell Networking W Configuration > WLANs** page, click **Add** to create a new WLAN, or click the pencil icon to edit an existing WLAN, then click **Basic**. This page provides a streamlined way to create or edit a WLAN.

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

An alternate way to create or edit WLANs is from the **Advanced** page. Refer to ["WLANs > Advanced" on page 47](#).

## WLANs > Advanced

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

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

## Profiles

### Understanding Dell Networking W Configuration Profiles

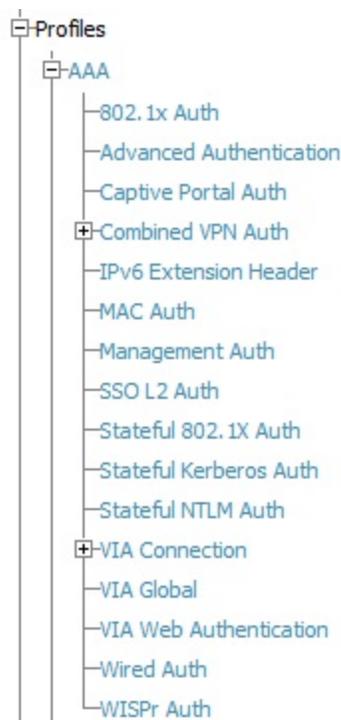
In AOS, related configuration parameters are grouped into a profile that you can apply as needed to an AP group or to individual APs. This section lists each category of AP profiles that you can configure and then apply to an AP group or to an individual AP. Note that some profiles reference other profiles.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

You can apply profiles to an AP or AP group.

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

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

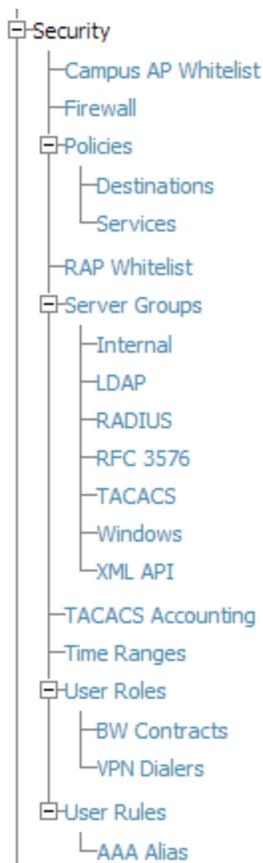
**Figure 21: AAA Profiles**



## Security

Controller Configuration supports user roles, policies, server groups, and additional security parameters with the profiles listed in the **Security** portion of the navigation pane on the **Controller Configuration** page, as illustrated in [Figure 22](#):

**Figure 22: Security Components in Dell Networking W Configuration**



This section describes the profiles, pages, parameters and default settings for all **Security** components in **Dell Networking W Configuration**, as follows:

- Campus AP Whitelist
- "Security > Policies" on page 51
  - "Security > Policies > Destinations" on page 51
  - "Security > Policies > Services" on page 51
- Security RAP Whitelist
- "Security > Server Groups" on page 52
  - "Security > Server Groups > Internal" on page 54
  - "Security > Server Groups > LDAP" on page 53
  - "Security > Server Groups > RADIUS" on page 53
  - "Security > Server Groups > RFC 3576" on page 54
  - "Security > Server Groups > TACACS" on page 53
  - "Security > Server Groups > Windows" on page 54
  - "Security > Server Groups > XML API" on page 54
- "Security > TACACS Accounting" on page 54
- "Security > Time Ranges" on page 55
- "Security > User Roles" on page 50
  - "Security > User Roles > BW Contracts" on page 50

- "Security > User Roles > VPN Dialers" on page 51
- "Security > User Rules" on page 55
  - Security > User Rules > AAA Alias

## Security > User Roles

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

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

In the Dell Networking W 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 a Dell Networking W 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 Dell Networking W Configuration and where they are used. Select **Add** to create a new user role.

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

## Security > User Roles > BW Contracts

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

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

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

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

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

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

## Security > User Roles > VPN Dialers

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

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

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

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

## Security > Policies

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

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

## Security > Policies > Destinations

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

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

## Security > Policies > Services

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

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

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

## Security > Server Groups

### Server Groups Page Overview

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

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

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

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

Before enabling fail-through authentication, note the following:

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

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

### Supported Servers

Dell Networking W-Series AOS supports the following external authentication servers:

- LDAP (Lightweight Directory Access Protocol)
- RADIUS (Remote Authentication Dial-In User Service)

- RFC 3576
- TACACS+ (Terminal Access Controller Access Control System)
- Windows
- XML API

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

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

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

### Adding a New Server Group

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

To create a new server group, click the **Add** button, or to edit an existing group, click the pencil icon next to that group. The **Add New Server Group** page appears.

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

### Security > Server Groups > LDAP

You can configure Lightweight Directory Access Protocol (LDAP) servers for use by a server group.

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

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

### Security > Server Groups > RADIUS

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

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

### Security > Server Groups > TACACS

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

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

## Security > Server Groups > Internal

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

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

## Security > Server Groups > XML API

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



---

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

---

The **Security > Server Groups > XML API** page lists any XML API servers currently available for use by server groups. From this page, click **Add** to create a new XML API server, or click the pencil icon next to an existing server to edit.

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

## Security > Server Groups > RFC 3576

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

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

Select **Add** to create a new RFC3576 server, or click the pencil icon next to an existing server to edit it.

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

## Security > Server Groups > Windows

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

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

## Security > TACACS Accounting

TACACS+ accounting allows commands issued on the controller to be reported to TACACS+ servers. You can specify the types of commands that are reported, and these are action, configuration, or show commands. You can have all commands reported as desired. Dell Networking W Configuration supports TACACS Accounting servers that can be referenced by server groups, so a TACACS Server Group must be configured first.

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

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

## Security > Time Ranges

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

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

To create a new time range profile, click the **Add New Time Range** button, or click the pencil icon next to an existing time range profile to adjust settings.

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

## Security > User Rules

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

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

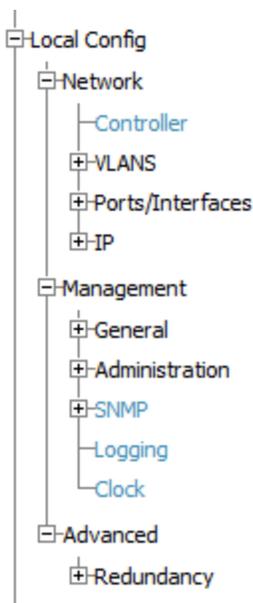
To add a new user rule, which is a derivation profile, click the Add New User Derivation Profile button. To edit an existing user rule, click the pencil icon next to an existing rule.

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

## Local Config

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

Figure 23: Local Config menu



## Local Config > Network

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

### Local Config > Network > Controller

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

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

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

### Local Config > Network > VLANs

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

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

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

## Local Config > Network > Ports/Interfaces

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

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

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

## Local Config > Network > IP

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

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

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

## Local Config > Management

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

### Local Config > Management > General

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

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

## Local Config > Management > Administration

Define controller management users and management user passwords. The settings in this profile also allows network administrators to bypass the enable password prompt and go directly to the privileged commands (config mode) after logging on to the controller. Select **Add** to create a new management administration profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. For more information, refer to the *Management Access* chapter of the Dell Networking W-Series AOS *User Guide* and the "mgmt-user" command in the *Dell Networking W-Series ArubaOS Command-line Interface Reference Guide*.

## Local Config > Management > SNMP

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

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



---

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

---

## Local Config > Management > Logging

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

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

## Local Config > Management > Clock

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

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

## Local Config > Advanced > Redundancy

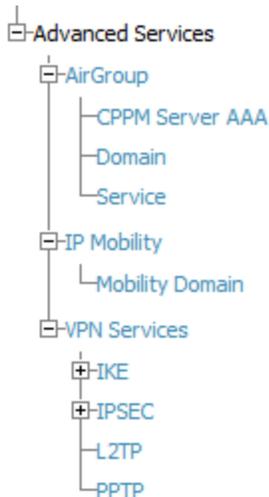
This section contains a configuration profile that defines the Virtual Router Redundancy Protocol (VRRP) values for the controller. You can configure VRRP to support controller redundancy solutions, including pairs of local controllers acting in an active-active mode or a hot-standby mode, a master controller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

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

## Advanced Services

This section describes the contents, parameters, and default settings for all **Advanced Services** components in **Dell Networking W Configuration**. Dell Networking W Configuration in AirWave supports advanced services such as AirGroup, IP Mobility and VPN services. For additional information about the AirGroup feature, IP Mobility domains, VPN services, and additional architecture or concepts, refer to the *Dell Networking W-Series ArubaOS User Guide*.

**Figure 24:** *Advanced Services menu*



### Advanced Services > AirGroup

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

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

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

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

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

### Advanced Services > AirGroup > CPPM Server AAA

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

register their personal devices.

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

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

## Advanced Services > AirGroup > Domain

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

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

Refer to the AirGroup chapter in the *Dell Networking W-Series ArubaOS User Guide* and the "airgroup" command in the *Dell Networking W-Series ArubaOS Command-Line Interface Reference Guide* for information about the options that are available on this form.

## Advanced Services > AirGroup > Service

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

The following services are enabled by default on the controller:

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

The following services are disabled by default on the controller:

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

Select **Add** to create a new AirGroup Services profile, or click the pencil icon next to an existing profile to view or edit the profile configuration. Refer to the AirGroup chapter in the *Dell Networking W-Series ArubaOS User Guide* and the

"airgroup" command in the *Dell Networking W-Series ArubaOS Command-Line Interface Reference Guide* for information about the options that are available on this form.

## Advanced Services > IP Mobility

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

Select **Add** to create a new **IP Mobility** profile, or click the pencil icon next to an existing profile to modify settings on an existing profile.

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

## Advanced Services > IP Mobility > Mobility Domain

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

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

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

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

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

Navigate to **Advanced Services > IP Mobility > Mobility Domain** from the **Dell Networking W Configuration** navigation pane. This page displays all currently configured IP Mobility domains. Select **Add** to create a new IP Mobility Domain, or click the pencil icon next to an existing profile to modify an existing domain.

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

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

## Advanced Services > VPN Services

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

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

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

Before enabling VPN authentication, you must configure the following:

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

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

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

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

**Table 5:** *Advanced Services > VPN Services*

Profile Type	Refer to
IKE Profile	Refer to "Advanced Services > VPN Services > IKE Profile" on page 62
IPSEC Profile	Refer to "Advanced Services > VPN Services > IPSEC Profile" on page 63.
L2TP Profile	Refer to "Advanced Services > VPN Services > L2TP Profile" on page 64.
PPTP Profile	Refer to "Advanced Services > VPN Services > PPTP Profile" on page 64.

### Advanced Services > VPN Services > IKE Profile

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



---

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

---

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

Refer to the Virtual Private Networks chapter in the *Dell Networking W-Series ArubaOS User Guide* for information about IKE.

## Advanced Services > VPN Services > IKE > IKE Policy

Navigate to the **Advanced Services > VPN Services > IKE > IKE Policy** page from the **Dell Networking W Configuration** navigation pane to add a new IKE policy.

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

## Advanced Services > VPN Services > IPSEC Profile

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

L2TP/IPSec requires two levels of authentication:

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

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

Select **Add** to create a new **IPSEC** profile, or click the pencil icon next to an existing profile to modify settings.

Refer to the Virtual Private Networks chapter in the *Dell Networking W-Series ArubaOS User Guide* for information about IPSEC profiles.

## Advanced Services > VPN Services > IPSEC > Dynamic Map

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

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

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

Select **Add** to create a new **Dynamic Map**, or click the pencil icon next to an existing map to modify settings.

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

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

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

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

Select **Add** to create a new **Transform Set**, or click the pencil icon next to an existing Transform Set to modify settings.

Refer to the Virtual Private Networks chapter in the *Dell Networking W-Series ArubaOS User Guide* for information about Transform Sets.

## Advanced Services > VPN Services > L2TP Profile

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

L2TP/IPSec requires two levels of authentication:

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

Navigate to the **Advanced Services > VPN Services > L2TP** page from the **Dell Networking W Configuration** navigation pane. This page lists all L2TP profiles that are currently available. Select **Add** to create a new **L2TP** profile, or click the pencil icon next to an existing profile to modify settings.

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

## Advanced Services > VPN Services > PPTP Profile

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

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

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

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

## Groups > Controller Config Page

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

1. Navigate to the **Groups > List** page.
2. Select the name of the Dell Networking W AP Group to view and edit, and navigate to the **Controller Config** page, illustrated in [Figure 25](#):

**Figure 25:** Groups > Controller Config Page (partial view)

The screenshot displays the 'Dell PowerConnect W Controller Config Page' with several configuration sections:

- Dell PowerConnect W AP Groups:** Select the Dell PowerConnect W AP Groups to apply to devices in this Group. Includes a 'Show All' link, a checked 'default' option, and 'Select All - Unselect All' buttons.
- AP Overrides:** Select the AP Overrides to apply to devices in this Group. Includes a 'Show Only Selected' link and 'Select All - Unselect All' buttons.
- Additional Dell PowerConnect W Profiles:** A list of profiles with dropdown menus and edit/delete icons. All are currently set to 'default':
  - 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
  - Campus AP Whitelist: default
- Dell PowerConnect W User Roles:** Select additional Roles to apply to devices in this Group. Includes a 'Show All' link, checked options for 'ap-role', 'stateful-dot1x', and 'sys-ap-role', and 'Select All - Unselect All' buttons.
- Dell PowerConnect W Policies:** Select additional Policies to apply to devices in this Group. Includes a 'Show All' link, checked options for 'stateful-dot1x', 'sys-ap-acl', 'sys-control', and 'validuser', and 'Select All - Unselect All' buttons.

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

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

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

Section	Additional Information Available In These Locations
Dell Networking W AP Groups Section	<ul style="list-style-type: none"> <li>• "Dell Networking W AP Groups" on page 38</li> <li>• "Dell Networking W AP Groups Procedures and Guidelines" on page 27</li> <li>• "Setting Up Initial Dell Networking W Configuration" on page 20</li> </ul>
AP Overrides	<ul style="list-style-type: none"> <li>• "AP Overrides" on page 41</li> <li>• "Supporting APs with Dell Networking W Configuration" on page 30</li> </ul>
Dell Networking W User Roles	<ul style="list-style-type: none"> <li>• "Security &gt; User Roles" on page 50</li> <li>• "Visibility in Dell Networking W Configuration" on page 32</li> </ul>
Dell Networking W Policies	<ul style="list-style-type: none"> <li>• "Security &gt; Policies" on page 51</li> <li>• "Visibility in Dell Networking W Configuration" on page 32</li> </ul>



**A**

- Adaptive Radio Management (ARM) 30
- Advanced Services
  - defined 14
  - pages and field descriptions 55
- Advanced Services > IP Mobility 59, 61
- Advanced Services > IP Mobility page 59, 61
- Advanced Services > VPN Services 62
- Advanced Services > VPN Services > IKE 62
- Advanced Services > VPN Services > IPSEC 63
- Advanced Services > VPN Services > L2TP 64
- Advanced Services > VPN Services > PPTP 64
- AP Groups
  - general procedures and guidelines 27
- AP Overrides
  - guidelines 30
  - pages and field descriptions 41
- APs
  - using in groups and folders 32
- APs/Devices > List 10
- APs/Devices > Manage 15
- APs/Devices > Monitor 16

**D**

- Device Configuration
  - Advanced Services 14
  - Folders, Users, and Visibility 20
  - Initial Setup 20
  - Initial Setup Procedure 21
  - Prerequisites 21
  - Profiles 13
  - Security 14
  - WLANs 12
- device groups
  - using with APs 32
- Device Setup 9

**E**

- Encryption 30

**F**

- folders
  - using with APs 32

**G**

- groups
  - using with APs 32
- Groups > Basic 17

**P**

- Profiles
  - defined 13
  - embedded configuration 17
  - overview 47
  - pages and field descriptions 47

**S**

- Save, Save and Apply, and Revert buttons 19
- Security
  - defined 14
  - pages and field descriptions 48
- Security > Policies 51
- Security > Policies > Destinations 51
- Security > Policies > Services 51
- Security > Server Groups 52
- Security > Server Groups > Internal 54
- Security > Server Groups > LDAP 53
- Security > Server Groups > RADIUS 53
- Security > Server Groups > RFC 3576 54
- Security > Server Groups > TACACS 53
- Security > Server Groups > Windows 54
- Security > Server Groups > XML API 54
- Security > TACACS Accounting 54
- Security > Time Ranges 55
- Security > User Roles 50
- Security > User Roles > BW Contracts 50
- Security > User Roles > VPN Dialers 51
- Security > User Rules 55
- SSIDs 12, 25, 30, 40, 46-47

**W**

- WLANs 46
  - defined 12
  - pages and field descriptions 46
- WLANs > Advanced 47
- WLANs > Basic 47

