


# **Dell PowerConnect W-AirWave 7.6 Configuration Guide**



## Copyright

© 2013 Aruba Networks, Inc. Aruba Networks trademarks include  , Aruba Networks<sup>®</sup>, Aruba Wireless Networks<sup>®</sup>, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System<sup>®</sup>. Dell<sup>™</sup>, the DELL<sup>™</sup> logo, and PowerConnect<sup>™</sup> 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.

# Contents

<b>Dell PowerConnect W Configuration in AirWave</b> .....	<b>1</b>
Requirements, Restrictions, and ArubaOS Support in AirWave .....	1
Requirements .....	1
Restrictions .....	1
ArubaOS Support in AirWave .....	1
Overview of Dell PowerConnect W Configuration in AirWave .....	2
Device Setup > Dell PowerConnect W Configuration Page .....	3
Groups > Dell PowerConnect W Config Page with Global Configuration Enabled .....	4
Groups > Dell PowerConnect W Config when Global Configuration is Disabled .....	4
Dell PowerConnect W Configuration Sections in the Tree View .....	4
Dell PowerConnect W AP Groups Section .....	5
AP Overrides Section .....	5
WLANs Section .....	6
Profiles Section .....	7
Security Section .....	7
Local Config Section .....	8
Advanced Services Section .....	8
APs/Devices > List Page .....	8
APs/Devices > Manage Page .....	9
APs/Devices > Monitor Page .....	9
APs/Devices > Audit Page .....	10
Groups > Basic Page .....	10
Additional Concepts and Components .....	10
Global Configuration and Scope .....	10
Referenced Profile Setup .....	11
Save, Save and Apply, and Revert Buttons .....	12
Additional Concepts and Benefits .....	12
Scheduling Configuration Changes .....	12
Auditing and Reviewing Configurations .....	12
Licensing and Dependencies in Dell PowerConnect W Configuration .....	13
Setting Up Initial Dell PowerConnect W Configuration .....	13
Prerequisites .....	13
Procedure .....	13
Additional Capabilities .....	18
<b>Dell PowerConnect W Configuration in Daily Operations</b> .....	<b>19</b>
Dell PowerConnect W AP Groups Procedures and Guidelines .....	19
Guidelines and Pages for Dell PowerConnect W AP Groups .....	19

Selecting Dell PowerConnect W AP Groups .....	20
Configuring Dell PowerConnect W AP Groups .....	20
General WLAN Guidelines .....	20
Guidelines and Pages for WLANs in Dell PowerConnect W Configuration .....	20
General Profiles Guidelines .....	20
General Controller Procedures and Guidelines .....	21
Using Master, Standby Master, and Local Controllers .....	21
Pushing Device Configurations to Controllers .....	21
Supporting APs with Dell PowerConnect W Configuration .....	22
AP Overrides Guidelines .....	22
Changing Adaptive Radio Management (ARM) Settings .....	22
Changing SSID and Encryption Settings .....	22
Changing the Dell PowerConnect W AP Group for an AP Device .....	22
Using AirWave to Deploy Dell PowerConnect W-Series APs .....	23
Using General AirWaveDevice Groups and Folders .....	24
Visibility in Dell PowerConnect W Configuration .....	25
Visibility Overview .....	25
Defining Visibility for Dell PowerConnect W Configuration .....	25
<b>Configuration Reference .....</b>	<b>29</b>
Introduction .....	29
Dell PowerConnect W AP Groups .....	30
About Dell PowerConnect W AP Groups .....	31
AP Overrides .....	34
WLANs .....	38
Overview of WLANs Configuration .....	38
WLANs .....	38
WLANs > Basic .....	39
WLANs > Advanced .....	40
Profiles .....	43
Understanding Dell PowerConnect W Configuration Profiles .....	43
Security .....	44
Security > User Roles .....	46
Security > User Roles > BW Contracts .....	48
Security > User Roles > VPN Dialers .....	49
Security > Policies .....	51
Security > Policies > Destinations .....	53
Security > Policies > Services .....	54
Security > Server Groups .....	55
Server Groups Page Overview .....	55
Supported Servers .....	56
Adding a New Server Group .....	56
Security > Server Groups > LDAP .....	58
Security > Server Groups > RADIUS .....	59
Security > Server Groups > TACACS .....	60
Security > Server Groups > Internal .....	61

Security > Server Groups > XML API .....	62
Security > Server Groups > RFC 3576 .....	62
Security > Server Groups > Windows .....	63
Security > TACACS Accounting .....	63
Security > Time Ranges .....	64
Security > User Rules .....	65
Local Config of SNMP Management .....	66
Advanced Services .....	67
Advanced Services > IP Mobility .....	68
Advanced Services > IP Mobility > Mobility Domain .....	70
Advanced Services > VPN Services .....	71
Advanced Services > VPN Services > IKE .....	73
Advanced Services > VPN Services > IKE > IKE Policy .....	73
Advanced Services > VPN Services > L2TP .....	75
Advanced Services > VPN Services > PPTP .....	76
Advanced Services > VPN Services > IPSEC .....	77
Advanced Services > VPN Services > IPSEC > Dynamic Map .....	77
Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set .....	78
Groups > Dell PowerConnect W Config Page .....	79



# Chapter 1

## Dell PowerConnect W Configuration in AirWave

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

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

- ["Requirements, Restrictions, and ArubaOS Support in AirWave" on page 1](#)
- ["Additional Concepts and Components" on page 10](#)
- ["Setting Up Initial Dell PowerConnect W Configuration" on page 13](#)

---

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

---

## Requirements, Restrictions, and ArubaOS Support in AirWave

### Requirements

Dell PowerConnect W Configuration has the following requirements in AirWave:

- AirWave 6.3 or a later version must be installed and operational on the network.
- Dell PowerConnect W-Series controllers on the network must have ArubaOS 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 PowerConnect W Configuration has the following restrictions in AirWave

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

### ArubaOS 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 config for organizations who have near-identical deployments on all of their controllers
- Group-level GUI config for organizations who have two or more configuration strategies

- Configuration changes are pushed to the 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 PowerConnect W AP Groups, Servers and Roles are supported, as is the ArubaOS WLAN Wizard. **Controller IP addresses, VLANs, and interfaces are not supported, nor are Advanced Services, with the exception of VPN and IP Mobility.**

Other features of Dell PowerConnect W Configuration in AirWave include the following:

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

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

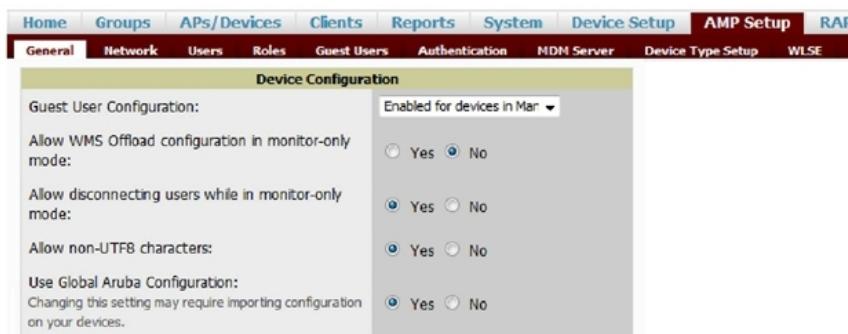
For more detailed information about this feature, as well as steps to transition from template-based configuration to web-based configuration, refer to additional chapters in this user guide. For known issues and details on the ArubaOS version supported by each release, refer to the AirWave Release Notes at [dell.com/support](http://dell.com/support).

## Overview of Dell PowerConnect W Configuration in AirWave

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

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

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



AirWave supports Dell PowerConnect W Configuration with the following pages:

- "[Device Setup > Dell PowerConnect W Configuration Page](#)" on page 3—Deploys and maintains *global* Dell PowerConnect W Configuration in AirWave. You can limit the view to a folder.



- ["Groups > Dell PowerConnect W Config Page with Global Configuration Enabled" on page 4](#)—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 > Dell PowerConnect W Config** page manages Dell PowerConnect W AP group and other controller-wide settings defined on the **Device Setup > Dell PowerConnect W Configuration** page.
  - If global configuration is disabled, the **Groups > Dell PowerConnect W Config** page resembles the **Device Setup > Dell PowerConnect W Configuration** tree navigation (the same sections listed in the previous bullet are available), but the **Groups > Dell PowerConnect W Config** pages do not display the **Folder** as a column in the list tables or as a field in the individual profiles.
- ["Groups > Dell PowerConnect W Config when Global Configuration is Disabled" on page 4](#)— this page modifies or reboots all devices when Global Dell PowerConnect W Configuration is enabled.
- ["APs/Devices > Manage Page" on page 9](#)—supports device-level settings and changes in AirWave.
- ["APs/Devices > Monitor Page" on page 9](#)—supports device-level monitoring in AirWave.
- ["APs/Devices > Audit Page" on page 10](#)—supports device level configuration importing in AirWave.
- ["Groups > Basic Page" on page 10](#)—For device groups containing Dell PowerConnect 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 PowerConnect W GUI Config are managed here.

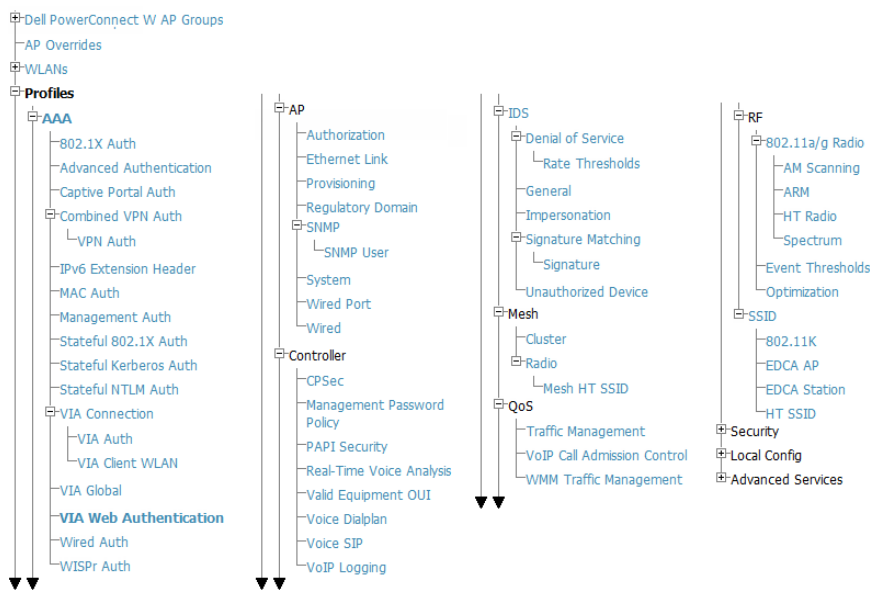
## Device Setup > Dell PowerConnect W Configuration Page



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

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

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



## Groups > Dell PowerConnect W Config Page with Global Configuration Enabled

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

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

**Figure 3: Groups > Dell PowerConnect W Config Page Illustration (Partial Display)**

The screenshot displays the configuration interface for Dell PowerConnect W AP Groups. It is divided into several sections:

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

## Groups > Dell PowerConnect W Config when Global Configuration is Disabled

If Use Global Dell PowerConnect W Configuration in AMP Setup > General is set to No, the Groups > Dell PowerConnect W Config page can be used to manage two or more distinctive configuration strategies using the same tree navigation as the Device Setup > Dell PowerConnect W Configuration page. Each of the sections is explained in "[Dell PowerConnect W Configuration Sections in the Tree View](#)" on page 4.

### Dell PowerConnect W Configuration Sections in the Tree View

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

- "[Dell PowerConnect W AP Groups Section](#)" on page 5
- "[AP Overrides Section](#)" on page 5
- "[WLANs Section](#)" on page 6
- "[Profiles Section](#)" on page 7
- "[Security Section](#)" on page 7
- "[Local Config Section](#)" on page 8

- ["Advanced Services Section" on page 8](#)



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

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

## Dell PowerConnect W AP Groups Section

A Dell PowerConnect W AP Group is a collection of configuration profiles that define specific settings on Dell PowerConnect W-Series controllers and the devices that they govern. A Dell PowerConnect W AP Group references multiple configuration profiles, and in turn links to multiple WLANs.

Navigate to the **Dell PowerConnect W Configuration > Dell PowerConnect W AP Groups** page. The figure below illustrates one example of this page.

**Figure 4: Dell PowerConnect W Configuration > Dell PowerConnect W AP Groups Navigation**

Name	Number of APs	Group	User Role	RAP Whitelist	Authorization	Controller	Folder
corp	0	-	-	-	-	-	Top
corp1344	11	-	-	-	-	-	Top
corp1344-2ndfloor	17	-	-	-	-	-	Top
Corp1344-AM	9	-	-	-	-	-	Top
corp1344-am-ch1	0	-	-	-	-	-	Top
Corp1344-AM-Ch11	3	-	-	-	-	-	Top
Corp1344-AM-Ch6	4	-	-	-	-	-	Top
corp1344-AP85	0	-	-	-	-	-	Top
corp1344-ebc	0	-	-	-	-	-	Top
Corp1344-mesh	0	-	-	-	-	-	Top



NOTE: Dell PowerConnect 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 PowerConnect W AP Groups have the following characteristics:

- Any Dell PowerConnect W-Series controller can support multiple Dell PowerConnect W AP Groups.
- Dell PowerConnect W AP Groups are assigned to folders, and folders define visibility. Using conventional AirWave folders to define visibility, Dell PowerConnect 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 PowerConnect W Configuration" on page 25](#).
- You can import a controller configuration file from ArubaOS for Dell PowerConnect W AP Group deployment in AirWave.

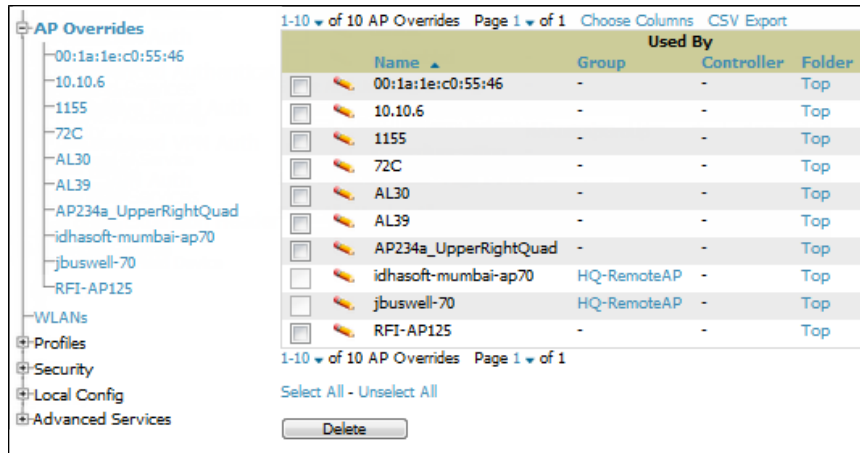
For additional information, refer to the following sections in this document:

- ["Setting Up Initial Dell PowerConnect W Configuration" on page 13](#)
- ["Dell PowerConnect W AP Groups Procedures and Guidelines" on page 19](#)

## AP Overrides Section

The second major component of Dell PowerConnect W Configuration is the **AP Overrides** page, appearing immediately below **Dell PowerConnect W AP Groups** in the Navigation Pane. [Figure 5](#) illustrates this location and access:

**Figure 5: Dell PowerConnect W > Configuration > AP Overrides Navigation**



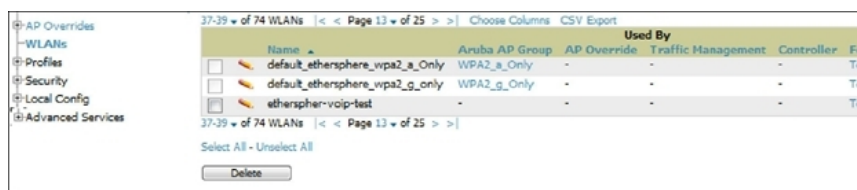
AP Overrides operate as follows in Dell PowerConnect W Configuration:

- Custom-created AP Overrides appear in the Dell PowerConnect W Configuration navigation pane, as illustrated in [Figure 5](#).
- Dell PowerConnect W-Series controllers and AP devices operate in Dell PowerConnect W AP Groups that define shared parameters for all devices in those groups. The **Dell PowerConnect W Configuration > Dell PowerConnect W AP Groups** page displays all current Dell PowerConnect W AP groups.
- AP Override allows you to change some parameters for any specific device without having to create a Dell PowerConnect 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 34](#).

## WLANs Section

Access WLANs with Dell PowerConnect W Configuration > WLANs, illustrated in [Figure 6](#).

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



The following concepts govern the use of WLANs in Dell PowerConnect W Configuration:

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

This document describes WLAN configuration in the following sections:

- ["Setting Up Initial Dell PowerConnect W Configuration" on page 13](#)
- ["General WLAN Guidelines" on page 20](#)

- "WLANs" on page 38

## Profiles Section

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

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



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

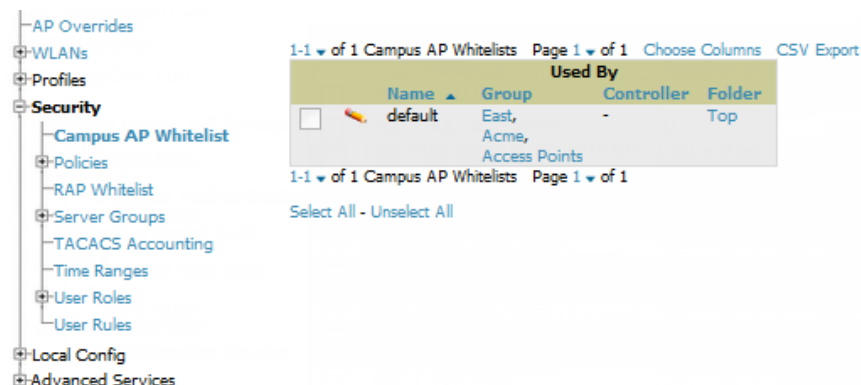
For additional information about profile procedures and guidelines, refer to the following sections in this document:

- "Setting Up Initial Dell PowerConnect W Configuration" on page 13
- "General Profiles Guidelines" on page 20
- "Profiles" on page 43

## Security Section

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

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



The following general guidelines apply to Security profiles in Dell PowerConnect W configuration:

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

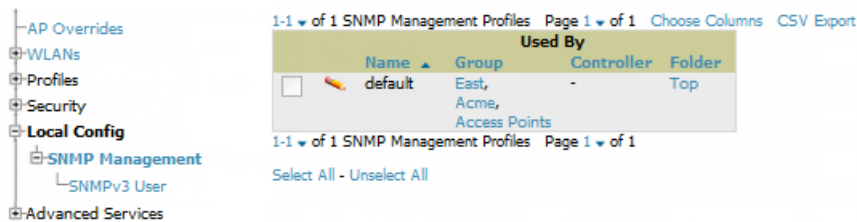
For additional information about Security, refer to ["Security" on page 44](#) in the Appendix.

## Local Config Section

The Local Config section is used for local configuration of Dell PowerConnect W-Series controllers. Locally configured settings are not pushed to local controllers by master controllers.

SNMP trap settings for controllers are managed locally.

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

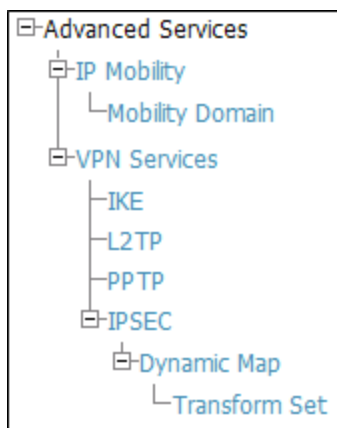


For complete details on the Local Config section, refer to ["Local Config of SNMP Management" on page 66](#).

## Advanced Services Section

Navigate to Advanced Services with the **Dell PowerConnect W Configuration > Advanced Services** path. The Advanced Services section includes IP Mobility and VPN Services. [Figure 10](#) illustrates this navigation and the components.

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

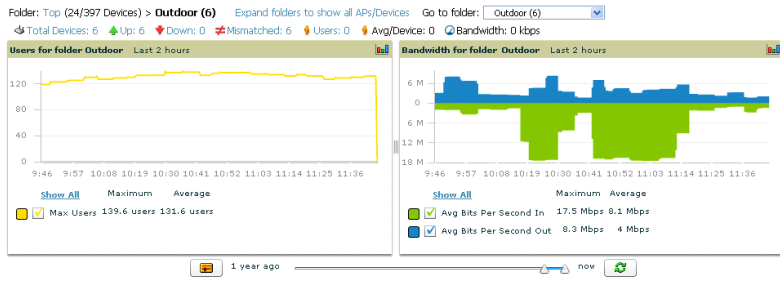


For additional information about IP Mobility and VPN Services, refer to ["Advanced Services" on page 67](#).

## APs/Devices > List Page

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

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



Modify Devices

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

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

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

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

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

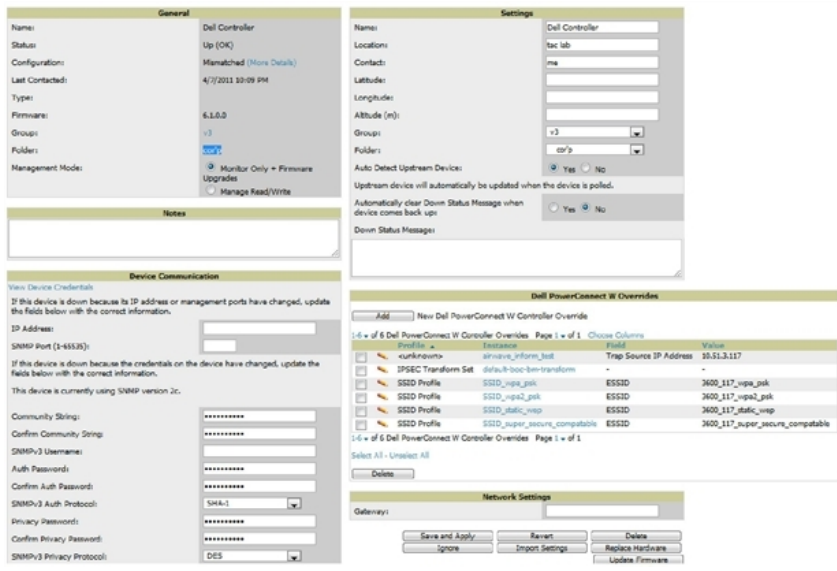
Add New Folder

## APs/Devices > Manage Page

This page configures device-level settings, including Manage mode, that enable pushing configurations to controllers. For additional information, refer to "Pushing Device Configurations to Controllers" on page 21.

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 PowerConnect W AP Groups that differ by one more settings. Controller overrides can be added from the controller's APs/Devices > Manage page. Figure 12 illustrates an APs/Devices > Manage page with controller overrides.

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



## APs/Devices > Monitor Page

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

- Status information

- Controller's License link
- Radio Statistics of some Dell PowerConnect W thin APs
- User and Bandwidth interactive graphs
- CPU Utilization and Memory Utilization interactive graphs
- APs Managed by this controller list (when viewing a controller)
- Alert Summary
- Recent Events
- Audit Log

For additional information, refer to ["Pushing Device Configurations to Controllers" on page 21](#).

## APs/Devices > Audit Page

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

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

## Groups > Basic Page

The **Groups > Basic** page deploys the following aspects of Dell PowerConnect 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, you should disable Dell PowerConnect W GUI configuration from the **Groups > Basic** page and use template-based configuration. See the Templates chapter of the *Dell PowerConnect W-AirWave 7.6 User Guide* at [dell.com/support/manuals](http://dell.com/support/manuals) for more information on templates.

## Additional Concepts and Components

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

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

## Global Configuration and Scope

Dell PowerConnect W Configuration supports ArubaOS as follows:

- AirWave supports global configuration from both a master-local controller deployment and an all-master-controller deployment:
  - In a master-local controller deployment, ArubaOS is the agent that pushes global configurations from master controllers to local controllers. AirWave supports this ArubaOS functionality.
  - In an all-master-controller scenario, every master controller operates independent of other master controllers. AirWave provides the ability to push configuration to all master controllers in this scenario.



- Dell PowerConnect W Configuration supports ArubaOS profiles, Dell PowerConnect W AP Profiles, Servers, and User Roles.













































For additional information about these and additional functions, refer to ["General Controller Procedures and Guidelines" on page 21](#).

## Referenced Profile Setup

AirWave allows you to add or reconfigure many configuration profiles while guiding you through a larger configuration sequence for a Dell PowerConnect W AP Group or WLAN. Consider the following example:

- When you create a new Dell PowerConnect W AP Group from the **Device Setup > Dell PowerConnect W Configuration** page, the **Referenced Profile** section appears as shown in [Figure 13](#):

**Figure 13:** Referenced Profile Configuration for a Dell PowerConnect WAP Group

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

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

## Save, Save and Apply, and Revert Buttons

Several **Add** or **Detail** pages in Dell PowerConnect 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 may see the following alert on other Dell PowerConnect W Configuration pages. You can apply the configuration when all changes are complete at a later time.

**Figure 14:** *Unapplied Dell PowerConnect W Configuration Changes Message*

Note: You have unapplied Dell PowerConnect W Configuration changes. You must click 'Save and Apply' to make them take effect.

- **Save and Apply** —This button saves and applies the configuration with reference to **Manage** and **Monitor** modes. For example, you must click **Save and Apply** for a configuration profile to propagate to all 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 21](#).
- **Revert**—This button cancels out of a new configuration or reverts back to the last saved configuration.

## Additional Concepts and Benefits

### Scheduling Configuration Changes

You can schedule deployment of Dell PowerConnect 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 21](#).



NOTE: 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 PowerConnect 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 ArubaOS 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 PowerConnect 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 PowerConnect 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 PowerConnect 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 ArubaOS, refer to the *Dell PowerConnect W-Series ArubaOS User Guide* for that release, available at [dell.com/support/manuals](http://dell.com/support/manuals).

## Setting Up Initial Dell PowerConnect W Configuration

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



---

NOTE: Dell PowerConnect W Configuration is enabled by default in AirWave.

---

### Prerequisites

- Complete the AirWave upgrade to AirWave 6.4 or later. Upon upgrade, global Dell PowerConnect W Configuration is enabled by default in groups with devices in monitor-only mode that have ArubaOS firmware of 3.3.2.10 or greater.
- Back up your ArubaOS controller configuration file. Information about backing up AirWave is available in the *Dell PowerConnect W-AirWave 7.6 User Guide* in the "Performing Daily Operations in AirWave" chapter.

### Procedure

Perform the following steps to deploy Dell PowerConnect W Configuration when at least one Dell PowerConnect W AP Group currently exists on at least one Dell PowerConnect 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 PowerConnect W Configuration** accordingly.
2. On the **Groups > Basic** page, enable device preferences for Dell PowerConnect 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 PowerConnect W Configuration. One important setting on this page is the **Dell PowerConnect W GUI Config** option. Ensure that setting is **Yes**, which is the default setting.
3. Authorize Dell PowerConnect W-Series controllers into the device group in **Monitor Only** mode.



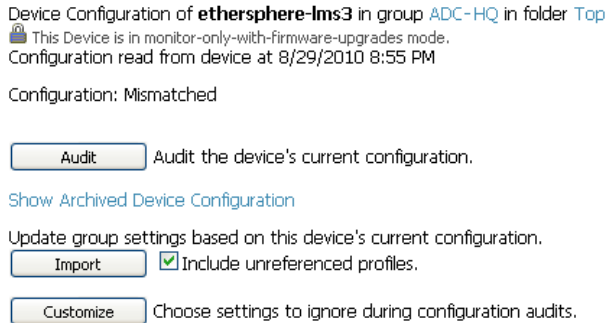
---

CAUTION: 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 would remove critical network configuration and status.

---

4. Navigate to the **APs/Devices > Audit** page for the first controller to prepare for importing an existing Dell PowerConnect W-Series controller configuration file. [Figure 15](#) illustrates the information available on this page if the device is mismatched.

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



If the page reports a device mismatch, the page will display an **Import** button that allows you to import the Dell PowerConnect W-Series controller settings from a Dell PowerConnect 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** checkbox. If you deselect the checkbox, AirWave will delete the unreferenced profiles/AP Groups on the controller when that configuration is pushed later, and they will not be imported.

*In Global Configuration:*

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

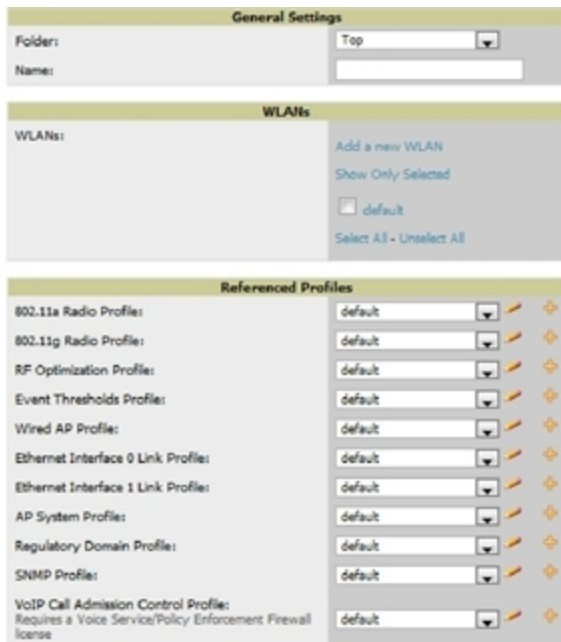
The folder for all the Profiles and Dell PowerConnect W AP Groups is set to the top folder of the AirWave user who imports the configuration. This folder is **Top** in the case of managing administrators with read/write privileges.

*In Group Configuration:*

Importing this configuration creates Profiles and Dell PowerConnect W AP Groups in the controller's **Groups > Dell PowerConnect W Config** page.

5. After configuration file import is complete, refresh the page to verify the results of the import and add or edit as required.
6. Navigate to the **Dell PowerConnect W Configuration** page.
  - This page displays a list of APs authorized on AirWave that are using the Dell PowerConnect W AP Group.
  - The **User Role** is the Dell PowerConnect W User Role used in firewall settings. For additional information, refer to "[Security > User Roles](#)" on page 46.
  - *Global Configuration only:* The **Folder** column cites the visibility level to devices in each Dell PowerConnect W AP Group. For additional information, refer to "[Visibility in Dell PowerConnect W Configuration](#)" on page 25.
7. Add or modify Dell PowerConnect W AP Groups as required.
  - a. Navigate to the **Dell PowerConnect W Configuration > Dell PowerConnect W AP Groups** page.
  - b. Click **Add** from the **Dell PowerConnect W AP Groups** page to create a new Dell PowerConnect 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. [Figure 16](#) illustrates this page.

**Figure 16: Dell PowerConnect W Configuration > Dell PowerConnect W AP Groups > Add/Edit Details Page (Partial View)**



For additional information about configuring Dell PowerConnect W AP Groups, see "[Dell PowerConnect W AP Groups Procedures and Guidelines](#)" on page 19.

8. Add or edit WLANs in Dell PowerConnect W Configuration as required.
  - a. Navigate to the **Dell PowerConnect 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 new WLAN, or click the pencil icon to edit an existing WLAN.

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

- **Basic**—This display is essentially the same as the ArubaOS Wizard View on the Dell PowerConnect W-Series controller. This page does not require in-depth knowledge of the profiles that define the Dell PowerConnect W AP Group.
- **Advanced**—This display allows you to select individual profiles that define the WLAN and associated Dell PowerConnect 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 20
- "[WLANs](#)" on page 38 for details on all WLAN settings

9. Add or edit Dell PowerConnect W Configuration Profiles as required.
  - a. Navigate to the **Dell PowerConnect 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 PowerConnect 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 PowerConnect W-Series controllers can be defined on the **Dell PowerConnect W Configuration** page. The following section in this document provides additional information about configuring profiles:

["General Profiles Guidelines" on page 20](#)

10. Provision multiple Dell PowerConnect 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 PowerConnect W AP Groups. With global configuration enabled, configure such Dell PowerConnect W AP Groups settings on the **Group > Dell PowerConnect W Config** page. With group configuration, use the Dell PowerConnect W AP Groups. The following section of this document provides additional information:

["Dell PowerConnect W AP Groups Procedures and Guidelines" on page 19](#)

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

["Selecting Dell PowerConnect W AP Groups" on page 20](#)

12. Each AP can be assigned to a single Dell PowerConnect 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 PowerConnect W Configuration" on page 22](#).

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

General		Settings	
Name:	ethersphere-lms3	Name:	ethersphere-lms3
Status:	Up (OK)	Location:	Networks
Configuration:	Mismatched (More Details)	Contact:	
Last Contacted:	10/7/2009 11:03 AM	Latitude:	
Type:	Aruba 6000	Longitude:	
Firmware:	3.4.0.2-vowifi	Altitude (m):	
Group:	HQ	Group:	HQ (SSID: aruba-ap)
Folder:	Top	Folder:	Top
Management Mode:	<input type="radio"/> Monitor Only + Firmware Upgrades <input type="radio"/> Manage Read/Write	Auto Detect Upstream Device:	<input checked="" type="radio"/> Yes <input type="radio"/> No
		Upstream device will automatically be updated when the device is polled.	
		Automatically clear Down Status Message when device comes back up:	<input type="radio"/> Yes <input checked="" type="radio"/> No
		Down Status Message:	
<b>Notes</b>		<b>Network Settings</b>	
If this device is down because its IP address or management ports have changed, update the fields below with the correct information. IP Address: 10.254.254.254 SNMP Port: 161 If this device is down because the credentials on the device have changed, update the fields below with the correct information. This device is currently using SNMP version 2c.		Gateway: 10.254.254.254	
Community String: ***** Confirm Community String: ***** SNMPv3 Username: Auth Password: Confirm Auth Password: SNMPv3 Auth Protocol: SHA-1 Privacy Password: Confirm Privacy Password: SNMPv3 Privacy Protocol: DES Telnet/SSH Username: viewonly Telnet/SSH Password: ***** Confirm Telnet/SSH Password: ***** "enable" Password: ***** Confirm "enable" Password: *****		<input type="button" value="Save and Apply"/> <input type="button" value="Revert"/> <input type="button" value="Delete"/> <input type="button" value="Ignore"/> <input type="button" value="Import Settings"/> <input type="button" value="Replace Hardware"/> <input type="button" value="Update Firmware"/>	

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.

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

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

Configuration: Error (Too Many Errors Fetching Existing Configuration)

Audit the device's current configuration.

Show Archived Device Configuration

Update group settings based on this device's current configuration.  
 Choose settings to ignore during configuration audits.

Show entire config  
 View Telnet/SSH Command log

Refresh this page

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

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

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

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

**Users for folder Sale HQ** Last 2 hours

Show All Maximum Average  
 Max Users 139.6 users 131.6 users

**Bandwidth for folder Sale HQ** Last 2 hours

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

1 year ago now

Modify Devices

Device	Status	Upstream Device	APs	Users	BW (kbps)	Uptime	Configuration	Aruba AP Group	Group	Controller
AL16	Up	-	11	810	-	11 hrs 9 mins	Mismatched	corp	Ethersphere-Ins3	ethersphere-Ins3
AL25	Up	-	8	101	-	11 hrs 8 mins	Mismatched	corp	Ethersphere-Ins3	ethersphere-Ins3
ethersphere-Ins4	Up	-	1	0	0	11 hrs 14 mins	Mismatched	-	Aruba HQ	-

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

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

4 Folders

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

- Once Dell PowerConnect 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 PowerConnect W-AirWave 7.6 User Guide* at [dell.com/support/manuals](http://dell.com/support/manuals).
- 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 ArubaOS configurations and settings. Refer to the following additional resources on [dell.com/support/manuals](http://dell.com/support/manuals) for more information:

- *Dell PowerConnect W-Series ArubaOS User Guide*
- *Dell PowerConnect W-AirWave 7.6 User Guide*
- *Dell PowerConnect W-AirWave 7.6 Best Practices Guide*



## Chapter 2

### Dell PowerConnect W Configuration in Daily Operations

This section presents common tasks or concepts after initial setup of Dell PowerConnect W Configuration is complete, as described in the section ["Setting Up Initial Dell PowerConnect W Configuration" on page 13](#). This chapter emphasizes frequent procedures as follows:

- ["Dell PowerConnect W AP Groups Procedures and Guidelines" on page 19](#)
- ["General WLAN Guidelines" on page 20](#)
- ["General Controller Procedures and Guidelines" on page 21](#)
- ["Supporting APs with Dell PowerConnect W Configuration" on page 22](#)
- ["Visibility in Dell PowerConnect W Configuration" on page 25](#)
- ["Using AirWave to Deploy Dell PowerConnect W-Series APs" on page 23](#)



---

NOTE: For a complete reference on all Configuration pages, field descriptions, and certain additional procedures that are more specialized, refer to ["Configuration Reference" on page 29](#).

---

## Dell PowerConnect W AP Groups Procedures and Guidelines

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

The fields and default settings for Dell PowerConnect W AP Groups are described in ["Dell PowerConnect W AP Groups" on page 30](#). The following guidelines govern the configuration and use of Dell PowerConnect W AP Groups across AirWave:

- Dell PowerConnect W AP Groups function with standard AirWave groups that contain them. Add Dell PowerConnect 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 PowerConnect W AP Groups must be pushed to Dell PowerConnect 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 21](#).

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

- The **Dell PowerConnect W Configuration** navigation pane displays standard ArubaOS components and your custom-configured Dell PowerConnect W AP Groups, WLANs, and AP Overrides.
- You define or modify Dell PowerConnect W AP Groups on the **Dell PowerConnect W Configuration** page. Click **Dell PowerConnect W AP Groups** from the navigation pane.
- With Global configuration enabled, select **Dell PowerConnect W AP Groups** to associate with AirWave Groups with the **Groups > Dell PowerConnect W Config** page.

- You modify devices in Dell PowerConnect 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 PowerConnect W AP Group.

## Selecting Dell PowerConnect W AP Groups

To select Dell PowerConnect W AP Groups, navigate to the **Dell PowerConnect W Configuration > Dell PowerConnect W AP Groups** page. This page is central to defining Dell PowerConnect 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 PowerConnect W AP Groups

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

1. Browse to the **Dell PowerConnect 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 PowerConnect 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 PowerConnect W AP Groups Procedures and Guidelines" on page 19](#).
3. Click **Add** or **Save** to finish creating or editing the Dell PowerConnect 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 PowerConnect 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 PowerConnect 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 21](#).

Once Dell PowerConnect W AP groups are defined, ensure that all desired WLANs are referenced in Dell PowerConnect W AP Groups, as required. Repeat the above procedure to revise WLANs as required. You can add or edit AP devices in Dell PowerConnect 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 PowerConnect W Configuration

- The **Dell PowerConnect W Configuration** navigation pane displays custom-configured WLANs and Dell PowerConnect W AP Groups. You define or modify WLANs on the **Dell PowerConnect 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 PowerConnect W-Series controllers to become active on the network.

### General Profiles Guidelines

ArubaOS elements can be added or edited after an ArubaOS configuration file is imported to AirWave and pushed to controllers with the steps described in ["Setting Up Initial Dell PowerConnect W Configuration" on page 13](#).

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

- Profiles define nearly all parameters for Dell PowerConnect W AP Groups and WLANs, and Dell PowerConnect 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 PowerConnect W AP Group or WLAN setup. In the latter case, AirWave takes you to profile setup on separate pages, then returns to the Dell PowerConnect W AP Group or WLAN setup.

For additional information about Profiles, refer to ["Profiles" on page 43](#).

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

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




---

**NOTE:** If you click **Save and Apply** when a device is in **Monitor** mode, this initiates a verification process in which 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 PowerConnect 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 PowerConnect W Configuration

### AP Overrides Guidelines

The **AP Override** component of Dell PowerConnect 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 PowerConnect W AP Group. To do so, refer to the following topics that describe ARM in relation to Dell PowerConnect W AP groups and device-level radio settings:

- ["Configuring Dell PowerConnect W AP Groups" on page 20](#)
- ["Dell PowerConnect W AP Groups Procedures and Guidelines" on page 19](#)
- ["Profiles" on page 43](#)

### Changing SSID and Encryption Settings

You can adjust SSID and Encryption parameters for devices by adjusting the profiles that define these settings, then applying those profiles to Dell PowerConnect 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 PowerConnect W AP Groups" on page 20](#)
- ["Guidelines and Pages for WLANs in Dell PowerConnect W Configuration" on page 20](#)
- ["Profiles" on page 43](#)

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

You can change the Dell PowerConnect 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 PowerConnect W AP Groups currently configured in AirWave. Navigate to the **Dell PowerConnect W Configuration** page, and click **Dell PowerConnect 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 PowerConnect 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 AP controller that is to support this AP device. For additional information, refer to "[Pushing Device Configurations to Controllers](#)" on page 21.

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

In addition to migrating Dell PowerConnect W-Series access points (APs) from ArubaOS-oriented administration to AirWave administration, you can use AirWave to deploy Dell PowerConnect W-Series APs for the first time without separate ArubaOS 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 PowerConnect W-Series APs
  - managing Dell PowerConnect W-Series controllers with AirWave
- In this scenario, when a new Dell PowerConnect W-Series AP boots up, AirWave may discover the AP before you have a chance to configure and launch it through ArubaOS configuration on the Dell PowerConnect 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 PowerConnect 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 PowerConnect W-Series AP device name is to deploy Dell PowerConnect W-Series APs in AirWave with the following steps:

1. Define communication settings for Dell PowerConnect 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 PowerConnect 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 PowerConnect W AP Group and the Dell PowerConnect W-Series controller with the `show ap databaseasos` command.
8. To set the appropriate Dell PowerConnect 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 PowerConnect W Group** below the list of the devices, select the appropriate group, and the click **Move**.

---

 NOTE: If the list of Dell PowerConnect W AP Groups is not there, either create these AP groups manually on the **Device Setup > Dell PowerConnect 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.

---

 NOTE: Dell PowerConnect W APs can also belong to Dell PowerConnect 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 PowerConnect W Configuration

## Visibility Overview

Dell PowerConnect 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:

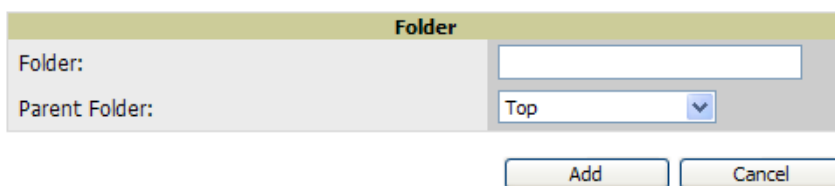
- Administrative and Management users in AirWave can view the **Dell PowerConnect W Configuration** page and the **APs/Devices > Manage** pages.
  - Administrative users are enabled to view all configurations.
  - Management users have access to all profiles and Dell PowerConnect W AP groups for their respective folders.
- The **Device Setup > Dell PowerConnect W Configuration** page has a limit to folder drop-down options for customers that manage different accounts and different types of users.
- Dell PowerConnect W Configuration entails specific user role and security profiles that define some components of visibility, as follows:
  - ["Security > User Roles" on page 46](#)
  - ["Security > Policies" on page 51](#)
- AirWave continues to support the standard operation of folders, users, and user roles as described in the *Dell PowerConnect W-AirWave 7.6 User Guide*.

## Defining Visibility for Dell PowerConnect W Configuration

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

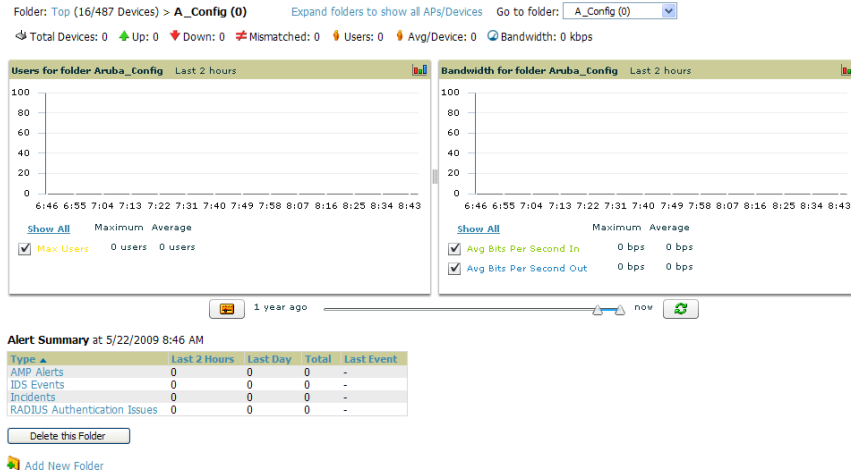
1. As required, create a new AirWave device folder with management access.
  - a. Navigate to the **APs/Device > List** page, scroll to the bottom of the page. (An alternate page supporting new folders is **Users > Connected** page.)
  - b. Click the **Add New Folder** link. The **Folder** detail page appears, as illustrated in [Figure 20](#):

**Figure 20: 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 21](#) illustrates an unpopulated device page for an example folder.

**Figure 21: APs/Devices > List Page With No Devices**



2. Add Dell PowerConnect W-Series controller devices to that folder as required. Use the **Device Setup > Add** page following instructions available in the *Dell PowerConnect W-AirWave 7.6 User Guide*.
3. As required, create or edit a user role that is to have rights and manage privileges required to support their function in Dell PowerConnect 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 PowerConnect 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 22](#).

**Figure 22: AMP Setup Setup > Roles > Add/Edit Role Page Illustration**

**Role**

Name:

Enabled:  Yes  No

Type:

AP/Device Access Level:

Top Folder:

RAPIDS:

VisualRF:

Helpdesk:  Yes  No

- c. As per standard AirWave configuration, complete the settings on this page. The most important fields with regard to Dell PowerConnect 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 PowerConnect W-Series controller, devices, and general Dell PowerConnect 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 PowerConnect W Configuration. This step creates or edits users to have rights appropriate to Dell PowerConnect W Configuration. This user inherits visibility to Dell PowerConnect W-Series controllers and Dell PowerConnect 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 PowerConnect W-AirWave 7.6 User Guide* as required.
  5. Observe visibility created or edited with this procedure.

The user, role, and device folder created with this procedure are now available to configure, manage, and support Dell PowerConnect 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 PowerConnect W-AirWave 7.6 User Guide*.
  7. Continue to other elements of Dell PowerConnect W Configuration described in the Reference section of this document.



# Appendix A

## Configuration Reference

### Introduction

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

- Dell PowerConnect W Configuration components are summarized in "[Additional Concepts and Components](#)" on [page 10](#).
- For procedures that use several of these components, refer to earlier chapters in this document.
- For architectural information about ArubaOS, refer to the *Dell PowerConnect W-Series ArubaOS User Guide*.



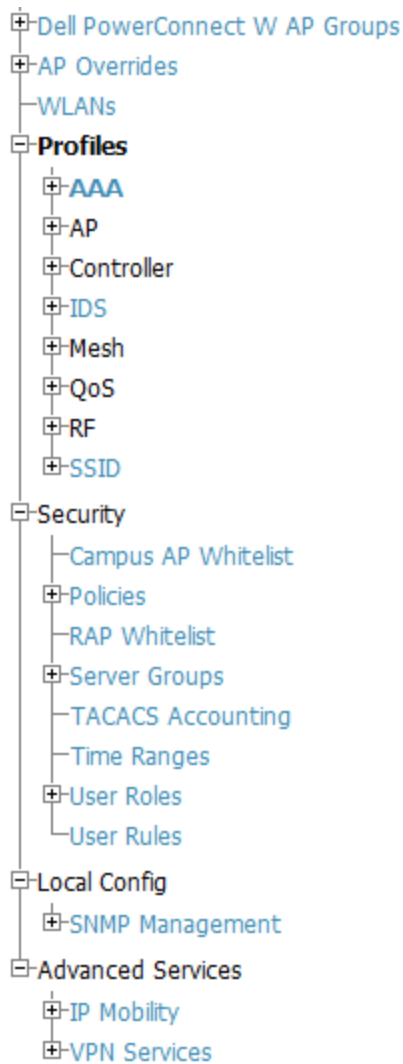
---

NOTE: The default values of profile parameters or functions may differ slightly between ArubaOS releases.

---

Access all pages and field descriptions in this appendix from the **Device Setup > Dell PowerConnect W Configuration** page, illustrated in [Figure 23](#). The one exception is the additional **Groups > Dell PowerConnect W Config** page that you access from the standard AirWave navigation menu.

**Figure 23: Dell PowerConnect W Configuration Components**



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

- "Dell PowerConnect W AP Groups" on page 30
- "AP Overrides" on page 34
- "WLANs" on page 38
- "Profiles" on page 43
- "Security" on page 44
- "Local Config of SNMP Management" on page 66
- "Advanced Services" on page 67
- "Groups > Dell PowerConnect W Config Page" on page 79

## Dell PowerConnect W AP Groups

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

## About Dell PowerConnect W AP Groups

The Dell PowerConnect W AP Groups page displays all configured Dell PowerConnect W AP Groups and enables you to add or edit Dell PowerConnect W AP Groups. For additional information about using this page, refer to ["Dell PowerConnect W AP Groups Procedures and Guidelines" on page 19](#).

The Dell PowerConnect W AP Groups page displays the following information for every group currently configured:

**Table 1:** *Dell PowerConnect W Configuration > Dell PowerConnect W AP Groups Page*

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

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

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Displays the folder with which the AP Group is associated. The drop-down menu displays all folders available for association with the AP Group. Folders provide a way to organize the visibility of device parameters that is separate from the configuration groups of devices. Using folders, you can view basic statistics about device, and define which users have visibility to which device parameters.
Name	Default	Enter the name of the AP Group.
<b>WLANs</b>		
Add a new WLAN		Select this link to create a new WLAN to support Dell PowerConnect W Configuration. Once created, that new WLAN will appear with others on this page.
Show only		To set the WLANs that appear on this page, select (check) the desired WLANs, then click

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

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>
802.11a Traffic Management Profile	default	<p>Specify the minimum percentage of available bandwidth to be allocated to a specific SSID when there is congestion on the wireless network, and sets the interval between bandwidth usage reports. This setting pertains specifically to 802.11a.</p>
IDS Profile	default	<p>Selects the IDS profile to be associated with the new AP Group. The drop-down menu contains these options:</p> <ul style="list-style-type: none"> <li>• ids-disabled</li> </ul>

Field	Default	Description
		<ul style="list-style-type: none"> <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 PowerConnect W AP Group. This group now appears in the navigation pane of the Dell PowerConnect W Configuration page.

## AP Overrides

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

**Figure 24: AP Overrides Page Illustration**

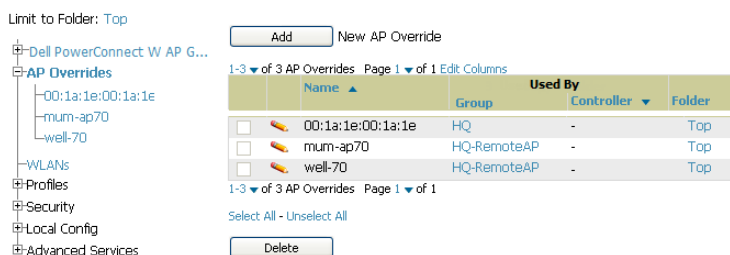


Table 3 describes the fields on this page.



**Table 3: AP Overrides Fields and Descriptions**

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

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

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

Field	Default	Description
Name	Blank	Name of the AP Override. Use the name of the AP device to which it applies.
Folder	Top	Displays the folder with which the WLAN is associated. The drop-down menu displays all folders available for association with the WLAN.
<b>WLANs</b>		
WLANs		This section lists the WLANs currently defined in Dell PowerConnect W Configuration by default. You can display selected WLANs or all WLANs.  Select one or more WLANs for which AP Override is to apply.
<b>Excluded WLANs</b>		
Excluded WLANs		This section displays WLANs currently defined in Dell PowerConnect 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> .
<b>Referenced Profiles</b>		
802.11a Radio Profile	5_am	Defines AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.  Select the <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.
802.11g Radio Profile	2.4_am	Defines AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Each 802.11a and 802.11b radio profile includes a reference to an Adaptive Radio Management (ARM) profile.  If you would like the ARM feature to select dynamically the best channel and transmission power for the radio, verify that the 802.11a/802.11g radio profile references an active and enabled ARM profile. If you want to manually select a channel for each AP group, create separate 802.11a and 802.11g profiles for each AP group and assign a different transmission channel for each profile.  The drop-down menu displays these options: <ul style="list-style-type: none"> <li>● default</li> </ul>

Field	Default	Description
		<ul style="list-style-type: none"> <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 PowerConnect 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>
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 PowerConnect 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>

Field	Default	Description
Regulatory Domain Profile	default	<p>Defines an AP's country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios.</p> <p>Select the pencil icon next to this field to display the <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>
802.11a Traffic Management Profile	default	<p>Specify the minimum percentage of available bandwidth to be allocated to a specific SSID when there is congestion on the wireless network, and sets the interval between bandwidth usage reports. This setting pertains specifically to 802.11a.</p>
IDS Profile	default	<p>Selects the IDS profile to be associated with the new AP Group. The drop-down menu contains these options:</p> <ul style="list-style-type: none"> <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	<p>Determines many of the settings used by mesh nodes to establish mesh links and the path to the mesh portal, including the maximum number of children a mesh node can accept, and transmit rates for the 802.11a and 802.11g radios.</p>
AP Authorization Profile		<p>Selects the AP Authorization profile to be associated with the new AP Group. This profile requires a Remote Access Points license.</p>
AP Provisioning Profile		<p>Selects the AP Provisioning profile to be associated with the new AP Group.</p>
Ethernet Interface 0-4		<p>Selects the Ethernet port configuration to be associated with the new AP Group.</p>

Field	Default	Description
Port Configuration		This profile allows you to configure all AP wired port profiles and their status. The drop-down menu contains these options: <ul style="list-style-type: none"> <li>• default</li> <li>• NoWiredAuthPort</li> <li>• shutdown</li> </ul>
<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 PowerConnect 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 PowerConnect W-AirWave 7.6 User Guide* for additional information.

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

- The **Device Setup > Dell PowerConnect W Configuration** navigation pane displays custom-configured WLANs and Dell PowerConnect W AP Groups. All other components of the navigation pane are standard across all deployments of Dell PowerConnect W Configuration.
- You define or modify WLANs on the **Device Setup > Dell PowerConnect 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 PowerConnect W Configuration and enables you to add or edit WLANs. For additional information about using this page, refer to "[General WLAN Guidelines](#)" on page 20.

The **Dell PowerConnect W Configuration > WLANs** page contains additional information as described in [Table 5](#):

**Table 5: Dell PowerConnect 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 PowerConnect W AP Group	Lists the Dell PowerConnect 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 PowerConnect W AP Groups.
Traffic Management	Lists Traffic Management profiles that are currently configured and deployed on the WLAN.
Folder	Lists the folder for the WLAN.

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

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

## WLANs > Basic

From the **Dell PowerConnect 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. [Table 6](#) describes the fields for this page.

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

Field	Default	Description
Name	Blank	Enter the name of the WLAN.
Folder	Top	Displays the folder with which the WLAN is associated. The drop-down menu displays all folders available for association with the WLAN.
SSID		Select the SSID profile that defines encryption, EDCA or high-throughput SSID parameters. Access these SSID profiles by clicking <b>Profiles &gt; SSID</b> in the navigation pane at left.
Radio Type		Define whether the supported radio type on the WLAN is 802.11a, 802.11g, or all.
Enable 802.11n	Yes	Define whether the WLAN is to support 802.11n.
VLAN	1	Select the VLAN ID number to be supported on this WLAN.
Intended Use	Internal	Define whether this WLAN is <b>Internal</b> to the enterprise or to support <b>Guest</b> users.
Encryption	opensystem	Select one or more encryption types, as desired, to be supported by this WLAN.
Use Captive Portal	No	Select whether this WLAN will use captive portal authentication. Captive portal authentication directs clients to a special web page that typically requires them to enter a username and password before accessing the network.

Field	Default	Description
Authenticated User Role	logon	For the captive portal authentication profile, you specify the previously-created auth-guest user role as the default user role for authenticated captive portal clients and the authentication server group (Internal). Refer to " <a href="#">Security &gt; User Roles</a> " on page 46.

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

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

## WLANs > Advanced

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

**Table 7:** WLANs > Advanced Page Fields

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Displays the folder with which the WLAN is associated. The drop-down menu displays all folders available for association with the WLAN.
Name	Blank	Name of the WLAN.
<b>Referenced Profiles</b>		
SSID Profile		Select the SSID profile that defines encryption, EDCA or high-throughput SSID parameters. Access these SSID profiles by clicking <b>Profiles &gt; SSID</b> in the navigation pane at left.
AAA Profile		Select the AAA profile that defines RADIUS, TACACS+, or other AAA server configurations for this WLAN. Access these SSID profiles by clicking <b>Profiles &gt; AAA</b> in the navigation pane at left.
802.11k Profile		Manages settings for the 802.11k protocol. The 802.11k protocol allows APs and clients to dynamically query their radio environment and take appropriate connection actions. For example, in a 802.11k network if the AP with the strongest signal reaches its CAC (Call Admission Control) limits for voice calls, then on-hook voice clients may connect to an under utilized AP with a weaker signal. You can configure the following options in 802.11k profile: <ul style="list-style-type: none"> <li>• Enable or disable 802.11k support on the AP</li> <li>• Forceful disassociation of on-hook voice clients</li> <li>• Measurement mode for beacon reports.</li> </ul> For more details, see the Configuring 802.11k Protocol topic in the <i>Dell PowerConnect W-Series ArubaOS User Guide</i> .
WMM Traffic Management Profile		Manages settings for the bandwidth management profile for Wi-Fi Multimedia (WMM).
<b>Other Settings</b>		
Virtual AP Enable	Yes	Enable this setting to allow virtual AP configurations to be deployed on this WLAN.

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

Field	Default	Description
		<p>to 0 for the above authentication methods, which means that there is no limit to the number of times a client can attempt to authenticate.</p> <p>With 802.1x authentication, you can also configure blacklisting of clients who fail machine authentication.</p> <p><b>NOTE:</b> This requires that the External Services Interface (ESI) license be installed in the controller.</p> <p><b>NOTE:</b> When clients are blacklisted because they exceed the authentication failure threshold, they are blacklisted indefinitely by default. You can configure the duration of the blacklisting.</p>
Fast Roaming	No	Fast roaming is a component of virtual AP profiles in which client devices are allowed to roam from one access point to another without requiring reauthentication by the main RADIUS server.
Strict Compliance	No	Define whether clients should have strict adherence to settings on this page for network access.
VLAN Mobility	No	Define whether clients in the WLAN and VLAN should have mobility or roaming privileges.
Remote AP Operation	Standard	<p>Define the rights for remote APs in this WLAN. Options are as follows:</p> <ul style="list-style-type: none"> <li>• standard</li> <li>• persistent</li> <li>• backup</li> <li>• always</li> </ul> <p>Remote APs connect to a controller using Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec). AP control and 802.11 data traffic are carried through this tunnel. Secure Remote Access Point Service extends the corporate office to the remote site. Remote users can use the same features as corporate office users. Secure Remote Access Point Service can also be used to secure control traffic between an AP and the controller in a corporate environment. In this case, both the AP and controller are in the company's private address space.</p>
Drop Broadcast and Multicast	No	Specify whether the WLAN should drop broadcast and multicast mesh network advertising on the WLAN.
Convert Broadcast ARP Requests to Unicast	No	Specify whether ARP table information should be distributed in broadcast (default) or unicast fashion.
Deny Inter User Traffic	No	If enabled, this setting disables traffic between all untrusted users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic. Requires a minimum version of 6.1.0.0.
Band Steering	No	Enable or disable band steering on the WLAN. Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5GHz band than on the 2.4GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40MHz or 20MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.
Steering Mode	Prefer-5ghz	<p>Band steering supports three different band steering modes.</p> <ul style="list-style-type: none"> <li>• <b>Force-5GHz:</b> When the AP is configured in <b>force-5GHz</b> band steering mode, the AP will try to force 5GHz-capable APs to use that radio band.</li> <li>• <b>Prefer-5GHz (Default):</b> If you configure the AP to use <b>prefer-5GHz</b> band steering</li> </ul>



Field	Default	Description
		<p>mode, the AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts.</p> <ul style="list-style-type: none"> <li>• <b>Balance-bands:</b> In this band steering mode, the AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5GHz band has more channels than the 2.4 GHz band, and that the 5GHz channels operate in 40MHz while the 2.5GHz band operates in 20MHz.</li> </ul> <p><b>NOTE:</b> Steering modes do not take effect until the band steering feature has been enabled. The band steering feature in ArubaOS versions 3.3.2-5.0 does not support multiple band-steering modes. The band-steering feature in these versions of ArubaOS functions the same way as the default <b>prefer-5GHz</b> steering mode available in ArubaOS 6.0 and later.</p>
Dynamic Multicast Optimization (DMO)	No	If enabled, DMO techniques will be used to reliably transmit video data.
Dynamic Multicast Optimization (DMO) Threshold (2-255)	6	Maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops.
Preserve Client VLAN	No	Whether to preserve the client VLAN. Requires version between 3.4.4.3 and 5.0.0.0, or version 6.1.0.0 and above.
Disable conversion of IPv6 multicast Router Advertisements to unicast	No	Enable or disable converting advertised IPv6 multicast routers to unicast to reduce unnecessary traffic. Firmware version 6.1.2.0 is required.

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

## Profiles

### Understanding Dell PowerConnect 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.

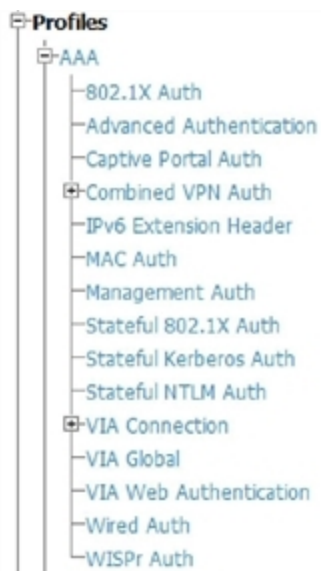
You can apply profiles to an AP or AP group.

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

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

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

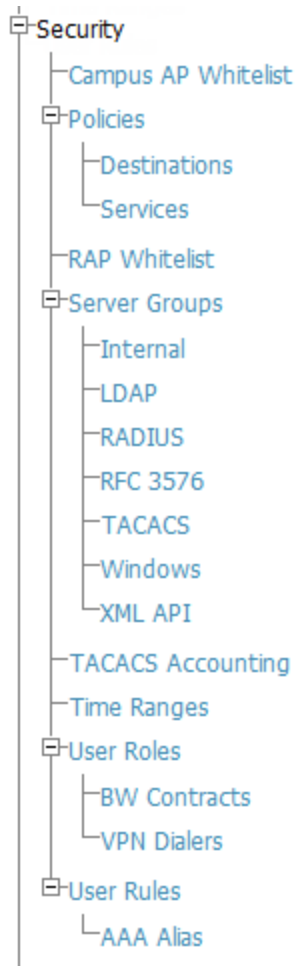
**Figure 25:** Profiles



## Security

Dell PowerConnect W Configuration supports user roles, policies, server groups, and additional security parameters with profiles that are listed in the **Security** portion of the navigation pane on the **Dell PowerConnect W Configuration** page, as illustrated in [Figure 26](#):

**Figure 26: Security Components in Dell PowerConnect W Configuration**



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

- Campus AP Whitelist
- "Security > Policies" on page 51
  - "Security > Policies > Destinations" on page 53
  - "Security > Policies > Services" on page 54
- Security RAP Whitelist
- "Security > Server Groups" on page 55
  - "Security > Server Groups > Internal" on page 61
  - "Security > Server Groups > LDAP" on page 58
  - "Security > Server Groups > RADIUS" on page 59
  - "Security > Server Groups > RFC 3576" on page 62
  - "Security > Server Groups > TACACS" on page 60
  - "Security > Server Groups > Windows" on page 63
  - "Security > Server Groups > XML API" on page 62
- "Security > TACACS Accounting" on page 63
- "Security > Time Ranges" on page 64

- "Security > User Roles" on page 46
  - "Security > User Roles > BW Contracts" on page 48
  - "Security > User Roles > VPN Dialers" on page 49
- "Security > User Rules" on page 65
  - 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 PowerConnect W Vendor-Specific Attributes (VSA) for RADIUS server authentication. A role derived from a Dell PowerConnect W VSA takes precedence over any other user roles.

In the Dell PowerConnect 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 PowerConnect 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).




---

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

---

This page displays the current user roles in Dell PowerConnect W Configuration and where they are used. This page contains the columns described in [Table 8](#):

**Table 8:** *Security > User Roles Page Contents*

Column	Description
Name	Name of the user role.

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

The Security > User Roles > Add New User Role page contains the following fields, as described in [Table 9](#):

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the User Role is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the user role.
<b>Other Settings</b>		
Captive Portal Profile	None	(Optional) Select the Captive Portal Auth profile, if any, that is to be referenced by the user role. Select the add icon to create a new profile, or click the pencil icon to edit an existing profile.
Downstream Bandwidth Contract	None	(Optional) You can assign a bandwidth contract to provide an upper limit to upstream or downstream bandwidth utilized by clients in this role. You can select the Per User option to apply the bandwidth contracts on a per-user basis instead of to all clients in the role. Refer to " <a href="#">Security &gt; User Roles &gt; BW Contracts</a> " on page 48.
Downstream Contract Applies Per User	No	If you selected a DS BW contract in the prior field, this gray field becomes active. Select <b>Yes</b> or <b>No</b> .
Upstream Bandwidth Contract	None	(Optional) You can assign a bandwidth contract to provide an upper limit to upstream or downstream bandwidth utilized by clients in this role. You can select the Per User option to apply the bandwidth contracts on a per-user basis instead of to all clients in the role. Refer to " <a href="#">Security &gt; User Roles &gt; BW Contracts</a> " on page 48.
Upstream Contract Applies Per User	No	If you selected an US BW contract in the prior field, this gray field becomes active. Select <b>Yes</b> or <b>No</b> .
Maximum Number of Datapath Sessions	None	Use this field to configure a maximum number of sessions per user in this role. You can configure any value between 0-65535.

Field	Default	Description
Allowed		
Reauthentication Interval Time	0	(Optional) Set the time, in minutes, after which the client is required to re-authenticate. Enter a value between 0-4096. 0 disables reauthentication.
VLAN To Be Assigned		(Optional) By default, a client is assigned a VLAN on the basis of the ingress VLAN for the client to the controller. Use this field to override this assignment and configure the VLAN ID that is to be assigned to the user role.
VPN Dialer Profile	None	(Optional) Use this field to assign a VPN dialer to a user role. Select a dialer from the drop-down list and assign it to the user role. This dialer will be available for download when a client logs in using captive portal and is assigned this role. For additional VPN information, refer to <a href="#">"Security &gt; User Roles &gt; VPN Dialers"</a> on page 49.
VIA Connection Profile	None	Use this field to assign a VIA connection to a user role.
<b>Policies</b>		
Add New Policy		Select this button to add a new policy to the user role. The following two columns appear: <ul style="list-style-type: none"> <li>• Policy</li> <li>• Dell PowerConnect W AP Group</li> </ul>
Policy	allow-diskservices	Select the policy to apply to this user role. Once any policy is selected, you can edit the policy by clicking the pencil icon. You can create a new policy by clicking the add icon. Refer to <a href="#">"Security &gt; Policies"</a> on page 51.
Dell PowerConnect WAP Group	None	Select the Dell PowerConnect W AP group in which this policy and user role will apply. Refer to <a href="#">"Dell PowerConnect W AP Groups Procedures and Guidelines"</a> on page 19.

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

## Security > User Roles > BW Contracts

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

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

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

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

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

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

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

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

## Security > User Roles > VPN Dialers

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

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

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

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

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

Field	Default	Description
Enable PPTP	No	<p>Enable PPTP with this setting as desired.</p> <p>Point-to-Point Tunneling Protocol (PPTP) is an alternative to L2TP/IPSec. Like L2TP/IPSec, PPTP provides a logical transport mechanism to send PPP frames as well as tunneling or encapsulation so that the PPP frames can be sent across an IP network. PPTP relies on the PPP connection process to perform user authentication and protocol configuration.</p> <p>With PPTP, data encryption begins after PPP authentication and connection process is completed. PPTP connections use Microsoft Point-to-Point Encryption (MPPE), which uses the Rivest-Shamir-Aldeman (RSA) RC-4 encryption algorithm. PPTP connections require user-level authentication through a PPP-based authentication protocol (MSCHAPv2) is the currently-supported method).</p>
Enable L2TP	Yes	<p>Enable L2TP with this setting as desired.</p> <p>The combination of Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec) is a highly secure technology that enables VPN connections across public networks such as the Internet. L2TP/IPSec provides both a logical transport mechanism on which to transmit PPP frames as well as tunneling or encapsulation so that the PPP frames can be sent across an IP network. L2TP/IPSec relies on the PPP connection process to perform user authentication and protocol configuration. With L2TP/IPSec, the user authentication process is encrypted using the Data Encryption Standard (DES) or Triple DES (3DES) algorithm.</p> <p>L2TP/IPSec requires two levels of authentication:</p> <ul style="list-style-type: none"> <li>• Computer-level authentication with a preshared key to create the IPsec security associations (SAs) to protect the L2TP-encapsulated data.</li> <li>• User-level authentication through a PPP-based authentication protocol using passwords, SecurID, digital certificates, or smart cards after successful creation of the SAs.</li> </ul>
Send traffic to the direct network in clear	No	Use this setting if no encryption is to be used and packets passing between the wireless client and the controller are to be in clear text.
Disable wireless devices when client is wired	No	Use this setting to disable wireless clients when a wired device is known to be on the VPN.
Enable SecurID New and Next Pin Mode	No	<p>Use this setting to enable or disable SecurID PIN modes.</p> <p>The SecurID authentication scheme authenticates the user on a RSA ACE/Server. When challenged, the user has to enter a password that is a combination of two numbers: a personal identification number (PIN), supplied by RSA, combined with a token code, which is the number displayed on the RSA SecurID authenticator.</p> <p>New PIN mode is applied in cases where the authentication process requires additional verification of the PIN. In this case, the user is required to use a new PIN. The new PIN is derived from one of the following two sources, depending on the configuration of the RSA ACE/Server:</p> <ul style="list-style-type: none"> <li>• The user is prompted to select and enter a new PIN.</li> <li>• The server supplies the user with a new PIN.</li> </ul> <p>The user is then required to re-authenticate with the new PIN. The use of the New PIN mode is optional and can be enabled or disabled.</p>
PPP Authentication Modes	CHAP MSCHAP MSCHAPv2 PAP	<p>Use this section to select the authentication modes to be supported for PPP in the VPN. The following options are available:</p> <ul style="list-style-type: none"> <li>• CHAP</li> <li>• Cache SecurID Token</li> <li>• MSCHAP</li> <li>• MSCHAPv2</li> </ul>



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

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

## Security > Policies

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

Policy button. To edit an existing policy, click the pencil icon.

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

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the policy is associated. The drop-down menu displays all folders available for association with the policy.
Name	Blank	Enter the name of the policy.
<b>Rules</b>		
IPv6	No	Select whether to use the IPv6 protocol. If you select <b>No</b> , AirWave displays options for the IPv4 protocol instead. <b>NOTE:</b> As of AOS 6.0, you can mix IPv4 and IPv6 rules on one policy.
Source Traffic Match	any	The traffic source, which can be one of the following: <ul style="list-style-type: none"> <li>● <b>alias:</b> After choosing this option, specify the network resource from the <b>Source Alias</b> drop-down menu that appears. Select the pencil icon to edit, or the plus icon to add a new alias.</li> <li>● <b>any:</b> match any traffic (wildcard)</li> <li>● <b>host:</b> This refers to traffic from a specific host. When this option is chosen, you must configure the source IP address of the host. For example, 2002:d81f:f9f0:1000:c7e:5d61:585c:3ab</li> <li>● <b>localip:</b> (IPv4 only) specify the local IP address to match traffic</li> <li>● <b>network:</b> This refers to a traffic that has a source IP from a subnet of IP addresses. When this option is chosen, you must configure the source address and network mask of the subnet. For example, 2002:ac10:fe::ffff:ffff:ffff:..</li> <li>● <b>user:</b> This refers to traffic from the wireless client.</li> </ul>
Destination Traffic Match	any	The traffic destination, which can be any of the same types as the Source Traffic Match options.
Service Type	any	Type of traffic, which can be one of the following: <ul style="list-style-type: none"> <li>● <b>any:</b> This option specifies that this rule applies to any type of traffic.</li> <li>● <b>tcp:</b> Using this option, configure a range of TCP port(s) to match for the rule to be applied.</li> <li>● <b>udp:</b> Using this option, configure a range of UDP port(s) to match for the rule to be applied.</li> <li>● <b>service:</b> Selecting this option creates a new field called <b>Service</b> underneath <b>Service Type</b> with a drop-down list of pre-defined services (common protocols such as HTTPS, HTTP, and others) as the protocol to match for the rule to be applied. Select the pencil icon to edit the Netservice Profile (refer to "<a href="#">Security &gt; Policies &gt; Services</a>" on page 54), or the plus sign to create a new Netservice profile.</li> <li>● <b>protocol:</b> Using this option, specify a different layer 4 protocol (other than TCP/UDP) by configuring the IP protocol value.</li> <li>● <b>icmpv6:</b> Use this option to configure ICMPv6. Requires IPv6 enabled.</li> </ul>
Action	permit	Action if rule is applied, which can be one of the following: <ul style="list-style-type: none"> <li>● <b>reject:</b> deny packets. A new field will appear where you can Send Deny Response</li> <li>● <b>dst-nat:</b> perform destination NAT on packets. New fields appear to specify the Dual NAT Pool and Dual NAT Port.</li> </ul>

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

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

## Security > Policies > Destinations

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

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

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

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

Field	Default	Description
Name	Blank	Enter the name of the destination.
<b>Rules</b>		
Invert	No	Use this field to invert the destination from one end of the VPN connection to the other.
IPv6	No	Select this button to create a new rule for this destination profile. Clicking this button displays the <b>Net Destination Rule</b> section for the selected protocol, which is comprised of two settings: <ul style="list-style-type: none"> <li><b>Rule Type</b>—Specify whether the rule applies to <b>Host</b>, <b>Network</b>, or <b>Range</b>.</li> <li><b>IP Address</b>—Enter the IP address for the net destination rule.</li> </ul>

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

## Security > Policies > Services

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

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

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the security policy service is associated. The drop-down menu displays all folders available for association with the service.
Name	Blank	Enter the name of the destination.
<b>Other Settings</b>		
Protocol	TCP	Specify the protocol that is to support the security policy service being configured. The service options are: <ul style="list-style-type: none"> <li>TCP</li> <li>UDP</li> <li>IP</li> </ul> The remaining fields on this page change according to which protocol you have selected.
Port Selection	Range	Choose whether to list ports by <b>Range</b> (which causes the Port and Max Port fields to appear below) or <b>List</b> (which introduces a Port List field and requires a minimum version of 6.0.0.0).
TCP/UDP Port		Appears if <b>Range</b> is specified in Port Selection. Specify the TCP/UDP port or range of ports to support the service being configured.
TCP/UDP Max Port		Appears if <b>Range</b> is specified in Port Selection. Specify the highest port that will

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

## Security > Server Groups

### Server Groups Page Overview

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

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

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

The first available server in the list is used for authentication. If the server responds with an authentication failure, there is no further processing for the user or client for which the authentication request failed. You can optionally enable fail-through authentication for the server group so that if the first server in the list returns an authentication deny, the 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 PowerConnect W-Series ArubaOS supports the following external authentication servers:

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

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

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

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

## Adding a New Server Group

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

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

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

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

Field	Default	Description
<b>Other Settings</b>		
Fail Through	No	<p>Enable or disable a fail through server.</p> <p>When fail-through authentication is enabled, users that fail authentication on the first server in the server list should be authenticated with the second server. The 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.</p> <p>This feature is useful in environments where there are multiple, independent authentication servers; users may fail authentication on one server but can be authenticated on another server.</p>
Add New Server		<p>Select this button to add a new server to the Server Group being configured. A new <b>Server</b> section and Server Group Server Rules section appear with the following settings to be defined:</p> <p><b>Server Section</b></p> <ul style="list-style-type: none"> <li>• <b>Trim FQDN</b>—Default setting is <b>No</b>. Change to <b>Yes</b> to enable. You can use the <b>match FQDN</b> option for a server match rule. With a match FQDN rule, the server is selected if the &lt;domain&gt; portion of the user information in the formats &lt;domain&gt;\&lt;user&gt; or &lt;user&gt;@&lt;domain&gt; exactly matches a specified string. This rule does not support client information in the <b>host/&lt;pc-name&gt;.&lt;domain&gt;</b> format, so it is not useful for 802.1x machine authentication. The <b>match FQDN</b> option performs matches on only the &lt;domain&gt; portion of the user information sent in an authentication request. The <b>match-authstring</b> option (described previously) allows you to match all or a portion of the user information sent in an authentication request.</li> <li>• <b>Server Type</b>—Select the server type for the new server being added. Options are <b>RADIUS</b> (default), <b>LDAP</b>, <b>TACACS</b>, <b>Internal</b>, or <b>Windows</b>.</li> <li>• <b>Server</b>—Select the server from the drop-down menu that the new server is to use. You can edit an existing server or create a new server.</li> </ul> <p><b>Server Group Server Rules Section</b></p> <p>Select the <b>Add</b> button to add a new rules section. The page that appears contains the following settings to define:</p> <ul style="list-style-type: none"> <li>• <b>Match Type</b>—From the drop-down menu, select <b>Authstring</b> or <b>FQDN</b>. The following settings complete the configuration.</li> <li>• <b>Operator</b>—For <b>Authstring</b> only, specify how to process the string (<b>contains</b>, <b>equals</b>, <b>starts with</b>).</li> <li>• <b>Match String</b>—Enter the string or string fragment.</li> </ul> <p>Finish by clicking the <b>Add New Server Group Server Rules</b> button.</p>
<b>Server Group Rule</b>		
Field to set	role	Specify whether the server group rule is a <b>role</b> or a <b>VLAN</b> . The <b>Role/VLAN</b> field at the bottom of the page changes in response to your selection here.
Attribute	ARAP-Features	From the drop-down menu, click the attribute that defines the server group rule being configured. Many options are supported.
Operation	contains	Select the criteria by which to process the <b>Operand</b> , which you specify in the following field.
Operand		Enter a text string.
Role/VLAN	ap-role	Select the role or VLAN to associate with this new server group rule from the drop-down menu.

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

## Security > Server Groups > LDAP

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

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

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server.
<b>Other Settings</b>		
Host IP Address	0.0.0.0	Enter the IP address of the LDAP server.
Admin-DN		Enter the distinguished name for the admin user who has read/search privileges across all the entries in the LDAP database. The user need not have write privileges but the user should be able to search the database, and read attributes of other users in the database.
Admin Password		Enter the password for the admin user.
Allow Clear-text	No	Enable this setting to allows clear-text (unencrypted) communication with the LDAP server.
Auth Port	389	Enter the port number used for authentication on the LDAP server.
Base-DN		Enter the distinguished name of the node which contains the entire user database to use.
Filter	(objectclass=*)	Select the filter that should be applied to any search of the user in the LDAP database.
Key Attribute	sAMAccountName	Enter the attribute that should be used as a key in search for the LDAP server. For Active Directory, the value is sAMAccountName.
Timeout (1030 sec)	20	Define the timeout period of a LDAP request, in seconds.
Enable	Yes	Use this field to enable or disable the LDAP server being configured. You can configure the LDAP server as disabled, but return later to enable it.
Preferred Connection Type	ldap-s	Select the connection type for the LDAP server from the drop-down menu. LDAP servers support the following connection types: <ul style="list-style-type: none"> <li>clear-text - No encryption is used.</li> </ul>



Field	Default	Description
		<ul style="list-style-type: none"> <li>• ldap-s - Uses SSL encryption.</li> <li>• start-tls - Uses TLS encryption.</li> </ul>
Maximum Number of Non-admin Connections	4	The number of non-administrative connections that should not be exceeded.

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

## Security > Server Groups > RADIUS

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

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

**Table 17:** *Security > Server Groups > RADIUS*

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server.
<b>Other Settings</b>		
Host IP Address		Set the IP address of the authentication server.
Key (Confirm Key)		Set the shared secret between the controller and the authentication server. The maximum length is 48 bytes.
Auth Port	1812	Set the authentication port on the server.
Acct Port	1813	Set the accounting port on the server.
Retransmits (0-3)	3	Set the Maximum number of retries sent to the server by the controller before the server is marked as down.
Timeout	(1-30 sec)	Set the maximum time, in seconds, that the controller waits before timing out the request and resending it.
NAS ID		Set the Network Access Server (NAS) identifier to use in RADIUS packets.
NAS IP		Set the NAS IP address to send in RADIUS packets. You can configure a global NAS IP address that the controller uses for communications with all RADIUS servers. If you do not configure a server-specific NAS IP, the global NAS IP is used.

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

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

## Security > Server Groups > TACACS

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

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

**Table 18:** *Security > Server Groups > TACACS*

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name	Blank	Enter the name of the server.
<b>Other Settings</b>		
Host IP Address	0.0.0.0	
Key (Confirm Key)		Set the shared secret to authenticate communication between the TACACS+ client and server.
TCP Port	49	Set the TCP port to be used by the server.
Retransmits (0-3)	3	Set the maximum number of times a request is retried.
Tmeout (1-30 sec)	20	Set the timeout period for TACACS+ requests, in seconds.
Enable	Yes	Enable or disable the TACACS server.
Session Authorization	No	Enables or disables session authoriaztion. Session authorization turns on the optional authorization session for admin users.

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

## Security > Server Groups > Internal

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

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

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays all folders available for association with the server group.
Name		Enter the name of the server.
<b>Other Settings</b>		
Maximum Expiration (mins)		Set the maximum expiration time (in minutes) for guest accounts. If the guest-provisioning user attempt to add a guest account that expires beyond this time period, an error message is displayed and the guest account is created with the maximum time you configured.
<b>Internal Server Users</b>		
Add New Internal Server User		This section displays internal server users currently configured for use on the Internal Server. Select this button to add a new user. The <b>Internal Server User</b> section appears with the following settings.
<b>Internal Server User</b>		
User Name		Enter the name of a user, or click <b>Generate</b> to create an anonymous ID for this user.
Password		Enter the password in plain text, or click <b>Generate</b> to create a random password for this user.
User Role	guest	From the drop-down menu, select the user role to associate with this user. The role establishes read/write privileges, manage/monitor privileges, and other settings.
E-Mail		Enter the email address of the guest user.
Enabled	Yes	Specify whether this guest user is enabled or disabled on the internal server.
Expire User	No	Specify whether to expire the guest user after a period of time. If you click <b>Yes</b> , a new field appears with instructions about the date and time in which the guest user is expired from the internal server.

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

## Security > Server Groups > XML API

Dell PowerConnect 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.

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

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

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

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

## Security > Server Groups > RFC 3576

RFC 3576 servers support dynamic authorization extensions to Remote Authentication Dial-In User Service (RADIUS). Dell PowerConnect 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. The **Security > Server Groups > Add RFC 3576 Server** page contains the following fields, as described in [Table 21](#).

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the server is associated. The drop-down menu displays

Field	Default	Description
		all folders available for association with the server group.
Name	Blank	Enter the name of the server.
<b>Other Settings</b>		
Key (Confirm Key)	Blank	Set the shared secret to authenticate communication between the RFC 3576 client and server.

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

## Security > Server Groups > Windows

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

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

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

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

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

## Security > TACACS Accounting

TACACS+ accounting allows commands issued on the 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 PowerConnect W Configuration supports TACACS Accounting servers that can be referenced by server groups.

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

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

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

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

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

## Security > Time Ranges

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

The **Security > Time Ranges** page displays all time ranges that are currently available in Dell PowerConnect 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. The **Security > Time Range > Add/Edit New Time Range** page contains the following fields, as described in [Table 24](#):

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

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

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

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

## Security > User Rules

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

Navigate to the **Security > User Rules** page in the Dell PowerConnect 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 **Add New User Derivation Profile**. To edit an existing user rule, click the pencil icon next to an existing rule. [Table 25](#) describes the contents of this page.

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the rule set is associated. The drop-down menu displays all folders available for association with the rule set.
Name	Blank	Enter the name of the rule set.
<b>User Derivation Rules</b>		
Add New User Derivation Rule		Select this button to create a new rule. Additional fields appear that require configuration, as follows.
Set Type	role	Select whether the rule is based on role, VLAN, or AAA profile (Requires a Public Wi-Fi Access license).
Rule Type	bssid	<p>Select one of the following options from the drop-down menu. Your selection in this field changes an ensuing field that must be completed, as follows:</p> <ul style="list-style-type: none"> <li>• <b>bssid</b>—Selecting this option displays the <b>BSSID</b> field below. Specify the BSSID in text.</li> <li>• <b>dhcp-option-77</b>—Selecting this option displays the <b>DHCP Option 77</b> field below. Enter this information in text.</li> <li>• <b>dhcp-option</b> - Selecting this option displays a <b>DHCP Option</b> entry field below.</li> <li>• <b>encryption-type</b>—Selecting this option displays the <b>Encryption Type</b> field below, in which you must select the encryption type from the drop-down</li> </ul>

Field	Default	Description
		<p>menu. Select <b>open</b>, <b>static-wep</b>, or another other encryption type from the drop-down menu.</p> <ul style="list-style-type: none"> <li>• <b>ssid</b>—Selecting this option displays <b>ESSID</b> field below, in which you enter the ESSID in text.</li> <li>• <b>location</b>—Selecting this option displays the <b>Location</b> field below, in which you enter the location in text.</li> <li>• <b>macaddr</b>—Selecting this option displays the MAC Address field below, in which you must enter the MAC address.</li> </ul>
Operator		Select the matching operator.
User Role/VLAN	ap-role	<p>If you selected <b>role</b> for the <b>Set Type</b> field above, then select the specific user role from this drop-down menu.</p> <p>If you selected <b>VLAN</b> for the <b>Set Type</b> field above, then select the specific VLAN from this drop-down menu.</p>

## Local Config of SNMP Management

The Local Config component is used for local configuration Dell PowerConnect W-Series controllers. Locally configured settings are not pushed to local controllers by master controllers.

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



**CAUTION:** 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.

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

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

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

Field	Description
<b>General Settings</b>	
Folder	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Enter the name of the profile.
<b>SNMP Settings</b>	
Community Strings	Community strings used to authenticate requests for SNMP versions before version 3. <b>NOTE:</b> This is needed only if using SNMP v2c and is not needed if using version 3.
Enable Trap Generation	Enables generation of SNMP traps to configured SNMP trap receivers.
Engine ID	Sets the SNMP server engine ID as a hexadecimal number. 24 character maximum.
Inform Queue Length (100-350)	Specify the length for the SNMP inform queue. Default is 250.



Field	Description
Always use the controller's IP address as source address	Set whether to use the IP address of the controller as the trap source.
Trap Source IP Address	Enter the source IP address for sending traps.
<b>SNMP Trap Hosts</b>	
IP Address	Enter the IP address of the trap host.
SNMP Version	Configures the SNMP version as 1, 2c, or 3. <ul style="list-style-type: none"> <li>If 2c is selected, the Send Inform field appears at the bottom of this section.</li> <li>If 3 is selected, the <b>SNMP User</b> field will appear as a drop-down menu containing any configured v3 users. Select the plus icon to add them via the <b>SNMP Management &gt; SNMPv3 User</b> profile.</li> </ul>
Community String	Configure the security string for notification messages. Does not appear if <b>SNMP Version</b> is set to 3.
UDP Port (1-65535)	The port number to which trap notification messages are sent. Default is 162.
Send Informs	Whether to send SNMP inform messages to the configured host. Displays when <b>2c</b> is selected in <b>SNMP Version</b> .
<b>SNMPv3 Users</b> If you are using SNMPv3 to obtain values from the Dell PowerConnect W-Series controller, navigate to <b>Local Config &gt; SNMP Management &gt; SNMPv3 User</b> to configure the following parameters:	
User name	A string representing the name of the user.
Authentication protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: <ul style="list-style-type: none"> <li>MD5: HMAC-MD5-96 Digest Authentication Protocol</li> <li>SHA: HMAC-SHA-96 Digest Authentication Protocol</li> </ul>
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption Protocol).
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol.

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

## Advanced Services

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

## Advanced Services > IP Mobility

Navigate to **Advanced Services > IP Mobility** page from the **Dell PowerConnect 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. The **Advanced Services > IP Mobility Profile Details** page contains the following fields, as described in [Table 27](#):

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the profile is associated. The drop-down menu displays all folders available for association with the profile.
Name	Blank	Enter the name of the profile.
<b>Mobility Domains</b>		
Mobility Domains	None selected	This section displays all domains that are available for association with this IP mobility profile. You can show all, or show only selected domains. Select one or more mobility domains to associate with this IP Mobility profile.
<b>Foreign Agent</b>		
Registration Lifetime Requested by Proxy (10-65,534 sec)	180	Specify the client registration time on the foreign network. A foreign agent receives traffic that is intercepted by the home agent on the home network, and forwards to the client on the foreign network. This setting defines the registration time of a client on the foreign network.
Maximum Number of Active Visitors (0-5000)	5000	Set the maximum number of users to be supported by the foreign network.
Maximum Number of Requests Retransmits (0-5)	3	Set the maximum number of times that a retransmit is to be supported on the foreign network by proxy.
Retransmit Interval (100-10000 msec)	1000	Set the foreign agent retransmit time in milliseconds. The retransmit interval defines retransmission between the home agent and the foreign agent.
<b>Home Agent</b>		
Replay Protection Time Value (0-300 sec)	7	Define the time period over which message replay is to be detected. Message replay detects if a message that is intended for a client has been intercepted and replayed. This setting defines how long replay detection is to monitor for replay.
Maximum Number of Active Bindings (0-5000)	5000	Define the maximum number of bindings in which the home agent network is to support a client when the client is out of range of the network, or otherwise disconnected.
<b>Proxy Mobile IP</b>		

Field	Default	Description
Trigger Mobility on Station Association	Yes	<p>Enable this setting to trigger client mobility processing on the network once a client has associated to the network in mobile fashion.</p> <p>The proxy mobile IP module in a mobility-enabled controller detects when a mobile client has moved to a foreign network and determines the home agent for a roaming client. The proxy mobile IP module performs the following functions:</p> <ul style="list-style-type: none"> <li>Derives the address of the home agent for a mobile client from the HAT using the mobile client's IP address. If there is more than one possible home agent for a mobile client in the HAT, the proxy mobile IP module uses a discovery mechanism to find the current home agent for the client.</li> <li>Detects when a mobile client has moved. Client moves are detected based on ingress port and VLAN changes and mobility is triggered accordingly. For faster roaming convergence between AP(s) on the same controller, it is recommended that you keep the <b>on station association</b> option enabled. This helps trigger mobility as soon as 802.11 association packets are received from the mobile client.</li> </ul>
Enable Support for Standalone APs	No	Select this option to support standalone APs on the IP Mobility domain.
Log User Moves	Yes	Enable this option to log client movement in the IP Mobility domain. This setting is derived from station association in a foreign network.
Allow Roaming for Authenticated Stations Only	Yes	Enable this setting to require authentication for roaming stations.
Filter out DHCP Release from Stations	No	Enable or disable the filtering of DHCP information when a client is released from a station.
Re-home Idle Voice Capable Client	No	Enable or disable re-homing for idle voice-capable clients. This setting reassigns the home network in relation to a voice-capable client that is idle (non-roaming).
Maximum Number of Station Mobility Events Per Second (1-65535)	10	Set the maximum number of events, per second, that station mobility events can be supported.
Maximum Interval Mobility Will Hold Inactive Host Trail (120-3600 sec)	600	Define how long inactive host trails are to be supported in IP mobility.
Maximum Entries in User Mobility Trail (1-30)	10	Define how many events are to be logged in IP mobility.
Mobility Host Entry Hold Time After Connectivity Loss (30-3600 sec)	60	Define how long IP mobility is to support hosts should there be a disconnection.
Mobility Host Entry Lifetime When Mobility Cannot Be Provided (30-60000 sec)	120	Define how long host entries in the IP mobility domain are to be maintained when they are without mobility.
<b>Proxy DHCP</b>		
Maximum Number of BOOTP Packets Per Transaction (0-65534)	25	Define the maximum number of BOOTP packets that can be supported for a given transaction in proxy DHCP. All BOOTP packets are at least 300 bytes

Field	Default	Description
		in size, by specification. BOOTP packets are used when a host configures itself dynamically at boot time.
Maximum Time Allowed for a DHCP Transaction to Complete (10-600 sec)	60	Set the maximum allowable time for proxy DHCP transactions to complete.
Proxy DHCP Session Hold Time after Completion (dangerous) (1-600 sec)	5	Specify the length of time a proxy DHCP session is to be supported after DHCP processes are complete. Longer times are not considered advisable.
Terminate Proxy DHCP on Aggressive Transaction ID Change (dangerous)	No	If proxy DHCP is subject aggressive transaction ID change, this setting terminates upon detection.
Performs Proxy-DHCP for BOOTP Packets Without DHCP-options (dangerous)	No	Use this setting to support Proxy DHCP for BOOTP packets, but without DHCP options.
<b>Revocation</b>		
Retransmit Interval (100-10000 msec)	1000	Set the interval in milliseconds in which to retransmit in revocation. A home agent or foreign agent can send a registration revocation message, which revokes registration service for the mobile client. For example, when a mobile client roams from one foreign agent to another, the home agent can send a registration revocation message to the first foreign agent so that the foreign agent can free any resources held for the client.
Maximum Number of Request Retransmits (0-5)	3	Use this setting to define how many retransmits are supported before revocation is enacted.

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

## Advanced Services > IP Mobility > Mobility Domain

You configure mobility domains on master 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 PowerConnect 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. The **Advanced Services > IP Mobility > Add/Edit IP Mobility Domain** page contains the following fields, as described in [Table 28](#):

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the domain is associated. The drop-down menu displays all folders available for association with the domain.
Name	Blank	Enter the name of the domain.
<b>Other Settings</b>		
Active	No	Define whether the IP Mobility Domain is active or inactive.
Description		Add a description for the domain (requires AOS 6.0.0.0 or later)
<b>Mobile IP Home Agents</b>		
Add		<p>Use this button to create new home agents. Once you click <b>Add</b>, the following additional fields appear in the Mobile IP Home Agent section. Complete these settings.</p> <ul style="list-style-type: none"> <li>• <b>Subnet</b>—Define the subnet mask for the IP Mobility Domain.</li> <li>• <b>Netmask</b>—Define the net mas for the IP Mobility Domain.</li> <li>• <b>VLAN ID (1-4094)</b>—Set the VLAN to be supported on the IP Mobility Domain.</li> <li>• <b>Home Agent</b>—Set the home agent for the IP Mobility Domain. When you enable IP mobility in a mobility domain, the proxy mobile IP module determines the home agent for a roaming client.</li> </ul> <p>Select <b>Add</b> to create the home agent.</p>

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.

## 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 PowerConnect 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.

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

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the VPN service profile is associated. The drop-down menu displays all folders available for association with the VPN services profile.
Name	Blank	Enter the name of the VPN services profile.
<b>Other Settings</b>		
IKE Profile		Select an IKE profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing IKE profile. Refer to " <a href="#">Advanced Services &gt; VPN Services &gt; IKE</a> " on page 73
PPTP Profile		Select a PPTK profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing PPTP profile. Refer to " <a href="#">Advanced Services &gt; VPN Services &gt; L2TP</a> " on page 75.
L2TP Profile		Select an L2TP profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing L2TP profile. Refer to " <a href="#">Advanced Services &gt; VPN Services &gt; L2TP</a> " on page 75.
IPSEC Profile		Select an IPSEC profile from the drop-down menu. Select the add icon to add a new profile of this type, or click the pencil icon to edit an existing IPSEC profile. Refer to " <a href="#">Advanced Services &gt; VPN Services &gt; IPSEC</a> " on page 77.

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

## Advanced Services > VPN Services > IKE

Navigate to the **Advanced Services > VPN Services > IKE** page from the **Dell PowerConnect 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.



NOTE: 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. [Table 30](#) describes the fields on the **Advanced Services > VPN Services > IKE Add/Edit Detail** page.

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the IKE profile is associated. The drop-down menu displays all folders available for association with the IKE services profile.
Name	Blank	Enter the name of the IKE profile.
<b>Other Settings</b>		
IKE Aggressive Group Name		Enter the authentication group name for aggressive mode. Make sure that the group name matches the group name configured in the VPN client software. Aggressive Mode condenses the IKE SA negotiations into three packets (versus six packets for Main Mode). A group associates the same set of attributes to multiple clients.
Enable IKE RAP PSKL Refresh/Caching	No	Use this setting to enable refresh and caching for IKE on remote APs.
<b>IKE Shared Secrets</b>		
Add		Select this button to add an IKE shared secret. The following settings appear. Complete these settings and click <b>Add</b> in this section. <ul style="list-style-type: none"> <li><b>Subnet</b>—Enter the subnet for the shared secret.</li> <li><b>Subnet Mask</b>—Enter the subnet mask for the shared secret.</li> <li><b>IKE Shared Secret</b>—Type the shared secret, and confirm.</li> </ul>

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

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

Navigate to the **Advanced Services > VPN Services > IKE > IKE Policy** page from the **Dell PowerConnect W Configuration** navigation pane to add a new IKE policy, as follows:

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the IKE policy profile is associated. The drop-down menu displays all folders available for association with the IKE Policy profile.
Priority	Blank	Enter the priority number of this IKE policy.
<b>Other Settings</b>		
Encryption		From the drop-down menu, select the encryption type to be supported in the IKE policy. <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES</li> <li>• AES128</li> <li>• AES192</li> <li>• AES256</li> </ul>
Hash Algorithm		Select the hash algorithm for this IKE policy. <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA</li> <li>• SHA1-96</li> <li>• SHA2-256-128</li> <li>• SHA2-384-192</li> </ul> <b>NOTE:</b> 'SHA2-256-128' and 'SHA2-384-192' require an Advanced Cryptography license and a minimum version of 6.1.0.0.
Authentication		Dell PowerConnect W-Series ArubaOS VPNs support client authentication using pre-shared keys, RSA digital certificates, or Elliptic Curve Digital Signature Algorithm (ECDSA) certificates. To set the authentication type for the IKE rule, click the <b>Authentication</b> drop-down list and select one of the following types: <ul style="list-style-type: none"> <li>• Pre-Share (for IKEv1 clients using pre-shared keys)</li> <li>• RSA (for clients using certificates)</li> <li>• ECDSA-256 (for clients using certificates)</li> <li>• ECDSA-384 (for clients using certificates)</li> </ul> <b>NOTE:</b> 'ECDSA-256' and 'ECDSA-384' require an Advanced Cryptography license and a minimum version of 6.1.0.0.
Diffie-Hellman Group		Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie Hellman Group for the ISAKMP policy, click the <b>Diffie Hellman Group</b> drop-down list and select one of the following groups: <ul style="list-style-type: none"> <li>• Group 1: 768-bit Diffie Hellman prime modulus group.</li> <li>• Group 2: 1024-bit Diffie Hellman prime modulus group.</li> <li>• Group 19: 256-bit random Diffie Hellman ECP modulus group.</li> <li>• Group 20: 384-bit random Diffie Hellman ECP modulus group.</li> </ul> <b>NOTE:</b> 'EC 256-bit (19)' and 'EC 384-bit (20)' require an Advanced Cryptography license and a minimum version of 6.1.0.0.
Lifetime	empty	Set the Security Association Lifetime to define the lifetime of the security association, in seconds.
Version	1	Select 1 to configure the VPN for IKEv1, or 2 for IKEv2.



## Advanced Services > VPN Services > L2TP

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

L2TP/IPSec requires two levels of authentication:

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

Navigate to the **Advanced Services > VPN Services > L2TP** page from the **Dell PowerConnect 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. The **Advanced Services > VPN Services > L2TP Add/Edit Details** page contains the following fields, as described in [Table 32](#).

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

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

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

## Advanced Services > VPN Services > PPTP

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

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

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

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

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

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

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

## Advanced Services > VPN Services > IPSEC

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

L2TP/IPSec requires two levels of authentication:

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

Navigate to the **Advanced Services > VPN Services > IPSEC** page from the **Dell PowerConnect 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. The **Add/Edit Details** page contains the following fields, as described in [Table 34](#):

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the IPSEC profile is associated. The drop-down menu displays all folders available for association with the IPSEC profile.
Name	Blank	Enter the name of the IPSEC profile.
<b>Other Settings</b>		
Maximum MTU Size (1034-1500 bytes)	1500	Define the Maximum transmission unit (MTU) size in bytes.
<b>Dynamic Maps</b>		
Dynamic Maps		Select one or more dynamic maps that the IPSEC profile is to reference. You can add or edit dynamic maps as required. Refer to " <a href="#">Advanced Services &gt; VPN Services &gt; IPSEC &gt; Dynamic Map</a> " on page 77.

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

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

VPN Services may reference IPSEC profiles. IPSEC profiles reference Dynamic Maps, and Dynamic Maps reference Transform Sets. This interrelationship is conveyed in the navigation pane of **Device Setup > Dell PowerConnect 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. The **Add/Edit Details** page contains the fields as described in [Table 35](#):

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the Dynamic Map is associated. The drop-down menu displays all folders available for association with the Dynamic Map.
Name	Blank	Enter the name of the Dynamic Map.
<b>Other Settings</b>		
Priority		Specify the priority in which this Dynamic Map should be processed in relation to additional Dynamic Maps that may be configured and used by IPSEC profiles.
Diffie-Hellman Group		<p>Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie Hellman Group for the ISAKMP policy, click the <b>Diffie Hellman Group</b> drop-down list and select one of the following groups:</p> <ul style="list-style-type: none"> <li>Group 1: 768-bit Diffie Hellman prime modulus group.</li> <li>Group 2: 1024-bit Diffie Hellman prime modulus group.</li> <li>Group 19: 256-bit random Diffie Hellman ECP modulus group.</li> <li>Group 20: 384-bit random Diffie Hellman ECP modulus group.</li> </ul> <p><b>NOTE:</b> 'EC 256-bit (19)' and 'EC 384-bit (20)' require an Advanced Cryptography license and a minimum version of 6.1.0.0.</p>
Lifetime (300-86400 sec)		Define the lifetime in seconds for the dynamic map, when deployed in IPSEC profiles.
Transform Set 1-4		From the drop-down menu, select up to four transform sets in the sequence in which they should be referenced by the Dynamic Map. You can add a new Transform Set by clicking the add icon, or you can edit an existing Transform Set by clicking the pencil icon. Refer to " <a href="#">Advanced Services &gt; VPN Services &gt; IPSEC &gt; Dynamic Map &gt; Transform Set</a> " on page 78.
Version	1	Select 1 to configure the VPN for IKEv1, or 2 for IKEv2.

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

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

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

Navigate to **Advanced Services > VPN Services > IPSEC > Dynamic Map > Transform Set** from the **Dell PowerConnect 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. The **Add/Edit Details** page contains the following fields, as described in [Table 36](#):

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

Field	Default	Description
<b>General Settings</b>		
Folder	Top	Set the folder with which the Transform Set is associated. The drop-down menu displays all folders available for association with the Transform Set.
Name	Blank	Enter the name of the Transform Set.
<b>Other Settings</b>		
Encryption	168-bit 3DES-CBC	Select the encryption for the transform set from the drop-down menu.
Hash Algorithm	SHA (HMAC Variant)	Select the hash algorithm from the drop-down menu.

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

## Groups > Dell PowerConnect W Config Page

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

1. Navigate to the **Groups > List** page.
2. Select the name of the Dell PowerConnect W AP Group to view and edit, and navigate to the **Dell PowerConnect W Config** page, illustrated in [Figure 27](#):

**Figure 27: Groups > List > Dell PowerConnect W Config Page Illustration**

The screenshot displays the configuration page for Dell PowerConnect W, divided into several sections:

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

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

- Complete the profile assignments on this page, referring to additional topics in this appendix for additional information. [Table 37](#) provides a summary of topics supporting these settings.

**Table 37: Information Resources for the Groups > List > Dell PowerConnect W Config Page**

Section	Additional Information Available In These Locations
Dell PowerConnect W AP Groups Section	<ul style="list-style-type: none"> <li>"Dell PowerConnect W AP Groups" on page 30</li> <li>"Dell PowerConnect W AP Groups Procedures and Guidelines" on page 19</li> <li>"Setting Up Initial Dell PowerConnect W Configuration" on page 13</li> </ul>
AP Overrides	<ul style="list-style-type: none"> <li>"AP Overrides" on page 34</li> <li>"Supporting APs with Dell PowerConnect W Configuration" on page 22</li> </ul>
Dell PowerConnect W User Roles	<ul style="list-style-type: none"> <li>"Security &gt; User Roles" on page 46</li> <li>"Visibility in Dell PowerConnect W Configuration" on page 25</li> </ul>
Dell PowerConnect W Policies	<ul style="list-style-type: none"> <li>"Security &gt; Policies" on page 51</li> <li>"Visibility in Dell PowerConnect W Configuration" on page 25</li> </ul>