


**Dell PowerConnect W-Series  
Instant Access Point  
6.2.0.0-3.2.0.0  
User Guide**



## Copyright

© 2013 Aruba Networks, Inc. Aruba Networks trademarks include  Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

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

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

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. 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

---

Contents .....	3
About This Guide .....	15
<b>Dell PowerConnect W-Instant Access Point Overview</b> .....	15
Supported Devices .....	15
Objective .....	15
Intended Audience .....	16
Conventions .....	16
Contacting Support .....	16
Initial Configuration .....	17
Initial Setup .....	17
Pre-Installation Checklist .....	17
Connecting a W-IAP .....	18
Assigning an IP Address to the W-IAP .....	18
Connecting to a Provisioning Wi-Fi Network .....	18
Disabling the Provisioning Wi-Fi Network .....	20
Assigning a Static IP .....	20
Log in to the Dell W-Series Instant UI .....	21
Specifying a Country Code .....	21
W-IAP Cluster .....	22
Dell W-Instant User Interface .....	23
Understanding the Dell W-Series Instant UI Layout .....	23
Banner .....	24
Search .....	24
Tabs .....	24
Networks Tab .....	24
Access Points Tab .....	25
Clients Tab .....	25
Links .....	26
New Version Available .....	27

---

<b>Settings</b> .....	27
<b>RF</b> .....	29
<b>PEF</b> .....	30
<b>WIP</b> .....	30
<b>VPN</b> .....	31
<b>Wired</b> .....	31
<b>Maintenance</b> .....	32
<b>Support</b> .....	32
<b>Help</b> .....	32
<b>Logout</b> .....	33
<b>Monitoring</b> .....	33
<b>Info</b> .....	33
<b>RF Dashboard</b> .....	34
<b>Usage Trends</b> .....	35
<b>Spectrum</b> .....	36
<b>Overview (Device list)</b> .....	36
<b>Channel Utilization and Monitoring</b> .....	36
<b>Channel Details</b> .....	37
<b>Alerts</b> .....	37
<b>Client Alerts</b> .....	37
<b>Fault History</b> .....	38
<b>Active Faults</b> .....	38
<b>IDS</b> .....	39
<b>Configuration</b> .....	39
<b>AirGroup</b> .....	40
<b>Language</b> .....	40
<b>Dell PowerConnect W-AirWave Setup</b> .....	40
<b>Pause/Resume</b> .....	41
<b>Views</b> .....	41
<b>Wireless Network</b> .....	43
<b>Network Types</b> .....	43
<b>Employee Network</b> .....	44

---

<b>Adding an Employee Network</b> .....	44
<b>Voice Network</b> .....	53
<b>Adding a Voice Network</b> .....	53
<b>Guest Network</b> .....	60
<b>Adding a Guest Network</b> .....	60
<b>Editing a Network</b> .....	68
<b>Deleting a Network</b> .....	68
<b>Number of WLAN SSIDs Supported</b> .....	68
<b>Enabling the Extended SSID Option</b> .....	69
<b>VLAN Pooling</b> .....	69
<b>Managing W-IAPs</b> .....	71
<b>Preferred Band</b> .....	71
<b>Auto Join Mode</b> .....	71
<b>Disabling Auto Join Mode</b> .....	71
<b>Terminal Access</b> .....	72
<b>LED Display</b> .....	72
<b>TFTP Dump Server</b> .....	72
<b>Extended SSID</b> .....	73
<b>Deny Inter User Bridging and Deny Local Routing</b> .....	73
<b>Syslog Server</b> .....	73
<b>Syslog Facility Levels</b> .....	74
<b>Adding a W-IAP to the Network</b> .....	74
<b>Removing a W-IAP from the Network</b> .....	75
<b>Editing W-IAP Settings</b> .....	75
<b>Changing W-IAP Name</b> .....	75
<b>Changing IP Address of the W-IAP</b> .....	76
<b>Configuring Adaptive Radio Management</b> .....	78
<b>Configuring Uplink Management VLAN</b> .....	79
<b>Configuring Wired Bridging on Ethernet 0</b> .....	79
<b>Migrating to a Dell PowerConnect W-Series Mobility Controller Managed Network</b> .....	80
<b>Converting a W-IAP to RAP Mode</b> .....	80
<b>Converting a W-IAP to CAP</b> .....	83

---

<b>Converting a W-IAP to Standalone Mode</b> .....	83
<b>Converting Back to a W-IAP</b> .....	84
<b>Rebooting the W-IAP</b> .....	84
<b>Firmware Image Server in Cloud Network</b> .....	86
<b>Upgrade Using Dell PowerConnect W-AirWave and Image Server</b> .....	86
<b>Image Management Using Cloud Server</b> .....	86
<b>Image Management Using Dell PowerConnect W-AirWave</b> .....	86
<b>Automatic Firmware Image Check and Upgrade</b> .....	87
<b>Upgrading to New Version</b> .....	88
<b>Manual</b> .....	88
<b>Automatic</b> .....	90
<b>Layer-3 Mobility</b> .....	91
<b>Overview</b> .....	91
<b>Configuring a Mobility Domain</b> .....	92
<b>Home Agent Load Balancing</b> .....	95
<b>Spectrum Monitor</b> .....	97
<b>Creating Spectrum Monitors and Hybrid APs</b> .....	97
<b>Converting W-IAPs into Hybrid W-IAPs</b> .....	97
<b>Converting a W-IAP to a Spectrum Monitor</b> .....	98
<b>Spectrum Data</b> .....	100
<b>Overview - Device List</b> .....	100
<b>Non Wi-Fi Interferers</b> .....	101
<b>Channel Metrics</b> .....	103
<b>Channel Details</b> .....	104
<b>Spectrum Alerts</b> .....	105
<b>Time Management</b> .....	107
<b>NTP Server</b> .....	107
<b>Configuring an NTP Server</b> .....	107
<b>Daylight Saving Time</b> .....	108
<b>Enabling Daylight Saving Time</b> .....	108
<b>Virtual Controller</b> .....	109
<b>Master Election Protocol</b> .....	109

Preference to an IAP with 3G/4G Card .....	109
Preference to a W-IAP with Non-Default IP .....	109
Virtual Controller IP Address .....	110
Specifying Name and IP Address for the Virtual Controller .....	110
Configuring the DHCP Server .....	110
Authentication .....	111
Authentication Methods in Dell W-Instant .....	111
802.1X Authentication .....	111
Internal RADIUS Server .....	112
External RADIUS Server .....	112
Authentication Terminated on W-IAP .....	112
Configuring an External RADIUS Server .....	113
Enabling RADIUS Server Support .....	115
Authentication Survivability .....	115
RADIUS Server Authentication with VSA .....	118
List of Supported VSA .....	118
Management Authentication Settings .....	120
Captive Portal .....	121
Internal Captive Portal .....	121
Configuring Internal Captive Portal Authentication when Adding a Guest Network .....	122
Configuring Internal Captive Portal Authentication when Editing a Guest Network .....	123
Configuring Internal Captive Portal with External RADIUS Server Authentication when Adding a Guest Network .....	124
Customizing a Splash Page .....	125
Disabling Captive Portal Authentication .....	126
External Captive Portal .....	127
Configuring External Captive Portal Authentication when Adding a Guest Network .....	127
Configuring External Captive Portal Authentication when Editing a Guest Network .....	129
External Captive Portal Authentication using ClearPass Guest .....	131
Creating a Web Login page in the ClearPass Guest .....	131
Configuring the RADIUS Server in Instant .....	131
WISPr Authentication .....	132
Configuring WISPr Authentication .....	132

MAC Authentication .....	133
Configuring MAC Authentication .....	134
Walled Garden Access .....	134
Creating a Walled Garden Access .....	134
MAC + 802.1X Authentication .....	136
Configuring MAC + 802.1X Authentication .....	136
MAC + Captive Portal Authentication .....	137
Configuring MAC + Captive Portal Authentication .....	137
Wired Authentication on a W-IAP .....	138
Certificates .....	138
Loading Certificates using Dell W-Series Instant UI .....	139
Loading Certificates using Dell PowerConnect W-AirWave .....	140
Encryption .....	143
Encryption Types Supported in Dell W-Instant .....	143
WEP .....	143
TKIP .....	143
AES .....	143
Encryption Recommendations .....	143
Understanding WPA and WPA2 .....	144
Recommended Authentication and Encryption Combinations .....	144
Role Derivation .....	145
User Roles .....	145
Creating a New User Role .....	145
Creating Role Assignment Rules .....	147
MAC-Address Attribute .....	147
DHCP Option and DHCP Fingerprinting .....	148
802.1X-Authentication-Type .....	148
User VLAN Derivation .....	149
User VLAN Derivation .....	149
Vendor Specific Attributes (VSA) .....	149
VLAN Derivation Rule .....	150
Configuring VLAN Derivation Rules on a W-IAP .....	150



---

<b>User Role</b> .....	151
<b>Configuring a User Role</b> .....	151
<b>SSID Profile</b> .....	152
<b>Configuring VLAN Derivation Rules Using an SSID Profile</b> .....	153
<b>Instant Firewall</b> .....	155
<b>Service Options</b> .....	156
<b>Destination Options</b> .....	158
<b>Examples for Access Rules</b> .....	158
<b>Allow TCP Service to a Particular Network</b> .....	158
<b>Allow POP3 Service to a Particular Server</b> .....	159
<b>Deny FTP Service except to a Particular Server</b> .....	160
<b>Deny bootp Service except to a Particular Network</b> .....	161
<b>Content Filtering</b> .....	163
<b>Enabling Content Filtering</b> .....	163
<b>Enterprise Domains</b> .....	164
<b>OS Fingerprinting</b> .....	167
<b>Adaptive Radio Management</b> .....	169
<b>ARM Features</b> .....	169
<b>Channel or Power Assignment</b> .....	169
<b>Voice Aware Scanning</b> .....	169
<b>Load Aware Scanning</b> .....	169
<b>Band Steering Mode</b> .....	169
<b>Airtime Fairness Mode</b> .....	170
<b>Airtime Fairness Modes</b> .....	170
<b>Access Point Control</b> .....	171
<b>Customize Valid Channels</b> .....	171
<b>Min Transmit Power</b> .....	171
<b>Max Transmit Power</b> .....	171
<b>Client Aware</b> .....	171
<b>Scanning</b> .....	171
<b>Wide Channel Bands</b> .....	171
<b>Monitoring the Network with ARM</b> .....	172

---

ARM Metrics .....	172
<b>Configuring Administrator Assigned Radio Settings for W-IAP</b> .....	172
Configuring Radio Profiles in Instant .....	173
Intrusion Detection System .....	177
Rogue AP Detection and Classification .....	177
Wireless Intrusion Protection (WIP) .....	177
Containment Methods .....	181
SNMP .....	183
SNMP Parameters for W-IAP .....	183
SNMP Traps .....	185
Ethernet Downlink .....	187
Ethernet Downlink Overview .....	187
Ethernet Downlink Profile Parameters .....	187
Assigning a Profile to the Ethernet Port .....	190
Hierarchical Deployment .....	193
Deployment .....	193
Uplink Configuration .....	195
Uplink Interface Configuration .....	195
Ethernet Uplink .....	195
3G/4G Uplink .....	196
Types of Modems .....	196
Provisioning 3G/4G Uplink Manually .....	198
Provisioning 3G Uplink Automatically .....	199
Provisioning a 3G/4G Switch Network .....	199
Wi-Fi Uplink .....	200
Provisioning Wi-Fi Uplink .....	200
Provisioning 3G/4G and Wi-Fi Uplink with Factory Setting .....	200
Uplink Management .....	201
Enforce Uplink .....	201
Uplink Preemption .....	201
Uplink Switchover .....	201
Uplink Switching Based on VPN Status .....	201

Uplink Switching Based on Internet Connectivity Status .....	202
PPPoE .....	202
Configuring PPPoE .....	202
<b>Dell PowerConnect W-AirWave Integration and Management .....</b>	<b>205</b>
<b>Dell PowerConnect W-AirWave Features .....</b>	<b>205</b>
Image Management .....	205
W-IAP and Client Monitoring .....	205
Template-based Configuration .....	205
Trending Reports .....	206
Intrusion Detection System .....	206
Wireless Intrusion Detection System (WIDS) Event Reporting to Dell PowerConnect W-AirWave .....	206
RF Visualization Support for Dell W-Instant .....	207
<b>Configuring Dell PowerConnect W-AirWave .....</b>	<b>207</b>
Creating your Organization String .....	207
About Shared Key .....	208
Entering the Organization String and AMP Information into the W-IAP .....	208
Dell PowerConnect W-AirWave Discovery through DHCP Option .....	208
Standard DHCP option 60 and 43 on Windows Server 2008 .....	208
Alternate Method for Defining Vendor-Specific DHCP Options .....	212
<b>AirGroup .....</b>	<b>215</b>
Introducing AirGroup .....	215
What is Bonjour and Zero Configuration Networking? .....	215
WLANs and Bonjour .....	216
AirGroup Solution .....	216
AirGroup Features .....	217
Dell PowerConnect W-ClearPass Policy Manager and ClearPass Guest Features .....	217
AirGroup Architecture .....	217
How Does AirGroup Work? .....	218
Use Case: Higher Education Wireless LAN .....	219
The AirGroup Solution Components .....	219
Configuring AirGroup on W-Instant .....	220
Using the Dell W-Series Instant UI .....	220

<b>Enabling or Disabling AirGroup</b> .....	220
<b>Disallow Role</b> .....	221
<b>Disallow VLAN</b> .....	222
<b>Configuring AirGroup-CPPM Interface in W-Instant</b> .....	223
<b>Creating a RADIUS Server</b> .....	223
<b>Assign a Server to AirGroup</b> .....	224
<b>Configure CPPM to Enforce Registration</b> .....	225
<b>Change of Authorization (CoA)</b> .....	225
<b>AirGroup Monitoring</b> .....	226
<b>Troubleshooting and Log Messages</b> .....	226
<b>Monitoring</b> .....	229
<b>Virtual Controller View</b> .....	229
<b>Monitoring Link</b> .....	230
<b>Info</b> .....	230
<b>RF Dashboard</b> .....	230
<b>Usage Trends</b> .....	230
<b>Client Alerts Link</b> .....	232
<b>IDS Link</b> .....	232
<b>Network View</b> .....	232
<b>Info</b> .....	233
<b>Usage Trends</b> .....	233
<b>Dell W-Instant Access Point View</b> .....	235
<b>Info</b> .....	235
<b>RF Dashboard</b> .....	235
<b>Overview</b> .....	236
<b>Client View</b> .....	243
<b>Info</b> .....	244
<b>RF Dashboard</b> .....	244
<b>RF Trends</b> .....	244
<b>Mobility Trail</b> .....	247
<b>Alert Types and Management</b> .....	249
<b>Alert Types</b> .....	249

<b>Policy Enforcement Firewall</b> .....	251
<b>Authentication Servers</b> .....	251
<b>Users for Internal Server</b> .....	251
<b>Roles</b> .....	252
<b>Extended Voice and Video Functionalities</b> .....	253
<b>QoS for Microsoft Office OCS and Apple Facetime</b> .....	253
<b>Microsoft OCS</b> .....	254
<b>Apple Facetime</b> .....	254
<b>Client Blacklisting</b> .....	255
<b>Types of Client Blacklisting</b> .....	256
<b>Manual Blacklisting</b> .....	256
<b>Adding a Client to the Manual Blacklist</b> .....	256
<b>Dynamic Blacklisting</b> .....	257
<b>Authentication Failure Blacklisting</b> .....	257
<b>Session Firewall Based Blacklisting</b> .....	257
<b>PEF Settings</b> .....	258
<b>Firewall ALG Configuration</b> .....	258
<b>Firewall-based Logging</b> .....	259
<b>VPN Configuration</b> .....	261
<b>VPN Configuration</b> .....	261
<b>Fast Failover</b> .....	262
<b>Routing Profile Configuration</b> .....	262
<b>DHCP Server Configuration</b> .....	263
<b>NAT DHCP Configuration</b> .....	264
<b>Distributed L2 DHCP Configuration</b> .....	265
<b>Distributed L3 DHCP Configuration</b> .....	266
<b>Centralized L2 DHCP Configuration</b> .....	267
<b>User Database</b> .....	269
<b>Adding a User</b> .....	269
<b>Editing User Settings</b> .....	270
<b>Deleting a User</b> .....	270
<b>Regulatory Domain</b> .....	271

---

Country Codes List .....	271
Controller Configuration for VPN .....	277
Whitelist DB Configuration .....	277
VPN Local Pool Configuration .....	277
W-IAP VPN Profile Configuration .....	278
Dell PowerConnect W-ClearPass Configuration for AirGroup .....	279
Dell PowerConnect W-ClearPass Setup .....	279
Testing .....	283
Troubleshooting .....	283
IAP-VPN .....	285
Licensing Requirements .....	285
VPN Configuration .....	286
Creating a W-IAP Whitelist .....	286
Controller Whitelist DB .....	286
External Whitelist DB .....	286
VPN Local Pool Configuration .....	287
VPN Profile Configuration .....	287
Radius Proxy for VPN Connected IAPs .....	287
Viewing Branch Status .....	288
Example .....	288
Troubleshooting .....	289
Viewing Logs .....	289
Support Commands .....	289
Abbreviations .....	295
Abbreviations .....	295

# Chapter 1

## About This Guide

---

### Dell PowerConnect W-Instant Access Point Overview

Thank you for choosing Dell PowerConnect W-Instant Access Point 6.2.0.0-3.2.0.0. Dell PowerConnect W-Instant Access Point virtualizes Dell PowerConnect W-Series MobilityController capabilities on 802.11n access points (APs), creating a feature-rich enterprise-grade wireless LAN (WLAN) that combines affordability and configuration simplicity.

Dell W-Instant is a simple, easy to deploy turn-key WLAN solution consisting of one or more access points. An Ethernet port with routable connectivity to the Internet or a self-enclosed network, is used to deploy an Instant Wireless Network. An Instant Access Point (W-IAP) can be installed at a single site or deployed across multiple geographically-dispersed locations. Designed specifically for easy deployment, and proactive management of networks, Instant is ideal for small customers or remote locations without any on-site IT administrator.

Dell W-Instant consists of an Instant Access Point (W-IAP) and a Virtual Controller (VC). The Virtual Controller resides within one of the access points. In an Dell W-Instant deployment, only the first W-IAP needs to be configured. After the first W-IAP is deployed, the subsequent W-IAPs inherit all the required information from the Virtual Controller.

### Supported Devices

The following is a list of Instant devices supported by Dell:

- W-IAP92
- W-IAP93
- W-IAP104
- W-IAP105
- W-IAP134
- W-IAP135
- W-IAP175P/175AC
- W-IAP3WN/3WNP
- W-IAP108
- W-IAP109



---

NOTE: All APs support an unlimited number of W-IAPs, however W-IAP92 and W-IAP93 support up to 16 W-IAPs only.

---

### Objective

This user guide describes the various features supported by Dell W-Instant and provides detailed instructions for setting up and configuring an Dell W-Instant network.

## Intended Audience

This guide is intended for customers who configure and use Dell W-Instant.

## Conventions

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

**Table 1 - Conventions**

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and provide cross-references to other books.
Screen input and output	This style is used to illustrate: <ul style="list-style-type: none"><li>• Screen output</li><li>• On screen system prompt</li><li>• Filenames, software devices, and specific commands</li></ul>
<b>Bold</b>	This style is used to emphasize Instant UI elements. For example, name of a text box or the name of a drop-down list.

The following informational icons are used throughout this guide:



---

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

---



---

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

---



---

**WARNING:** Indicates a risk of personal injury or death.

---

## Contacting Support

Web Site Support	
Main Website	<a href="http://dell.com">dell.com</a>
Support Website	<a href="http://dell.com/support">dell.com/support</a>
Documentation Website	<a href="http://dell.com/support/manuals">dell.com/support/manuals</a>



# Chapter 2

## Initial Configuration

This section provides information required to setup Dell W-Instant and access the Dell W-Series Instant User Interface.

### Initial Setup

This section provides a pre-installation checklist and describes the initial procedures required to set up Dell W-Instant.

#### Pre-Installation Checklist

Before installing the Instant Access Point (W-IAP), make sure that you have the following:

- Ethernet cable of required length to connect the W-IAP to the home router.
- One of the following power sources:
  - IEEE 802.3af/at-compliant Power over Ethernet (PoE) source. The PoE source can be any power source equipment (PSE) switch or a midspan PSE device.
  - Dell power adapter kit (this kit is sold separately).

---

**NOTE:** PoE is a method of delivering power on the same physical Ethernet wire that is used for data communication. Power for devices is provided in one of the following two ways:

Endspan— The switch that the W-IAP is connected to can provide power.

Midspan— A device can sit between the switch and the W-IAP.

The choice of endspan or midspan depends on the capabilities of the switch to which the IAP is connected. Typically if a switch is in place and does not support PoE, midspan power injectors are used.

---

**NOTE:** A DNS server functions as a phonebook for the internet and internet users. It converts human readable computer hostnames into IP addresses and vice-versa. A DNS server stores several records for a domain name, such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server because it provides the required IP address for a network peripheral or element.

The Dynamic Host Configuration Protocol (DHCP) is an auto-configuration protocol used on IP networks. Computers or any network peripherals that are connected to IP networks must be configured before they can communicate with other computers on the network. DHCP allows a computer to be configured automatically, eliminating the need for a network administrator. DHCP also provides a central database to keep a track of computers connected to the network. This database helps in preventing any two computers from being configured with the same IP address.

---

To complete the initial setup, perform the following tasks in the given order:

1. ["Connecting a W-IAP" on page 18](#)

2. ["Assigning an IP Address to the W-IAP" on page 18](#)
3. ["Connecting to a Provisioning Wi-Fi Network" on page 18](#)
4. ["Log in to the Dell W-Series Instant UI" on page 21](#)
5. ["Specifying a Country Code " on page 21](#) — Skip this step if you are installing the W-IAP in the United States or Japan.

## Connecting a W-IAP

Based on the type of the power source that is used, perform one of the following steps to connect the W-IAP to the power source:

- PoE switch— Connect the ENET 0 port of the W-IAP to the appropriate port on the PoE switch.
- PoE midspan— Connect the ENET 0 port of W-IAP to the appropriate port on the PoE midspan.
- AC to DC power adapter— Connect the 12V DC power jack socket to the AC to DC power adapter.

## Assigning an IP Address to the W-IAP

The W-IAP needs an IP address for network connectivity. When you connect the W-IAP to a network, the W-IAP receives an IP address from a DHCP server.

To get an IP address for a W-IAP:

1. Connect the ENET 0 port of W-IAP to a switch or router using an Ethernet cable. Ensure that the DHCP service is enabled on the network.
2. Connect the W-IAP to a power source. The W-IAP receives an IP address provided by the switch or router.



---

**NOTE:** If there is no DHCP service on the network, the W-IAP can be assigned a static IP address. If that doesn't happen, the W-IAP will get auto-assigned an IP within the 169.254 subnet.

---

## Connecting to a Provisioning Wi-Fi Network

To connect to a provisioning Wi-Fi network:

1. Connect a wireless enabled client to a provisioning Wi-Fi network. The provisioning network is called **instant**.
2. In the Microsoft Windows operating system, click the wireless network connection icon in the system tray.  
The **Wireless Network Connection** window appears.
3. Click on the **instant** network and click **Connect**.
4. In the Mac OS, click the **AirPort** icon. A list of available Wi-Fi networks is displayed.
5. Click on the **instant** network.



NOTE: Instant SSIDs are only broadcasted in 2.4 GHz.



NOTE: While connecting to the provisioning Wi-Fi network, ensure that the client is not connected to any wired network.

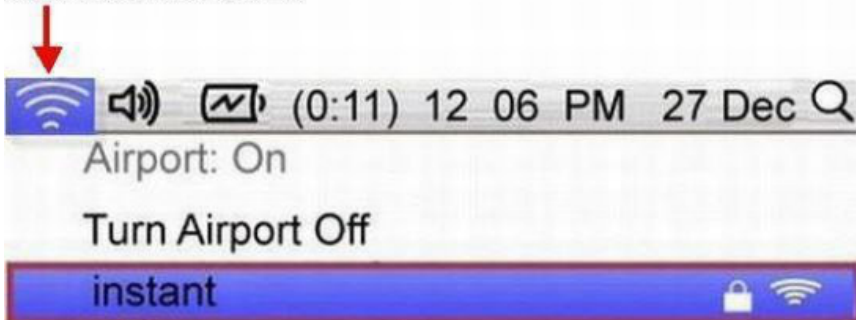
Figure 1 - Connecting to a provisioning Wi-Fi Network — Microsoft Windows



Click here to see the list of wireless networks.  
Select instant from the list.

Figure 2 - Connecting to a provisioning Wi-Fi Network — Mac OS

Click here to see the list of wireless networks.  
Select instant from the list.



## Disabling the Provisioning Wi-Fi Network

The provisioning network is enabled by default. Instant provides the option to disable the provisioning network in APBoot through console. Use this option when you do not want the default SSID **instant** to appear in your network.

To disable the provisioning network:

1. Connect a terminal or PC/workstation running a terminal emulation program to the **Console** port on the W-IAP.
2. Configure the terminal or terminal emulation program to use the following communication settings.
3. Power on the W-IAP. You see an autoboot countdown prompt that allows you to interrupt the normal startup process and access APBoot.
4. Click **Enter** before the timer expires. The W-IAP goes into apboot mode through console.

**Table 2 - Terminal Communication Settings**

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

5. In the apboot mode, use the following commands to disable the provisioning network:
  - apboot> factory\_reset
  - apboot> setenv disable\_prov\_ssid 1
  - apboot> saveenv
  - apboot> reset

## Assigning a Static IP

To assign a static IP to a W-IAP using APBoot:

1. Connect a terminal or PC/workstation running a terminal emulation program to the **Console** port on the W-IAP.
2. Configure the terminal or terminal emulation program to use the following communication settings.
3. Power on the W-IAP. You see an autoboot countdown prompt that allows you to interrupt the normal startup process and access APBoot.
4. Click **Enter** before the timer expires. The W-IAP goes into apboot mode through console.
5. In the apboot mode, use the following commands to assign a static IP to a W-IAP.

```
Hit <Enter> to stop autoboot: 0
apboot>
apboot> setenv ipaddr 10.1.1.1
apboot> setenv netmask 255.255.255.0
apboot> setenv gatewayip 10.1.1.254
apboot> save
Saving Environment to Flash...
Un-Protected 1 sectors
.done
Erased 1 sectors
Writing
```

Use the printenv command to view the configuration.

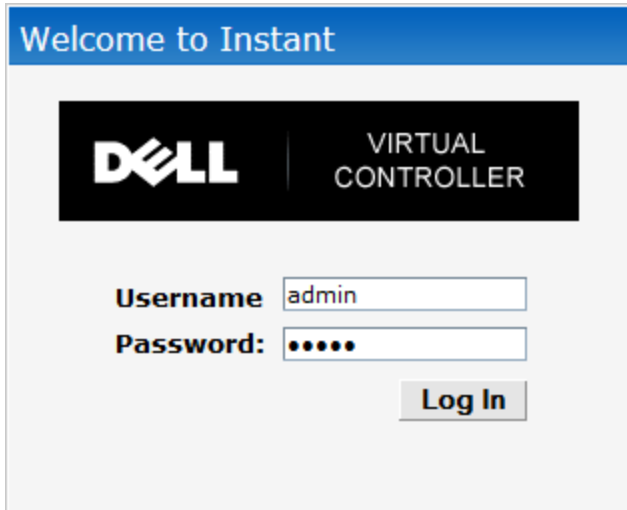
```
apboot> printenv
```

## Log in to the Dell W-Series Instant UI

Launch a web browser and enter [instant.dell-pcw.com](http://instant.dell-pcw.com). In the login screen, enter the following credentials:

- Username— admin
- Password— admin

**Figure 3** - Dell W-Series Instant UI Login Screen



Welcome to Instant

**DELL** | VIRTUAL CONTROLLER

Username:

Password:

When you use a provisioning Wi-Fi network to connect to the Internet, all browser requests are directed to the Dell W-Series Instant UI. For example, if you enter [www.example.com](http://www.example.com) in the address field, you are directed to the Instant user interface. You can change the default login credentials after you log in for the first time.

## Specifying a Country Code



---

**NOTE:** Skip this section if you are installing the W-IAP in the United States or Japan.

---

Dell W-Instant Access Points are shipped in three variants:

- W-IAP-US (United States)
- W-IAP-JP (Japan)
- W-IAP-ROW (Rest of World)

After you successfully log in to the Dell W-Series Instant User Interface, the **Country Code** window appears if W-IAP-ROW APs are installed. Select the country code for the W-IAP-ROW APs installed.

For the complete list of the countries that are supported in the W-IAP-ROW variant type, see "[Regulatory Domain](#)" on page 271.

Figure 4 - Specifying a Country Code



## W-IAP Cluster

W-IAPs in the same VLAN automatically find each other and form a single functioning network managed by a Virtual Controller.



**CAUTION:** Moving a W-IAP from one cluster to another requires a factory reset of the W-IAP that is being moved. See ["Managing W-IAPs" on page 71](#) for more information

# Chapter 3

## Dell W-Instant User Interface

The Dell W-Series Instant User Interface (UI) provides a standard web based interface that allows you to configure and monitor a Wi-Fi network. It is accessible through a standard web browser from a remote management console or workstation. JavaScript must be enabled on the web browser to view the Dell W-Series Instant UI.

Supported browsers are:

- Internet Explorer 8.0.7601.17514 and 9.0.11
- Safari 6.0.2
- Google Chrome 23.0.1271.95 m
- Mozilla Firefox 17.0



**NOTE:** The Dell W-Series Instant UI logs out automatically if the window is inactive for fifteen minutes.

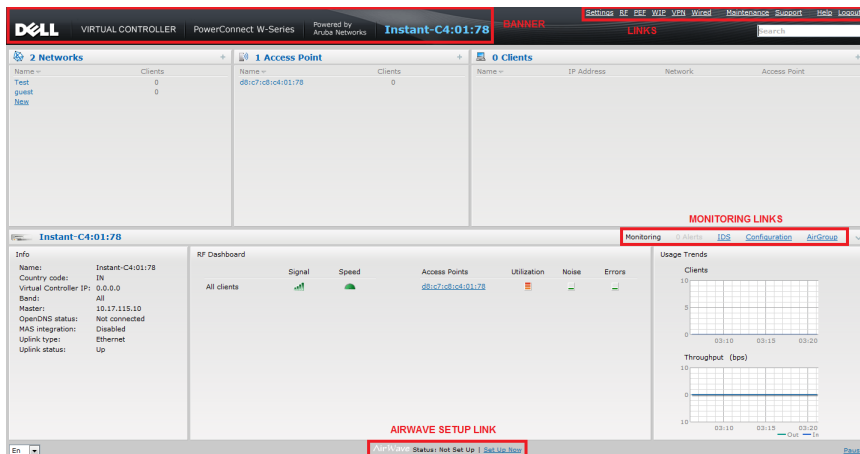
### Understanding the Dell W-Series Instant UI Layout

The Dell W-Series Instant UI consists of the following elements:

- "Banner" on page 24
- "Search" on page 24
- "Tabs" on page 24
- "Links" on page 26
- "Views" on page 41

These elements are explained in the following sections.

**Figure 5 - Dell W-Series Instant UI Interface**



## Banner

The banner is a horizontal grey rectangle that appears at the top left corner of the Dell W-Series Instant UI. It displays the company name, logo, and Virtual Controller's name.

## Search

Administrators can search a W-IAP, client, or a network using a simple **Search** window in the Dell W-Series Instant UI. This Search option helps fill in the blank when you type in a word and suggested matches are automatically displayed in a dynamic list. The list is more relevant and detailed when more number of keywords are typed in. This is similar to the auto-complete feature of Google Search.

## Tabs

The Dell W-Series Instant UI consists of the following tabs:

- **Networks**— Provides information about the Wi-Fi networks in the Dell W-Instant network.
- **Access Points**— Provides information about the W-IAPs in the W-Instant network.
- **Clients**— Provides information about the clients in the W-Instant network.

Each tab appears in a compressed view by default. A number, specifying the number of networks, W-IAPs, or clients in the network precedes the tab names. Click on the tabs to see the expanded view and click again to compress the expanded view. Items in each tab are associated with a triangle icon. Click on the triangle icon to sort the data in increasing or decreasing order. Each tab is explained in the following sections.

### Networks Tab

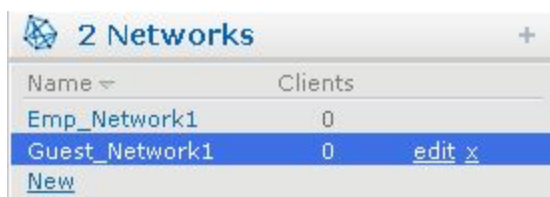
This tab displays a list of Wi-Fi networks that are configured in the Dell W-Instant network. The network names appear as links. The expanded view displays the following information about each Wi-Fi network:

- **Name (SSID)**— Name of the network.
- **Clients**— Number of clients that are connected to the network.
- **Type**— Network type: Employee, Guest, or Voice.
- **Band**— Band in which the network is broadcast: 2.4 GHz band, 5 GHz band, or both.
- **Authentication Method**— Authentication method required to connect to the network.
- **Key Management**— Authentication key type.
- **IP Assignment**— Source of IP address for the client.

To add a Wi-Fi network, click the **New** link in the **Networks** tab. For more information about a wireless network and the procedure to add a wireless network, see ["Wireless Network" on page 43](#).

An **edit** link appears on clicking the network name in the **Networks** tab. For information about editing a wireless network, see ["Network Types" on page 43](#). To delete a network, click on the link **x** located next to the **edit** link.

**Figure 6 - Networks Tab— Compressed View and Expanded View**



Name	Clients
Emp_Network1	0
Guest_Network1	0

New



Name	Clients	Type	Band	Authentication Method	Key Management	IP Assignment
Emp_Network1	0	Employee	All	None	WPA2-AES	Default VLAN
Guest_Network1	0	Guest	All	None	None	NAT Mode

## Access Points Tab

If the Auto Join Mode feature is enabled, a list of enabled and active W-IAPs in the Dell W-Instant network is displayed in the **Access Points** tab. The W-IAP names are displayed as links.

If the Auto Join Mode feature is disabled, a **New** link appears. Click on this link to add a new W-IAP to the network. If a W-IAP is configured and not active, its MAC Address is displayed in red.

The expanded view displays the following information about each W-IAP:

- **Name**— Name of the access point.
- **IP Address**— IP address of the W-IAP.
- **Mode**— Mode of the W-IAP.
  - **Access**— In this mode, the AP serves clients and scans the home channel for spectrum analysis while monitoring channels for rogue APs in the background
  - **Monitor** — In this mode, the AP acts as a dedicated Air Monitor (AM), scanning all channels for rogue APs and Clients.
- **Spectrum**— When enabled, the AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring APs or from non Wi-Fi devices such as microwaves and cordless phones. When Spectrum is enabled, the AP does not provide access services to clients.
- **Clients**— Number of clients that are connected to the W-IAP.
- **Type**— Model number of the W-IAP.
- **Channel**— Channel the W-IAP is currently broadcasting on.
- **Power (dB)**— Maximum transmit EIRP of the radio.
- **Utilization (%)**— Percentage of time that the channel is utilized.
- **Noise (dBm)**— Noise floor of the channel.

An **edit** link appears on clicking the W-IAP name. For details about editing W-IAP settings see ["Editing W-IAP Settings" on page 75](#).

**Figure 7 - Access Points Tab— Compressed View and Expanded View**

1 Access Point													
Name	Clients												
Instant Access Point	0											<a href="#">edit</a>	

1 access point														
Name	IP Address	Mode	Spectrum	Clients	Type	Mesh Role	Channel	Power (dB)	2.4 GHz		5.0 GHz		Noise (dBm)	
									Utilization (%)	Noise (dBm)	Channel	Power (dB)	Utilization (%)	Noise (dBm)
db1c7f81c04:01178	10.17.115.10	Access	Disabled	0	93	N/A	6/0/0	7	58	-96	-	-	-	-

## Clients Tab

This tab displays a list of clients that are connected to the Dell W-Instant network. The client names appear as links. The expanded view displays the following information about each client:

- **Name**— User name of the client or guest users if available.
- **IP Address**— IP address of the client.
- **MAC Address**— MAC address of the client.

- **OS**— Operating system that runs on the client.
- **Network**— The network to which the client is connected.
- **Access Point**— W-IAP to which the client is connected.
- **Channel** — The client operating channel.
- **Type**— Wi-Fi type of the client: A, G, AN, or GN.
- **Role**— Role assigned to the client.
- **Signal**— Signal strength of the client, as detected by the AP.
- **Speed (mbps)**— Current PHY rate.

**Figure 8 - Client Tab— Compressed View and Expanded View**

**1 Client Associated with Instant Access Point**

Name	IP Address	Network	Access Point
--	10.13.32.59	Emp_Network1	Instant Access Point

**1 Client**

Name	IP Address	MAC Address	OS	Network	Access Point	Channel	Type	Role	Signal	Speed (mbps)
--	10.13.32.59	58-94-4b-79-73-58	--	Emp_Network1	Instant Access Point	157+	AN	Emp_Network1	5	0

## Links

The following links allow you to configure the features and settings for the W-Instant network. Each of these links are explained in the subsequent sections.

- ["New Version Available" on page 27](#)
- ["Settings" on page 27](#)
- ["RF" on page 29](#)
- ["PEF" on page 30](#)
- ["WIP" on page 30](#)
- ["VPN" on page 31](#)
- ["Wired" on page 31](#)
- ["Maintenance" on page 32](#)
- ["Support" on page 32](#)
- ["Help" on page 32](#)
- ["Logout" on page 33](#)
- ["Monitoring" on page 33](#)
- ["Spectrum" on page 36](#)
- ["Alerts" on page 37](#)
- ["IDS" on page 39](#)
- ["Configuration" on page 39](#)
- ["AirGroup" on page 40](#)
- ["Language" on page 40](#)
- ["Dell PowerConnect W-AirWave Setup" on page 40](#)
- ["Pause/Resume" on page 41](#)

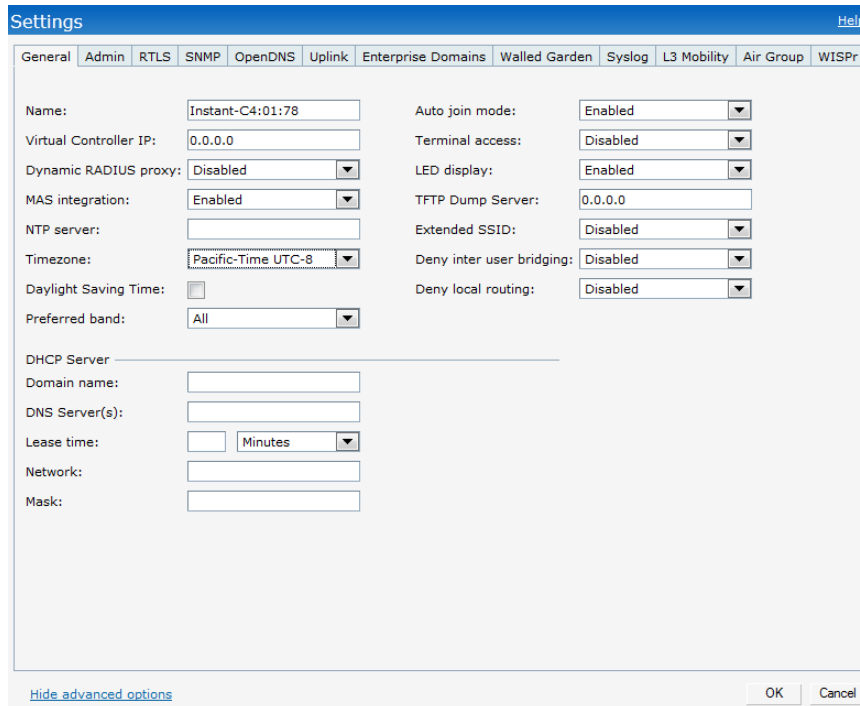
## New Version Available

This link appears in the top right corner of Dell W-Series Instant UI only if a new image version is available on the image server and Dell PowerConnect W-AirWave is not configured. For more information about the **New version available** link and its functions, see ["Firmware Image Server in Cloud Network"](#) on page 86.

## Settings

This link displays the **Settings** window. The **Settings** consists of the following tabs:

**Figure 9 - Settings Link - Default View**



The screenshot shows the 'Settings' window with the 'General' tab selected. The window has a blue header with the title 'Settings' and a 'Help' link. Below the header is a tabbed interface with the following tabs: General, Admin, RTLS, SNMP, OpenDNS, Uplink, Enterprise Domains, Walled Garden, Syslog, L3 Mobility, Air Group, and WISPr. The 'General' tab is active and contains the following settings:

Name:	Instant-C4:01:78	Auto join mode:	Enabled
Virtual Controller IP:	0.0.0.0	Terminal access:	Disabled
Dynamic RADIUS proxy:	Disabled	LED display:	Enabled
MAS integration:	Enabled	TFTP Dump Server:	0.0.0.0
NTP server:		Extended SSID:	Disabled
Timezone:	Pacific-Time UTC-8	Deny inter user bridging:	Disabled
Daylight Saving Time:	<input type="checkbox"/>	Deny local routing:	Disabled
Preferred band:	All		

Below these settings is a section for DHCP Server configuration:

Domain name:	
DNS Server(s):	
Lease time:	<input type="text"/> Minutes
Network:	
Mask:	

At the bottom left of the window is a link 'Hide advanced options'. At the bottom right are 'OK' and 'Cancel' buttons.



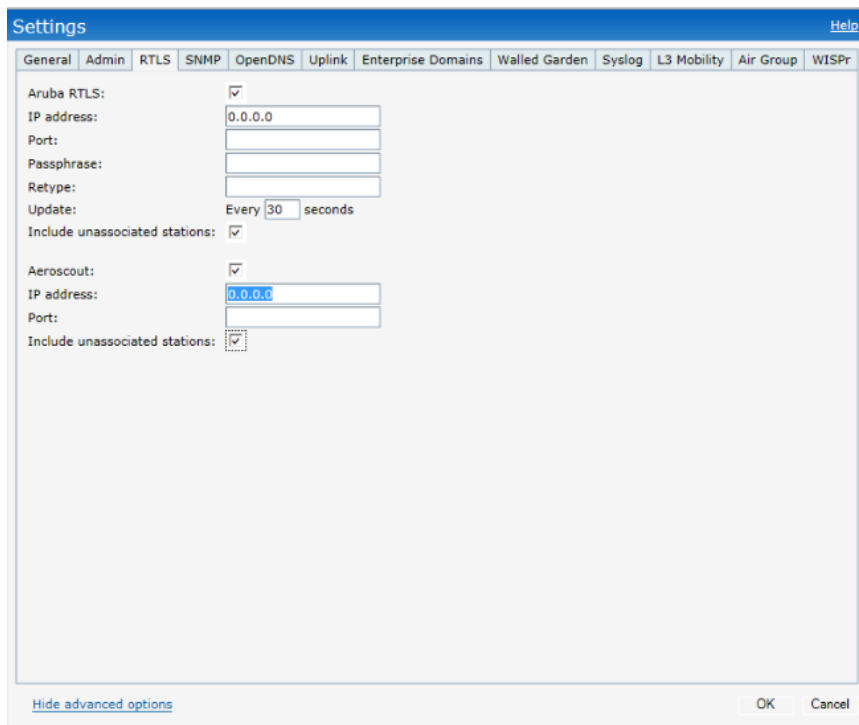
**NOTE:** Use the **Show/Hide Advanced** option on the bottom-left of the Settings window to view or hide the advanced options.

- **General**— View or edit the Name, IP address, NTP Server, and DHCP server settings of the Virtual Controller.
  - For information about Virtual Controller settings and NTP Server, see ["Virtual Controller"](#) on page 109 and ["Time Management"](#) on page 107.
  - For information about Auto join mode, Terminal Access, LED display, TFTP Dump Server, and Deny inter user bridging see ["Managing W-IAPs"](#) on page 71.
- **Admin**— View or edit the admin credentials for access to the Virtual Controller Management User Interface. See ["802.IX Authentication"](#) on page 111 for more information. You can also configure Dell PowerConnect W-AirWave in this tab. See ["Configuring Dell PowerConnect W-AirWave"](#) on page 207 for more information.
- **RTLS**— View or edit the Real-Time Location Server (RTLS) settings.
  - **Dell RTLS**— Enable this to integrate Dell W-Instant with Dell PowerConnect W-AirWave Management platform, Ekahau Real-Time Location Server and Nearby Real Time Location Server. Specify the IP address and port number of the server (to which

location reports are sent), a shared secret key, and the frequency at which packets are sent to the server.

- **Aeroscout**— Enable this option to send the RFID tag information to an AeroScout RTLS. Specify the IP address and port number of the AeroScout server, to which location reports should be sent.
- **Include unassociated stations**— Enable this option to send mobile unit reports to the Aeroscout and the Dell RTLS servers for the client stations that are not associated to any W-IAP (unassociated stations).

**Figure 10 - RTLS**



- **SNMP**— View or specify SNMP agent settings. See "SNMP" on page 183 for more information.
- **OpenDNS**— Instant supports OpenDNS business solutions which requires an OpenDNS (www.opendns.com) account comprising a username and a password. These credentials are used by W-Instant to access OpenDNS to provide enterprise-level content filtering.



---

**NOTE:** For OpenDNS to work, enable **Content Filtering** feature while creating a new network. Click **New** in the **Networks** tab and then select **Enabled** from the **Content filtering** drop-down list.

---



---

**NOTE:** If the network firewall setup already has openDNS integration, do not configure it on the W-IAP.

---

- **Uplink**— View or configure uplink settings. See "Uplink Configuration" on page 195 for more information.
- **Enterprise Domains**— This tab indicates (displays) the DNS domain names that are valid in the enterprise network. The domain names are used for determining the procedure for routing

**Content Filtering** is enabled for a network, the domain names that do not match the names in the list are sent to OpenDNS server.

- **Walled Garden**— The Walled Garden directs the user's navigation within particular areas to allow access to a selection of websites and/or prevent access to other websites. For more information, see ["Walled Garden Access" on page 134](#).
- **Syslog**— View or specify a Syslog Server for sending syslog messages to the external servers. See ["Syslog Server" on page 73](#) for more information.
- **L3 Mobility**— View or configure the Layer-3 mobility settings. See ["Layer-3 Mobility" on page 91](#) for more information.
- **AirGroup** — View or configure the AirGroup settings. See ["AirGroup" on page 215](#) for more information.
- **WISPr** — View or configure the WISPr settings. See ["WISPr Authentication" on page 132](#) for more information.

## RF

This link displays the configuration parameters Adaptive Radio Management (ARM) and Radio features.

**Figure 11 - RF**

The screenshot shows a configuration window titled "RF" with a "Help" link in the top right corner. The window has two tabs: "ARM" and "Radio", with "Radio" currently selected. The "Radio" tab contains the following settings:

- Client Control**
  - Band steering mode: Prefer 5Ghz (dropdown menu)
  - Airtime fairness mode: Fair Access (dropdown menu)
- Access Point Control**
  - Customize valid channels:
  - Min transmit power: 18 (dropdown menu)
  - Max transmit power: Max (dropdown menu)
  - Client aware: Enabled (dropdown menu)
  - Scanning: Enabled (dropdown menu)
  - Wide channel bands: 5GHz (dropdown menu)

At the bottom of the window, there is a link for "Hide advanced options" and "OK" and "Cancel" buttons.

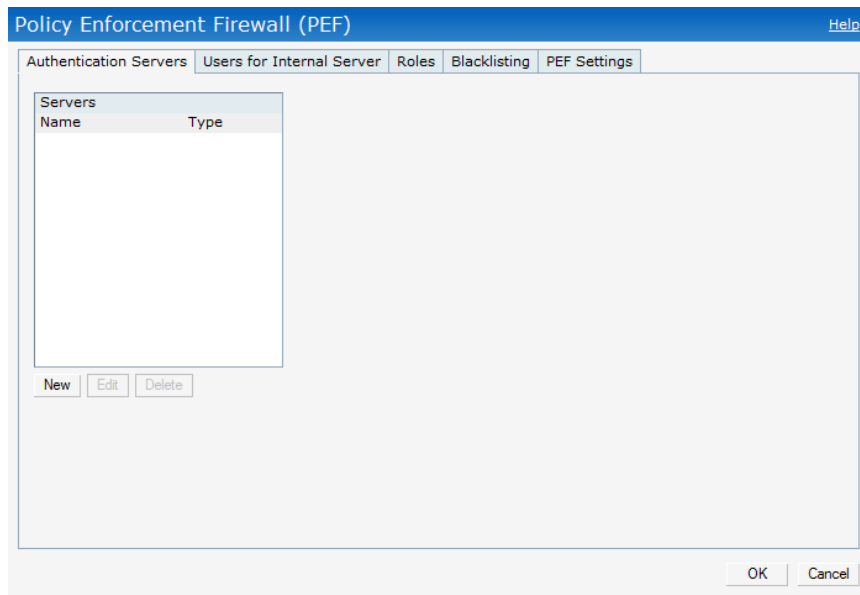
**ARM** — View or assign channel and power settings for all the W-IAPs in the network. For information about ARM (Adaptive Radio Management), see ["ARM Features" on page 169](#).

**Radio** — View or configure radio settings for 2.4 GHz and the 5 GHz radio profiles. For information about Radio, see ["Configuring Radio Profiles in Instant" on page 173](#).

## PEF

This link displays the following features.

**Figure 12 - PEF**



**Authentication Servers**— Use this window to configure an external RADIUS server for a wireless network. See ["802.1X Authentication" on page 111](#) for more information.

**Users for Internal Server**— Use this window to populate the system's internal authentication server with users. This list is used by networks for which per-user authorization is specified using the Virtual Controller's internal authentication server. For more information about users, see ["User Database" on page 269](#).

**Roles**— This window displays all the roles defined for all the Networks. The Access Rules part indicates the permissions for each role. For more information, see ["User Roles" on page 145](#).

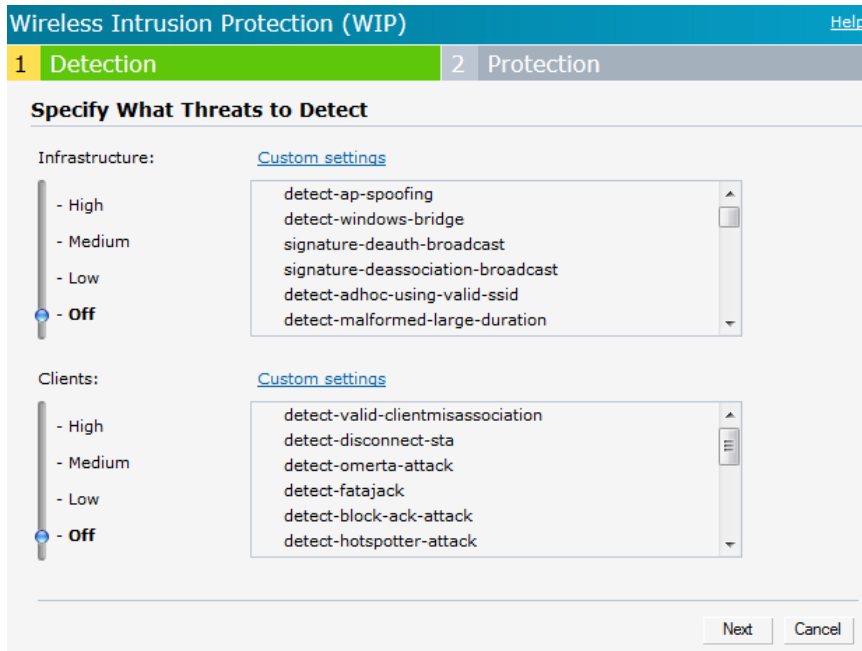
**Blacklisting**— Use this window to manually blacklist clients. See ["Client Blacklisting" on page 255](#) for more information.

**Policy Enforcement Firewall (PEF) Settings**— Use this window to enable/disable Application Layer Gateway (ALG) supporting address and port translation for various protocols. See ["Policy Enforcement Firewall" on page 251](#) for more information.

## WIP

Wireless Intrusion Protection (WIP) offers a wide selection of intrusion detection and protection features to protect the network against wireless threats. Use this window to specify desired levels of threat detection. See ["Rogue AP Detection and Classification" on page 177](#) for more information.

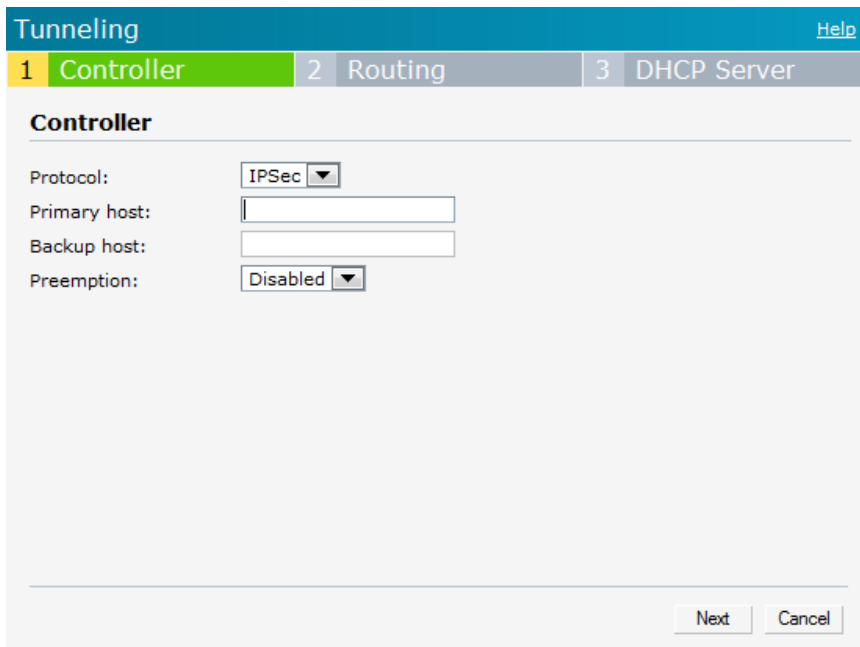
Figure 13 - WIP - Default View



## VPN

Use this window to define how the W-IAP communicates with the remote controller. See "[VPN Configuration](#)" on page 261 for more information.

Figure 14 - VPN - Default View



## Wired

Specify the desired profile for each port of the W-IAP. See "[Ethernet Downlink](#)" on page 187 for more information.

## Maintenance

This link displays the **Maintenance** window. The **Maintenance** window allows you to maintain the Wi-Fi network. It consists of the following tabs:

- **About**— Displays the Build Time, W-IAP model name, Dell OS version, Web address of Dell Networks, and Copyright information.
- **Configuration**— Displays the current configuration of the network.
  - **Clear Configuration**— Click to delete or clear the current configuration of the network and reset to provisioning configuration.
  - **Backup Configuration**— Use this feature to create local W-Instant configuration backup. Click **Backup Configuration** to save the configuration file named `instant.cfg`.
  - **Restore Configuration**— Click **Restore Configuration** to browse and locate the backup file to restore. Reboot the W-IAP for the changes to take effect.
- **Certificates** — Displays information about the current certificate installed in the network. Provides an interface to upload new certificates and to set a passphrase for the certificates. For more information, see "[Certificates](#)" on page 138.
- **Firmware** — Displays the current firmware version and provides options to upgrade to a new firmware version. For more information, see "[Firmware Image Server in Cloud Network](#)" on page 86
- **Reboot** — Displays the W-IAPs in the network and provides an option to reboot the required access point or all access points. For more information, see "[Rebooting the W-IAP](#)" on page 84.
- **Convert** — Provides an option to change the network from W-Instant to an Dell PowerConnect W-Series Mobility Controller managed network or standalone AP. For more information, see "[Migrating to a Dell PowerConnect W-Series Mobility Controller Managed Network](#)" on page 80.

## Support

This link displays the **Support** window. It consists of the following fields:

- **Command**— Provides various options for which you can generate support logs.
- **Target**— Provides a list of W-IAPs in the network.
- **Run**— Click this to generate the support log for the selected option and W-IAP.
- **Auto Run**— The selected commands run on the selected APs according to the specified time schedule.
- **Filter**— Enter a string and click to display the filtered content of any command.
- **Clear**— Click to clear the text box
- **Save Results**— Click to open the results in another window and save it as an HTML or text file.

For additional details, see "[Troubleshooting](#)" on page 289.

## Help

The **Help** link at the top right corner of the Dell W-Series Instant UI allows you to view a short description or definition of selected terms and fields in the Dell W-Series Instant UI.

To activate the context-sensitive help:

1. At the top right corner of Dell W-Series Instant UI, click the **Help** link.



**Figure 15 - Help Link**


For Help, click any text in *green italics* [Done](#)

2. Click any text or term displayed in green italics to view its description or definition.
3. To disable the help mode, click **Done**.

## Logout

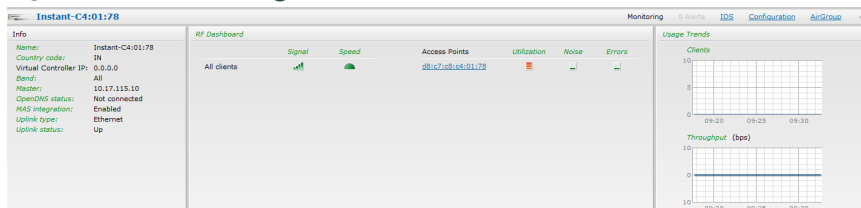
Use this link to logout of the Dell W-Series Instant UI.

## Monitoring

This link displays the Monitoring pane. This pane can be used to monitor the Dell W-Instant network. Use the down arrow  located to the right side of these links to compress or expand the monitoring pane. The monitoring pane consists of the following sections:

- "Info " on page 33
- "RF Dashboard" on page 34
- "Usage Trends " on page 35

**Figure 16 - Monitoring on Instant UI**



## Info

Displays the configuration information of the Virtual Controller by default. In a "Network View" on page 232, this section displays configuration information of the selected network. Similarly, in an "Dell W-Instant Access Point View" on page 235 or "Client View" on page 243, this section displays the configuration information of the selected W-IAP or the client.

**Figure 17 - Info Section in the Monitoring Pane**



## RF Dashboard

Allows you to view trouble spots in the network. It displays the following information:

**Figure 18 - RF Dashboard in the Monitoring Pane**



The RF Dashboard displays the following information:

- Clients— Lists the clients with low speed or signal strength in the network.
- Access Points— Lists the W-IAPs whose utilization, noise, or errors are not within the specified threshold. The W-IAP names appear as links. When the W-IAP is clicked, the W-IAP configuration information is displayed in the Info section. The RF Dashboard section is pushed to the bottom left corner of the Dell W-Series Instant UI. The RF Trends section appears in its place. This section consists of the Utilization, Band frames, Noise Floor, and Errors graphs. For more information on the graphs, see "Monitoring" on page 229.

The following table lists the icons available on the RF Dashboard pane:

**Table 3- RF Dashboard Icons**

Icon	Name	Description
1	Signal Icon	<p>Displays the signal strength of the client. Depending on the signal strength of the client, the color of the lines on the Signal bar changes from Green &gt; Orange &gt; Red.</p> <ul style="list-style-type: none"> <li>• Green— Signal strength is more than 20 decibels.</li> <li>• Orange— Signal strength is between 15-20 decibels.</li> <li>• Red— Signal strength is less than 15 decibels.</li> </ul> <p>To view the signal graph for a client, click on the signal icon against the client in the <b>Signal</b> column.</p>
2	Speed icon	<p>Displays the data transfer speed of the client. Depending on the data transfer speed of the client, the color of the Signal bar changes from Green &gt; Orange &gt; Red.</p> <ul style="list-style-type: none"> <li>• Green— Data transfer speed is more than 50 percent of the maximum speed supported by the client.</li> <li>• Orange— Data transfer speed is between 25-50 percent of the maximum speed supported by the client.</li> <li>• Red— Data transfer speed is less than 25 percent of the maximum speed supported by the client.</li> </ul> <p>To view the data transfer speed graph of a client, click on the speed icon against the client in the <b>Speed</b> column.</p>
3	Utilization icon	<p>Displays the radio utilization rate of the IAPs. Depending on the percentage of utilization, the color of the lines on the Utilization icon changes from Green &gt; Orange &gt; Red.</p>

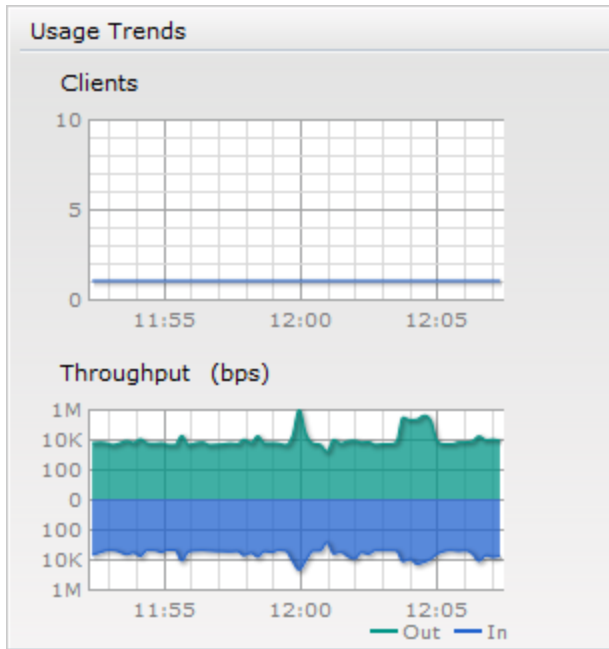
Icon	Name	Description
		<ul style="list-style-type: none"> <li>• Green— Utilization is less than 50 percent.</li> <li>• Orange— Utilization is between 50-75 percent.</li> <li>• Red— Utilization is more than 75 percent.</li> </ul> <p>To view the utilization graph of a W-IAP, click on the Utilization icon against the W-IAP in the Utilization column.</p>
4	Noise icon	<p>Displays the noise floor of the W-IAPs. Noise is measured in decibels/meter. Depending on the noise floor, the color of the lines on the Noise icon changes from Green &gt; Orange &gt; Red.</p> <ul style="list-style-type: none"> <li>• Green— Noise floor is more than 87 dBm.</li> <li>• Orange— Noise floor is between 80 dBm-87 dBm.</li> <li>• Red— Noise floor is less than 80 dBm.</li> </ul> <p>To view the noise floor graph of a W-IAP, click on the noise icon against the W-IAP in the Noise column.</p>
5	Errors icon	<p>Displays the errors for the W-IAPs. Depending on the errors, color of the lines on the Errors icon changes from Green &gt; Yellow &gt; Red.</p> <ul style="list-style-type: none"> <li>• Green— Errors are less than 5000 frames per second.</li> <li>• Orange— Errors are between 5000-10000 frames per second.</li> <li>• Red— Errors are more than 10000 frames per second.</li> </ul> <p>To view the errors graph of a W-IAP, click on the <b>Errors</b> icon against the W-IAP in the <b>Errors</b> column.</p>

### Usage Trends

Displays the following graphs:

- **Clients**— In the default homepage, the Clients graph displays the number of clients that were associated with the Virtual Controller in the last 15 minutes. In Network or W-IAP view, this graph displays the number of clients that were associated with the selected network or W-IAP in the last 15 minutes.
- **Throughput**— In the default homepage, the Throughput graph displays the incoming and outgoing throughput traffic for the Virtual Controller in the last 15 minutes. In the Network or W-IAP view, this graph displays the incoming and outgoing throughput traffic for the selected network or W-IAP in the last 15 minutes.

**Figure 19 - Usage Trends Section in the Monitoring Pane**



For more information about the graphs and monitoring procedures, see ["Monitoring" on page 229](#).

## Spectrum

The spectrum link (in the Access Point view) displays the spectrum data that is collected by a hybrid AP or by a W-IAP that has enabled spectrum monitor. The spectrum data is not reported to the VC.

The spectrum link displays the following:

### Overview (Device list)

The device list display consists of a device summary table and channel information for active non Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio.

**Figure 20 - Device List**

Non-WiFi Device List: 2GHz									
Type	ID	Cfreq(KHz)	Bandwidth(KHz)	Channels-affected	Signal(dBm)	Duty-cycle	Add-time	Update-time	
Cordless Network FH	1	2444000	80000	1 2 3 4 5 6 7 8 9 10 11 12 13 14	-75	5	2000-01-01 00:05:27	2000-01-01 00:27:45	

## Channel Utilization and Monitoring

This chart provides an overview of channel quality across the spectrum. It shows channel utilization information such as channel quality, availability, and utilization metrics as seen by a spectrum monitor for the 2.4 GHz and 5 GHz radio bands. The first bar for each channel represents the percentage of air time used by non Wi-Fi interferers and Wi-Fi devices. The remaining air time is available for use. The second bar indicates the channel quality. A higher percentage value indicates better quality.

## Channel Details

When you move your mouse over a channel, the channel details or the summary of the 5 GHz and 2.4 GHz channels as detected by a spectrum monitor are displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference and the Signal-to-Noise and Interference Ratio (SNIR). Spectrum monitors display spectrum analysis data seen on all channels in the selected band, and hybrid W-IAPs display data from the one channel they are monitoring.

Figure 21 - Channel Details Information

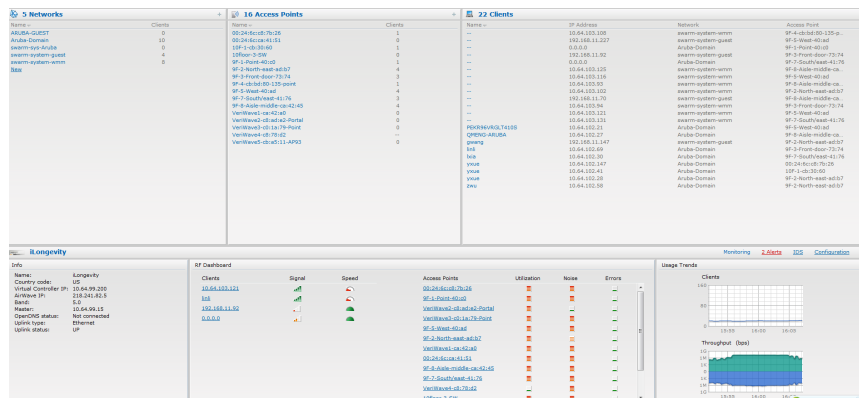
Channel 10			
Quality(%):	61	KnownAPs:	2
Utilization(%):	78	UnknownAPs:	62
WiFi(%):	39	Noise Floor(dBm):	-87
Bluetooth(%):	0	MaxAP Signal(dBm):	-26
Microwave(%):	0	Max AP SSID:	Tenda_hbchen
Cordless Phone(%):	0	Max AP BSSID:	c8:3a:35:2b:14:48
Total nonwifi(%):	39	Max Interference(dBm):	-56
		SNIR(dB):	30

For more information on spectrum monitoring, see "Spectrum Monitor" on page 97.

## Alerts

Alerts are generated when a user faces problems while accessing or connecting to the Wi-Fi network. The Alerts link appears in red if there are any Client Alerts, or Active Faults.

Figure 22 - Alerts Link



## Client Alerts

These alerts occur when clients are connected to the W-Instant network. A client alert consists of the following fields:

- Timestamp— Displays the time at which the client alert was recorded.
- MAC address— Displays the MAC address of the client which caused the alert.
- Description— Provides a short description of the alert.
- Access Points— Displays the IP address of the W-IAP to which the client is connected.
- Details— Provides complete details of the alert.

**Figure 23 - Client Alerts**

5 Networks		16 Access Points		20 Clients	
Name	Clients	Name	Clients	Name	IP Address
ARUBA-CUSTP	0	0024-6c0b-7b26	2	--	192.168.11.79
Aruba-Domain	0	0024-6c0b-7b26	0	--	192.168.11.227
swarm-system-aruba	0	10P-1-cb3030	0	--	10.64.103.110
swarm-system-guest	3	10P-3-SW	0	--	10.64.103.102
swarm-system-warm	0	WF-1-Wave-40-00	0	--	10.64.103.112
test	0	WF-2-North-east-007	5	--	10.64.103.94
		WF-3-Front-door-7574	1	--	10.64.103.108
		WF-4-cb1801330-point	1	--	0.0.0.0
		WF-5-Wave-40-ad	3	--	10.64.103.83
		WF-7-South/West-4176	1	--	192.254.99.45
		WF-8-Aruba-Modem-2412145	5	--	10.64.103.121
		VeriWave4-cb182-ad	0	--	10.64.103.123
		VeriWave2-cb182-Partial	0	--	PER95V6DLT4108
		VeriWave4-cb18279-Point	0	--	QMRNG-ARUBA
		VeriWave4-cb178102	--	--	test
		VeriWave5-cb1811-APP3	0	--	xxxx
				--	192.168.11.147
				--	yyyy
				--	10.64.102.41
				--	yyyy
				--	10.64.102.28
				--	zww
				--	10.64.102.58

Client Alerts					
Timestamp	MAC Address	Description	Access Point	Details	
15:48:27	4c:9f:ba:d3:fc:3e	DHCP request timed out	WF-5-Wave-40-ad	more	

**Fault History**

These alerts occur in the event of a system fault. A Fault History consists of the following fields:

- Time— Displays the system time when an event occurs.
- Number— Indicates the number of sequence.
- Cleared by— Displays the module which cleared this fault.
- Description— Displays the event details.

**Figure 24 - Fault History**

5 Networks		16 Access Points		20 Clients	
Name	Clients	Name	Clients	Name	IP Address
ARUBA-CUSTP	0	0024-6c0b-7b26	2	--	192.168.11.79
Aruba-Domain	0	0024-6c0b-7b26	0	--	192.168.11.227
swarm-system-aruba	0	10P-1-cb3030	0	--	10.64.103.110
swarm-system-guest	3	10P-3-SW	0	--	10.64.103.112
swarm-system-warm	0	WF-1-Wave-40-00	0	--	10.64.103.94
test	0	WF-2-North-east-007	5	--	10.64.103.108
		WF-3-Front-door-7574	1	--	0.0.0.0
		WF-4-cb1801330-point	1	--	10.64.103.93
		WF-5-Wave-40-ad	3	--	192.254.99.45
		WF-7-South/West-4176	1	--	10.64.103.121
		WF-8-Aruba-Modem-2412145	5	--	10.64.103.123
		VeriWave4-cb182-ad	0	--	10.64.102.21
		VeriWave2-cb182-Partial	0	--	PER95V6DLT4108
		VeriWave4-cb18279-Point	0	--	QMRNG-ARUBA
		VeriWave4-cb178102	--	--	test
		VeriWave5-cb1811-APP3	0	--	xxxx
				--	192.168.11.147
				--	yyyy
				--	10.64.102.41
				--	yyyy
				--	10.64.102.28
				--	zww
				--	10.64.102.58

Fault History				
Time	Number	Cleared by	Description	
15:47:08	2	System	Access point 0024-6c0b-7b26 is down	
06:20:14	2	System	Access point 0024-6c0b-7b26 is down	
06:21:19	3	System	Access point 0024-6c0b-7b26 is down	
06:26:33	0	System	Access point 0024-6c0b-7b26 is down	

**Active Faults**

These alerts occur in the event of a system fault. An Active Fault consists of the following fields:

- Time— Displays the system time when an event occurs.
- Number— Indicates the number of sequence.
- Description— Displays the event details.

**Figure 25 - Active Faults**

5 Networks		16 Access Points		19 Clients	
Name	Clients	Name	Clients	Name	IP Address
ARUBA-CUSTP	0	0024-6c0b-7b26	2	--	192.168.11.227
Aruba-Domain	0	0024-6c0b-7b26	0	--	10.64.103.110
swarm-system-aruba	0	10P-1-cb3030	0	--	10.64.103.112
swarm-system-guest	3	10P-3-SW	0	--	10.64.103.102
swarm-system-warm	0	WF-1-Wave-40-00	0	--	10.64.103.94
test	0	WF-2-North-east-007	5	--	10.64.103.108
		WF-3-Front-door-7574	1	--	192.254.99.45
		WF-4-cb1801330-point	1	--	0.0.0.0
		WF-5-Wave-40-ad	3	--	10.64.103.83
		WF-7-South/West-4176	1	--	192.168.11.70
		WF-8-Aruba-Modem-2412145	4	--	10.64.103.121
		VeriWave4-cb182-ad	0	--	10.64.102.21
		VeriWave2-cb182-Partial	0	--	PER95V6DLT4108
		VeriWave4-cb18279-Point	0	--	QMRNG-ARUBA
		VeriWave4-cb178102	--	--	test
		VeriWave5-cb1811-APP3	0	--	xxxx
				--	192.168.11.147
				--	yyyy
				--	10.64.102.41
				--	yyyy
				--	10.64.102.28
				--	zww
				--	10.64.102.58

Active Faults			
Time	Number	Description	
06:22:03	1	Access point 0024-6c0b-42145 is down	

For more information about alerts, see "Alert Types and Management" on page 249.

## IDS

This link displays a list of foreign APs and foreign clients that are detected in the network. It consists of the following sections:

- Foreign Access Points Detected— Lists the APs that are not controlled by the Virtual Controller. The following information is displayed for each foreign AP:
  - MAC address— Displays the MAC address of the foreign AP.
  - Network— Displays the name of the network to which the foreign AP is connected.
  - Classification— Displays the classification of the foreign AP: Interfering W-IAP or Rogue W-IAP.
  - Channel— Displays the channel in which the foreign AP is operating.
  - Type— Displays the Wi-Fi type of the foreign AP.
  - Last seen— Displays the time when the foreign AP was last detected in the network.
  - Where— Provides information about the W-IAP that detected the foreign AP. Click the pushpin icon to view the information.
- Foreign Clients Detected— Lists the clients that are not controlled by the Virtual Controller. The following information is displayed for each foreign client:
  - MAC address— Displays the MAC address of the foreign client.
  - Network— Displays the name of the network to which the foreign client is connected.
  - Classification— Displays the classification of the foreign client: Interfering client.
  - Channel— Displays the channel in which the foreign client is operating.
  - Type— Displays the Wi-Fi type of the foreign client.
  - Last seen— Displays the time when the foreign client was last detected in the network.
  - Where— Provides information about the W-IAP that detected the foreign client. Click the pushpin icon to view the information.

For more information on the intrusion detection feature, see ["Intrusion Detection System" on page 177](#).

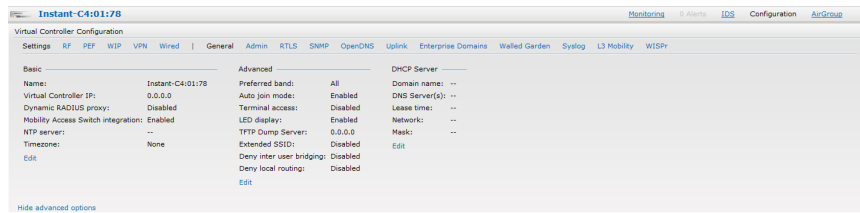
**Figure 26 - Intrusion Detection on Instant UI**

Foreign Access Points Detected						Foreign Clients Detected							
MAC address	Network	Classification	Chan.	Type	Last Seen	Where	MAC address	Network	Classification	Chan.	Type	Last Seen	Where
00:14:8c:8d:48:72	docomo	Interfering	1	G	11:31:07		00:26:cd:b7:7a:76	ethersphere-voip	Interfering	1	GN 20MHz	11:31:07	
00:0b:86:96:29:31	NTT-SPOT	Interfering	1	G	11:31:07		1c:80:94:a1:9e:b6	ethersphere-wpa2	Interfering	1	GN 20MHz	11:31:07	
00:24:8c:0b:94:32	docomo	Interfering	1	G	11:31:07		58:94:6b:57:50:38	ethersphere-wpa2	Interfering	1	GN 20MHz	11:31:07	
00:24:8c:0f:9d:42	docomo	Interfering	1	G	11:31:07		24:77:03:7a:67:5c	UI_Dashboard	Interfering	1	G	11:31:07	
00:24:8c:0d:3c:62	docomo	Interfering	1	G	11:31:07		00:14:68:30:7e:d8	ethersphere-wpa2	Interfering	1	GN 20MHz	11:30:51	
00:24:8c:8a:9a:05	anub-a-p	Interfering	1	GN 20MHz	11:31:07		04:46:6b:8c:00:a3	ethersphere-wpa2	Interfering	1	GN 20MHz	11:30:35	
00:0b:86:96:34:32	docomo	Interfering	1	G	11:31:07		24:77:03:7a:65:5c	pvt-alpha	Interfering	1	GN 20MHz	11:30:35	
00:0b:86:96:29:32	docomo	Interfering	1	G	11:31:07		00:27:62:a2:d8:b2	ethersphere-voip	Interfering	1	GN 20MHz	11:30:20	
00:24:8c:32:0c:11	NTT-SPOT	Interfering	1	G	11:31:07		00:03:2a:02:5b:b7	alkvoices	Interfering	1	G	11:30:20	
6c:03:71:18:66:68	hospod_sash	Interfering	157	AN 40MHz	11:31:07		00:02:af:9e:8a:b5	ethersphere-wpa2	Interfering	1	GN 20MHz	11:29:34	
00:24:8c:33:0c:12	docomo	Interfering	1	G	11:31:07		00:17:ca:a8:7a:a5	ethersphere-voip	Interfering	1	B	11:29:05	
6c:03:71:18:66:60	nyrapi	Interfering	1	GN 20MHz	11:31:07		84:29:99:11:23:0d	mido-roaming	Interfering	11	GN 20MHz	11:29:05	
d8:c7:c8:27:33:65	sandp-test	Interfering	11	GN 20MHz	11:31:07		5c:0a:5b:13:a5:c3	ethersphere-voip	Interfering	11	GN 20MHz	11:28:50	
00:24:8c:0b:30:40	7SPOT	Interfering	1	GN 20MHz	11:31:07		20:64:32:51:62:3f	pvt-alpha	Interfering	1	GN 20MHz	11:27:49	
00:24:8c:0e:82:60	7SPOT	Interfering	1	GN 20MHz	11:31:07		20:64:32:51:62:37	ethersphere-wpa2	Interfering	1	GN 20MHz	11:23:34	
00:24:8c:80:4b:f1	ARUBA-VISITOR	Interfering	1	GN 20MHz	11:31:07		58:94:6b:31:f7:00	mido-roaming	Interfering	11	B	11:21:49	
00:0b:86:70:4b:f4	san-media-gsk	Interfering	1	GN 20MHz	11:31:07		00:16:6f:31:8b:8a	UI_Dashboard	Interfering	6	G	11:18:18	
d8:c7:c8:27:33:c2	Miford_Staff	Interfering	1	GN 20MHz	11:31:07		00:26:cd:ba:68:b8	ethersphere-voip	Interfering	6	GN 20MHz	11:18:18	

## Configuration

This link provides an overall view of your Virtual Controller configuration. Click on each of the features to view or edit the settings.

**Figure 27 - Configuration Link**



## AirGroup

This link provides an overall view of your AirGroup configuration. Click on each of the features to view or edit the settings.

**Figure 28- AirGroup Link**



- **MAC** — Displays the MAC address of the AirGroup servers.
- **IP** — Displays the IP address of the AirGroup servers.
- **Host Name** — Displays the machine name or hostname of the AirGroup servers.
- **Service**— Displays the type of the services such as AirPlay or AirPrint.
- **Wired/Wireless** — Displays if the AirGroup server is connected via wired or wireless interface.
- **Role** — Indicates the role assigned to the specified AirGroup server. Normally it is the SSID name, in case of a wireless client.
- **Username** — If the server is connected using 802.1X, this field displays the user name. If the server is connected via PSK or open auth, this field will be blank.
- **AP-NAME**— Displays the MAC address of the IAP where the server is connected.
- **Update no/hash**— This is used for debugging issues. Use this to identify the internal database of AirGroup.
- **CPPM**— By clicking on this, you get details of the registered rules in Dell PowerConnect W-ClearPass Policy Manager (CPPM) for this server.
- **MDNS Cache**— By clicking on this, you receive MDNS record details of a particular server.

## Language

The language links are provided in the login screen to allow users to select the preferred language before logging in to the Dell W-Series Instant UI. In addition, this link is also located at the bottom left corner of the Dell W-Series Instant UI. A default language is selected based on the language preferences in the client desktop operating system or browser. If Dell W-Instant cannot detect the language, then English (En) is used as the default language.

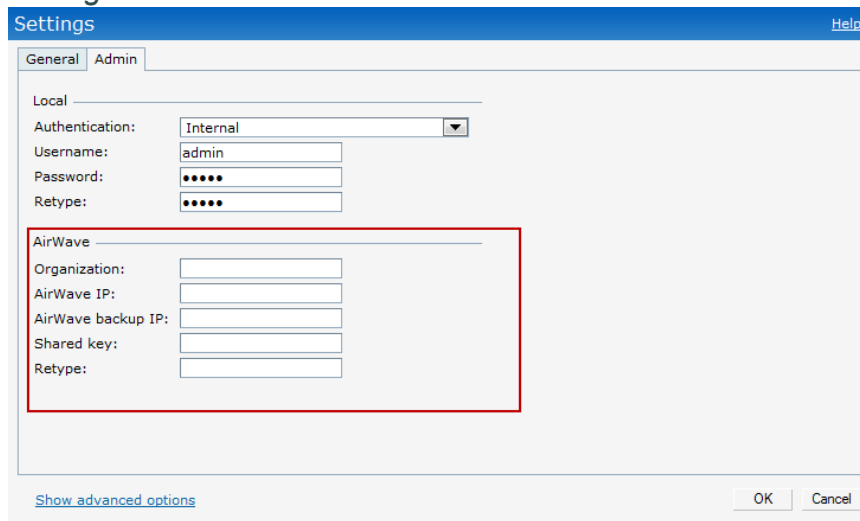
## Dell PowerConnect W-AirWave Setup

Dell PowerConnect W-AirWave is a solution for managing rapidly changing wireless networks. When enabled, Dell PowerConnect W-AirWave allows you to manage the W-Instant network. For more information on Dell PowerConnect W-AirWave, see "[Dell PowerConnect W-AirWave Integration and Management](#)" on page 205. The Dell PowerConnect W-AirWave status is displayed on the right side of the language links in the Dell W-Series Instant UI. If the Dell PowerConnect W-AirWave status is **Not Set Up**, click the **Set Up Now** link to set up the Dell



PowerConnect W-AirWave. The **Settings** window appears with **Admin** tab selected. For information to configure Dell PowerConnect W-AirWave, see "[Configuring Dell PowerConnect W-AirWave](#)" on page 207.

**Figure 29 - Dell PowerConnect W-AirWave Setup Link – Dell PowerConnect W-AirWave Configuration**



## Pause/Resume

The **Pause/Resume** link is located at the bottom right corner of the Dell W-Series Instant UI. The Dell W-Series Instant UI is automatically refreshed after every 15 seconds by default.

Click the **Pause** link to pause the automatic refreshing of the Dell W-Series Instant UI. When the automatic Dell W-Series Instant UI refreshing is paused, the **Pause** link changes to **Resume**. Click the **Resume** link to resume automatic refreshing.

The **Pause** link is useful when you want to analyze or monitor the network or a network element and therefore do not want the user interface to refresh. Automatic refreshing allows you to get the latest information about the network and network elements.

## Views

Depending on the link or tab that is clicked, the Dell W-Series Instant UI displays information about the Virtual Controller, Wi-Fi networks, W-IAPs, or the clients in the Info section. The views on the Dell W-Series Instant UI are classified as follows:

- Virtual Controller view— The Virtual Controller view is the default view. This view allows you to monitor the Dell W-Instant network.
- Network view— The Network view provides information that is necessary to monitor a selected wireless network. All Wi-Fi networks in the Dell W-Instant network are listed in the **Networks** tab. Click the name of the network that you want to monitor. Network view for the selected network appears.
- W-Instant Access Point view— The W-Instant Access Point view provides information that is necessary to monitor a selected W-IAP. All W-IAPs in the Dell W-Instant network are listed in the **Access Points** tab. Click the name of the W-IAP that you want to monitor. Access Point view for that W-IAP appears.
- Client view— The Client view provides information that is necessary to monitor a selected client. In the Client view, all the clients in the Dell W-Instant network are listed in the

**Clients** tab. Click the IP address of the client that you want to monitor. Client view for that client appears.

For more information on the graphs and the views, see "[Monitoring](#)" on page 229.

# Chapter 4

## Wireless Network

In a Wireless LAN (WLAN), laptops, desktops, PDAs, and other computer peripherals are connected to each other without any network cables. These network elements or clients use radio signals to communicate with each other. Wireless networks are set up based on the IEEE 802.11 standards. The IEEE 802.11 is a set of standards that are categorized based on the radio wave frequency and the data transfer rate. For more information about the IEEE 802.11 standards, see [Table 4](#).

**Table 4 - IEEE 802.11 Standards**

IEEE Network Standard	Frequency Used (in GHz)	Maximum Data Transfer Rate (in Mbps)
802.11a	5.0	54
802.11b	2.4	11
802.11g	2.4	54
802.11n	2.4 or 5.0	300

During start up, a wireless client searches for radio signals or beacon frames that originate from the nearest W-IAP. After locating the W-IAP, the following transactions take place between the client and the W-IAP:

1. Authentication— The W-IAP communicates with a RADIUS server to validate or authenticate the client.
2. Connection— After successful authentication, the client establishes a connection with the W-IAP.

### Network Types

Dell W-Instant wireless networks are categorized as:

- "Employee Network" on page 44
- "Voice Network" on page 53
- "Guest Network" on page 60



**NOTE:** When a client is associated to the Voice network, all data traffic is marked and placed into the high priority queue in QoS (Quality of Service). QoS refers to the capability of a network to provide better service to selected network traffic over various technologies.

## Employee Network

An Employee network is a classic Wi-Fi network. This network type is supported with full customization on Dell W-Instant. It is used by the employees in the organization. Passphrase based or 802.1X based authentication methods are supported on this network type. Employees can access the protected data of an enterprise through the employee network after successful authentication.

### Adding an Employee Network

This section provides the procedure to add an employee network.

1. In the **Networks** tab, click the **New** link. The **New WLAN** window appears.

**Figure 30 - Adding an Employee Network — WLAN Settings Tab**

2. In the **WLAN Settings** tab, perform the following steps:
  - a. **Name (SSID)**— Enter a name that uniquely identifies a wireless network.
  - b. **Primary usage**— Select **Employee** (this is selected by default) from the **Primary usage** options. This selection determines whether the network is primarily intended to be used for employee data, guest data, or voice traffic.
3. Click the **Show advanced options** link and perform the following steps.
  - a. **Broadcast/Multicast**
    - **Broadcast filtering**— When set to **All**, the W-IAP drops all broadcast and multicast frames except for DHCP and ARP. When set to **ARP**, in addition to the above, the W-IAP converts ARP requests to unicast and send frames directly to the associated client. When **Disabled**, all broadcast and multicast traffic is forwarded.
    - **DTIM interval**— Indicates the DTIM (delivery traffic indication message) period in beacons. You can configure this option for every WLAN SSID profile. The default value is 1, which means the client checks for buffered data on the W-IAP at every beacon. You may choose to configure a larger DTIM value for power saving.
    - **Multicast transmission optimization**— When **Enabled**, the W-IAP chooses the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. The default values are 1 Mbps for 2.4 GHz and 6

Mbps for 5.0 GHz bands. Multicast traffic can be sent at up to 24 Mbps when this option is enabled. This option is disabled by default.

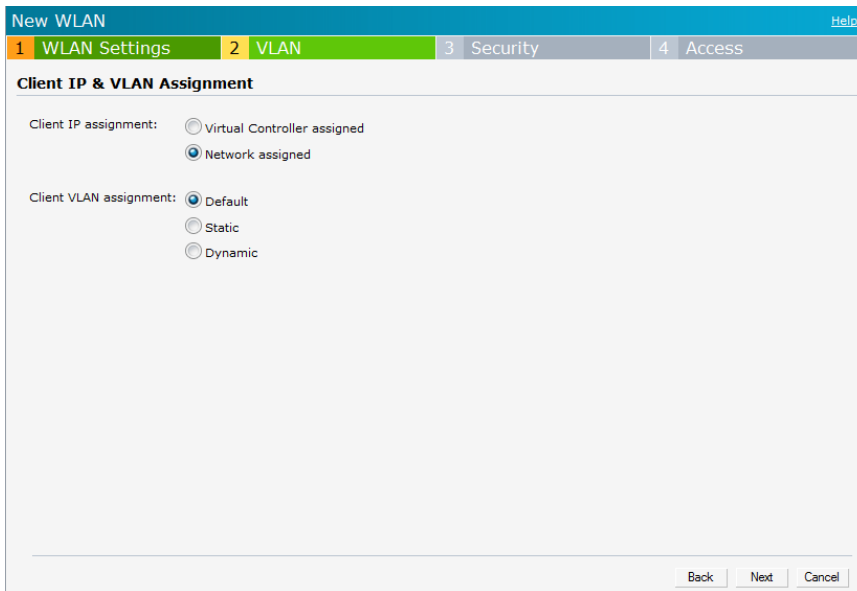
- **Dynamic multicast optimization**— When Enabled, the W-IAP converts multicast streams into unicast streams over the wireless link. DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to non-video clients.
- **DMO channel utilization threshold**— When dynamic multicast optimization is enabled, the W-IAP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90 and the maximum threshold value is 100%.

If the threshold value exceeds the maximum value, then the W-IAP sends multicast traffic over the wireless link.

- b. **Bandwidth Limits**— You can specify three types of bandwidth limits.
  - **Airtime**— Indicates the aggregate amount of airtime that all clients on this Network can use to send/receive data.
  - **Each user**— Indicates the throughput for any single user on this Network. The throughput value is specified in kbps.
  - **Each radio**— Indicates the aggregate amount of throughput each radio (some AP models have multiple radios) is allowed to provide for all clients connected to that radio.
- c. **Transmit Rates**— Indicates the ability to configure the basic and supported rates per SSID for Dell W-Instant. Select to set the minimum and maximum legacy (non-802.11n) transmit rates for each band — 2.4 GHz and 5 GHz.
- d. **Miscellaneous**
  - **Content filtering**— When enabled, all DNS requests to non-corporate domains on this wireless network are sent to OpenDNS.
  - **Band**— Set the band at which the network transmits radio signals. Available options are 2.4 GHz, 5 GHz and All. The All option is selected by default. It is also the recommended option.
  - **Inactivity timeout**— Indicates the time in seconds after which an idle client ages out. The minimum value is 60 seconds and the default value is 1000 seconds.
  - **Hide SSID**— Select this check box if you do not want the SSID (network name) to be visible to users.
  - **Max clients threshold**— Indicates the maximum number of clients that can be configured for each BSSID on a WLAN. The supported range is 0 - 255 and the default value is 64.
  - **Local probe request threshold**— Enter the threshold value below which incoming probe requests will get ignored. The supported range of RSSI (Received signal strength indication) values is 0-100 dB. When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID.

4. Click **Next** to continue.

**Figure 31 - Adding an Employee Network— VLAN Tab**



5. Select the required Client IP assignment option — **Virtual Controller assigned** or **Network assigned**.

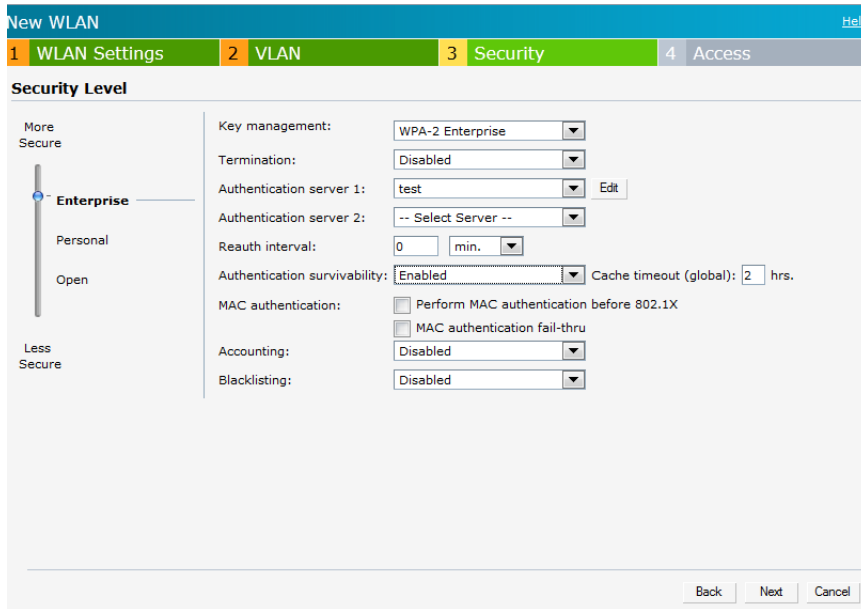
**Table 5 - Conditions for Client IP and VLAN assignment**

If you select	then
Virtual Controller assigned	<p>The client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the W-IAP for the wireless clients. The Virtual Controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi site wireless network. See <a href="#">"Virtual Controller" on page 109</a> for configuring the DHCP server.</p>
Network assigned	<p>By default, the client VLAN is assigned to the native VLAN on the wired network.</p> <ul style="list-style-type: none"> <li>• <b>Default</b>— The client obtains the IP address in the same subnet as the W-IAPs.</li> <li>• <b>Static</b>— Select to specify a single VLAN, a comma separated list of VLANs, or a range of VLANs for all clients on this network.</li> <li>• <b>Dynamic</b>— Select to create rules for per-user VLAN assignment. See <a href="#">"VLAN Derivation Rule " on page 150</a> for more information.</li> </ul> <p><b>NOTE:</b> Select the <b>Static</b> option in the <b>Client VLAN assignment</b> section to configure VLAN pooling. See <a href="#">"VLAN Pooling" on page 69</a> for additional details.</p>

6. Click **Next** to continue.

- Set the appropriate security levels using the slider in the Security tab. The default level is **Personal**. The available options are **Enterprise**, **Personal**, and **Open** which are described in the following tables.

**Figure 32 - Employee Security Tab— Enterprise**



**Table 6 - Conditions for Adding an Employee Network— Security Tab**

If	then,
<p>You select the <b>Enterprise</b> security level</p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>Select the required key options from the <b>Key management</b> drop-down list. Available options are: <ul style="list-style-type: none"> <li>WPA-2 Enterprise</li> <li>WPA Enterprise</li> <li>Both (WPA-2 &amp; WPA)</li> <li>Dynamic WEP with 802.1X</li> <li><b>Use Session Key for LEAP</b>— Use the <b>Session Key for LEAP</b> instead of using Session Key from the RADIUS Server to derive pair wise unicast keys. This is required for old printers that use dynamic WEP via LEAP authentication. This is <b>Disabled</b> by default.</li> </ul> <p>For more information on encryption and recommended encryption type, see <a href="#">"Encryption" on page 143</a>.</p> </li> <li><b>Termination</b>— Enable this option to terminate the EAP portion of 802.1X authentication on the W-IAP instead of the RADIUS server. For more information, see <a href="#">"External RADIUS Server" on page 112</a>.</li> <li><b>Authentication server 1</b>— Select the required Authentication server option from the drop-down list. Available options are: <ul style="list-style-type: none"> <li><b>New</b>— If you select this option, an</li> </ul> </li> </ol>

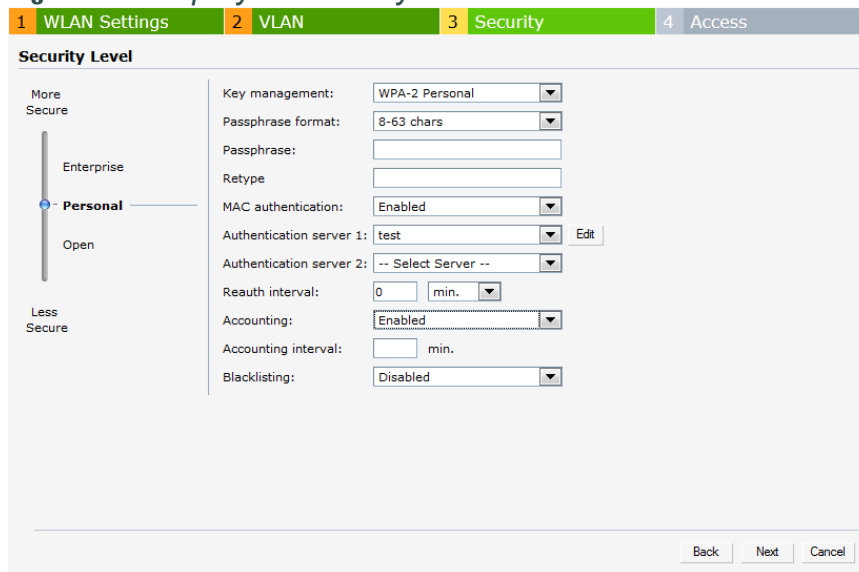
If	then,
	<p>external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see <a href="#">"Authentication" on page 111</a>.</p> <ul style="list-style-type: none"> <li>• <b>Internal Server</b>— If you select this option, users who are required to authenticate with the internal RADIUS server must be added. Click the <b>Users</b> link to add the users. For information on adding a user, see <a href="#">"Adding a User" on page 269</a>.</li> <li>4. <b>Reauth interval</b>— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.</li> <li>5. <b>Blacklisting</b>— Select <b>Enabled</b> to enable blacklisting of the clients with a specific number of authentication failures.</li> <li>6. <b>Authentication survivability</b>— This feature requires Dell PowerConnect W-ClearPass Policy Manager (6.0.2 and above) and is visible in the UI only when you select <b>New</b> to configure an external RADIUS server for authentication. If you select your RADIUS server as an internal server, then this feature is not applicable. When enabled, this feature allows W-Instant to authenticate the previously connected clients using EAP-PEAP authentication even when connectivity to Dell PowerConnect W-ClearPass Policy Manager is temporarily lost. <ul style="list-style-type: none"> <li><b>Cache timeout (global)</b>—Indicates the duration after which the authenticated credentials in the cache expire. When the cache expires, the clients are required to authenticate again. The supported range is 1 - 99 hours and the default value is 24 hours.</li> </ul> </li> <li>7. <b>MAC authentication</b> — Indicates per-user authentication using MAC address. <ul style="list-style-type: none"> <li><b>Perform MAC authentication before 802.1X</b>—Indicates per-user authentication using MAC address. This feature is optional.</li> <li><b>MAC authentication fail-thru</b>—When this option is enabled, if MAC authentication fails, 802.1X authentication will be attempted. When this option is disabled, if MAC authentication fails, no further authentication will be attempted.</li> </ul> </li> <li>8. Click <b>Upload Certificate</b> and browse to upload a certificate file for the internal server. See <a href="#">"Certificates" on page 138</a> for more information.</li> </ul>
<p>You want to use the default security level, <b>Personal</b></p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Select the required key options from the</li> </ol>



If	then,
	<p><b>Key management</b> drop-down list. Available options are:</p> <ul style="list-style-type: none"> <li>• WPA-2 Personal</li> <li>• WPA Personal</li> <li>• Both (WPA-2 &amp; WPA)</li> <li>• Static WEP— If you have selected <b>Static WEP</b>, do the following: <ul style="list-style-type: none"> <li>• Select appropriate <b>WEP key size</b> from the WEP key size drop-down list. Available options are 64-bit and 128-bit.</li> <li>• Select appropriate Tx key from the <b>Tx Key</b> drop-down list. Available options are <b>1, 2, 3, and 4</b>.</li> <li>• Enter an appropriate <b>WEP key</b> and reconfirm.</li> </ul> </li> </ul> <p>For more information on encryption and recommended encryption type, see <a href="#">"Encryption" on page 143</a>.</p> <p>2. <b>WPA-2 Personal</b>—</p> <ul style="list-style-type: none"> <li>• Select a passphrase format from the <b>Passphrase format</b> drop-down list. Available options are: <ul style="list-style-type: none"> <li>• 8-63 alphanumeric chars</li> <li>• 64 hexadecimal chars</li> </ul> </li> </ul> <p>3. Enter a passphrase in the <b>Passphrase</b> text box and reconfirm.</p> <p>4. Select the required option from the <b>MAC authentication</b> drop-down list. Available options are <b>Enabled</b> and <b>Disabled</b>. When <b>Enabled</b>, user must configure at least one RADIUS server for authentication server. See <a href="#">"MAC Authentication" on page 133</a> for further details.</p> <p>5. <b>Authentication server 1</b>— Select the required Authentication server option from the drop-down list. Available options are: <ul style="list-style-type: none"> <li>• <b>New</b>— If you select this option, an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see <a href="#">"Authentication" on page 111</a>.</li> </ul> </p> <p>6. <b>Reauth interval</b>— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.</p> <p>7. <b>Accounting</b> — When enabled, the Access Points posts accounting information as RADIUS START and RADIUS STOP accounting records to the RADIUS server.</p> <p>8. <b>Accounting interval</b> — When set to a value greater than zero, the Access Point periodically posts accounting information as RADIUS INTERIM accounting records to the RADIUS server.</p> <p>9. <b>Blacklisting</b>— Select <b>Enabled</b> to enable</p>

If	then,
	<p>blacklisting of the clients with a specific number of authentication failures.</p> <p>10. <b>Max authentication failures</b>— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.</p> <p>11. <b>Internal server</b>— If you select this option, users who are required to authenticate with the internal RADIUS server must be added. Click the <b>Users</b> link to add the users. For information on adding a user, see <a href="#">"Adding a User" on page 269</a>.</p> <p><b>NOTE:</b> Navigate to <b>PEF &gt; Blacklisting</b> in the Dell W-Series Instant UI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.</p> <p>12. Click <b>Upload Certificate</b> and browse to upload a certificate file for the internal server. See <a href="#">"Certificates" on page 138</a> for more information.</p>

**Figure 33 - Employee Security Tab— Personal**



**Table 7 - Conditions for Adding an Employee Network— Security Tab**

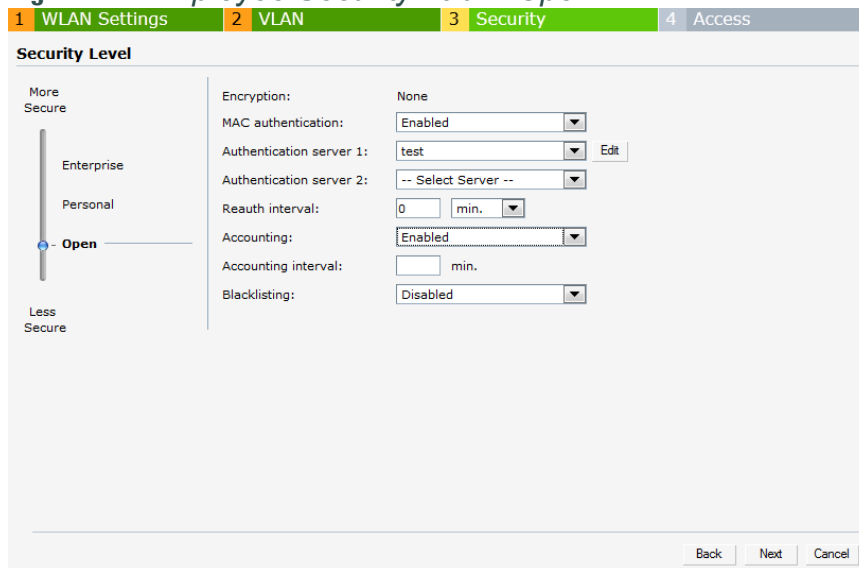
If	then,
You select the <b>Open</b> security level	<ol style="list-style-type: none"> <li>Select the required MAC authentication from the <b>MAC authentication</b> drop-down list. Available options are— Enabled and Disabled <ul style="list-style-type: none"> <li>When <b>Enabled</b>, user must configure at least one RADIUS server for authentication server. See <a href="#">"MAC Authentication" on</a></li> </ul> </li> </ol>

If

then,

- [page 133](#) for further details.
2. **Authentication server 1**— Select the required Authentication server option from the drop-down list. Available options are:
    - **New**— If you select this option, an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see "[Authentication](#)" on [page 111](#).
  3. **Reauth interval**— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.
  4. **Accounting** — When enabled, the Access Points posts accounting information as RADIUS START and RADIUS STOP accounting records to the RADIUS server.
  5. **Accounting interval** — When set to a value greater than zero, the Access Point periodically posts accounting information as RADIUS INTERIM accounting records to the RADIUS server.
  6. **Blacklisting**— Select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
  7. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.  
**NOTE:** Navigate to **PEF > Blacklisting** in the Dell W-Series Instant UI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.
  8. **Internal server**— If you select this option, users who are required to authenticate with the internal RADIUS server must be added. Click the **Users** link to add the users. For information on adding a user, see "[Adding a User](#)" on [page 269](#).
  9. Click **Upload Certificate** and browse to upload a certificate file for the internal server. See "[Certificates](#)" on [page 138](#) for more information.

**Figure 34 - Employee Security Tab— Open**



10. Click **Next** to continue.
11. Use the **Access Rules** page to specify optional access rules for this network.
12. **Network-based**— Set the slider to **Network-based** if you want the same rules to apply to all users. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. W-Instant Firewall treats packets based on the first rule matched. For more information, see ["Instant Firewall" on page 155](#).

To edit the default rule:

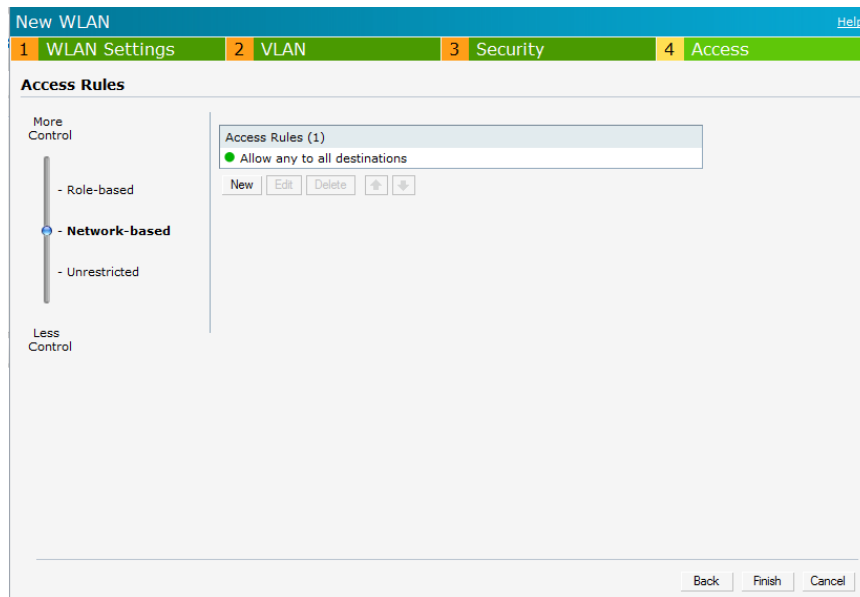
- a. Select the rule and then click **Edit**.
- b. Select appropriate options in the **Edit Rule** window and click **OK**.

To define an access rule:

- a. Click **New**.
- b. Select appropriate options in the **New Rule** window.
- c. Click **OK**.

1. **Role-based**— Select **Role-based** if you want to specify per-user access rules. See ["Creating a New User Role" on page 145](#) for more information.
  2. **Unrestricted**— Select this to set no restrictions on access based on destination or type of traffic.
13. Click **Finish**. The network is added and listed in the **Networks** tab.

**Figure 35 - Adding an Employee Network— Access Rules Tab**



14. Click **Finish**. The network is added and listed in the **Networks** tab.

## Voice Network

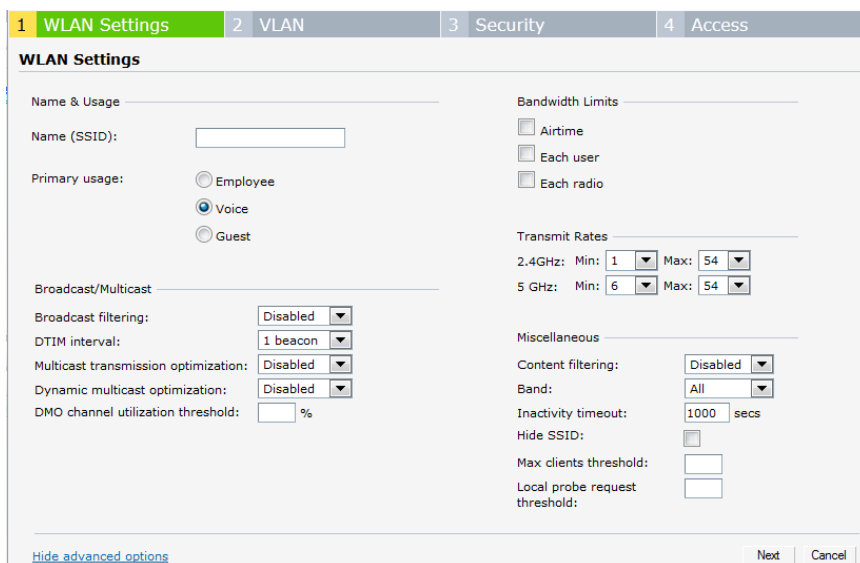
Use the Voice network type when you want devices that provide only voice services like handsets or only applications that require voice-like prioritization need connectivity.

### Adding a Voice Network

This section provides the procedure to add a voice network.

1. In the **Networks** tab, click the **New** link. The **New WLAN** window appears.

**Figure 36 - Adding a Voice Network— WLAN Settings Tab**



2. In the **WLAN Settings** tab, perform the following steps:
  - a. **Name (SSID)**— Enter a name that uniquely identifies a wireless network.

- b. **Primary usage**— Select **Voice** from the **Primary usage** options. This selection determines whether the network is primarily intended to be used for employee data, guest data, or voice traffic.
3. Click the **Show advanced options** link and perform the following steps.
    - a. **Broadcast/Multicast**
      - **Broadcast filtering**— When set to **All**, the W-IAP drops all broadcast and multicast frames except for DHCP and ARP. When set to **ARP**, in addition to the above, the W-IAP converts ARP requests to unicast and send frames directly to the associated client. When **Disabled**, all broadcast and multicast traffic is forwarded.
      - **DTIM interval**— Indicates the DTIM (delivery traffic indication message) period in beacons. You can configure this option for every WLAN SSID profile. The default value is 1, which means the client checks for buffered data on the W-IAP at every beacon. You may choose to configure a larger DTIM value for power saving.
      - **Multicast transmission optimization**— When **Enabled**, the W-IAP chooses the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. The default values are 1 Mbps for 2.4 GHz and 6 Mbps for 5.0 GHz bands. Multicast traffic can be sent at up to 24 Mbps when this option is enabled. This option is disabled by default.
      - **Dynamic multicast optimization**— When **Enabled**, the W-IAP converts multicast streams into unicast streams over the wireless link. DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to non-video clients.
      - **DMO channel utilization threshold**— When dynamic multicast optimization is enabled, the W-IAP converts multicast streams into multicast unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90 and the maximum threshold value is 100%.

If the threshold value exceeds the maximum value, then the W-IAP sends multicast traffic over the wireless link.

- b. **Bandwidth Limits**— You can specify three types of bandwidth limits.
  - **Airtime**— Indicates the aggregate amount of airtime that all clients on this Network can use to send/receive data.
  - **Each user**— Indicates the throughput for any single user on this Network. The throughput value is specified in kbps.
  - **Each radio**— Indicates the aggregate amount of throughput each radio (some AP models have multiple radios) is allowed to provide for all clients connected to that radio
- c. **Transmit Rates**— Indicates the ability to configure the basic and supported rates per SSID for Dell W-Instant. Select to set the minimum and maximum legacy (non-802.11n) transmit rates for each band — 2.4 GHz and 5 GHz.
- d. **Miscellaneous**
  - **Content filtering**— When enabled, all DNS requests to non-corporate domains on this wireless network are sent to OpenDNS.
  - **Band**— Set the band at which the network transmits radio signals. Available options are 2.4 GHz, 5 GHz and All. The All option is selected by default. It is also the recommended option.
  - **Inactivity timeout**— Indicates the time in seconds after which an idle client ages out. The minimum value is 60 seconds and the default value is 1000 seconds.

- Hide SSID— Select this check box if you do not want the SSID (network name) to be visible to users.



**NOTE:** The Airtime Fairness and Bandwidth limits do not apply for voice traffic.

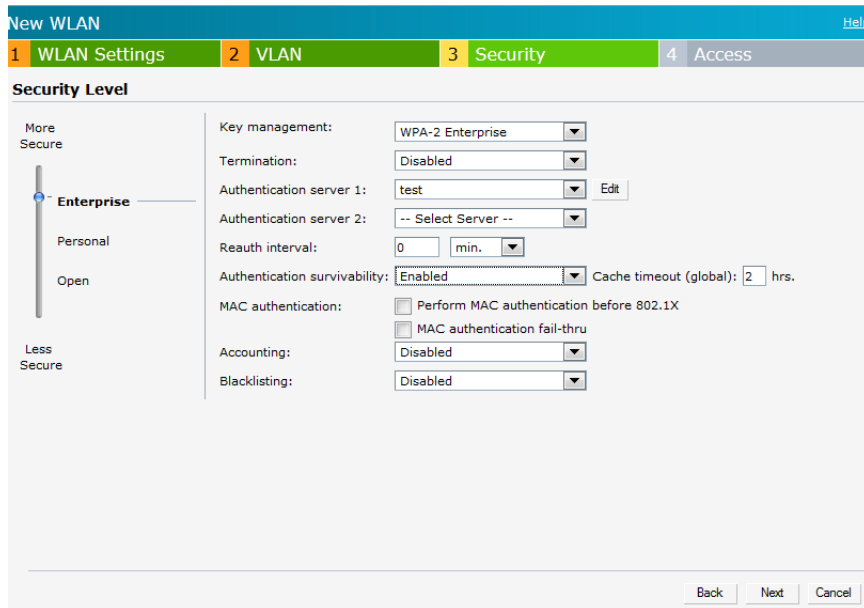
4. Click **Next** to continue.
5. Select the required Client IP assignment option— **Virtual Controller assigned** and **Network assigned**.

**Table 8 - Conditions for Client IP and VLAN Assignment**

If you select	then
Virtual Controller assigned	<p>The client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the W-IAP for the wireless clients. The Virtual Controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi site wireless network. See <a href="#">"Virtual Controller" on page 109</a> for configuring the DHCP server.</p>
Network assigned	<p>By default, the client VLAN is assigned to the native VLAN on the wired network.</p> <ul style="list-style-type: none"> <li>• <b>Default</b>— The client obtains the IP address in the same subnet as the W-IAPs.</li> <li>• <b>Static</b>— Select to specify a single VLAN, a comma separated list of VLANs, or a range of VLANs for all clients on this network.</li> <li>• <b>Dynamic</b>— Select to create rules for per-user VLAN assignment. See <a href="#">"VLAN Derivation Rule " on page 150</a> for more information.</li> </ul> <p><b>NOTE:</b> Select the <b>Static</b> option in <b>Client VLAN assignment</b> section to configure VLAN pooling. See <a href="#">"VLAN Pooling" on page 69</a> for additional details.</p>

6. Click **Next** to continue.
7. Slide and select the appropriate security levels in the **Security** tab. The default level is **Personal**. The available options are **Enterprise**, **Personal**, and **Open** which are described in the following tables.

**Figure 37 - Voice Security Tab— Enterprise**



**Table 9 - Conditions for Adding a Voice Network— Security Tab**

If	then,
<p>You select the <b>Enterprise</b> security level</p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Select the required key options from the <b>Key management</b> drop-down list. Available options are: <ul style="list-style-type: none"> <li>• WPA-2 Enterprise</li> <li>• WPA Enterprise</li> <li>• Both (WPA-2 &amp; WPA)</li> <li>• Dynamic WEP with 802.1X</li> <li>• <b>Use Session Key for LEAP:</b> Use the <b>Session Key for LEAP</b> instead of using Session Key from the RADIUS Server to derive pair wise unicast keys. This is required for old printers that use dynamic WEP via LEAP authentication. This is <b>Disabled</b> by default.</li> </ul> <p>For more information on encryption and recommended encryption type, see <a href="#">"Encryption" on page 143</a>.</p> </li> <li>2. <b>Termination</b>— Enable this option to terminate the EAP portion of 802.1X authentication on the W-IAP instead of the RADIUS server. For more information, see <a href="#">"External RADIUS Server" on page 112</a>.</li> <li>3. <b>Authentication server 1 and 2</b>— Select the required Authentication server option from the drop-down list. Available options are: <ul style="list-style-type: none"> <li>• <b>New</b>— If you select this option, then an external RADIUS server has to be configured to authenticate the users. For</li> </ul> </li> </ol>



If	then,
	<p>information on configuring an external RADIUS server, see <a href="#">"Authentication" on page 111</a>.</p> <ol style="list-style-type: none"> <li>4. <b>Reauth interval</b>— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.</li> <li>5. <b>Blacklisting</b>— Select <b>Enabled</b> to enable blacklisting of the clients with a specific number of authentication failures.</li> <li>6. <b>Max authentication failures</b>— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.</li> </ol> <p><b>NOTE:</b> Navigate to <b>PEF &gt; Blacklisting</b> in the Dell W-Series Instant UI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.</p>
<p>You want to use the default security level, <b>Personal</b></p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Select the required key options from the <b>Key management</b> drop-down list. Available options are: <ul style="list-style-type: none"> <li>• WPA-2 Personal</li> <li>• WPA Personal</li> <li>• Both (WPA-2 &amp; WPA)</li> </ul> </li> <li>2. <b>Static WEP</b>— If you have selected <b>Static WEP</b>, then do the following: <ul style="list-style-type: none"> <li>• Select appropriate <b>WEP key size</b> from the WEP key size drop-down list. Available options are 64-bit and 128-bit.</li> <li>• Select appropriate Tx key from the <b>Tx Key</b> drop-down list. Available options are 1, 2, 3, and 4.</li> <li>• Enter an appropriate WEP key and reconfirm.</li> </ul> <p>For more information on encryption and recommended encryption type, see <a href="#">"Encryption" on page 143</a>.</p> </li> <li>3. <b>WPA-2 Personal</b>— Select a passphrase format from the <b>Passphrase format</b> drop-down list. Available options are: <ul style="list-style-type: none"> <li>• 8-63 alphanumeric chars</li> <li>• 64 hexadecimal chars</li> </ul> </li> <li>4. Enter a passphrase in the Passphrase text box and reconfirm.</li> <li>5. Select the required option from the MAC authentication drop-down list. Available options are: Enabled and Disabled. When <b>Enabled</b>, user must configure at least one RADIUS server for authentication server. See <a href="#">"MAC Authentication" on page 133</a> for further details.</li> <li>6. <b>Authentication server 1</b>— Select the required Authentication server option from</li> </ol>

If	then,
	<p>the drop-down list. Available options are:</p> <ul style="list-style-type: none"> <li>• <b>New</b>— If you select this option, then an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see <a href="#">"Authentication" on page 111</a>.</li> </ul> <ol style="list-style-type: none"> <li>7. <b>Reauth interval</b>— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.</li> <li>8. <b>Accounting</b> — When enabled, the Access Points posts accounting information as RADIUS START and RADIUS STOP accounting records to the RADIUS server.</li> <li>9. <b>Accounting interval</b> — When set to a value greater than zero, the Access Point periodically posts accounting information as RADIUS INTERIM accounting records to the RADIUS server.</li> <li>10. <b>Blacklisting</b>— Select <b>Enabled</b> to enable blacklisting of the clients with a specific number of authentication failures.</li> <li>11. <b>Max authentication failures</b>— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.</li> </ol> <p><b>NOTE:</b> Navigate to <b>PEF &gt; Blacklisting</b> in the Dell W-Series Instant UI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.</p> <ol style="list-style-type: none"> <li>12. <b>InternalServer</b>— If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the <b>Users</b> link to add the users. For information on adding a user, see <a href="#">"Adding a User" on page 269</a>.</li> <li>13. Click <b>Upload Certificate</b> and browse to upload a certificate file for the internal server. See <a href="#">"Certificates" on page 138</a> for more information.</li> </ol>
<p>You select the <b>Open</b> security level</p>	<ol style="list-style-type: none"> <li>1. Select the required MAC authentication from the <b>MAC authentication</b> drop-down list. Available options are— Enabled and Disabled. <ul style="list-style-type: none"> <li>• When <b>Enabled</b>, user must configure at least one RADIUS server for authentication server. See <a href="#">"MAC Authentication" on page 133</a> for further details.</li> </ul> </li> <li>2. <b>Authentication server 1</b>— Select the required Authentication server option from the drop-down list. Available options are: <ul style="list-style-type: none"> <li>• <b>New</b>— If you select this option, then an external RADIUS server has to be configured to authenticate the users. For information on configuring an external</li> </ul> </li> </ol>

If	then,
	<p>RADIUS server, see <a href="#">"Authentication" on page 111</a>.</p> <ol style="list-style-type: none"> <li>3. <b>Reauth interval</b>— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.</li> <li>4. <b>Accounting</b> — When enabled, the Access Points posts accounting information as RADIUS START and RADIUS STOP accounting records to the RADIUS server.</li> <li>5. <b>Accounting interval</b> — When set to a value greater than zero, the Access Point periodically posts accounting information as RADIUS INTERIM accounting records to the RADIUS server.</li> <li>6. <b>Blacklisting</b>— Select <b>Enabled</b> to enable blacklisting of the clients with a specific number of authentication failures.</li> <li>7. <b>Max authentication failures</b>— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.</li> </ol> <p><b>NOTE:</b> Navigate to <b>PEF &gt; Blacklisting</b> in the Dell W-Series Instant UI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.</p> <ol style="list-style-type: none"> <li>8. <b>InternalServer</b>— If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the Users link to add the users. For information on adding a user, see <a href="#">"Adding a User" on page 269</a>.</li> <li>9. Click <b>Upload Certificate</b> and browse to upload a certificate file for the internal server. See <a href="#">"Certificates" on page 138</a> for more information.</li> </ol>

10. Click **Next** to continue.

11. Use the Access Rules page to specify optional access rules for this network.

- **Network-based**— Set the slider to **Network-based** if you want the same rules to apply to all users. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. Instant Firewall treats packets based on the first rule matched. For more information, see ["Instant Firewall" on page 155](#).

To edit the default rule:

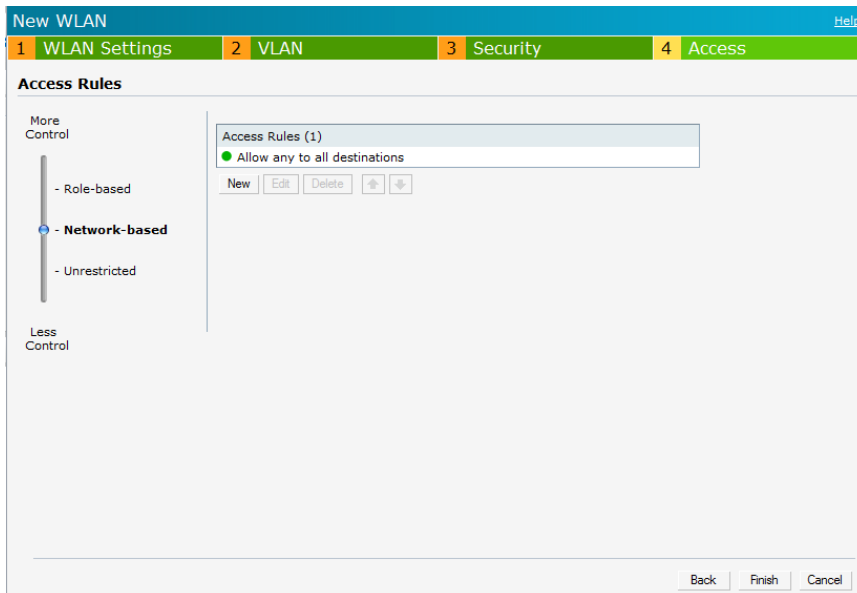
- a. Select the rule and then click **Edit**.
- b. Select appropriate options in the **Edit Rule** window and click **OK**.

To define an access rule:

- a. Click **New**.
- b. Select appropriate options in the **New Rule** window.
- c. Click **OK**.

- **Role-based**— Select **Role-based** if you want to specify per-user access rules. See "[Creating a New User Role](#)" on page 145 for more information.
- **Unrestricted**— Select this to set no restrictions on access based on destination or type of traffic.

**Figure 38 - Adding a Voice Network— Access Rules Tab**



12. Click **Finish**. The network is added and listed in the **Networks** tab.

## Guest Network

The Guest wireless network is created for guests, visitors, contractors, and any non-employee users who use the enterprise Wi-Fi network. The Virtual Controller assigns the IP address for the guest clients. Captive portal or passphrase based authentication methods can be set for this wireless network. Typically, a guest network is an un-encrypted network. However, you can specify encryption settings in the **Security** tab.

### Adding a Guest Network

This section provides the procedure to add a guest network.

**Figure 39 - Adding a Guest Network— WLAN Settings Tab**

**WLAN Settings**

**Name & Usage**

Name (SSID):

Primary usage:

Employee

Voice

Guest

**Broadcast/Multicast**

Broadcast filtering:

DTIM interval:

Multicast transmission optimization:

Dynamic multicast optimization:

DMO channel utilization threshold:  %

**Bandwidth Limits**

Airtime

Each user

Each radio

**Transmit Rates**

2.4GHz: Min:  Max:

5 GHz: Min:  Max:

**Miscellaneous**

Content filtering:

Band:

Inactivity timeout:  secs

Hide SSID:

Max clients threshold:

Local probe request threshold:

[Hide advanced options](#)

1. In the **Networks** tab, click the **New** link. The **WLAN Settings** window appears.
2. In the **WLAN Settings** tab, perform the following steps:
  - a. **Name (SSID)**— Enter a name that uniquely identifies a wireless network.
  - b. **Primary usage**— Select **Guest** from the **Primary usage** options. This selection determines whether the network is primarily intended to be used for employee data, guest data, or voice traffic.
3. Click the **Show advanced options** link and perform the following steps.
  - a. **Broadcast/Multicast**
    - **Broadcast filtering**— When set to **All**, the W-IAP drops all broadcast and multicast frames except for DHCP and ARP. When set to **ARP**, in addition to the above, the W-IAP converts ARP requests to unicast and send frames directly to the associated client. When **Disabled**, all broadcast and multicast traffic is forwarded.
    - **DTIM interval**— Indicates the DTIM (delivery traffic indication message) period in beacons. You can configure this option for every WLAN SSID profile. The default value is 1, which means the client checks for buffered data on the W-IAP at every beacon. You may choose to configure a larger DTIM value for power saving.
    - **Multicast transmission optimization**— When **Enabled**, the W-IAP chooses the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. The default values are 1 Mbps for 2.4 GHz and 6 Mbps for 5.0 GHz bands. Multicast traffic can be sent at up to 24 Mbps when this option is enabled. This option is disabled by default.
    - **Dynamic multicast optimization**— When **Enabled**, the W-IAP converts multicast streams into unicast streams over the wireless link. DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to non-video clients.
    - **DMO channel utilization threshold**— When dynamic multicast optimization is enabled, the W-IAP converts multicast streams into multicast unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90 and the maximum threshold value is 100%.

If the threshold value exceeds the maximum value, then the W-IAP sends multicast traffic over the wireless link.

- b. **Bandwidth Limits**— You can specify three types of bandwidth limits.
    - **Airtime**— Indicates the aggregate amount of airtime that all clients on this Network can use to send/receive data.
    - **Each user**— Indicates the throughput for any single user on this Network. The throughput value is specified in kbps.
    - **Each radio**— Indicates the aggregate amount of throughput each radio (some AP models have multiple radios) is allowed to provide for all clients connected to that radio
  - c. **Transmit Rates**— Indicates the ability to configure the basic and supported rates per SSID for Dell W-Instant. Select to set the minimum and maximum legacy (non-802.11n) transmit rates for each band — 2.4 GHz and 5 GHz.
  - d. **Miscellaneous**
    - **Content filtering**— When enabled, all DNS requests to non-corporate domains on this wireless network are sent to OpenDNS.
    - **Band**— Set the band at which the network transmits radio signals. Available options are 2.4 GHz, 5 GHz and All. The All option is selected by default. It is also the recommended option.
    - **Inactivity timeout**— Indicates the time in seconds after which an idle client ages out. The minimum value is 60 seconds and the default value is 1000 seconds.
    - **Hide SSID**— Select this check box to hide the SSID (network name).
4. Click **Next** to continue.
  5. Select the required Client IP assignment option — **Virtual Controller assigned** or **Network assigned**.

**Table 10 - Conditions for Client IP and VLAN assignment**

If you select	then
Virtual Controller assigned	<p>The client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the W-IAP for the wireless clients. The Virtual Controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi site wireless network. See <a href="#">"Virtual Controller" on page 109</a> for configuring the DHCP server.</p>
Network assigned	<p>By default, the client VLAN is assigned to the native VLAN on the wired network.</p> <ul style="list-style-type: none"> <li>• <b>Default</b>— The client obtains the IP address in the same subnet as the W-IAPs.</li> <li>• <b>Static</b>— Select to specify a single VLAN, a comma separated list of VLANs, or a range of VLANs for all clients on this network.</li> <li>• <b>Dynamic</b>— Select to create rules for per-user VLAN assignment. See <a href="#">"User VLAN Derivation" on page 149</a> for more information.</li> </ul>

If you select	then
	<p><b>NOTE:</b> Select the <b>Static</b> option in <b>Client VLAN assignment</b> section to configure VLAN pooling. See <a href="#">"VLAN Pooling"</a> on page 69 for additional details.</p>

6. Click **Next** to continue.
7. This tab allows you to configure the captive portal page and encryption for the Guest network. Select one of the following splash page types:

**Table 11 - Conditions for Adding a Guest Network— Security Tab**

Splash Page Type	Description and steps to set up
Internal — Authenticated	<p>The user has to accept the terms and conditions and enter a username and password on the captive portal page. If this option is selected, then add the users who are required to use the captive portal authentication to the user database. Click the <b>Users</b> link to add the users. For information about adding a user, see <a href="#">"Adding a User"</a> on page 269. For information on customizing the splash page, see <a href="#">"Customizing a Splash Page"</a> on page 125.</p> <ol style="list-style-type: none"> <li>1. Select the required Authentication server 1 option from the drop-down list. Available options are: <ul style="list-style-type: none"> <li>• <b>New</b> — If you select this option, then an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see <a href="#">"Configuring an External RADIUS Server"</a> on page 113.</li> <li>• <b>Internal Server</b> — If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the <b>Users</b> link to add the users. For information on adding a user, see <a href="#">"Adding a User"</a> on page 269.</li> </ul> </li> <li>2. <b>Reauth interval</b> — When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.</li> <li>3. <b>Blacklisting</b> — Select <b>Enabled</b> to enable blacklisting of the clients with a specific number of authentication failures.</li> <li>4. <b>Max authentication failures</b> — Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.</li> <li>5. <b>For Internal users</b> — Click <b>Users</b> to populate the system's internal authentication server with users. For information about adding a user, see <a href="#">"Adding a User"</a> on page 269.</li> </ol>

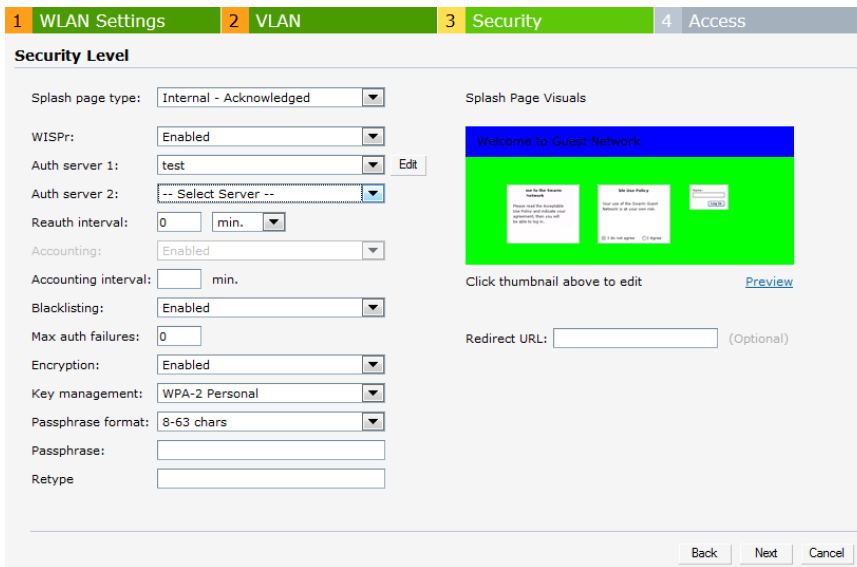
Splash Page Type	Description and steps to set up
	<ol style="list-style-type: none"> <li>6. Click <b>Upload Certificate</b> and browse to upload a certificate file for the internal server. See <a href="#">"Certificates" on page 138</a> for more information.</li> <li>7. <b>Redirect URL</b>— Users can be redirected to a specific URL (instead of the original URL) after successful captive portal authentication. This entry is optional.</li> </ol>
Internal — Acknowledged	<p>The user has to accept the terms and conditions for this splash page type. For information on customizing the splash page, see <a href="#">"Customizing a Splash Page" on page 125</a>.</p> <ol style="list-style-type: none"> <li>1. <b>Encryption</b> —Select Enabled from the Encryption drop-down list and perform the following steps (these steps are optional): <ol style="list-style-type: none"> <li>a. Select the required key management option from the Key management drop-down list. Available options are: <ul style="list-style-type: none"> <li>• WPA-2 Personal</li> <li>• WPA Personal</li> <li>• Both (WPA-2 &amp; WPA)</li> </ul> </li> </ol> </li> <li>2. <b>Passphrase format</b>— Specify either an alphanumeric or a hexadecimal string. Ensure that the hexadecimal string must be exactly 64 digits in length.</li> <li>3. <b>Passphrase</b>— Enter a pre-shared key (PSK) passphrase.</li> </ol>
External - RADIUS Server	<p>An external server is used to display the splash page to the user. If this option is selected, then do the following:</p> <p><b>External splash page</b></p> <ul style="list-style-type: none"> <li>• <b>IP or hostname</b>— Enter the IP or hostname of the external server in the IP or hostname text box.</li> <li>• <b>URL</b>— Enter the URL of the captive portal page in the URL text box.</li> <li>• <b>Port</b>— Enter the number of the port to be used for communicating with the external server in the Port text box.</li> </ul> <ol style="list-style-type: none"> <li>4. <b>Redirect URL</b>— By default, after entering the requested info at the splash page, the user is redirected to the URL that was originally requested. Specify a redirect URL if you want to override the user's original request and redirect them to another URL.</li> <li>5. <b>Auth server 1</b>— Select the required Authentication server 1 option from the drop-down list. Available options are: <ul style="list-style-type: none"> <li>• <b>New</b>— If you select this option, then an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see <a href="#">"Configuring an External RADIUS Server" on page 113</a>.</li> </ul> </li> </ol>



Splash Page Type	Description and steps to set up
	<ol style="list-style-type: none"> <li>6. <b>Reauth interval</b>— When set to a value greater than zero, the Access Points periodically reauthenticates all associated and authenticated clients.</li> <li>7. <b>Accounting</b> — When enabled, the Access Points posts accounting information as RADIUS START and RADIUS STOP accounting records to the RADIUS server.</li> <li>8. <b>Accounting interval</b> — When set to a value greater than zero, the Access Point periodically posts accounting information as RADIUS INTERIM accounting records to the RADIUS server.</li> <li>9. <b>Blacklisting</b>— Select <b>Enabled</b> to enable blacklisting of the clients with a specific number of authentication failures.</li> <li>10. <b>Max authentication failures</b>— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.</li> <li>11. <b>Walled Garden</b>— The walled garden directs the user’s navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see <a href="#">"Walled Garden Access" on page 134</a>.</li> </ol>
External - Authentication Text	<p>An external splash page returns a specified string to indicate successful authentication.</p> <ul style="list-style-type: none"> <li>• <b>IP or hostname</b>— Enter the IP or hostname of the external server in the IP or hostname text box.</li> <li>• <b>URL</b>— Enter the URL of the captive portal page in the URL text box.</li> <li>• <b>Port</b>— Enter the number of the port to be used for communicating with the external server in the Port text box.</li> <li>• <b>Auth text</b> — Indicates the text string returned by the external server after a successful authentication.</li> <li>• <b>Redirect URL</b>— Specify a redirect URL if you want to override the user's original request and redirect them to another URL. By default, after entering the requested info at the splash page, the user is redirected to the URL that was originally requested.</li> </ul> <ol style="list-style-type: none"> <li>1. <b>Reauth interval</b>— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.</li> <li>2. <b>Blacklisting</b>— Select <b>Enabled</b> to enable blacklisting of the clients with a specific number of authentication failures.</li> <li>3. <b>Max authentication failures</b>— Users who fail to authenticate the number of times specified here are dynamically</li> </ol>

Splash Page Type	Description and steps to set up
	blacklisted. The maximum value for this entry is 10. 4. <b>Walled Garden</b> — The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see " <a href="#">Walled Garden Access</a> " on page 134.
None	Select this option if you do not want to set the captive portal authentication.

**Figure 40- Adding a Guest Network — Splash Page Settings**



Select **Enabled** from the **Encryption** drop-down list and perform the following steps (these steps are optional):

- a. Select the required key management option from the **Key management** drop-down list. Available options are:
  - WPA-2 Personal
  - WPA Personal
  - Both (WPA-2 & WPA)
- b. **Passphrase format** — Specify either an alphanumeric or a hexadecimal string. Ensure that the hexadecimal string must be exactly 64 digits in length.
- c. **Passphrase** — Enter a pre-shared key (PSK) passphrase.

**Figure 41 - Configuring a Splash Page — Encryption Settings**

1 WLAN Settings   2 VLAN   3 Security   4 Access

### Security Level

Splash page type:

WISPr:

Auth server 1:

Auth server 2:

Reauth interval:  min.

Accounting:

Accounting interval:  min.

Blacklisting:

Max auth failures:

Encryption:


Key management:

Passphrase format:

Passphrase:

Retype:

### Splash Page Visuals



Click thumbnail above to edit [Preview](#)

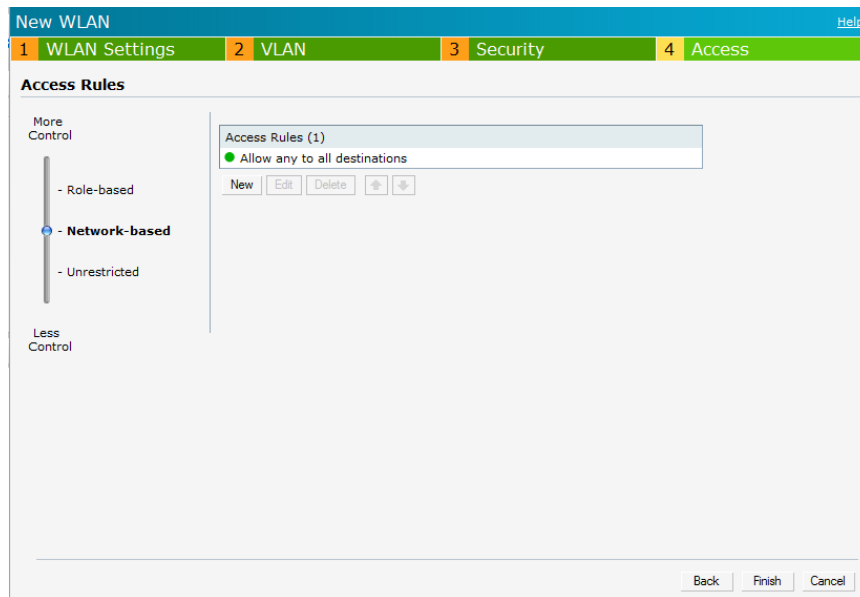
Redirect URL:  (Optional)



**NOTE:** You can customize the captive portal page using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters. Click on the banner, term, or policy in the **Splash Page Visuals** to modify the text in the red box. These fields accept double-byte characters or a combination of English and double-byte characters.

5. Use the Access Rules page to specify optional access rules for this network.
  - **Network-based**— Set the slider **Network-based** if you want the same rules to apply to all users. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. W-Instant Firewall treats packets based on the first rule matched. For more information, see "[Instant Firewall](#)" on page 155.To edit the default rule:
  - a. Select the rule and then click **Edit**.
  - b. Select appropriate options in the **Edit Rule** window and click **OK**.To define an access rule:
  - a. Click **New**.
  - b. Select appropriate options in the **New Rule** window.
  - c. Click **OK**.
  - **Role-based**— Select **Role-based** if you want to specify per-user access rules. See "[Creating a New User Role](#)" on page 145 for more information.
  - **Unrestricted**— Select this to set no restrictions on access based on destination or type of traffic.

**Figure 42 - Adding a Guest Network — Access Rules Tab**



6. Click **Finish**. The network is added and listed in the **Networks** tab.

## Editing a Network

To edit a network:

1. In the **Networks** tab, select the network that you want to edit. The edit link appears.
2. Click the **edit** link. The **Edit network** window appears.
3. Make the required changes in any of the tabs. Click **Next** or the tab name to move to the next tab.
4. Click **Finish**.

## Deleting a Network

To delete a network:

1. In the **Networks** tab, click the network which you want to delete. A **x** link appears against the network to be deleted.
2. Click **x**. A delete confirmation window appears.
3. Click **Delete Now**.

## Number of WLAN SSIDs Supported

By default, you can create up to six networks or WLANs. You can enable the Extended SSID option and create up to 16 WLANs. W-IAP175P, W-IAP104, and W-IAP105 devices support up to 8 SSIDs and W-IAP3WNP, W-IAP92, W-IAP93, W-IAP134, and W-IAP135 devices support up to 16 SSIDs. After you enable this option, the number of SSIDs that become active on each W-IAP depends on the W-IAP platform.



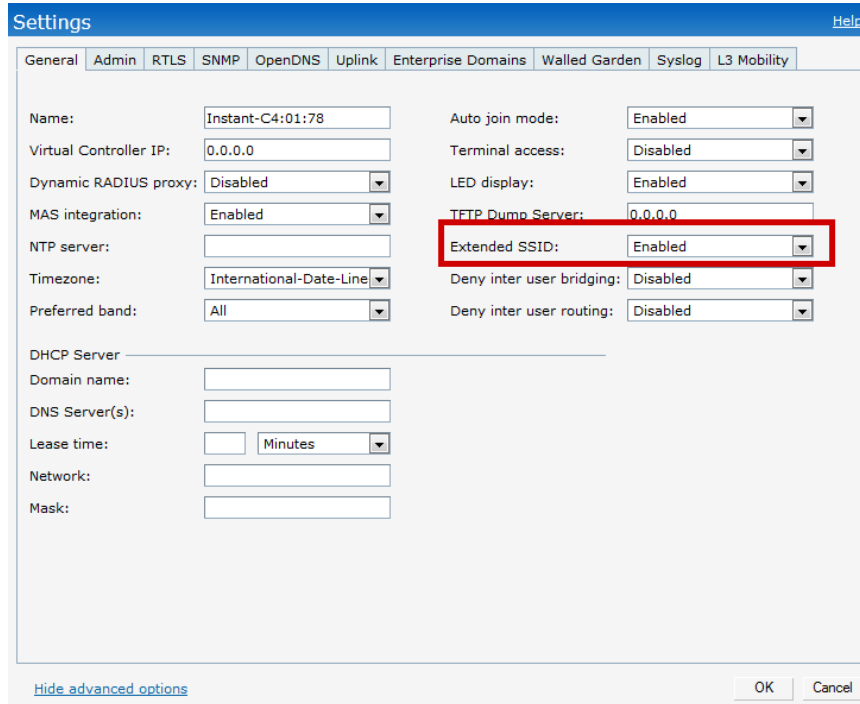
**NOTE:** Enabling the Extended SSID option disables mesh.

## Enabling the Extended SSID Option

To enable the extended SSID option:

1. Click the **Settings** link at the upper right corner of the Dell W-Series Instant UI.
2. Click the **Show advanced options** link.
3. In the **General** tab, select **Enabled** from the **Extended SSID** drop-down list.
4. Click **OK**.
5. Reboot the AP for the changes to take effect.  
After you enable the option and reboot, the Wi-Fi link and mesh are disabled automatically.

**Figure 43 - Enabling Extended SSID**



The screenshot shows the 'Settings' window for a Dell W-Series Instant Access Point. The 'General' tab is selected. The 'Extended SSID' dropdown menu is highlighted with a red box and is set to 'Enabled'. Other settings include: Name: Instant-C4:01:78, Virtual Controller IP: 0.0.0.0, Dynamic RADIUS proxy: Disabled, MAS integration: Enabled, NTP server: (empty), Timezone: International-Date-Line, Preferred band: All, Auto join mode: Enabled, Terminal access: Disabled, LED display: Enabled, TFTP Dump Server: 0.0.0.0, Deny inter user bridging: Disabled, Deny inter user routing: Disabled. The DHCP Server section is also visible with fields for Domain name, DNS Server(s), Lease time, Network, and Mask.

## VLAN Pooling

In a single W-IAP cluster, there can be a large number of clients in the same VLAN. This leads to a high level of broadcasts in the same subnet. The solution to this is to partition the network into reasonably-sized subnets and use L3-mobility between those subnets, when clients roam. However, there are various situations, like simple network design considerations, where a large number of clients need to be in the same subnet. VLAN pooling provides a solution in such scenarios. Each client is randomly assigned a VLAN from a pool of VLANs on the same SSID, thereby automatically partitioning a single broadcast domain of clients into multiple VLANs.



# Chapter 5

## Managing W-IAPs

This section describes the Preferred band, Auto join mode, Terminal Access, LED display, and Syslog server features in Dell W-Instant. In addition, this section provides procedures for adding and removing W-IAPs, editing the W-IAP settings, and upgrading the firmware on the W-IAP using the Dell W-Series Instant UI.

### Preferred Band

At the top right corner of Dell W-Series Instant UI, click the **Settings** link. The **Settings** window appears.

1. In the **Settings** window, click the **General** tab.
2. Select the **Preferred band** (2.4 GHz, 5 GHz, All) from the drop-down list for single-radio access points.



---

**NOTE:** Reboot the W-IAP after configuring the radio profile settings in order for the changes to take effect.

---

### Auto Join Mode

The Auto Join Mode feature allows W-IAPs to automatically,

1. Discover the Virtual Controller.
2. Join the network.
3. Begin functioning.

The **Auto Join Mode** feature is enabled by default. When the Auto Join Mode feature is disabled, a **New** link appears in the **Access Points** tab. Click this link to add W-IAPs to the network. For more information, see "[Adding a W-IAP to the Network](#)" on page 74. In addition, when this feature is disabled, W-IAPs that are configured but not active appear in red.

### Disabling Auto Join Mode

To disable Auto Join Mode:

At the top right corner of Dell W-Series Instant UI, click the **Settings** link. The **Settings** window appears.

1. In the **Settings** window, click the **General** tab.
2. Select **Disabled** from the **Auto join mode** drop-down list.

Figure 44 - Disabling Auto Join Mode

The screenshot shows the 'Settings' page with the 'General' tab selected. The 'Auto join mode' is set to 'Enabled'. Other settings include: Name: Instant-C4:01:78, Virtual Controller IP: 0.0.0.0, Dynamic RADIUS proxy: Disabled, MAS integration: Enabled, NTP server: (empty), Timezone: International-Date-Line, Preferred band: All, Terminal access: Disabled, LED display: Enabled, TFTP Dump Server: 0.0.0.0, Extended SSID: Disabled, Deny inter user bridging: Disabled, Deny local routing: Disabled. The DHCP Server section includes: Domain name: (empty), DNS Server(s): (empty), Lease time: (empty) Minutes, Network: (empty), Mask: (empty). At the bottom, there are 'OK' and 'Cancel' buttons, and a link for 'Hide advanced options'.

3. Click OK.

## Terminal Access

Instant supports terminal access for diagnostic purpose only. To enable or disable the SSH access to the W-IAPs CLI, navigate to **Settings > Advanced > Terminal access**.



**NOTE:** Telnet access to the CLI has been deprecated as of the 6.2.0.0-3.2.0.0 release. As of that release, when the Terminal Access option is enabled, only SSH access to the CLI will be possible.



**NOTE:** W-Instant does not support configuration using CLI.

## LED Display

Administrators have the ability to turn off LED for all W-IAPs in an Instant network. Navigate to **Settings > Advanced > LED Display** to enable or disable the LEDs. When **Disabled**, all the LEDs are turned off. Use this option in environments where LEDs can be a distraction.



**NOTE:** The LED display is always in **Enabled** mode while rebooting the W-IAP.

## TFTP Dump Server

Enter the IP address of a TFTP server to store core dump files.



## Extended SSID

You can increase the number of SSIDs or networks that can be created by enabling the extended SSID option. To enable this feature, navigate to **Settings > General** and click **Show advanced options** in the Dell W-Series Instant UI.

## Deny Inter User Bridging and Deny Local Routing

To enable or disable these features, navigate to **Settings > General** in the Dell W-Series Instant UI.

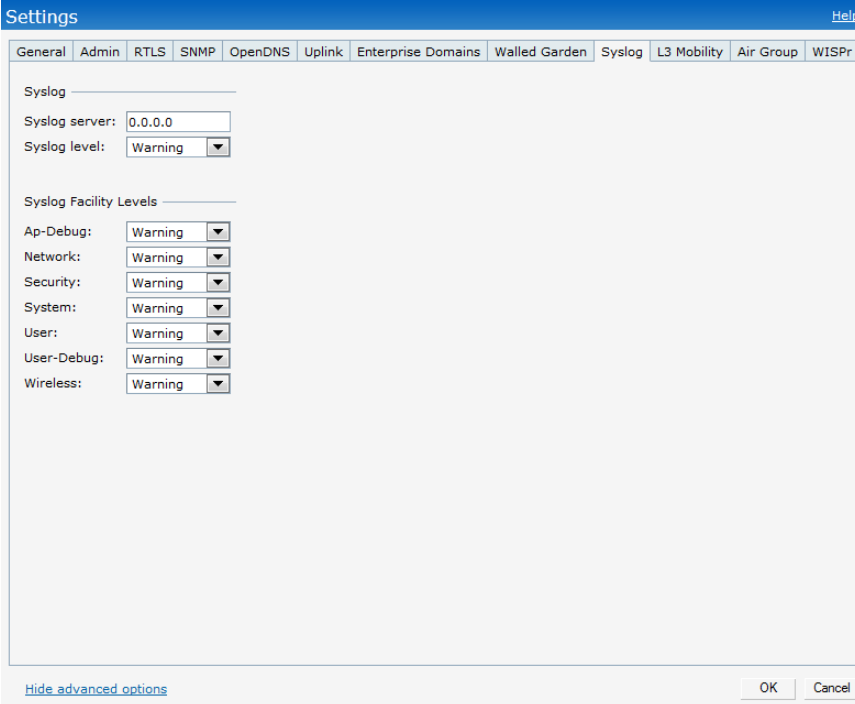
- **Deny inter user bridging**— This feature allows you to deny traffic between two clients which are directly connected to the same W-IAP or are on the same Instant network.
- **Deny local routing**— This feature allows you to deny local routing traffic between clients which are connected to the same W-IAP or are on the same Instant network.

## Syslog Server

To specify a Syslog Server for sending syslog messages to the external servers, navigate to **Settings > click Show advanced options > Syslog Server** in the Dell W-Series Instant UI and update the following fields.

- **Syslog server**— Enter the IP address of the server to send system logs to.
- **Syslog level**— For a global level configuration, select one of the logging levels from the standard list of syslog levels. The default value is **Notice**.

**Figure 45 - Syslog Server**



The screenshot shows the 'Settings' window with the 'Syslog' tab selected. The 'Syslog server' field is set to '0.0.0.0' and the 'Syslog level' is set to 'Warning'. Below this, the 'Syslog Facility Levels' section contains several dropdown menus, all set to 'Warning': Ap-Debug, Network, Security, System, User, User-Debug, and Wireless. At the bottom left, there is a link for 'Hide advanced options', and at the bottom right, there are 'OK' and 'Cancel' buttons.

## Syslog Facility Levels

Dell W-Instant supports facility-based logging levels. Syslog Facility is an information field associated with a syslog message. It is an application or operating system component that generates a log message. The following seven facilities are supported by Syslog:

- **AP-Debug**— Detailed log about AP device.
- **Network**— Log about change of network, for example, when a new W-IAP is added to a network.
- **Security**— Log about network security, for example, when a client connects using wrong password.
- **System**— Log about configuration and system status.
- **User**— Important logs about client.
- **User-Debug**— Detailed log about client.
- **Wireless**— Log about radio.

[Table 12](#) describes the logging levels in order of severity, from most to least severe.

**Table 12 - Logging Levels**

Logging Level	Description
Emergency	Panic conditions that occur when the system becomes unusable.
Alert	Any condition requiring immediate attention and correction.
Critical	Any critical conditions such as a hard drive error.
Errors	Error conditions.
Warning	Warning messages.
Notice	Significant events of a non-critical and normal nature.
Informational	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

## Adding a W-IAP to the Network

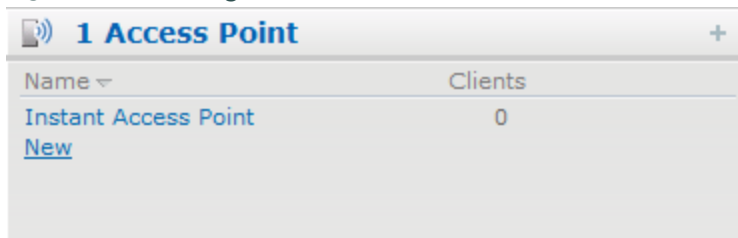
To add a W-IAP to the Dell W-Instant network, assign an IP address. For more information, see ["Assigning an IP Address to the W-IAP" on page 18](#).

After a W-IAP is connected to the network, if the Auto Join Mode feature is enabled, it is listed in the **Access Points** tab in the Dell W-Series Instant UI. The W-IAP inherits the configuration and image from the Virtual Controller.

If the Auto Join Mode is not enabled, then perform the following steps to add a W-IAP to the network:

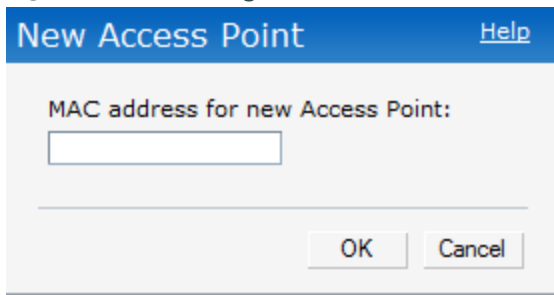
1. In the **Access Points** tab, click the **New** link.

**Figure 46 - Adding a W-IAP to the Instant Network**



2. In the New Access Point window, enter the MAC address for the new W-IAP.

**Figure 47 - Entering the MAC Address for the New W-IAP**



3. Click OK.

## Removing a W-IAP from the Network

A W-IAP can be manually removed from the network only if the "Auto Join Mode" on page 71 feature is disabled.

To manually remove a W-IAP from the network:

1. In the Access Points tab, click the W-IAP which you want to delete. An x appears against the W-IAP.
2. Click x to confirm the deletion.



---

**NOTE:** The deleted W-IAP(s) cannot join the W-Instant network anymore and no longer appear in the Dell W-Series Instant UI. However, the master W-IAP cannot be deleted from the Virtual Controller.

---

## Editing W-IAP Settings

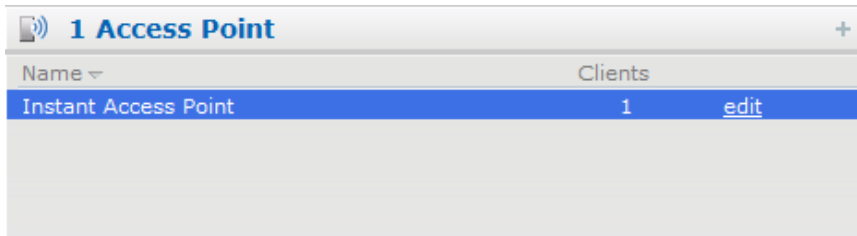
This section explains how to change the W-IAP settings such as Name, IP Address and steps for configuring Adaptive Radio Management (ARM), Wired Bridging on Ethernet 0 Port, Uplink Management VLAN, and migrating from a Virtual Controller Managed Network to Mobility Controller Managed Network.

### Changing W-IAP Name

To change the W-IAP name:

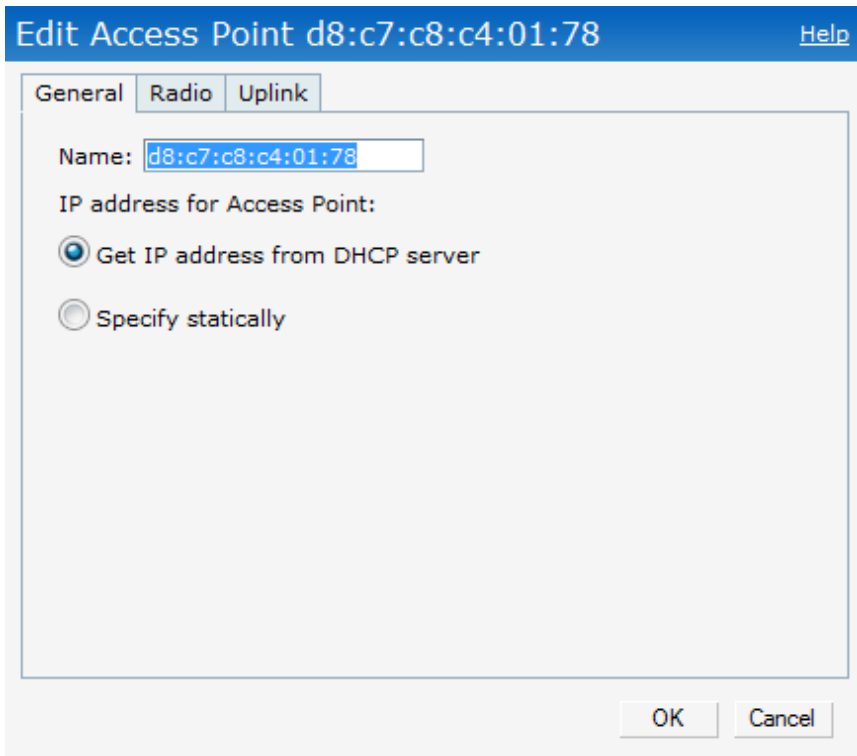
1. In the Access Points tab, click on the W-IAP that you want to rename.

**Figure 48- Editing W-IAP Settings**



2. Click the edit link.

**Figure 49- Changing W-IAP Name**



3. Edit the W-IAP name in the **Name** text box.
4. Click **OK**.

## Changing IP Address of the W-IAP

The Dell W-Series Instant UI allows you to change the IP address of the W-IAP connected to the network.

To change the IP address of the W-IAP:

1. In the **Access Points** tab, click the W-IAP for which you want to change the IP address. The **edit** link appears.
2. Click the **edit** link. The **Edit AP** window appears.

**Figure 50- Configuring W-IAP Settings — Connectivity Tab**

Edit Access Point d8:c7:c8:c4:01:78 [Help](#)

General Radio Uplink

Name:

IP address for Access Point:

Get IP address from DHCP server

Specify statically

IP address:

Netmask:

Default gateway:

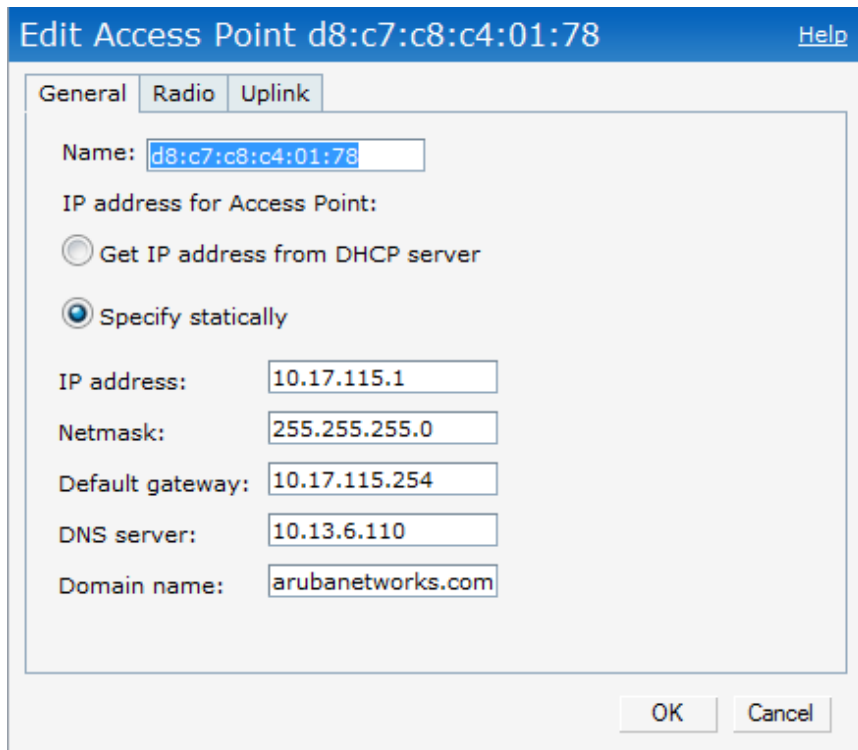
DNS server:

Domain name:

OK Cancel

3. Select either the **Get IP address from DHCP server** or **Specify statically** option. If you have selected the **Specify statically** option, then perform the following steps:
  - a. Enter the new IP address for the W-IAP in the **IP address** text box.
  - b. Enter the netmask of the network in the **Netmask** text box.
  - c. Enter the IP address of the default gateway in the **Default gateway** text box.
  - d. Enter the IP address of the DNS server in the **DNS server** text box.
  - e. Enter the domain name in the **Domain name** text box.

**Figure 51- Configuring W-IAP Connectivity Settings — Specifying Static Settings**



The screenshot shows a web-based configuration window titled "Edit Access Point d8:c7:c8:c4:01:78". The window has three tabs: "General", "Radio", and "Uplink", with "Radio" currently selected. The "Name" field contains the MAC address "d8:c7:c8:c4:01:78". Under "IP address for Access Point:", the "Specify statically" radio button is selected. The "IP address" field is set to "10.17.115.1", "Netmask" to "255.255.255.0", "Default gateway" to "10.17.115.254", "DNS server" to "10.13.6.110", and "Domain name" to "arubanetworks.com". "OK" and "Cancel" buttons are at the bottom right.

4. Click OK and reboot the W-IAP.

## Configuring Adaptive Radio Management

Adaptive Radio Management (ARM) is enabled in Dell W-Instant by default. However, if ARM is disabled, perform the following steps to enable it.

1. In the **Access Points** tab, click the W-IAP for which you want to configure ARM.
2. Click the **edit** link. An **Edit AP** window appears.
3. In the **Edit AP** window, select the **Radio** tab.
4. Select **Adaptive radio management assigned**.

Figure 52- Configuring W-IAP Radio Settings Mode — Access

The screenshot shows a web interface for editing an access point. The title bar reads "Edit Access Point d8:c7:c8:c4:01:78" with a "Help" link. There are three tabs: "General", "Radio", and "Uplink", with "Radio" being the active tab. The "Mode" dropdown is set to "Access". Under the "2.4 GHz band" section, the "Adaptive radio management assigned" radio button is selected, and the "Channel" dropdown is set to "1". The "Transmit power" field is empty, with "dBm" as a unit label. Under the "5 GHz band" section, the "Adaptive radio management assigned" radio button is selected, and the "Channel" dropdown is set to "36". The "Transmit power" field is empty, with "dBm" as a unit label. At the bottom right, there are "OK" and "Cancel" buttons.

5. Click OK.

For more information about ARM, see ["Adaptive Radio Management"](#) on page 169.

## Configuring Uplink Management VLAN

Instant supports a management VLAN for the uplink traffic on a W-IAP. After a W-IAP is provisioned with this parameter, all management traffic sent from the W-IAP is tagged with the management VLAN. Perform the following steps to configure a uplink management VLAN on a W-IAP:

1. In the **Access Points** tab, click the W-IAP.
2. Click the **edit** link. An **Edit AP** window appears.
3. In the **Edit AP** window, select the **Uplink** tab.
4. Specify the VLAN in the **Uplink Management VLAN** field.
5. Click OK.



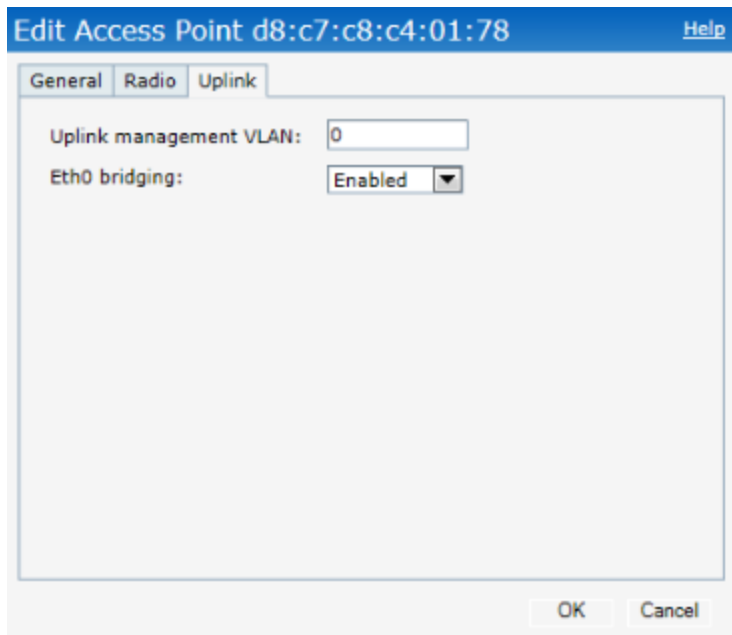
**NOTE:** This configuration requires a W-IAP reboot to take effect.

## Configuring Wired Bridging on Ethernet 0

Instant supports wired bridging on the Ethernet 0 port of a W-Instant AP. Perform the following steps to enable wired bridging on the Ethernet 0 port:

1. In the **Access Points** tab, click the W-IAP.
2. Click the **edit** link. An **Edit AP** window appears.
3. In the **Edit AP** window, select the **Uplink** tab.
4. Select **Enable** from the **Eth0 Bridging** drop box.

**Figure 53- Configuring Wired Bridging on Ethernet 0 of a W-IAP**



5. Click OK.

Enabling wired bridging on this port of the W-IAP makes the port available as a downlink wired bridge and allows client access via the port. You can also use the port to connect a wired device when a 3G uplink is used.



---

**NOTE:** Reboot the W-IAP after the bridging is set for the configuration to take effect.

---

## Migrating to a Dell PowerConnect W-Series Mobility Controller Managed Network

A W-IAP can be provisioned as a Campus AP (CAP) or Remote AP (RAP) in a controller-based network. Before converting the W-IAP, ensure that both the W-IAP and controller are configured to operate in the same regulatory domain.

### Converting a W-IAP to RAP Mode

For RAP conversion, the Virtual Controller sends the RAP convert command to all the other W-IAPs. The Virtual Controller along with the other slave W-IAPs then setup a VPN tunnel to the remote controller, and download the firmware by FTP. The Virtual Controller uses IPsec to communicate to the Dell PowerConnect W-Series Mobility Controller over the Internet.

- If the W-IAP obtains AirWave information via DHCP (Option 43 and Option 60), it establishes an HTTPS connection to the AirWave server and downloads the configuration and operates in W-IAP mode.
- If the W-IAP does not get AirWave information via DHCP provisioning, it tries provisioning via a firmware image server in the cloud (sends serial number MAC address). If an entry for the W-IAP is present in the firmware image cloud server and is provisioned as a W-IAP > RAP entry, the firmware image cloud server responds with controller IP address, AP group, and AP type. The W-IAP then contacts the controller, establishes certificate-based secure communication, and obtains configuration and image from the controller. The W-IAP then



reboots and comes up as a RAP. The W-IAP then establishes an IPSEC connection with the controller and begins operating in RAP mode.

- If a W-IAP entry for the AP is present in the firmware image cloud server, the W-IAP obtains AirWave server information from the cloud server and downloads configuration from Dell PowerConnect W-AirWave to operate in W-IAP mode.
- If there is no response from the cloud server or Dell PowerConnect W-AirWave, the W-IAP comes up in Dell W-Instant mode.



**NOTE:** A description of the firmware image cloud server can be found in the section named Firmware Image Server in Cloud Network, within this chapter.



**NOTE:** A mesh point cannot be converted to RAP because mesh does not support VPN connection.

A W-IAP can be converted to an W-Instant Campus AP and W-Instant Remote AP only if the controller is running W-Instant 6.1.4 or later.

The following table describes the supported W-IAP platforms and minimal AOS version for W-IAP to CAP/RAP conversion.

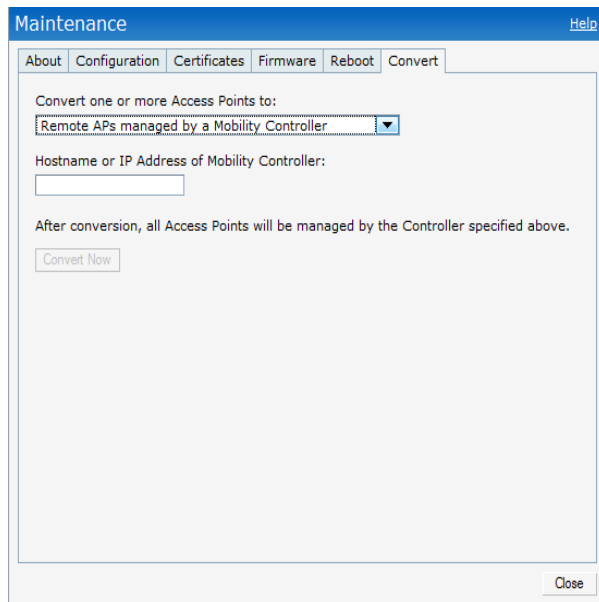
**Table 13- W-IAP Platforms and Minimal AOS and W-IAP Versions for W-IAP to RAP Conversion**

W-IAP Platform	AOS Version	W-Instant Version
W-IAP92	6.1.4 or later	1.0 or later
W-IAP93	6.1.4 or later	1.0 or later
W-IAP104	6.1.4 or later	3.0 or later
W-IAP105	6.1.4 or later	1.0 or later
W-IAP134	6.1.4 or later	2.0 or later
W-IAP135	6.1.4 or later	2.0 or later
W-IAP175AC	6.1.4 or later	3.0 or later
W-IAP175P	6.1.4 or later	3.0 or later
W-IAP3WN	6.1.4 or later	3.0 or later
W-IAP3WNP	6.1.4 or later	3.0 or later
W-IAP108	6.2.0.0 or later	3.2 or later
W-IAP109	6.2.0.0 or later	3.2 or later

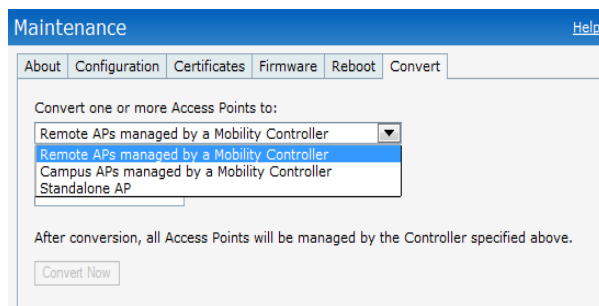
To convert a W-IAP to RAP, follow the instructions below:

1. Navigate to the **Maintenance** tab in the top right corner of the Dell W-Series Instant UI.
2. Click the **Convert** tab.

**Figure 54- Maintenance — Convert Tab**



**Figure 55- Convert options**



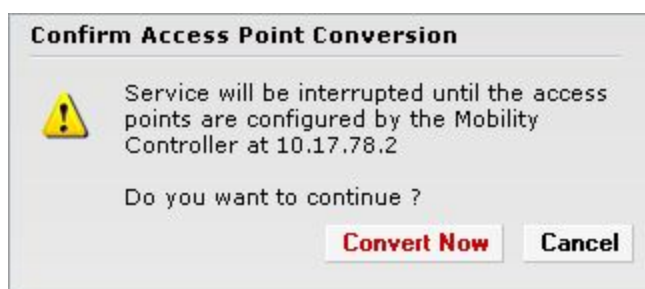
3. Select **Remote APs managed by a Mobility Controller** from the drop-down list.
4. Enter the hostname (fully qualified domain name) or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. This information is provided by your network administrator.



**NOTE:** Ensure the Mobility Controller IP Address is reachable by the W-IAPs.

5. Click **Convert Now** to complete the conversion.

**Figure 56- Confirm Access Point Conversion**



6. The W-IAP reboots and begins operating in RAP mode.

7. After conversion, the W-IAP is managed by the Dell PowerConnect W-Series Mobility Controller which has been specified in the Dell W-Series Instant UI.



---

**NOTE:** In order for the RAP conversion to work, ensure that you configure the W-Instant AP in the RAP white-list and enable the FTP service on the controller.

---



---

**NOTE:** If the VPN setup fails and an error message pops up, please click **OK**, copy the error logs and share them with your Dell support engineer.

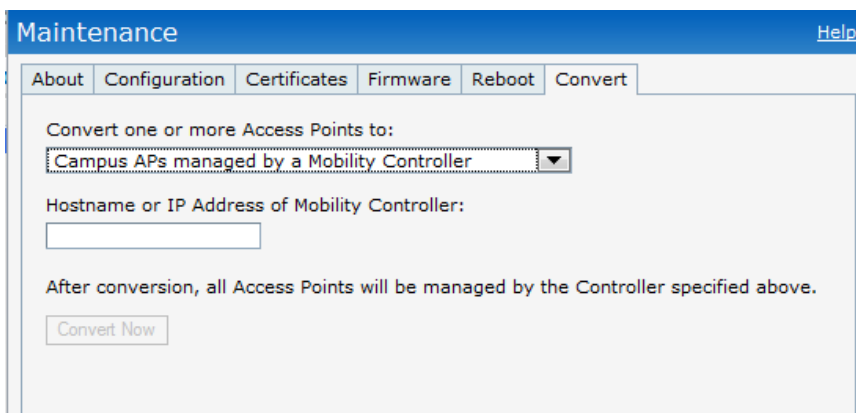
---

### Converting a W-IAP to CAP

To convert a W-IAP to Campus AP, do the following:

1. Navigate to the **Maintenance** tab in the top right corner of the Dell W-Series Instant UI.
2. Click the **Convert** tab.

**Figure 57- Converting a W-IAP to CAP**



3. Select **Campus APs managed by a Mobility Controller** from the drop-down list.
4. Enter the hostname (fully qualified domain name) or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. This is provided by your network administrator.



---

**NOTE:** Ensure the Mobility Controller IP Address is reachable by the W-IAPs.

---

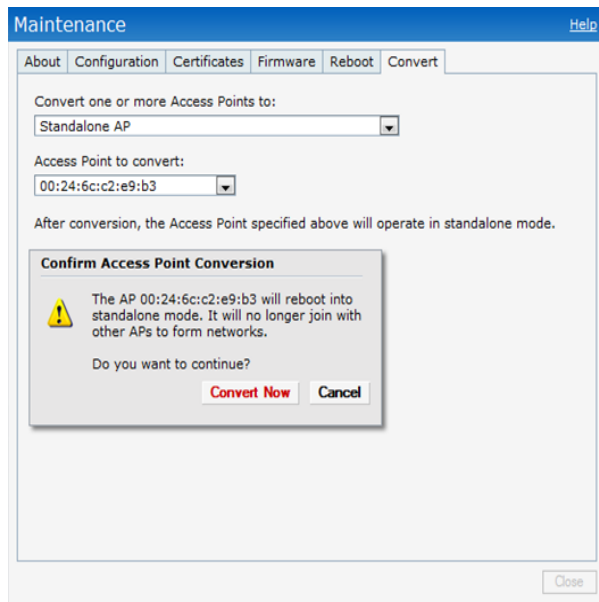
5. Click **Convert Now** to complete the conversion.

### Converting a W-IAP to Standalone Mode

This feature allows you to deploy a W-Instant AP as an autonomous AP which is a separate entity from the existing Virtual Controller cluster in the same Layer 2 domain.

1. Navigate to the **Maintenance** tab in the top right corner of the Dell W-Series Instant UI.
2. Click the **Convert** tab.

**Figure 58- Standalone AP Conversion**



3. Select **Standalone AP** from the drop-down list.
4. Select the Access Point from the drop-down list.
5. Click **Convert Now** to complete the conversion.
6. After the conversion the Access Point specified in the Dell W-Series Instant UI operates in standalone mode.

### **Converting Back to a W-IAP**

The reset button located on the rear of a W-IAP can be used to reset the W-IAP to factory default settings. If you have converted your W-IAP to a campus AP or a Remote AP, pressing the reset button converts it back to a W-IAP.

To reset a W-IAP, follow the instructions below:

1. Power off the W-IAP.
2. Press and hold the reset button using a small, narrow object, such as a paperclip.
3. Power on the W-IAP without releasing the reset button. The power LED flashes within 5 seconds indicating that the reset is completed.
4. Release the reset button.

The W-IAP then boots with the factory default settings.



---

**NOTE:** All APs have a reset button, except W-IAP175P and W-IAP175AC. Contact Dell support for the backward conversion process on these W-IAPs.

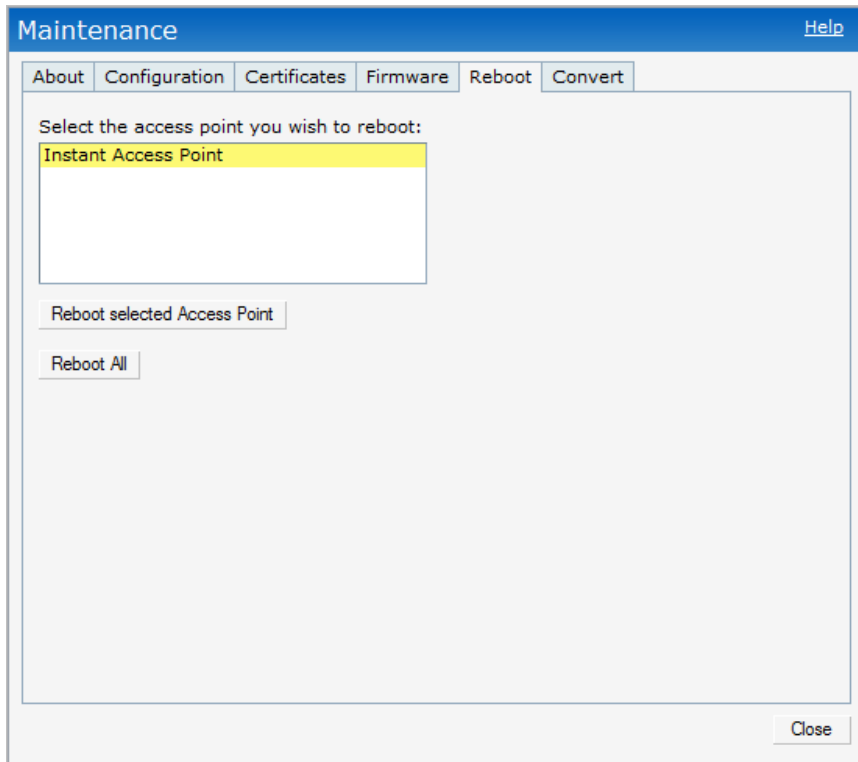
---

### **Rebooting the W-IAP**

If you encounter any problem with the W-IAPs, you can reboot all W-IAPs or selected W-IAPs in a network using the Dell W-Series Instant UI. To reboot a W-IAP:

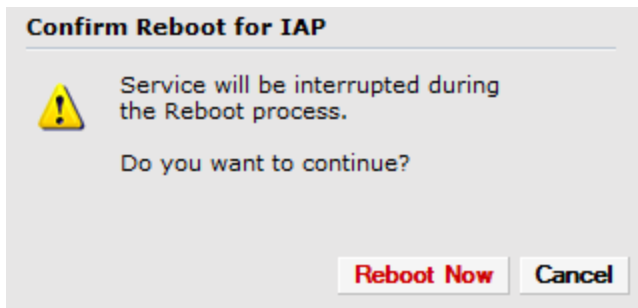
1. Click the **Maintenance** link. The **Maintenance** window appears.
2. Click the **Reboot** tab.

**Figure 59 - Rebooting the W-IAP**



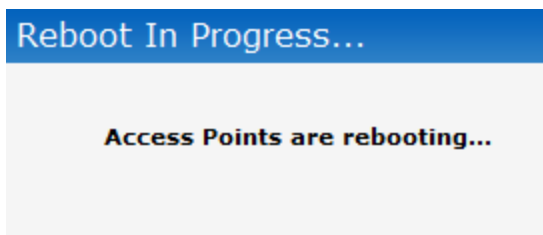
3. In the W-IAP list, select the W-IAP that you want to reboot and click **Reboot selected Access Point**. To reboot all the W-IAPs in the network, click **Reboot All**.
4. The **Confirm Reboot for W-IAP** window appears. Click **Reboot Now** to proceed.

**Figure 60 - Confirm Reboot message**



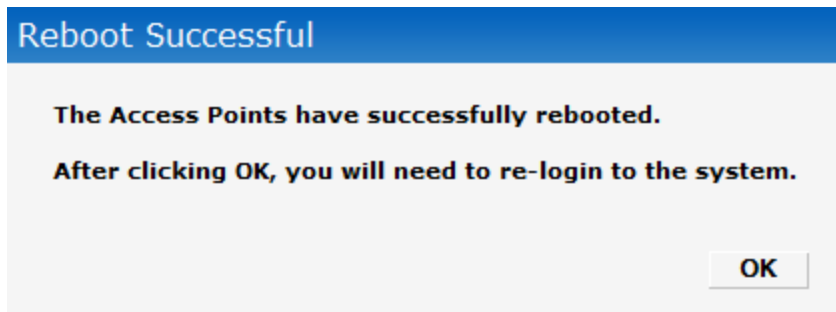
5. The **Reboot in Progress** message appears indicating that the reboot is in progress.

**Figure 61 - Reboot In Progress**



6. The **Reboot Successful** message appears once the process is complete. If the system fails to boot, then the **Unable to contact Access Points after reboot was initiated** message appears.

**Figure 62 - Reboot Successful**



7. Click **OK** to close the window and re-login to the system.

## Firmware Image Server in Cloud Network

The image check feature allows the W-IAP to discover new software image versions on a cloud-based image server hosted by Dell Networks. The location of the image server is fixed and cannot be changed by the user. Dell takes care of managing the image server, and ensures that the image server is loaded with latest versions of W-Instant software for its products.

### Upgrade Using Dell PowerConnect W-AirWave and Image Server

Dell W-Instant supports mixed AP-class instant deployment with all APs as part of the same Virtual Controller cluster.

#### Image Management Using Cloud Server

If the multi-class W-IAP network is not managed by Dell PowerConnect W-AirWave, image upgrades can be done through the cloud-based image check feature. When new W-IAPs joining the network need to synchronize its software with that of the Virtual Controller, and the new W-IAP is of a different class, the image file for the new W-IAP is provided by the cloud server.

#### Image Management Using Dell PowerConnect W-AirWave

If the multi-class W-IAP network is managed by Dell PowerConnect W-AirWave, image upgrades can only be done through the Dell PowerConnect W-AirWave UI. Users must upload W-IAP images for both classes on the AMP server. When new W-IAPs joining the network need to synchronize its software with that of the Virtual Controller, and the new W-IAP is of a different class, the image file for the new W-IAP is provided by Dell PowerConnect W-AirWave. If the AMP does not have the proper image file, the new AP is not be able to join the network.



---

**NOTE:** The Virtual Controller in W-Instant AP communicates with the Dell PowerConnect W-AirWave server or Image server, depending on the user's configuration. If Dell PowerConnect W-AirWave is not configured on the W-IAP, then the image is requested from the Image server. See "[Configuring Dell PowerConnect W-AirWave](#)" on page 207 for steps on how to configure Dell PowerConnect W-AirWave.

---

## Automatic Firmware Image Check and Upgrade

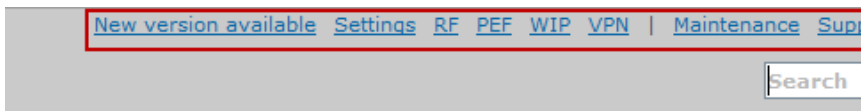
Automatic image check is enabled by default. If Dell PowerConnect W-AirWave is configured, then the automatic image check is automatically disabled, use the manual image check option to check for the latest image. For more information, see "[Upgrading to New Version](#)" on page 88 and "[Configuring Dell PowerConnect W-AirWave](#)" on page 207 for steps on how to configure Dell PowerConnect W-AirWave.

If the Automatic image check is enabled, then the following actions take place:

- once after every time the AP boots up
- once every week thereafter

If the image check locates a new version of the W-Instant software on the image server, then a **New version available** link appears at the top right corner of the Dell W-Series Instant UI.

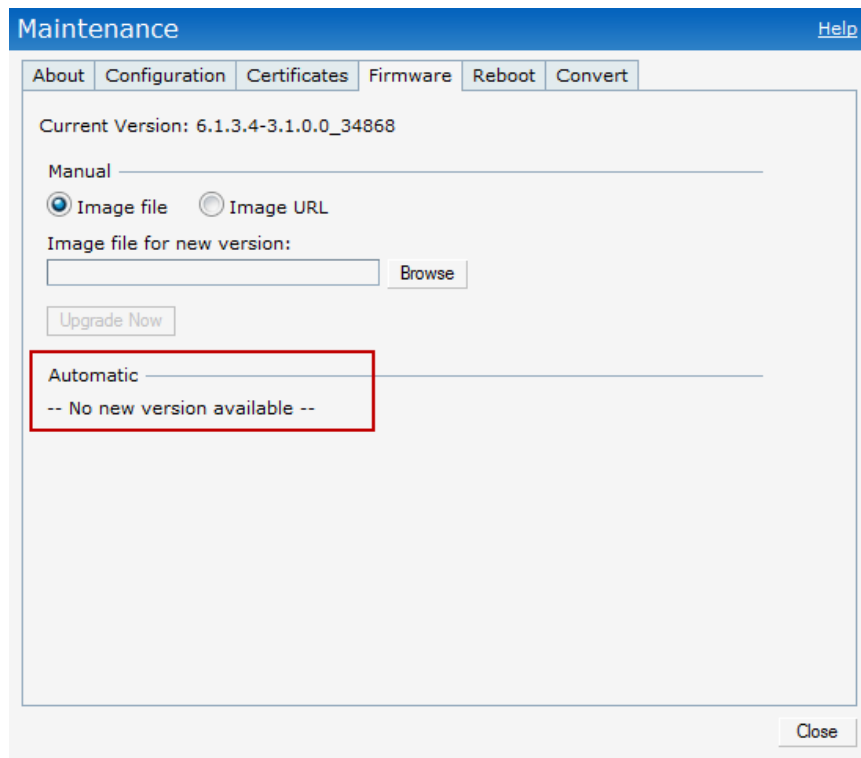
**Figure 63 - Automatic Image Check — New Version Available Link**



After the Automatic image check feature identifies a new version, perform the following steps to upgrade to the new version:

1. The **Maintenance** window appears. Click **Upgrade Now** to upgrade the W-IAP to the newer version.

**Figure 64 - New Version Available**



After you confirm, the AP downloads the new software image from the server, saves it to flash, and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:

- Upgrading — While image upgrading is in progress.
- Upgrade successful —When the upgrading is successful.
- Upgrade fail —When the upgrading fails.

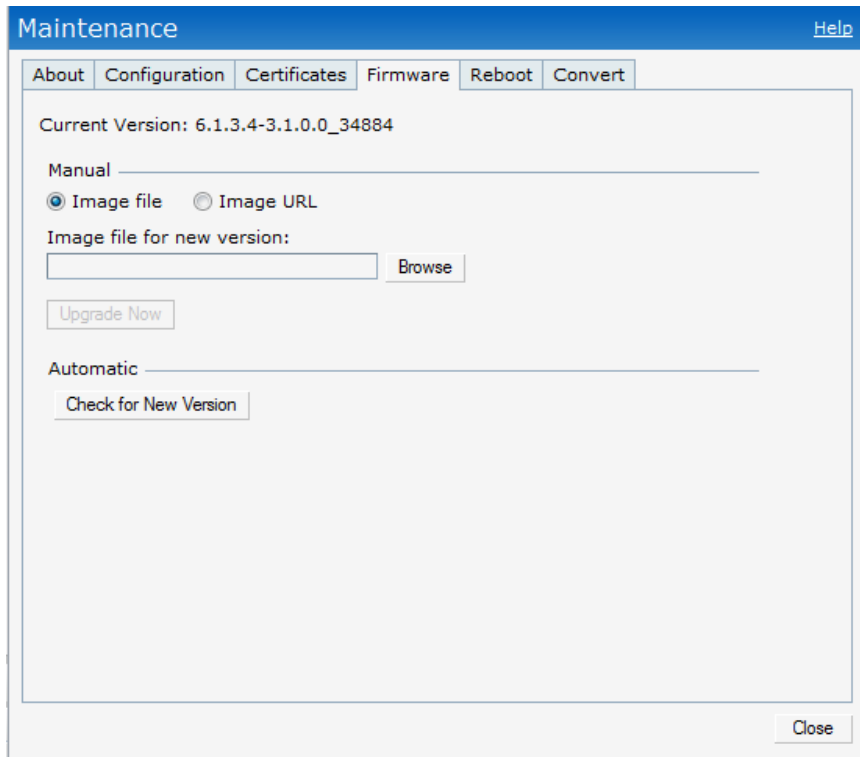
## Upgrading to New Version

To manually check for a new firmware image version:

### Manual

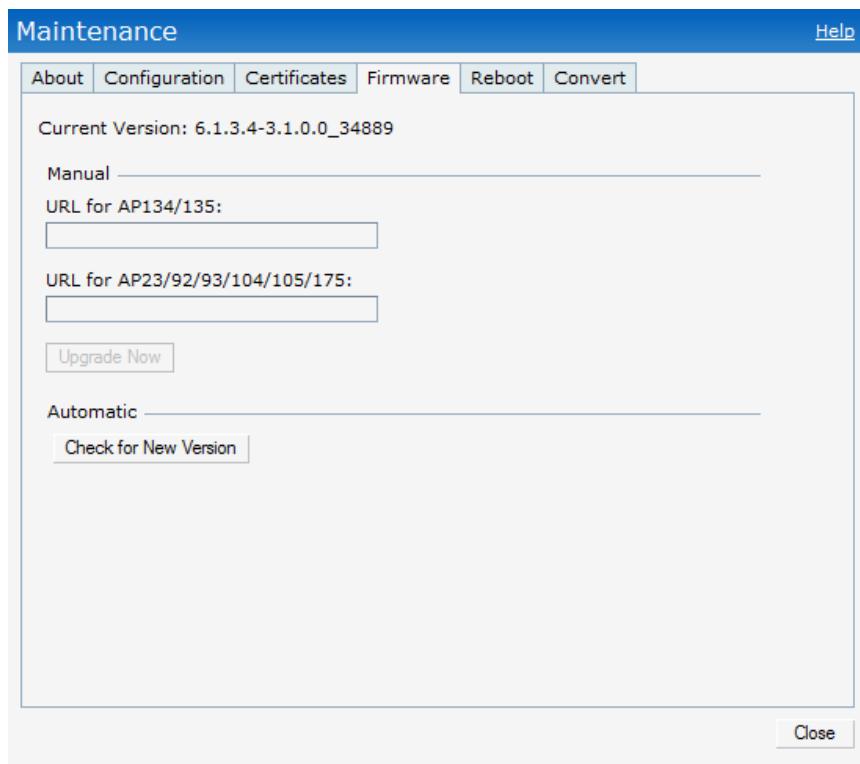
1. Navigate to **Maintenance > Firmware** to select and manually upgrade the image file.

**Figure 65 - Single class or Multi-class W-IAPNetworks Firmware Upgrade**





**Figure 66 - Mixed W-IAP Network Firmware Upgrade**



- **Image file**— Select to directly upload an image file. This method is only available for single-class W-IAPs.
  - Example: DellInstant\_Orion\_6.2.0.0-3.2.0.0\_xxxx
  - Example: DellInstant\_Cassiopeia\_6.2.0.0-3.2.0.0\_xxxx
  - Example: DellInstant\_Pegasus\_6.2.0.0-3.2.0.0\_xxxx
- **Image URL**— Select to obtain the image file from a TFTP, FTP and HTTP URL

The following examples describe the image file format for two different classes of W-IAPs:

TFTP:

- URL for W-IAP135/134: tftp://<IP-address>/DellInstant\_Cassiopeia\_6.2.0.0-3.2.0.0\_xxxx
- URL for W-IAP105/92/93: tftp://<IP-address>/DellInstant\_Orion\_6.2.0.0-3.2.0.0\_xxxx
- URL for W-IAP108/109: tftp://<IP-address>/DellInstant\_Pegasus\_6.2.0.0-3.2.0.0\_xxxx

FTP:

- ftp://<IP-address>/DellInstant\_Cassiopeia\_6.2.0.0-3.2.0.0\_xxxx
- ftp://<IP-address>/DellInstant\_Orion\_6.2.0.0-3.2.0.0\_xxxx
- ftp://<IP-address>/DellInstant\_Pegasus\_6.2.0.0-3.2.0.0\_xxxx

HTTP:

- http://<IP-address>/DellInstant\_Cassiopeia\_6.2.0.0-3.2.0.0\_xxxx
- http://<IP-address>/DellInstant\_Orion\_6.2.0.0-3.2.0.0\_xxxx
- http://<IP-address>/DellInstant\_Pegasus\_6.2.0.0-3.2.0.0\_xxxx

2. Click **Upgrade Now** to upgrade the W-IAP to the newer version.

### **Automatic**

1. Click **Check for New Version** to automatically check for images on the Dell image server in the cloud.

The field is replaced with the **Image Check in Progress** message. After the image check is completed, one of the following messages appears:

- No new version available— If there is no new version available.
  - Image server timed out— Connection or session between the image server and the W-IAP is timed out.
  - Image server failure— If the image server does not respond.
  - A new image version found— If a new image version is found.
2. If a new version is found, the **Upgrade Now** button becomes available and displays the version number.
  3. Click **Upgrade Now**.

The W-IAP downloads the image from the server, saves it to flash and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:

- Upgrading— While image upgrading is in progress.
- Upgrade successful— When the upgrading is successful.
- Upgrade fail— When the upgrading fails.

# Chapter 6

## Layer-3 Mobility

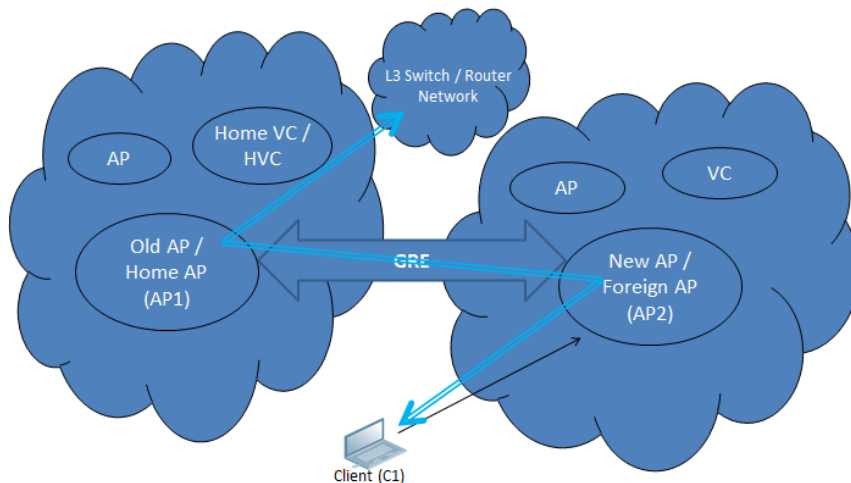
W-IAPs form a single W-Instant network when they are in the same L2 domain. As the number of clients increase, multiple subnets are required to avoid broadcast overhead. In such a scenario, a client should be allowed to roam away from the W-Instant network to which it first connected (home network) to another W-Instant network supporting the same WLAN access parameters (foreign network) and continue its existing sessions.

Layer-3 mobility allows a client to roam without losing its IP address and sessions. If WLAN access parameters are same across these networks, clients connected to APs in a given W-Instant network can roam to APs in a foreign W-Instant network and continue their existing sessions. Clients roaming across these networks are able to continue using their IP addresses after roaming. You can configure a list of Virtual Controller IP addresses across which L3 mobility is supported.

### Overview

Dell W-Instant Layer-3 mobility solution defines a Mobility Domain as a set of Instant networks, with same WLAN access parameters, across which client roaming is supported. The W-Instant network to which the client first connects is called its home network. When the client roams to a foreign network, an AP in the home network (home AP) anchors all traffic to or from this client. The AP to which the client is connected in the foreign network (foreign AP) tunnels all client traffic to or from the home AP through a GRE tunnel.

**Figure 67** - Routing of traffic when the client is away from its home network



When a client first connects to an W-Instant network, a message is sent to all configured Virtual Controller IP addresses to see if this is an L3 roamed client. On receiving an acknowledgement from any of the configured Virtual Controller IP addresses, the client is identified as an L3 roamed

client. If the AP has no GRE tunnel to this home network, a new tunnel is formed to an AP (home AP) from the client's home network.

Each foreign AP has only one home AP per W-Instant network to avoid duplication of broadcast traffic. Separate GRE tunnels are created for each foreign AP / home AP pair. If a peer AP is a foreign AP for one client and a home AP for another, two separate GRE tunnels are used to handle L3 roaming traffic between these APs.

If client subnet discovery fails on association due to some reason, the foreign AP identifies its subnet when it sends out the first L3 packet. If the subnet is not a local subnet and belongs to another Instant network, the client is treated as an L3 roamed client and all its traffic is forwarded to the home network via a GRE tunnel.

## Configuring a Mobility Domain

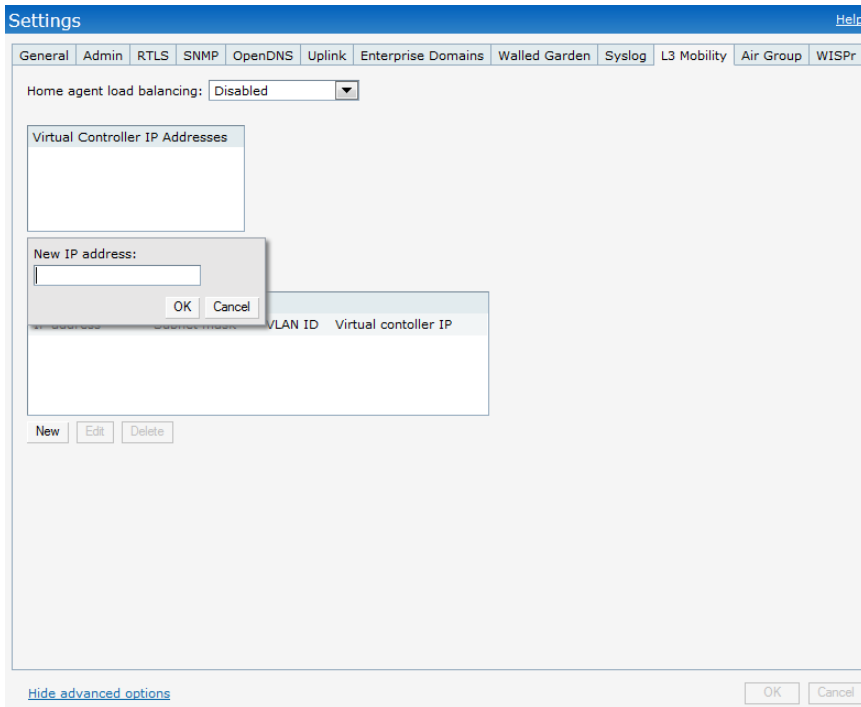
To configure a mobility domain, you have to specify the list of all W-Instant networks that form the mobility domain. In order to allow clients to roam seamlessly among all the APs, specify the Virtual Controller IP for each foreign subnet. You may include the local Instant/ VC IP address, so that the same configuration can be used across all W-Instant networks in the mobility domain. Best practice is to configure all client subnets in the mobility domain so that:

- If the client is from the local subnet, it is determined to be a local client as soon as it starts using the IP address and L3 roaming is aborted.
- If the client is from a foreign subnet, it is determined to be a foreign client as soon as it starts using the IP address and L3 roaming is immediately set up.

Perform the following steps to configure a mobility domain:

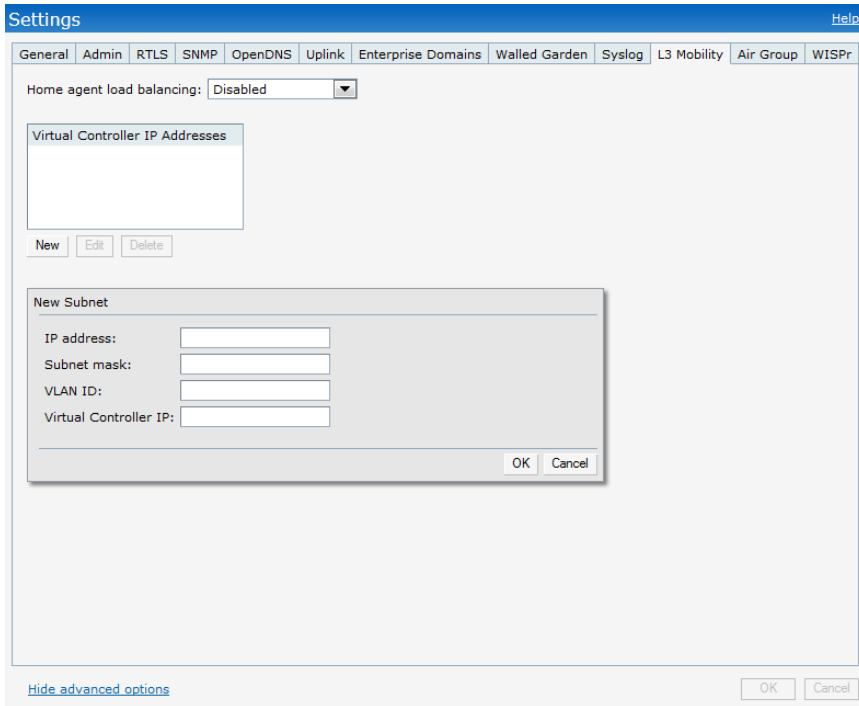
1. Click the **Settings** link at the upper right corner of the Dell W-Series Instant UI.
2. Click the **Show advanced options** link and then click **L3 Mobility**.
3. Click **New** in the **Virtual Controller IP Addresses** section, add the IP address of a VC that is part of the mobility domain, and click **OK**.

**Figure 68 - Add Virtual Controller IP Addresses**



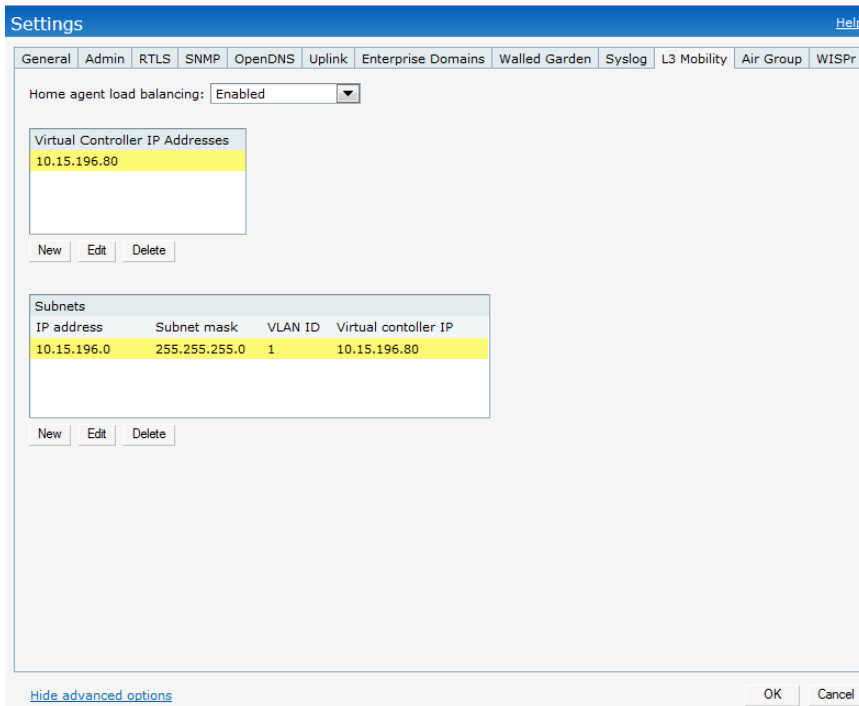
4. Repeat Step 3 to add the IP addresses of all Virtual Controllers that form the L3 mobility domain.
5. Click **New** in the **Subnets** section and specify the following:
  - a. Enter the client subnet in the **IP address** text box.
  - b. Enter the mask in the **Subnet mask** text box.
  - c. Enter the VLAN ID in the home network in the **VLAN ID** text box.
  - d. Enter the home VC IP address for this subnet in the **Virtual Controller IP** text box.

**Figure 69 - Add Subnets Information**



6. Click OK.

**Figure 70 - Example Layer-3 Configuration**



## Home Agent Load Balancing

Home Agent Load Balancing is required in large networks where multiple tunnels might terminate on a single border or lobby AP and overload it. When load balancing is enabled, the VC assigns the home AP for roamed clients by using a *round robin* policy. With this policy, the load for the APs acting as Home Agents for roamed clients is uniformly distributed across the W-Instant cluster. By default, home agent load balancing is disabled.

To enable home agent load balancing by performing the following steps:

1. Click the **Settings** link at the upper right corner of the Instant UI.
2. Click the **Show advanced options** link and then click **L3 Mobility**.
3. Select **Enabled** from the **Home agent load balancing** drop-down list.





# Chapter 7

## Spectrum Monitor

Wireless networks operate in environments with electrical and radio frequency devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference. The spectrum monitor software modules on W-IAPs that support this feature are able to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources. An analysis of the results can then be used to quickly isolate issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel.

Spectrum monitors (SMs) are W-IAP radios that gather spectrum data but do not service clients. Each SM scans and analyzes the spectrum band used by the SM's radio (2.4 GHz or 5 GHz). An AP radio in *hybrid AP* mode continues to serve clients as an access point while it analyzes spectrum analysis data for the channel the radio uses to serve clients. You can record data for both types of spectrum monitor devices. However, the recorded spectrum is not reported to the Virtual Controller. A spectrum alert is sent to the VC when a non Wi-Fi interference device is detected.

The spectrum monitor is supported on W-IAP104, W-IAP105, W-IAP134, and W-IAP135 radios.

### Creating Spectrum Monitors and Hybrid APs

A W-IAP can be provisioned to function as a spectrum monitor or as a hybrid W-IAP. The radios on groups of APs can be converted to dedicated spectrum monitors or hybrid APs via the AP group's 802.11a and 802.11g radio profiles.

### Converting W-IAPs into Hybrid W-IAPs

You can convert all W-IAPs in an Instant network into a hybrid W-IAPs by selecting the **Background spectrum monitoring** option in the Dell W-Instant network's 802.11a and 802.11g radio profiles. APs in Access Mode continue to provide normal access service to clients, while providing the additional function of monitoring RF interference. If any W-IAP in the W-Instant network does not support the spectrum monitoring feature, that AP continues to function as a standard W-IAP, rather than a hybrid W-IAP. By default, the background spectrum monitoring option is disabled. In the hybrid mode, spectrum monitoring is performed only on the home channel.

Follow the procedure below to convert W-IAPs in an Dell W-Instant network to hybrid mode:

1. Click the **RF** link at the top right corner of the Dell W-Series Instant UI.
2. Click **Show advanced options** to view the **Radio** tab.

**Figure 71 - Configuring a Hybrid W-IAP**

The screenshot shows the 'RF' configuration window with the 'Radio' tab selected. The '2.4 GHz band' section has the following settings: Legacy only (Disabled), 802.11d / 802.11h (Disabled), Beacon interval (100 ms), Interference immunity level (2), Channel switch announcement count (0), Channel reuse type (Disabled), Channel reuse threshold (0 dB), and Background spectrum monitoring (Enabled). The '5 GHz band' section has the following settings: Legacy only (Disabled), 802.11d / 802.11h (Disabled), Beacon interval (100 ms), Interference immunity level (2), Channel switch announcement count (0), Channel reuse type (Disabled), Channel reuse threshold (0 dB), Background spectrum monitoring (Enabled), and Standalone spectrum band (Lower). The 'Background spectrum monitoring' dropdowns in both sections are highlighted with a red box. At the bottom, there is a 'Hide advanced options' link and 'OK' and 'Cancel' buttons.

3. To enable a spectrum monitor on the 802.11g radio band, in the 2.4 GHz radio profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
4. To enable a spectrum monitor on the 802.11a radio band, in the 5 GHz radio profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
5. Click **OK**.

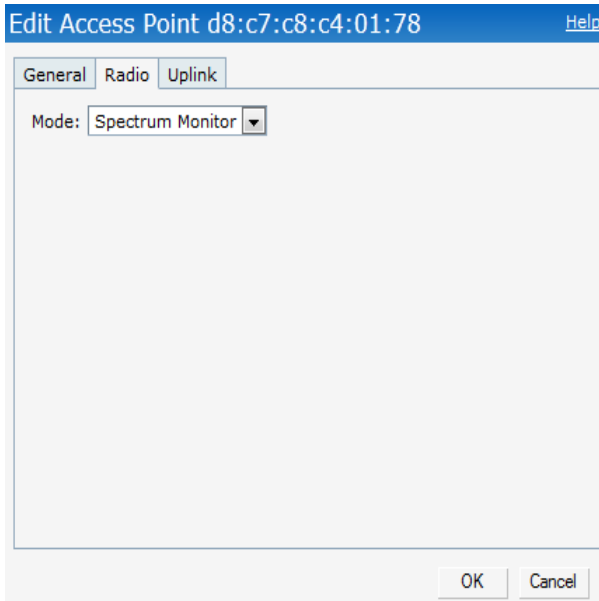
## Converting a W-IAP to a Spectrum Monitor

You can configure a W-IAP to function as a standalone spectrum monitor. In spectrum mode, spectrum monitoring is performed on entire bands. However for the 5 GHz radio, spectrum monitoring is performed on only one of the three bands: 5 GHz - lower, 5 GHz - middle, or 5 GHz - higher. By default, spectrum monitoring is performed on the 5 GHz - higher band.

Follow the procedure below to convert a W-IAP to a spectrum monitor.

1. In the **Access Points** tab, click the AP that you want to convert to a spectrum monitor. The **edit** link appears.
2. Click the **edit** link. The **Edit Access Point** window appears.
3. Click the **Radio** tab.
4. From the **Access Mode** drop-down list, select **Spectrum Monitor**.
5. Click **OK**.
6. Reboot the W-IAP for the changes to take effect.

**Figure 72 - Configuring a Spectrum Monitor**



By default, spectrum monitoring is performed on the 5 GHz - higher band.

7. To enable spectrum monitoring for any other band for the 5 GHz radio:
  - a. Click the **RF** link at the upper right corner of the Dell W-Series Instant UI.
  - b. Click **Show advanced options** to view the **Radio** tab.
  - c. For the 5 GHz radio, specify the spectrum band you want that radio to monitor by selecting **Lower**, **Middle**, or **Higher** from the **Standalone spectrum band** drop-down list.
  - d. Click **OK**.

Figure 73 - Monitor Middle Band for 5 GHz Radio.

The screenshot shows the 'RF' configuration window with the 'Radio' tab selected. It is divided into two sections: '2.4 GHz band' and '5 GHz band'. Each section contains several settings, most of which are set to 'Disabled'. The 'Standalone spectrum band' setting at the bottom of the 5 GHz band section is highlighted with a red box and is set to 'Middle'. At the bottom of the window, there are 'OK' and 'Cancel' buttons, and a link for 'Hide advanced options'.

Band	Setting	Value
2.4 GHz band	Legacy only:	Disabled
	802.11d / 802.11h:	Disabled
	Beacon interval:	100 ms
	Interference immunity level:	2
	Channel switch announcement count:	0
	Channel reuse type:	Disabled
	Channel reuse threshold:	0 dB
	Background spectrum monitoring:	Disabled
5 GHz band	Legacy only:	Disabled
	802.11d / 802.11h:	Disabled
	Beacon interval:	100 ms
	Interference immunity level:	2
	Channel switch announcement count:	0
	Channel reuse type:	Disabled
	Channel reuse threshold:	0 dB
	Background spectrum monitoring:	Disabled
	Standalone spectrum band:	Middle

## Spectrum Data

The spectrum data is collected by each W-IAP spectrum monitor and hybrid AP. The spectrum data is not reported to the VC. The **Spectrum** link is visible in the Dell W-Series Instant UI (Access Point view) only if you have enabled the spectrum monitoring feature. You can view the following spectrum data in the Dell W-Series Instant UI:

- ["Overview - Device List" on page 100](#)
- ["Channel Metrics" on page 103](#)
- ["Channel Details" on page 104](#)

### Overview - Device List

The device list consists of a device summary table and channel information for active non Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio. To view the device list, click **Spectrum** in the dashboard.

To view the device list, click **Spectrum** in the dashboard.

[Table 14](#) shows the details of the information that is displayed:

**Table 14 - Device Summary and Channel Information**

Column	Description
Type	<p>Device type. This parameter can be any of the following:</p> <ul style="list-style-type: none"> <li>• audio FF (fixed frequency)</li> <li>• bluetooth</li> <li>• cordless base FH (frequency hopper)</li> <li>• cordless phone FF (fixed frequency)</li> <li>• cordless network FH (frequency hopper)</li> <li>• generic FF (fixed frequency)</li> <li>• generic FH (frequency hopper)</li> <li>• generic interferer</li> <li>• microwave</li> <li>• microwave inverter</li> <li>• video</li> <li>• xbox</li> </ul> <p><b>NOTE:</b> For additional details about non Wi-Fi device types shown in this table, see <a href="#">Table 15</a>.</p>
ID	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device.
Channels-affected	Radio channels affected by the wireless device.
Signal-strength	Strength of the signal sent from the device, in dBm.
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add-time	Time at which the device was first detected.
Update-time	Time at which the device's status was updated.

## Non Wi-Fi Interferers

The following table describes each type of non Wi-Fi interferer detected by the spectrum monitor feature.

**Table 15 - Non Wi-Fi Interferer Types**

Non Wi-Fi Interferer	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a <i>Bluetooth</i> device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as <i>Fixed Frequency (Audio)</i> .

Non Wi-Fi Interferer	Description
Fixed Frequency (Cordless Phones)	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as <i>Fixed Frequency (Cordless Phones)</i> .
Fixed Frequency (Video)	Video transmitters that continuously transmit video on a single frequency are classified as <i>Fixed Frequency (Video)</i> . These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.
Fixed Frequency (Other)	All other fixed frequency devices that do not fall into one of the above categories are classified as <i>Fixed Frequency (Other)</i> . Note that the RF signatures of the fixed frequency audio, video and cordless phone devices are very similar and that some of these devices may be occasionally classified as Fixed Frequency (Other).
Frequency Hopper (Cordless Base)	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (i.e., no active phone calls), the cordless base is classified as <i>Frequency Hopper (Cordless Base)</i> .
Frequency Hopper (Cordless Network)	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as <i>Frequency Hopper (Cordless Network)</i> . Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as <i>Frequency Hopper (Xbox)</i> .
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into one of the above categories, it is classified as <i>Frequency Hopper (Other)</i> . Some examples include IEEE 802.11 FHSS devices, game consoles and cordless/hands-free devices that do not use one of the known cordless phone protocols.
Microwave	Common residential microwave ovens with a single magnetron are classified as a <i>Microwave</i> . These types of microwave ovens may be used in cafeterias, break rooms, dormitories and similar environments. Some industrial, healthcare or manufacturing environments may also have other equipment that behave like a microwave and may also be classified as a Microwave device.
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as <i>Microwave (Inverter)</i> . Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as Microwave (Inverter). As in the Microwave category described above, there may be other equipment that behave like inverter microwaves in some industrial, healthcare or manufacturing environments. Those devices may also be classified as Microwave (Inverter).
Generic Interferer	Any non-frequency hopping device that does not fall into one of the other categories described in this table is classified as a <i>Generic Interferer</i> . For

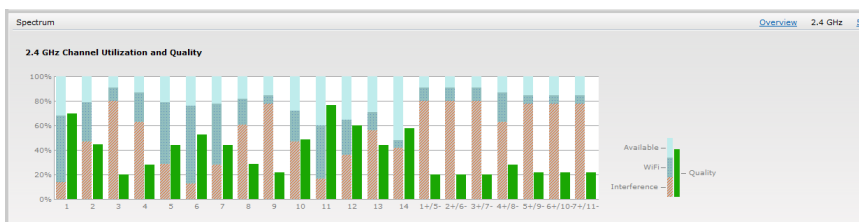
Non Wi-Fi Interferer	Description
	example a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a Generic Interferer. Similarly wide-band interfering devices may be classified as Generic Interferers.

## Channel Metrics

The channel metrics graph displays channel quality, availability and utilization metrics as seen by a spectrum monitor or hybrid AP. You can view the channel utilization data for the percentage of each channel that is currently being used by Wi-Fi devices, and the percentage of each channel being used by non Wi-Fi devices and 802.11 adjacent channel interference (ACI). This chart shows the channel availability, the percentage of each channel that is available for use, or the current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands. While spectrum monitors can display data for all channels in their selected band, hybrid APs display data for their one monitored channel only.

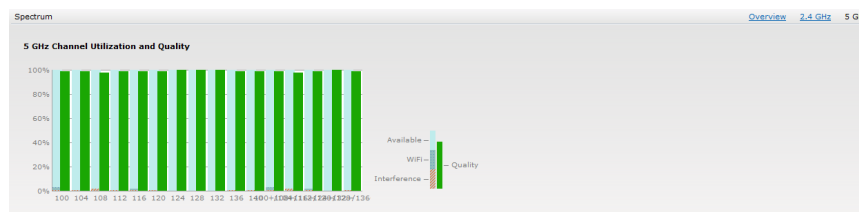
To view this graph, click **2.4 GHz** in the **Spectrum** section of the dashboard.

**Figure 74 - Channel Metrics for the 2.4 GHz Radio Channel**



To view this graph, click **5 GHz** in the **Spectrum** section of the dashboard.

**Figure 75 - Channel Metrics for the 5 GHz Radio Channel**



[Table 16](#) shows the information displayed in the channel metrics graph.

**Table 16 - Channel Metrics**

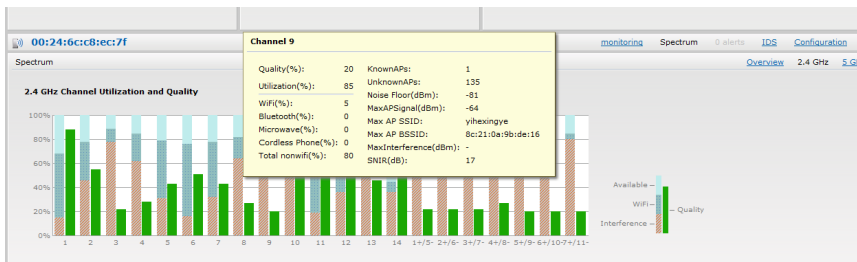
Column	Description
Channel	A 2.4 GHz or 5 GHz radio channel.
Quality(%)	Current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands, as determined by the percentage of packet retries, the current

Column	Description
	noise floor, and the duty cycle for non Wi-Fi devices on that channel.
Availability(%)	The percentage of the channel currently available for use.
Utilization(%)	The percentage of the channel being used.
WiFi Util(%)	The percentage of the channel currently being used by Wi-Fi devices.
Interference Util (%)	The percentage of the channel currently being used by non Wi-Fi interference + Wi-Fi ACI (Adjacent Channel Interference)

## Channel Details

When you move your mouse over a channel, the channel details or the summary of the 5 GHz and 2.4 GHz channels as detected by a spectrum monitor are displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference and the signal-to-noise-and-interference Ratio (SNIR). SNIR is the ratio of signal strength to the combined levels of interference and noise on that channel. Spectrum monitors display spectrum data seen on all channels in the selected band, and hybrid APs display data from the one channel they are monitoring.

**Figure 76 - Channel Details**



[Table 17](#) shows the information that you can view in the channel details graph.

**Table 17 - Channel Details Information**

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Quality(%)	Current relative quality of the channel.
Utilization(%)	The percentage of the channel being used.
Wi-Fi (%)	The percentage of the channel currently being used by Wi-Fi devices.
Type	Device type.
Total nonwifi (%)	The percentage of the channel currently being used by non Wi-Fi devices.
Known APs	Number of valid APs identified on the radio channel.



Column	Description
UnKnown APs	Number of invalid or rogue APs identified on the radio channel.
Channel Util (%)	Percentage of the channel currently in use.
Max AP Signal (dBm)	Signal strength of the AP that has the maximum signal strength on a channel.
Max Interference (dBm)	Signal strength of the non Wi-Fi device that has the highest signal strength.
SNIR (db)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

## Spectrum Alerts

When new non Wi-Fi device is found, an alert is reported to the Virtual Controller. The spectrum alert messages include the device ID, device type, IP address of the spectrum monitor or hybrid AP, and the timestamp. Virtual Controller reports the detailed device information to AMP.



# Chapter 8

## Time Management

### NTP Server

For successful and proper communication between various elements in a network, time synchronization between the elements and across the network is critical. Following are the uses of time synchronization:

- Trace and track security gaps, network usage, and troubleshoot network issues.
- Map event on one network element to a corresponding event on another.
- Maintain accurate time for billing services and similar.

Network Time Protocol (NTP) is required to obtain the precise time from a server and to regulate the local time in each network element. If NTP server is not configured in the Dell W-Instant network, a W-IAP reboot may lead to variation in time and data.

### Configuring an NTP Server

The NTP server is set to `pool.ntp.org` by default. To configure the NTP server on Dell W-Instant, perform the following steps.

1. Navigate to the **Settings** tab in the top right corner of the Dell W-Series Instant UI.

**Figure 77- Configuring NTP Server**

The screenshot shows the 'Settings' page of the Dell W-Series Instant UI. The 'General' tab is selected. The 'NTP server' section is visible, with the following configuration:

Name:	Instant-C4:01:78	Auto join mode:	Enabled
Virtual Controller IP:	0.0.0.0	Terminal access:	Disabled
Dynamic RADIUS proxy:	Disabled	LED display:	Enabled
MAS integration:	Disabled	TFTP Dump Server:	0.0.0.0
NTP server:		Extended SSID:	Disabled
Timezone:	Pacific-Time UTC-8	Deny inter user bridging:	Disabled
Daylight Saving Time:	<input type="checkbox"/>	Deny local routing:	Disabled
Preferred band:	All		

Below the NTP server section, there is a 'DHCP Server' section with the following configuration:

Domain name:	
DNS Server(s):	
Lease time:	<input type="text"/> Minutes
Network:	
Mask:	

At the bottom of the settings page, there is a link for 'Hide advanced options' and 'OK' and 'Cancel' buttons.

- In the **General** tab, enter the IP address or the URL (domain name) of the NTP server in the **NTP Server** text box.
- Select the timezone from the **Timezone** drop-down list. This indicates the time returned by the NTP server.



**NOTE:** You can enable daylight saving time on W-IAPs if the time zone you selected supports the daylight saving time. This feature ensures that the W-IAPs reflect the seasonal time changes in the region they serve.

- Click **OK**.

## Daylight Saving Time

Daylight saving time (DST), also known as summer time, is the practice of advancing clocks so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn. Many countries observe DST, and many do not. If the time zone you selected for a W-IAP supports DST, you can enable daylight saving time feature on this W-IAP to ensure the W-IAP reflects the seasonal time changes.

### Enabling Daylight Saving Time

To enable the Daylight Saving Time on Dell W-Instant, perform the following steps.

- Navigate to the **Settings** tab in the top right corner of the Dell W-Series Instant UI.
- In the **General** tab, select the check box beside the **Daylight Saving Time**. If the Time Zone selected does not support DST, the **Daylight Saving Time** option does not appear.

**Figure 78- Enabling Daylight Saving Time**

The screenshot shows the 'Settings' page with the 'General' tab selected. The 'Daylight Saving Time' checkbox is checked. Other settings include Name: Instant-C4:42:03, Virtual Controller IP: 1.1.1.1, Dynamic RADIUS proxy: Disabled, MAS integration: Disabled, NTP server: (empty), Timezone: Pacific-Time UTC-8, Preferred band: All, Auto join mode: Enabled, Terminal access: Enabled, LED display: Enabled, TFTP Dump Server: 0.0.0.0, Extended SSID: Disabled, Deny inter user bridging: Disabled, Deny local routing: Disabled, DHCP Server section with Domain name, DNS Server(s), Lease time (Minutes), Network: 1.0.0.0, and Mask: 255.0.0.0.

# Chapter 9

## Virtual Controller

Dell W-Instant does not require an external Dell PowerConnect W-Series Mobility Controller to regulate and manage the Wi-Fi network. Instead, one W-IAP in every network assumes the role of virtual controller. It coordinates, stores, and distributes all the settings required to provide a centralized functionality to regulate and manage the Wi-Fi network. The Virtual Controller (VC) is the single point of configuration and firmware management. When configured, the virtual controller sets up and manages the VPN tunnel to a Dell PowerConnect W-Series mobility controller in the data center.

The VC also functions like any other AP with full RF scalability. It also acts as a node, coordinating DHCP address allocation for network address translated clients ensuring mobility of the clients when they roam between different W-IAPs.

### Master Election Protocol

The Master Election Protocol enables the Dell W-Instant network to dynamically elect a W-IAP to take on a VC role, allow graceful failover to a new Virtual Controller when the existing VC is down, and avoid race conditions. This protocol ensures stability of the network during initial startup or when the VC goes down by allowing only one W-IAP to self-elect as a VC.

### Preference to an IAP with 3G/4G Card

The Master Election Protocol prefers the Instant AP (W-IAP) with a 3G/4G card, when electing a VC for the Dell W-Instant network during initial startup. The VC is selected as follows:

- If there are more than one W-IAP with 3G/4G cards, one of these W-IAPs is dynamically elected as the VC.
- When a W-IAP without 3G/4G card is elected as the VC but is up for less than 5 minutes, another W-IAP with 3G/4G card in the network will be elected as the VC to replace it and the previous VC reboots.
- When a W-IAP without 3G/4G card is already elected as the VC and is up for more than 5 minutes, the VC will not be replaced until it goes down.



---

NOTE: W-IAP135 is preferred over W-IAP105 when a VC is elected.

---

### Preference to a W-IAP with Non-Default IP

The Master Election Protocol prefers the W-Instant AP (W-IAP) with non-default IP, when electing a VC for the Dell W-Instant network during initial startup. If there are more than one W-IAPs with non-default IPs in the network, all W-IAPs with default IP will automatically reboot and the DHCP process is used to assign new IP addresses.

## Virtual Controller IP Address

You can specify a single static IP address that can be used to manage a multi-AP Dell W-Instant network. This IP address is automatically provisioned on a shadow interface on the W-IAP that takes the role of a Virtual Controller. When a W-IAP becomes a Virtual Controller, it sends three Address Resolution Protocol (ARP) messages with the static IP address and its own MAC address to update the network ARP cache.

### Specifying Name and IP Address for the Virtual Controller

To specify name and IP address for the Virtual Controller:

1. At the top right corner of the Dell W-Series Instant UI, click the **Settings** link. The **Settings** window appears.
2. Enter a name for the Virtual Controller in the **Name** text box.
3. Enter the appropriate IP address in the **Virtual Controller IP** text box.

### Configuring the DHCP Server

The DHCP Server is the built-in server, used for networks which have **Client IP Assignment** set to **Virtual Controller Assigned**. The default size of the IP address pool has been increased to 512. You can customize the DHCP pool's subnet and address range if you need to provide simultaneous access to more number of clients. The largest address pool supported is 2048.

To configure the domain name, DNS server, and lease time for the DHCP server, network, and mask, perform the following steps:

1. At the top right corner of the Dell W-Series Instant UI, click the **Settings** link.
2. In the **Settings** window, select the **General** tab.
3. Enter the domain name of the client in the **Domain name** text box.
4. Enter the IP addresses of the DNS servers separated by comma(,) in the **DNS server** text box.
5. Enter the duration of the DHCP lease in the **Lease time** text box.
6. Select **Minutes**, **Hours**, or **Days** for the lease time from the drop-down list next to **Lease time**.
7. Enter the network in the **Network** text box.
8. Enter the mask in the **Mask** text box.



---

**NOTE:** To provide simultaneous access to more than 512 clients, use the **Network** and **Mask** fields to specify a larger range. While the network (or prefix) is the common part of the address range, the mask (suffix) specifies how long the variable part of the address range is.

---

9. Click **Ok** to apply the changes.

# Chapter 10

## Authentication

### Authentication Methods in Dell W-Instant

Authentication is a process of identifying a user by having them to provide a valid username and password. Clients can also be authenticated based on their MAC addresses. The following authentication methods are supported in Dell W-Instant:

- ["802.1X Authentication" on page 111](#)
- ["Captive Portal" on page 121](#)
- ["MAC Authentication" on page 133](#)
- ["MAC + 802.1X Authentication" on page 136](#)
- ["MAC + Captive Portal Authentication" on page 137](#)

### 802.1X Authentication

802.1X is a method for authenticating the identity of a user before providing network access to the user. Remote Authentication Dial In User Service (RADIUS) is a protocol that provides centralized authentication, authorization, and accounting management. For authentication purpose, the wireless client can associate to a network access server (NAS) or RADIUS client such as a wireless W-IAP. The wireless client can pass data traffic only after successful 802.1X authentication. The steps involved in 802.1X authentication are:

1. The NAS requests authentication credentials from the wireless client.
2. The wireless client sends the authentication credentials to the NAS.
3. The NAS sends these credentials to a RADIUS server.
4. The RADIUS server checks the user identity and begins authentication with the client if the user identity is present in its database. The RADIUS server sends an Access-Accept message to the NAS.

If the RADIUS server cannot identify the user, it stops the authentication process and sends an Access-Reject message to the NAS. The NAS forwards this message to the client and the client must re-authenticate with correct credentials.

5. After the client is authenticated, the RADIUS server forwards the encryption key to the NAS. The encryption key is used to encrypt or decrypt traffic sent to and from the client.



**NOTE:** A NAS acts as a gateway to guard access to a protected resource. A client connecting to the wireless network first connects to the NAS.

The Dell W-Instant network supports internal RADIUS server and external RADIUS server for 802.1X authentication.

## Internal RADIUS Server

Each W-IAP has an instance of Free RADIUS server operating locally. When you enable the Internal RADIUS server option for the network, the authenticator on the W-IAP sends a RADIUS packet to the local IP address. The Internal RADIUS server listens and replies to the RADIUS packet. The following authentication methods are supported in Dell W-Instant network:

- EAP-TLS— The Extensible Authentication Protocol- Transport Layer Security method supports the termination of EAP-TLS security using the internal RADIUS server. The EAP-TLS requires both server and certification authority (CA) certificates installed onto the W-IAP. The client certificate is verified on the Virtual Controller (the client certificate must be signed by a known CA) before the user name is checked on the authentication server.
- EAP-TTLS (MSCHAPv2)— The Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) method uses server-side certificates to set up authentication between clients and servers. However, the actual authentication is performed using passwords.
- EAP-PEAP (MSCHAPv2)— Protected Extensible Authentication Protocol (PEAP) is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL / TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.
- LEAP— Lightweight Extensible Authentication Protocol (LEAP) uses dynamic WEP keys for authentication between the client and authentication server.



---

**NOTE:** Dell does not recommend to use the LEAP authentication method because it does not provide any resistance to network attacks.

---

## External RADIUS Server

In the external RADIUS server, the IP address of the Virtual Controller is configured as the NAS IP address. Instant RADIUS is implemented on the Virtual Controller, and this feature eliminates the need to configure multiple NAS clients for every W-IAP on the RADIUS server for client authentication. Instant RADIUS dynamically forwards all the authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an Access-Accept or Access-Reject message, and users are allowed or denied access to the network depending on the response from the RADIUS server.

When you enable the external RADIUS server option for the network, the authenticator on the W-IAP sends a RADIUS packet to the local IP address. The external RADIUS server then listens and responds to the RADIUS packet.

The following authentication methods are supported in Dell W-Instant network:

### Authentication Terminated on W-IAP

Dell W-Instant allows EAP termination for PEAP-GTC and PEAP-MSCHAV2. PEAP-GTC termination allows authorization against an LDAP server and external RADIUS server while PEAP-MSCHAV2 allows authorization against an external RADIUS server. This allows users to run PEAP-GTC termination with their own username and password to a local Microsoft Active Directory server with LDAP authentication.

The following EAP-Type methods are described below:



EAP-Generic Token Card (GTC)— This EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the W-IAP as a backup to an external authentication server.

EAP-Microsoft Challenge Authentication Protocol version 2 (MS-CHAPv2)— This EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the backend authentication server.

If you are using the W-IAP's internal database for user authentication, you need to add the names and passwords of the users to be authenticated. If you are using an LDAP server for user authentication, you need to configure the LDAP server on the Virtual Controller, and configure user IDs and passwords. If you are using a RADIUS server for user authentication, you need to configure the RADIUS server on the Virtual Controller.

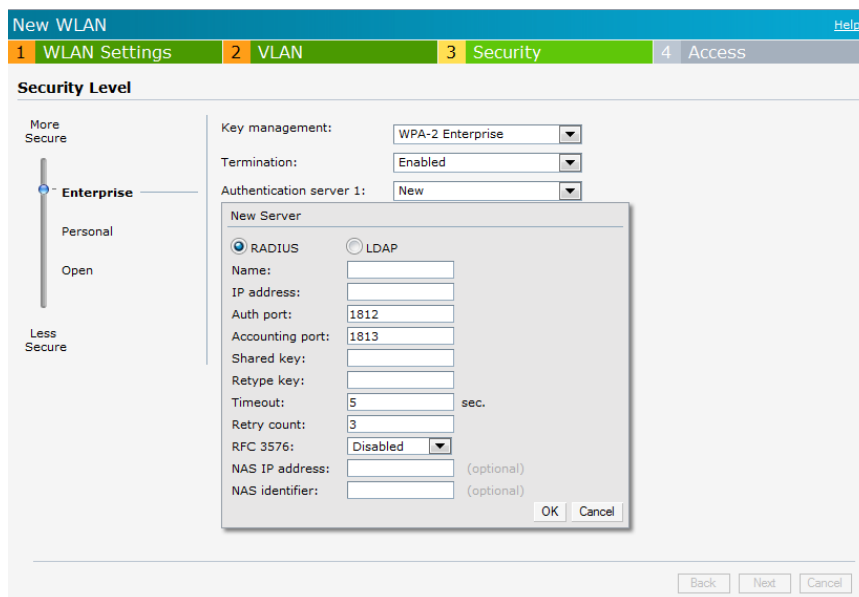
### Configuring an External RADIUS Server

To configure an external RADIUS server for a wireless network:

1. Click **New** in the **Networks** tab and select the appropriate **Primary usage**.
2. Click **Next** to continue.
3. Use the **VLAN** tab to specify how the clients on this network get their IP address and VLAN.
4. Click **Next** to continue.
5. In the **Security** tab, slide the bar to **Enterprise** and update the following fields:
  - a. **Key Management**— Select the type of key for encryption and authentication.
  - b. **Termination**— Select **Enabled** to terminate the EAP portion of 802.1X authentication on the access point instead of RADIUS server.
  - c. **Authentication server 1**— Select **New** from the drop-down list to authenticate user credentials for the RADIUS server at run time and update the following fields:
    - **RADIUS Server**
      - **Name**— Enter the name of the new external RADIUS server.
      - **IP address**— Enter the IP address of the external RADIUS server.
      - **Auth port**— Enter the authorization port number of the external RADIUS server. The port number is set to 1812 by default.
      - **Accounting port**— Enter the accounting port number. This port is used to send accounting records to the RADIUS server. The port number is set to 1813 by default.
      - **Shared key**— Enter a shared key for communicating with the external RADIUS server.
      - **Timeout**— Indicates the timeout for one RADIUS request. The W-IAP retries to send the request several times (as configured in the "Retry count") before the user gets disconnected. e.g. If the "Timeout" is 5 sec, "Retry counter" is 3, user is disconnected after 20 sec ("Timeout" x "Retry counter + 1"). The default value is 5 seconds.
      - **Retry count**— Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to server group, and the default value is 3 requests.
      - **RFC 3576**— When enabled, the Access Points process RFC 3576-compliant Change of Authorization (CoA) and Disconnect messages from the RADIUS server. Disconnect messages cause a user session to be terminated immediately, whereas CoA messages modify session authorization attributes such as data filters.

- NAS IP address— Enter the Virtual Controller IP address. The NAS IP address is the Virtual Controller IP address that is sent in data packets. Note: If you do not enter the IP address, the Virtual Controller IP address is used by default when Dynamic RADIUS Proxy is enabled.
  - NAS identifier— Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
- LDAP Server
  - Name— Enter the name of the new external RADIUS server.
  - IP address— Enter the IP address of the external RADIUS server.
  - Auth port— Enter the authorization port number of the external RADIUS server. The port number is set to 1812 by default.
  - Admin-DN— Enter a Distinguished Name for the admin user who has read/search privileges across all the entries in the LDAP database. The user may not have write privileges but is able to search the database, and read attributes of the other users in the database.
  - Admin password— Enter a admin password.
  - Base-DN— Enter a Distinguished Name of the node which contains the entire user database.
  - Filter— Indicates the filter that should be applied to search for the user in the LDAP database. The default filter string is (objectclass=\*).
  - Key Attribute— Indicates the attribute that should be used as a key in search for the LDAP server. For Active Directory, the value is sAMAccountName.
  - Timeout— Enter a value between 1 and 30 seconds. The default value is 5.
  - Retry count— Enter a value between 1 and 5. The default value is 3.

**Figure 79 - Configuring an External RADIUS Server**



6. Click OK after updating the fields.
7. **Reauth interval** — When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.

8. **Blacklisting**— Select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
  - **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.
9. Navigate to **PEF > Blacklisting** in the Dell W-Series Instant UI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.
10. **For Internal users**— Click **Users** to populate the system’s internal authentication server with users. For information about adding a user, see ["Adding a User" on page 269](#).
11. Click **Next** to continue and then click **Finish**.

## Enabling RADIUS Server Support

To enable RADIUS server support:

1. Click **Settings** at the top right corner of the Dell W-Series Instant UI.
2. Select **Enabled** from the **Dynamic RADIUS Proxy** drop-down list. When enabled, the Virtual Controller network uses the IP Address of the Virtual Controller for communication with external RADIUS servers. You must set the Virtual Controller IP address as a NAS client in the RADIUS server if Dynamic RADIUS Proxy is enabled.

**Figure 80 - Enabling RADIUS Server Support**

The screenshot shows the 'Settings' window with the 'Admin' tab selected. The 'Dynamic RADIUS proxy' dropdown menu is highlighted with a red box and is set to 'Enabled'. Other settings include: Name: Instant-C4:01:78, Virtual Controller IP: 0.0.0.0, MAS integration: Enabled, NTP server: (empty), Timezone: International-Date-Line, and Preferred band: All. At the bottom, there are 'Show advanced options', 'OK', and 'Cancel' buttons.

3. Click **OK**.

## Authentication Survivability

This feature provides authentication and authorization survivability against remote link failure for Dell PowerConnect W-Series Mobility Controllers when working with Dell PowerConnect W-ClearPass Policy Manager.

When enabled, this feature allows Instant to authenticate the previously connected clients using EAP-PEAP authentication even when connectivity to Dell PowerConnect W-ClearPass Policy Manager is temporarily lost.

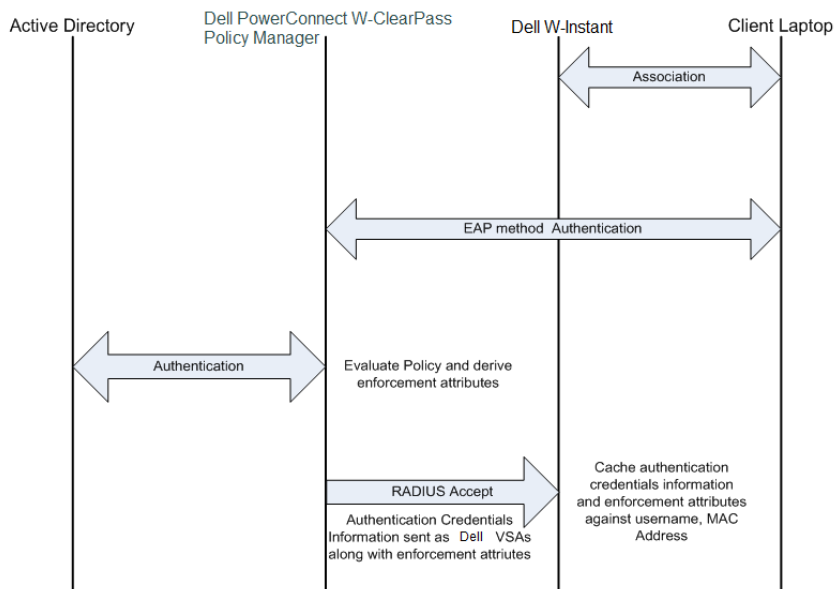
The following flow diagrams depict the interaction between the Dell PowerConnect W-ClearPass Policy Manager and the W-IAP for different network scenarios.

- 802.1X Authentication when Dell PowerConnect W-ClearPass Policy Manager is available (refer to [Figure 83](#))
- 802.1X Authentication using cached credentials when Dell PowerConnect W-ClearPass Policy Manager is not available (refer to [Figure 82](#))
- 802.1X Authentication when Dell PowerConnect W-ClearPass Policy Manager is available again (refer to [Figure 83](#))

[Figure 81](#) depicts a process wherein the W-IAP offloads EAP method authentication to ClearPass over a remote link connection. After authenticating the user against Active Directory and deriving enforcement attributes for the user, the ClearPass Policy Manager returns additional information in the RADIUS Access Accept message which the IAP caches to support authentication survivability.

As seen in the figure below, the information sent by the ClearPass Policy Manager varies depending on the authentication method used.

**Figure 81 - 802.1X Authentication when Dell PowerConnect W-ClearPass Policy Manager is reachable**



[Figure 82](#) depicts a situation when the remote link is not available and the W-IAP is no longer able to reach the Dell PowerConnect W-ClearPass Policy Manager. Here, the W-IAP will terminate and complete the EAP authentication using the cached credentials information.



**NOTE:** If both the W-IAP to which the client was associated and the CPPM are not available, then the client will be not be able to reauthenticate until the CPPM server is available again.

**Figure 82 - 802.1X Authentication using cached credentials**

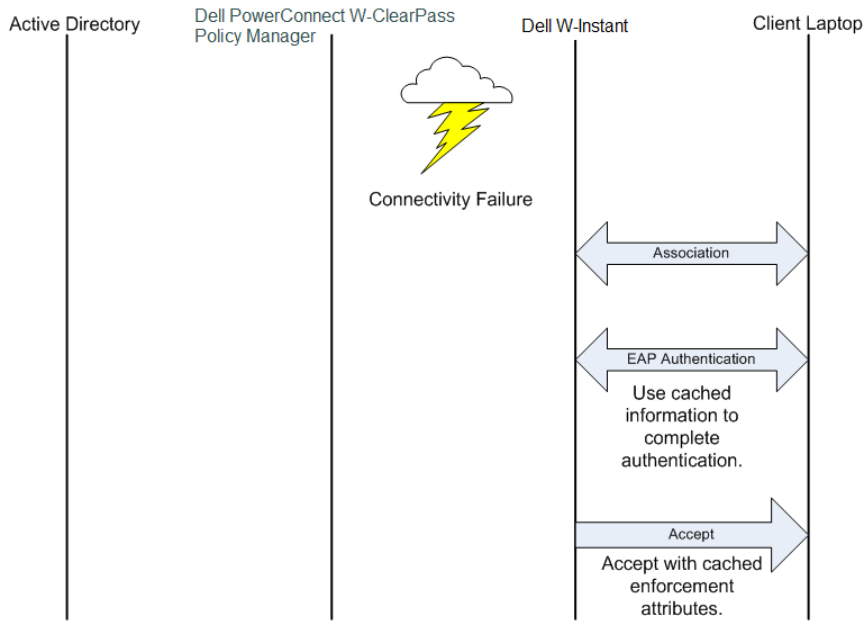
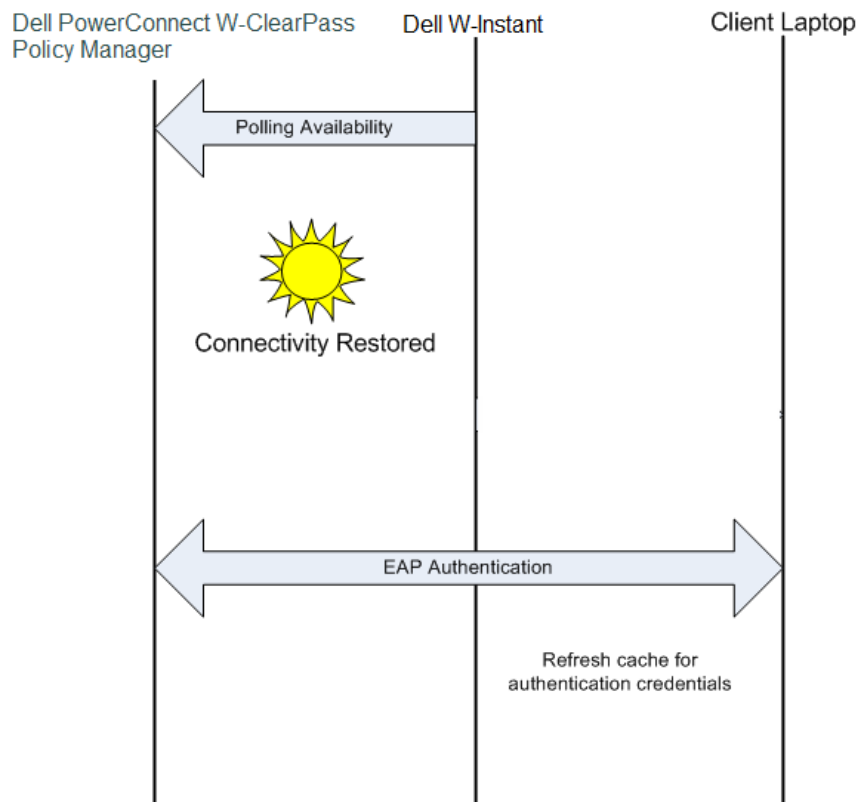


Figure 83 depicts a situation when the CPPM link is reachable again. The W-IAP will send the RADIUS-Request message to the CPPM server directly for client authentication.

**Figure 83 - 802.1X Authentication when Dell PowerConnect W-ClearPass Policy Manager is reachable again**



## RADIUS Server Authentication with VSA

An external RADIUS server authenticates network users and returns to the W-IAP the vendor-specific attribute (VSA) that contains the name of the network role for the user. The authenticated user is placed into the management role specified by the VSA.

### List of Supported VSA

Instant supports the following types of VSA's:

- AP-Group
- AP-Name
- ARAP-Features
- ARAP-Security
- ARAP-Security-Data
- ARAP-Zone-Access
- Acct-Authentic
- Acct-Delay-Time
- Acct-Input-Gigawords
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Link-Count
- Acct-Multi-Session-Id
- Acct-Output-Gigawords
- Acct-Output-Octets
- Acct-Output-Packets
- Acct-Session-Id
- Acct-Session-Time
- Acct-Status-Type
- Acct-Terminate-Cause
- Acct-Tunnel-Packets-Lost
- Add-Port-To-IP-Address
- Dell-AP-Group
- Dell-Admin-Role
- Dell-Essid-Name
- Dell-Location-Id
- Dell-Named-User-Vlan
- Dell-Port-Id
- Dell-Priv-Admin-User
- Dell-Template-User
- Dell-User-Role
- Dell-User-Vlan
- Dell-Auth-Survivability
- Dell-AS-User-Name
- Dell-AS-Credential-Hash

- CHAP-Challenge
- Callback-Id
- Callback-Number
- Class
- Connect-Info
- Connect-Rate
- Crypt-Password
- DB-Entry-State
- Digest-Response
- Domain-Name
- EAP-Message
- Error-Cause
- Event-Timestamp
- Exec-Program
- Exec-Program-Wait
- Expiration
- Fall-Through
- Filter-Id
- Framed-AppleTalk-Link
- Framed-AppleTalk-Network
- Framed-AppleTalk-Zone
- Framed-Compression
- Framed-IP-Address
- Framed-IP-Netmask
- Framed-IPX-Network
- Framed-MTU
- Framed-Protocol
- Framed-Route
- Framed-Routing
- Full-Name
- Group
- Group-Name
- Hint
- Huntgroup-Name
- Idle-Timeout
- Login-IP-Host
- Login-LAT-Node
- Login-LAT-Port
- Login-LAT-Service
- Login-Service
- Login-TCP-Port
- Menu

- Message-Auth
- NAS-Port-Type
- Password
- Password-Retry
- Port-Limit
- Prefix
- Prompt
- Rad-Authenticator
- Rad-Code
- Rad-Id
- Rad-Length
- Reply-Message
- Revoke-Text
- Server-Group
- Server-Name
- Service-Type
- Session-Timeout
- Simultaneous-Use
- State
- Strip-User-Name
- Suffix
- Termination-Action
- Termination-Menu
- Tunnel-Assignment-Id
- Tunnel-Client-Auth-Id
- Tunnel-Client-Endpoint
- Tunnel-Connection-Id
- Tunnel-Medium-Type
- Tunnel-Preference
- Tunnel-Private-Group-Id
- Tunnel-Server-Auth-Id
- Tunnel-Server-Endpoint
- Tunnel-Type
- User-Category
- User-Name
- User-Vlan
- Vendor-Specific

### **Management Authentication Settings**

Use this page to specify authentication for access to the Virtual Controller Management user interface.

1. Navigate to the **Settings** link in the Dell W-Series Instant UI.



2. Select the **Admin** tab.
3. In the **Authentication** drop-down list, select any one of the following:
  - **Internal**— Select to specify a single set of user credentials. Enter the **Username** and **Password** for accessing the Virtual Controller Management User Interface.
  - **RADIUS Server**— Specify one or two RADIUS servers to authenticate the Dell W-Series Instant UI. If two servers are configured users can use them in primary/backup mode or load-balancing mode, this is identical to the RADIUS server configuration for SSIDs. For information on configuring external RADIUS server, see ["External RADIUS Server" on page 112](#).
  - **RADIUS server w/ fallback to internal**— Specify the RADIUS servers as well as a Username and Password. If there is no response from the RADIUS server (RADIUS server timeout), the authentication switches to **Internal**.
4. Click **OK**.

**Figure 84 - Management Authentication Settings**

## Captive Portal

Dell W-Instant network supports captive portal authentication method for a Guest network type. In this method, a web page is displayed to a guest user who tries to access the Internet. The user has to authenticate or accept company's network usage policy in the web page. Two types of captive portal authentication are supported on Dell W-Instant.

- ["Internal Captive Portal" on page 121](#)
- ["External Captive Portal" on page 127](#)

### Internal Captive Portal

In the Internal Captive Portal type, an internal server is used to host the captive portal service. Internal captive portal authentication is classified as follows:

- **Internal Authenticated**— To gain access to the wireless network, a user must authenticate in the captive portal page. If this option is selected, then users who are required to authenticate have to be added to the user database. Click the **Users** link to add the users. For information about adding users, see ["Adding a User" on page 269](#).

- **Internal Acknowledged**— To gain access to the wireless network, a user must accept the terms and conditions.

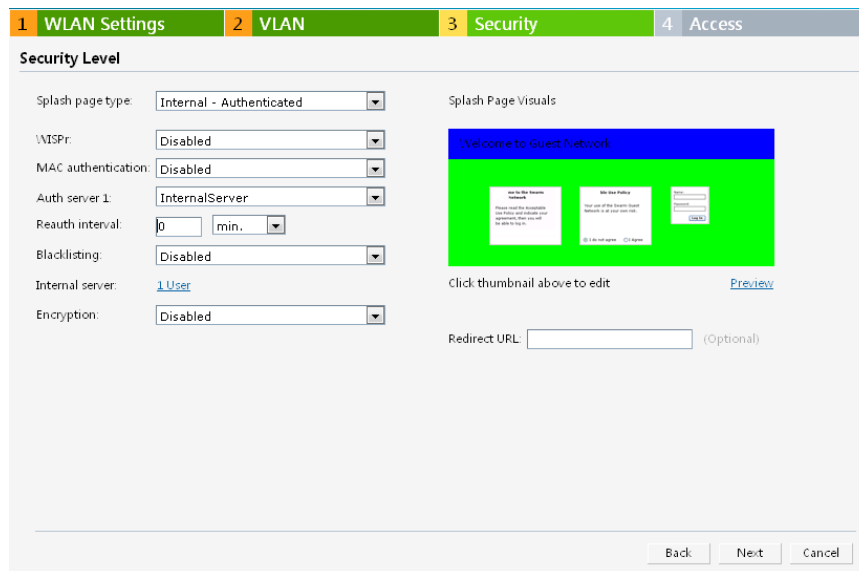
### Configuring Internal Captive Portal Authentication when Adding a Guest Network

To configure internal captive portal authentication when adding a guest network, perform the following steps:

1. In the **Network** tab, click the **New** link. The **New WLAN** window opens.
2. In the **WLAN Settings** tab, update the following information:
  1. Enter a name for the network in the **Name (SSID)** text box.
  2. Click **Guest** and then click **Next**.
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN.
4. Click **Next** to continue.
5. In the **Security** tab, select one of the following options for the splash page type:
  - a. **Internal - Authenticated**
  - b. **Internal - Acknowledged**
  - c. **External - RADIUS Server**
  - d. **External - Authentication text**
  - e. **None**

See "[Guest Network](#)" on page 60 for more information on the splash page type options.

**Figure 85 - Configuring Captive Portal when Adding A Guest Network**



The appearance of a splash page can be customized as required. For information on customizing a splash page, see "[Customizing a Splash Page](#)" on page 125.

6. Select **Disabled** or **Enabled** from the **WISPr** drop-down list to disable or enable the WISPr authentication. For information on WISPr authentication, see "[WISPr Authentication](#)" on page 132.
7. Select **Disabled** or **Enabled** from the **MAC authentication** drop-down list to disable or enable the MAC authentication. For information on MAC authentication, see "[MAC Authentication](#)" on page 133.

8. Select **InternalServer** from the **Auth server 1** drop-down list to authenticate user credentials at run time.
9. **Reauth interval** — When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.
10. **Blacklisting** — Select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
11. **Max authentication failures** — Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.
12. **Internal server** —
  - Click **User** to populate the system's internal authentication server with users. For information about adding a user, see ["Adding a User" on page 269](#).
  - Click **Upload Certificate** and browse to upload a certificate file for the internal server.
13. **Encryption**— Select **Enabled** from the drop-down list and perform the following steps (these steps are optional):
  - a. Select the required key management option from the **Key management** drop-down list. Available options are:
    - WPA-2 Personal
    - WPA Personal
    - Both (WPA-2 & WPA)
  - b. **Passphrase format** — Specify either an alphanumeric or a hexadecimal string. Ensure that the hexadecimal string must be exactly 64 digits in length.
  - c. **Passphrase** — Enter a pre-shared key (PSK) passphrase.
14. Click **Next** and click **Finish**.

### **Configuring Internal Captive Portal Authentication when Editing a Guest Network**

To configure internal captive portal authentication when editing a guest network, perform the following steps:

1. In the **Network** tab, click the network for which you want to configure internal captive portal authentication. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** window for the network appears.
3. Navigate to the **Security** tab and select one of the following options for the splash page type:
  - a. **Internal — Authenticated**
  - b. **Internal — Acknowledged**
  - c. **External — RADIUS Server**
  - d. **External — Authentication Text**
  - e. **None**

See ["Guest Network" on page 60](#) for more information.

**Figure 86 - Configuring Captive Portal when Editing a Guest Network**

The screenshot shows the 'Edit Guest' configuration interface with the 'Security' tab selected. The 'Security Level' section contains the following settings: Splash page type is 'Internal - Authenticated', WISPr is 'Disabled', MAC authentication is 'Disabled', Auth server 1 is 'InternalServer', Reauth interval is '0 hrs', Blacklisting is 'Disabled', Internal server is 'User', and Encryption is 'Disabled'. The 'Splash Page Visuals' section displays a preview of the splash page with the text 'Welcome to Guest Network' and a 'Preview' link. Below the preview is a 'Redirect URL' field labeled '(Optional)'. At the bottom of the page are 'Back', 'Next', and 'Cancel' buttons.

The appearance of a splash page can be customized as required. For information on customizing a splash page, see ["Customizing a Splash Page"](#) on page 125.

4. Click **Next** and click **Finish**.

### **Configuring Internal Captive Portal with External RADIUS Server Authentication when Adding a Guest Network**

To configure internal captive portal with external RADIUS server authentication, perform the following steps:

1. In the **Network** tab, click the **New** link. The **New WLAN** window opens.
2. In the **WLAN Settings** tab, perform the following:
  - a. Enter a name for the network in the **Name (SSID)** text box.
  - b. Select **Guest** and then click **Next**.
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN.
4. Click **Next** to continue.
5. In the **Security** tab, select **Internal — Authenticated** under the splash page type.
6. Select an external RADIUS server from the Authentication server drop-down list to authenticate user credentials at run time. If there is no external RADIUS server in the drop-down list, click **New** to add a RADIUS server. For information on configuring external RADIUS server, see ["External RADIUS Server"](#) on page 112.
7. Click **Next** and then click **Finish**.

**Figure 87 - Configuring Internal Captive Portal with External RADIUS Server Authentication**

1 WLAN Settings 2 VLAN 3 Security 4 Access

**Security Level**

Splash page type: External - RADIUS Server

WISPR: Disabled

MAC authentication: Disabled

Auth server 1: -- Select Server --

Auth server 2: -- Select Server --

Reauth interval: 0 hrs.

Blacklisting: Disabled

Walled garden: [Blacklist: 0 Whitelist: 0](#)

Encryption: Disabled

External splash page:

IP or hostname: localhost

URL: /

Port: 80

Redirect URL: (Optional)

Back Next Cancel

### Customizing a Splash Page

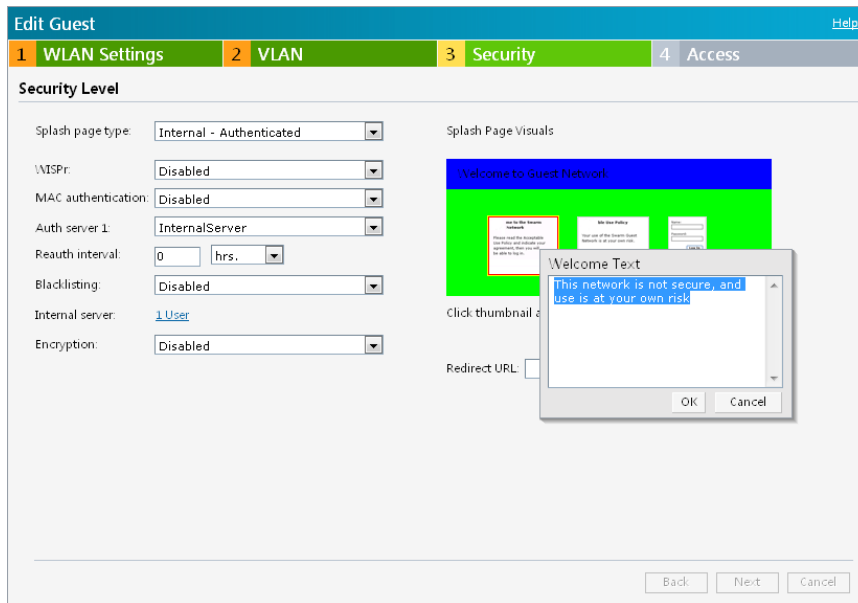
A splash page is a web page that is displayed to a guest user when they are trying to access the Internet. The appearance of a splash page can be customized as required. To customize a splash page, perform the following steps:



**NOTE:** The current release does not support per SSID splash page. When multiple SSIDs are configured to use customized splash page, changes to the page are reflected on all SSIDs.

1. In the **Network** tab, click the network for which you want to customize the splash page. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** window for the network appears.
3. Navigate to the **Security** tab and perform the following steps:
  - Splash Page Visuals** — Use the in-place editor below to specify text and colors for the initial page that users connecting to the network see. This page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal -Acknowledged) you set.
    - a. To change the color of the splash page, click the Splash page rectangle and select the required color from the **Background Color** palette.
    - b. To change the welcome text, click the first square in the splash page, type the required text in the **Welcome** text box, and click **OK**. The welcome text should not exceed 127 characters.
    - c. To change the policy text, click the second square in the splash page, type the required text in the **Policy** text box, and click **OK**. The policy text should not exceed 255 characters.

Figure 88 - Customizing a Splash Page



4. Click **Next** and then click **Finish**.



**NOTE:** You can customize the captive portal page using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters. Click on the banner, term, or policy in the **Splash Page Visuals** to modify the text in the red box. These fields accept double-byte characters or a combination of English and double-byte characters.

### Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

1. In the **Network** tab, click the guest network for which you want to disable captive portal authentication. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** window for the network appears.
3. Navigate to **Security** tab and select **None** from the **Splash page type** drop-down list.

**Figure 89 - Disabling Captive Portal Authentication**

The screenshot shows a configuration window with four tabs: 1 WLAN Settings (highlighted in green), 2 VLAN (highlighted in green), 3 Security (highlighted in green), and 4 Access (highlighted in grey). The main content area is titled "Security Level" and contains four dropdown menus: "Splash page type:" set to "None", "WISPr:" set to "Disabled", "Blacklisting:" set to "Disabled", and "Encryption:" set to "Disabled". At the bottom right of the window, there are three buttons: "Back", "Next", and "Cancel".

4. Click **Next** and then click **Finish**.

## External Captive Portal

Dell W-Instant supports external captive portal authentication. The external portal can be on the cloud or on a server outside the enterprise network.

### Configuring External Captive Portal Authentication when Adding a Guest Network

To configure external captive portal authentication when adding a guest network, perform the following steps:

1. In the **Network** tab, click the **New** link. The **New WLAN** window appears.
2. In the **WLAN Settings** tab, perform the following:
  1. Enter a name for the network in the **Name (SSID)** text box.
  2. Select **Guest** and click **Next** to continue.
3. Use the **VLAN** tab to specify how the clients on this network get their IP address and VLAN.
4. Click **Next** to continue.
5. In the **Security** tab, select **External - Authentication Text** from the **Splash page type** drop-down list and enter the **Auth text**. This entry is not mandatory. The Authentication text indicates the text string returned by the external server after a successful authentication.

Or

Select **External - RADIUS Server** from the **Splash page type** drop-down list and select **New** from the **Auth server 1** and **Auth server 2** to add a RADIUS server.

1. **IP or hostname** — Enter the IP address or the hostname of the external splash page server.
2. **URL** — Enter the URL for the external splash page server.
3. **Port** — Enter the number of the port to be used for communicating with the external splash page server.
4. **Redirect URL** — Specify a redirect URL if you want to override the user's original request and redirect them to another URL.

**Figure 90 - External Captive Portal when Adding a Guest Network - External RADIUS Server**

6. Select **Disabled** or **Enabled** from the **WISPr** drop-down list to disable or enable the WISPr authentication. For information on WISPr authentication, see ["WISPr Authentication" on page 132](#).
7. Select **Disabled** or **Enabled** from the **MAC authentication** drop-down list to disable or enable the MAC authentication. For information on MAC authentication, see ["MAC Authentication" on page 133](#).

**Figure 91 - External Captive Portal when Adding a Guest Network - External Authentication text**

8. **Authentication server 1:** Select **New** and update the fields for the external RADIUS server to authenticate user credentials at runtime. Refer to ["Configuring an External RADIUS Server" on page 113](#) for more details on server settings.
9. **Reauth interval** — When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.



10. **Blacklisting**— Select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
11. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.  
Navigate to **PEF > Blacklisting** in the Dell W-Series Instant UI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.
12. **Walled garden** — Click on the link to open the **Walled Garden** window. The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see "[Walled Garden Access](#)" on page 134.
13. Click **Next** to continue and then click **Finish**.

### **Configuring External Captive Portal Authentication when Editing a Guest Network**

To configure external captive portal authentication when editing a guest network, perform the following steps:

1. In the **Network** tab, click the network for which you want to configure the external captive portal authentication. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** window for the network appears.
3. Navigate to the **Security** tab and perform the following steps:
4. Select **External - RADIUS Server** or **External - Authentication Text** from the **Splash page type** drop down list.
5. Use the fields below to specify/edit the server for this guest network's splash page.

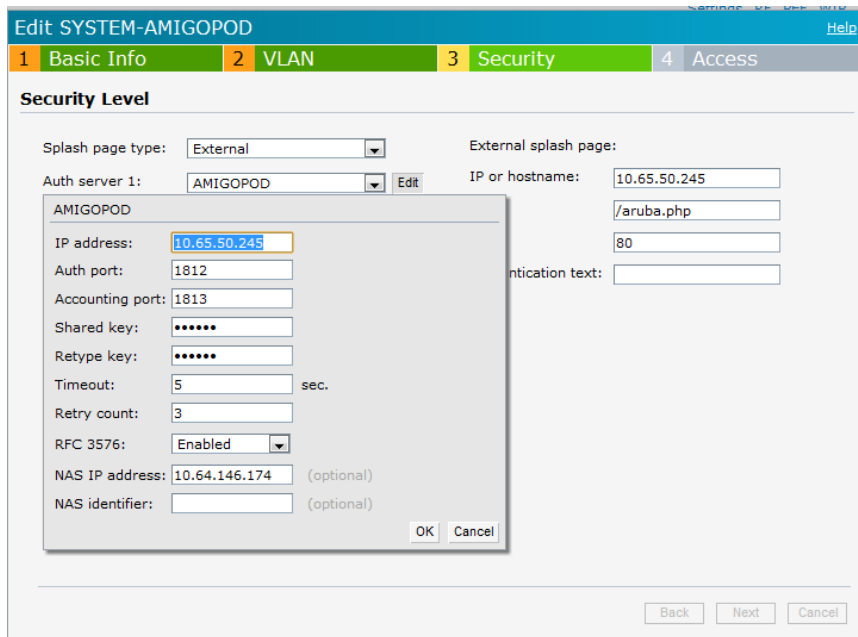
#### **Splash page type — External - Authentication Text**

- a. **Reauth interval** — When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.
- b. **Blacklisting**—Select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
- c. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.  
Navigate to **PEF > Blacklisting** in the Dell W-Series Instant UI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.
- d. **Walled Garden**— Click on the link to open the **Walled Garden** window. The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see "[Walled Garden Access](#)" on page 134.
- e. **Encryption**— Select **Enabled** from the drop-down list and perform the following steps (these steps are optional). Select the required key management option from the Key management drop-down list. Available options are:
  - WPA-2 Personal
  - WPA Personal
  - Both (WPA-2 & WPA)
  - Passphrase format — Specify either an alphanumeric or a hexadecimal string. Ensure that the hexadecimal string must be exactly 64 digits in length.
  - Passphrase — Enter a pre-shared key (PSK) passphrase.

#### **External splash page**

- IP or hostname**— Enter the IP address or the hostname of the external splash page server.
- URL**— Enter the URL for the external splash page server.
- Port**— Enter the number of the port to be used for communicating with the external splash page server.
- Auth text**— Enter the authentication text. This indicates the text string returned by the external server after a successful authentication.

**Figure 92 - Configuring External Captive Portal Authentication for a Guest Network**



- Redirect URL**— Specify a redirect URL if you want to override the user's original request and redirect them to another URL.

#### Splash page type — External- RADIUS Server

- Authentication server 1:** Click **Edit** to modify the external RADIUS servers settings. Refer to ["Configuring an External RADIUS Server" on page 113](#) for more details on server settings.
- Reauth interval**— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.
- Blacklisting**— Select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
- Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. Navigate to **PEF > Blacklisting** in the Instant UI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.
- Walled Garden**— Click on the link to open the Walled Garden window. The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see ["Walled Garden Access" on page 134](#).
- Encryption**— Select **Enabled** from the drop-down list and perform the following steps (these steps are optional). Select the required key management option from the Key management drop-down list. Available options are:

- WPA-2 Personal
- WPA Personal
- Both (WPA-2 & WPA)
- Passphrase format — Specify either an alphanumeric or a hexadecimal string. Ensure that the hexadecimal string must be exactly 64 digits in length.
- Passphrase — Enter a pre-shared key (PSK) passphrase.

#### External splash page

- a. **IP or hostname**— Enter the IP address or the hostname of the external splash page server.
  - b. **URL**— Enter the URL for the external splash page server.
  - c. **Port**— Enter the number of the port to be used for communicating with the external splash page server.
  - d. **Redirect URL**— Specify a redirect URL if you want to override the user's original request and redirect them to another URL.
6. Click **Next** and click **Finish**.

## External Captive Portal Authentication using ClearPass Guest

You can configure Instant to point to ClearPass Guest (formerly known as Amigopod) as an external Captive Portal server. User authentication is performed by:

- Matching a string in the server response
- RADIUS server (either ClearPass Guest or a different RADIUS server)

### Creating a Web Login page in the ClearPass Guest

The ClearPass Guest Visitor Management Appliance provides a simple and personalized user interface through which operational staff can quickly and securely manage visitor network access. With ClearPass Guest, your non-technical staff have controlled access to a dedicated visitor management user database. Through a customizable web portal, your staff can easily create an account, reset a password or set an expiry time for visitors. Visitors can be registered at reception and provisioned with an individual guest account that defines their visitor profile and the duration of their visit. By defining a web login page on the ClearPass Guest Visitor Management Appliance, you are able to provide a customized graphical login page for visitors accessing the network.

Refer to the *RADIUS Services* section in the **ClearPass Guest Deployment Guide** for information on setting up the RADIUS Web Login feature.

### Configuring the RADIUS Server in Instant

To configure Instant to point to ClearPass Guest as an external Captive Portal server, perform the following steps:

1. Navigate to the **Networks** tab in the Instant UI, click the **New** link. The **New WLAN** window appears.
2. In the **WLAN Settings** tab:
  - a. Enter a name for the network in the **Name (SSID)** text box. Example: ECP
  - b. Select **Guest** from the **Primary usage** options.
3. Click **Next** to continue.
4. Use the **VLAN** tab to specify how the clients on this network get their IP address and VLAN.
5. Click **Next** to continue.
6. In the **Security** tab, select **External- RADIUS Server** and update the following fields.

- a. Enter the IP address of the ClearPass Guest server in the **IP** or **hostname** field. The IP address is **10.65.77.245**.
  - b. Enter **/page\_name.php** in the **URL** field. This URL must correspond to the **Page Name** configured in the ClearPass Guest RADIUS Web Login page. For example, if the Page Name is **Dell**, then the URL should be **/Dell.php** in the Instant UI.
  - c. Enter the **Port** number (generally should be 80). The ClearPass Guest server uses this port for HTTP services.
  - d. To create an external RADIUS server, select **New** from the **Authentication server 1** drop-down list. Refer to "[Configuring an External RADIUS Server](#)" on page 113 for information on the new RADIUS server parameters.
7. The new network appears in the **Networks** tab. Click the wireless network icon on your desktop and select the new network.
  8. Open any browser and type any URL. Instant redirects the URL to ClearPass Guest login page.
  9. Log in to the network with the username and password specified used while configuring the RADIUS server in [Step d.](#)

## WISPr Authentication

Wireless Internet Service Provider roaming (WISPr) authentication allows a smart client to authenticate on the network when they roam between wireless Internet service providers, even if the wireless hotspot uses an Internet Service Provider (ISP) with whom the client may not have an account.

If you are a hotspot operator using WISPr authentication and a client that has an account with your ISP attempts to access the Internet at your hotspot, then your ISP's WISPr AAA server authenticates that client directly and allows the client access on the network. If the client only has an account with a *partner* ISP, then your ISP's WISPr AAA server forwards that client's credentials to the partner ISP's WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on your hotspot's own ISP as per their service agreements. The W-IAP assigns the default WISPr user role to the client when your ISP sends an authentication message to the W-IAP.

Instant supports the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the W-IAP.

## Configuring WISPr Authentication

To configure WISPr authentication:




---

**NOTE:** The following two types of WISPr authentication are supported:

- Internal – Authenticated
- External - RADIUS Server

Select the **Internal – Authenticated** or the **External - RADIUS Server** option from the **Splash page type** drop down before you configure WISPr authentication.

---

1. In the Dell W-Series Instant UI, click **Settings** in the top-right corner, then select the **WISPr** tab.
2. Enter the ISO Country Code section of the WISPr Location ID in the **ISO Country Code** text box.
3. Enter the E.164 Area Code section of the WISPr Location ID in the **E.164 Area Code** text box.
4. Enter the operator name of the Hotspot in the **Operator Name** text box.
5. Enter the E.164 Country Code section of the WISPr Location ID in the **E.164 Country Code** text box.
6. Enter the SSID/Zone section of the WISPr Location ID in the **SSID/Zone** text box.
7. Enter the name of the Hotspot location in the **Location Name** text box. If no name is defined, the parameter will use the name of the W-IAP to which the user has associated.
8. Click **OK** to apply the changes.

**Figure 93- Configuring WISPr Authentication**

The screenshot shows the 'Settings' window with the 'WISPr' tab selected. The window contains several input fields for configuration: 'ISO Country Code', 'E.164 Country Code', 'E.164 Area Code', 'SSID/Zone', 'Operator Name', and 'Location Name'. At the bottom, there are 'OK' and 'Cancel' buttons, and a 'Hide advanced options' link on the left.

The parameters described above, to define WISPr RADIUS attributes, are specific to the RADIUS server your ISP uses for WISPr authentication. Contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites ([www.iso.org](http://www.iso.org) and <http://www.itu.int>).



**NOTE:** A Boingo smart client uses a NAS identifier in the format <CarrierID>\_<VenueID> for location identification. To support Boingo clients, you must also configure the NAS identifier parameter in the Radius server profile for the WISPr server.

## MAC Authentication

Media Access Control (MAC) authentication is used to authenticate devices based on their physical MAC addresses. It is an early form of filtering. MAC authentication requires that the MAC address of a machine must match a manually defined list of addresses. This form of authentication does not scale past a handful of devices, because it is difficult to maintain the list

of MAC addresses. Additionally, it is easy to change the MAC address of a station to match one on the accepted list. This spoofing is trivial to perform with built-in driver tools, and it should not be relied upon to provide security.

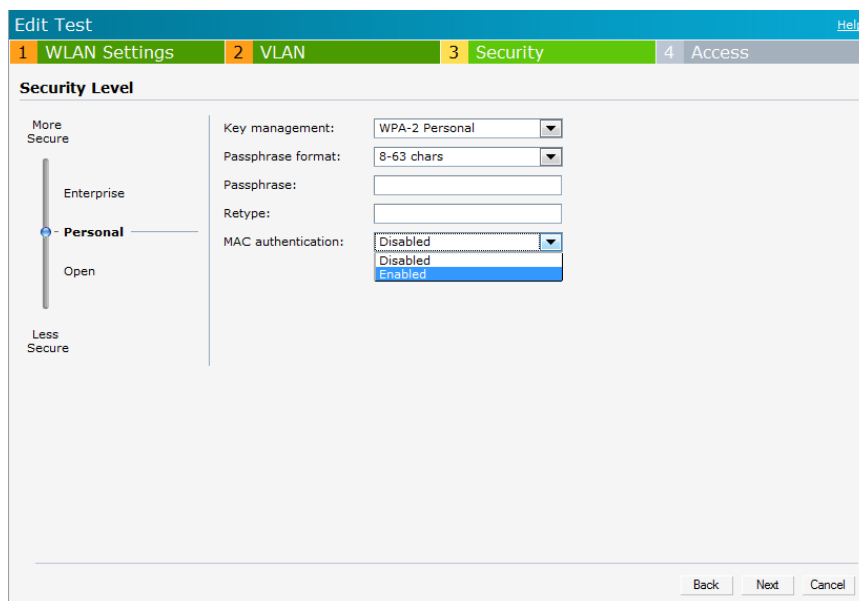
MAC authentication can be used alone, but typically it is combined with other forms of authentication, such as WEP authentication. Because MAC addresses are easily observed during transmission and easily changed on the client, this form of authentication should be considered nothing more than a minor hurdle. It is recommended that you do not use the MAC-based authentication.

## Configuring MAC Authentication

To enable MAC Authentication for a wireless network:

1. In the **Network** tab, click the network for which you want to enable MAC authentication. The **edit** link for the network appears.
2. Click the **edit** link and navigate to the **Security** tab.
3. For a network with **Personal** or **Open** security level, select **Enabled** from the **MAC authentication** drop-down list.
4. Click **OK** to continue.

**Figure 94 - Configuring MAC Authentication**



The screenshot shows the 'Edit Test' configuration window with the 'Security' tab selected. The 'Security Level' section on the left has a slider set to 'Personal'. The 'MAC authentication' dropdown menu is open, showing 'Enabled' selected. Other settings include 'Key management' set to 'WPA-2 Personal', 'Passphrase format' set to '8-63 chars', and 'Passphrase' and 'Retype' fields are empty. The 'Back', 'Next', and 'Cancel' buttons are visible at the bottom right.

5. Click **Next** and then click **Finish** to apply the changes.

## Walled Garden Access

On the Internet, a walled garden typically controls a user's access to web content and services. The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites.

## Creating a Walled Garden Access

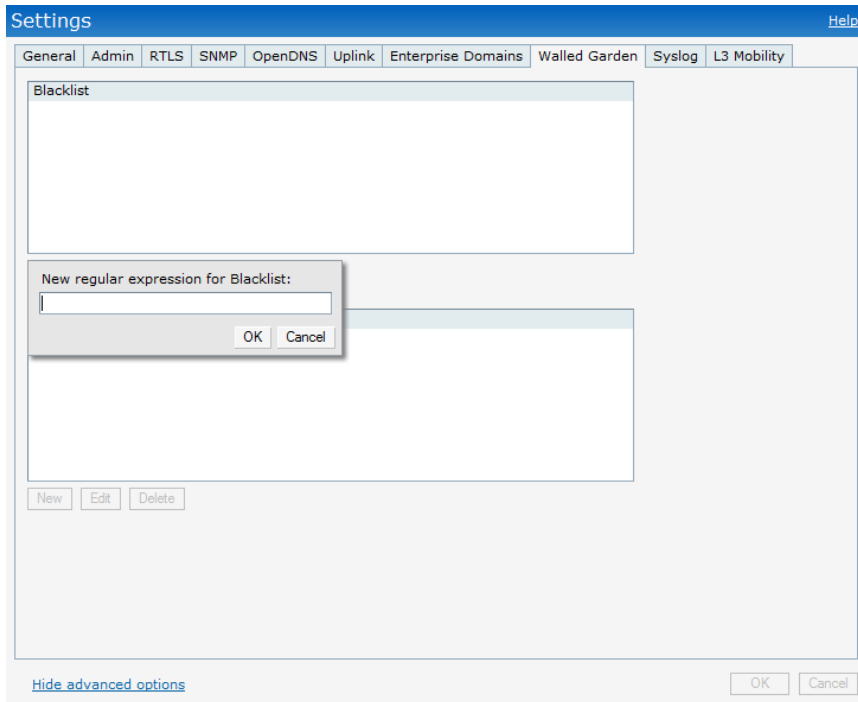
Walled garden access is needed when an external captive portal is used. A common example could be a hotel environment where unauthenticated users are allowed to navigate to a designated login

page (for example, a hotel website) and all its contents.

Users who do not sign up for Internet service can view “allowed” websites (typically hotel property websites). The website names must be DNS-based (not IP address based) and support the option to define wildcards. This works for client devices with or without HTTP proxy settings.

When a user attempts to navigate to other websites not configured in the white list walled garden profile, the user is redirected back to the login page. In addition, the black listed walled garden profile is configured to explicitly block navigation to websites from unauthenticated users.

**Figure 95 - Walled Garden**



To create a Walled Garden access:

1. Click the **Settings** at the top right corner of the Instant UI and select **Walled Garden**.
2. To allow users access to a domain, click **New** and enter the domain name or URL in the **Whitelist** section of the window. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)), for example:
  - yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
  - www.apple.com/library/test is only allow a subset of www.apple.com site corresponding to path /library/test/\*
  - favicon.ico allows access to /favicon.ico from all domains.
3. To deny users access to a domain, click **New** and enter the domain name or URL in the **Blacklist** section of the window. This prevents unauthenticated users from viewing specific websites. When a URL specified in blacklist is accessed by an unauthenticated user, W-Instant AP sends an HTTP 403 response to the client with a simple error message.  
If the requested URL neither appears on the blacklist or whitelist list then the request is redirected to the external captive portal.

4. Select the domain name/URL and click **Edit** to modify or **Delete** to remove the entry from the list.
5. Click **OK** to apply the changes.

## MAC + 802.1X Authentication

This authentication method has the following features:

- **MAC authentication must succeed before 802.1X authentication**  
The administrator is allowed to enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is done first. If MAC authentication fails, 802.1X authentication will not begin. If MAC authentication succeeds, 802.1X authentication is carried out. If 802.1X authentication succeeds, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.
- **MAC authentication only role**  
Allows an administrator to create a **mac-auth-only** role (similar to **machine-auth-only** role concept) for role-based access rules when MAC authentication is enabled for 802.1X authentication. The **macauth-only** role is assigned to a client if MAC authentication succeeds and 802.1X authentication fails. If 802.1X authentication succeeds, it will be overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.
- **L2 authentication fall-through**  
Allows an administrator to enable the **l2-authentication-fallthrough** mode. If this option is enabled and MAC authentication fails, 802.1X authentication is still allowed. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-fallthrough** mode is disabled by default.

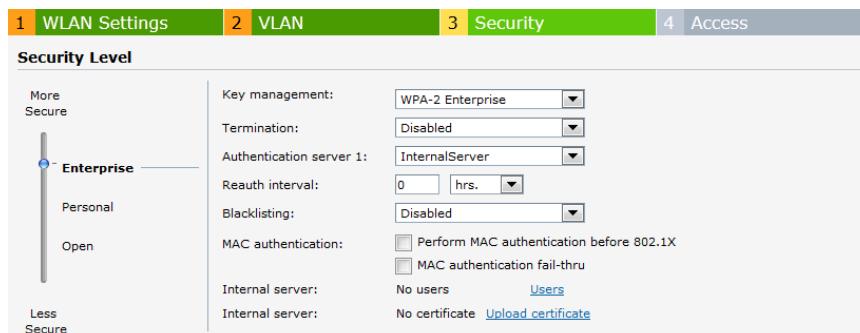
## Configuring MAC + 802.1X Authentication

To configure the MAC+802.1X authentication for a wireless network:

1. In the **Network** tab, click the network for which you want to enable MAC+802.1X authentication. The **edit** link for the network appears.
2. Click the **edit** link and navigate to the **Security** tab.
3. For a network with **Enterprise** level:
  - a. Select the check box **Perform MAC authentication before 802.1X** if you want to use 802.1X authentication only when MAC authentication is successful.
  - b. Select the check box **MAC authentication fail-thru** if you want to use 802.1X authentication even when the MAC authentication fails.



**Figure 96- Configuring MAC+802.1X Authentication**



4. Click **Next** and then click **Finish** to apply the changes.

## MAC + Captive Portal Authentication

This authentication method has the following features:

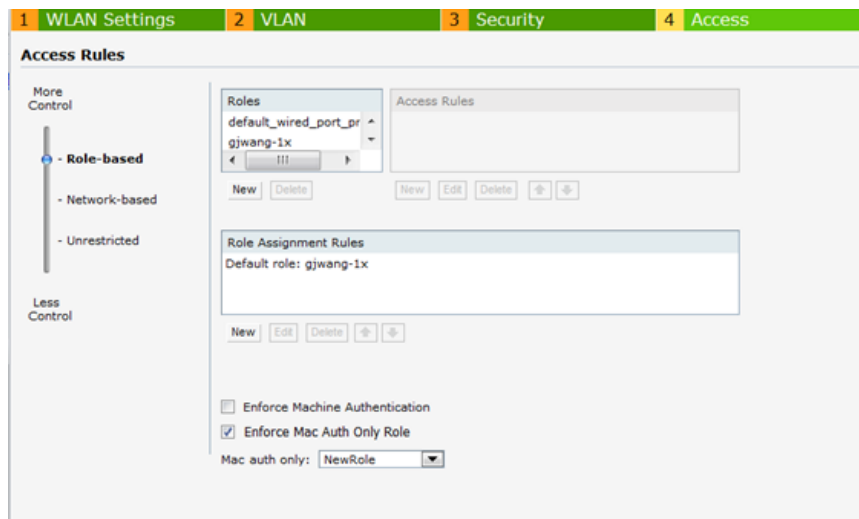
- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
- If the captive portal splash page type is **none**, MAC authentication cannot be enabled.
- MAC authentication only role— You can use the WLAN wizard to configure the **mac-auth-only** role in the role-based access rule configuration section when MAC authentication is enabled with captive portal authentication.

## Configuring MAC + Captive Portal Authentication

To configure the MAC + Captive Portal authentication for a wireless network:

1. In the **Network** tab, click the network for which you want to enable MAC+Captive Portal authentication. The **edit** link for the network appears.
2. Click the **edit** link and navigate to the **Security** tab.
3. For a network with **Role-Based** rules:
  - a. Select the check box **Enforce Machine Authentication** when MAC authentication is enabled for Captive Portal. If the MAC authentication fails, Captive Portal auth role is assigned to the client.
  - b. Select the check box **Enforce MAC Auth Only Role** when MAC authentication is enabled for Captive Portal. After successful MAC authentication, MAC auth only role is assigned to the client.

**Figure 97- Configuring MAC + Captive Portal Authentication**



4. Click **Next** and then click **Finish** to apply the changes.

## Wired Authentication on a W-IAP

W-Instant supports wired authentication on the Ethernet uplink (Ethernet 0) and downlink (Ethernet 1/Ethernet 2) ports of an W-Instant AP.

The following wired authentication methods are supported:

- MAC Authentication
- Captive Portal Authentication
- 802.1X Wired Authentication

To configure wired authentication on a W-IAP:

1. Click the **Wired** link on the upper right corner of the Dell W-Series Instant UI.
2. Click on the **Network assignments** drop-down lists to apply an existing Ethernet downlink profile to the Ethernet ports.



**NOTE:** Configure bridging on the Ethernet port before you apply a profile.

The devices (for example, IP phone / printer) connected to the wired ports are now authenticated using the profile that is applied to the port. A list of all the wired users is available in the **Wired** window.

## Certificates

A certificate is a digital file that certifies the identity of the organization or products of the organization. It is also used to establish your credentials for any web transactions. It contains the organization name, a serial number, expiration date, a copy of the certificate-holder's public key, and the digital signature of the certificate-issuing authority so that a recipient can ensure that the certificate is real.

Dell W-Instant supports the following certificate files:

- Server certificate: PEM or PKCS#12 format with passphrase (PSK)

- CA certificate: PEM or DER format

There are two ways to upload the certificates.

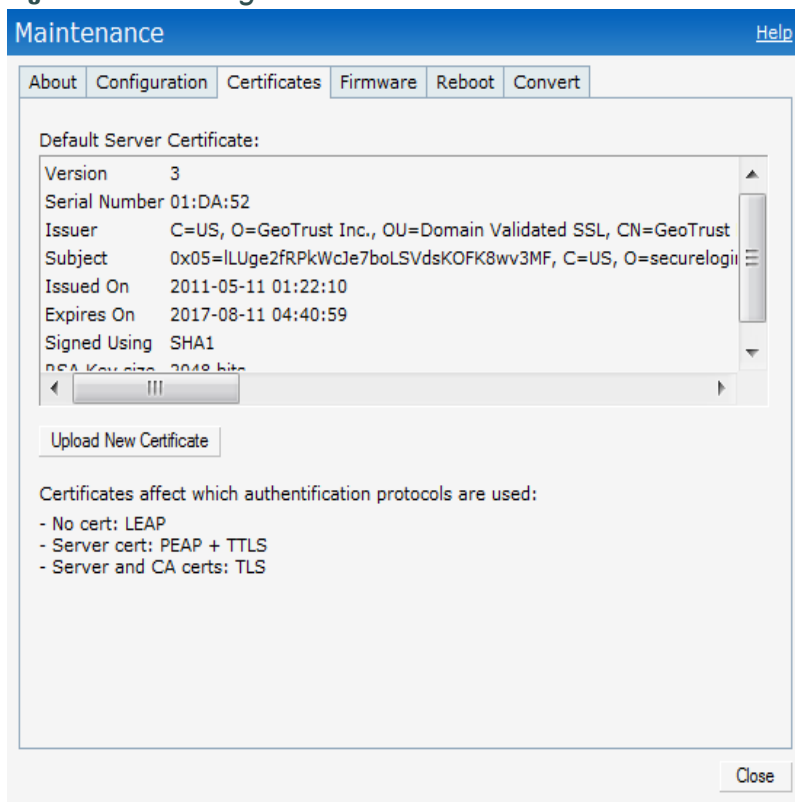
1. **Instant UI:** Navigate to **Maintenance > Certificates** and then click **Upload New Certificate** to directly upload the certificate. Refer to "[Loading Certificates using Dell W-Series Instant UI](#)" on page 139 for further instructions.
2. **Dell PowerConnect W-AirWave:** Navigate to **Device Setup > Certificate** and then click **Add New Certificate**. Refer to "[Loading Certificates using Dell PowerConnect W-AirWave](#)" on page 140 for further instructions.

### Loading Certificates using Dell W-Series Instant UI

To load a certificate in the Dell W-Series Instant UI:

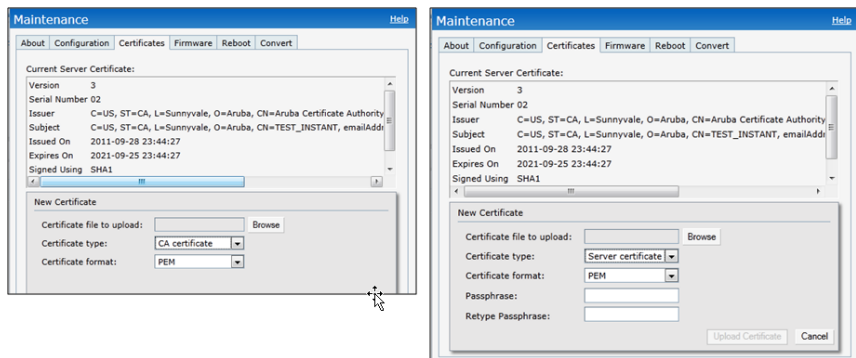
1. Navigate to the **Maintenance > Certificates** page.

**Figure 98 - Loading Certificates**



2. Click **Upload New Certificate** and the **New Certificate** window appears.

**Figure 99 - New Certificate**



3. Select the **Certificate type**— **CA certificate** and **Server certificate** from the drop-down list. The CA certificate is required to validate the client's certificate and the server certificate verifies the server's identity to the client.
4. Select the certificate format from the **Certificate format** drop-down list.
5. If you have selected **Server certificate** type, then enter a passphrase in **Passphrase** and reconfirm. The default password is **whatever**.
6. Click **Browse** and select the appropriate certificate file, and click **Upload Certificate**. The **Certificate Successfully Installed** window appears.

## Loading Certificates using Dell PowerConnect W-AirWave

You can now manage W-Instant AP certificates using the Dell PowerConnect W-AirWave Management server (AMP). The AMP directly provision the certificates for basic certificate verification (i.e certificate type, format, version, serial number etc) before accepting the certificate and uploading to a W-IAP network. The AMP packages the text of the certificate into an HTTPS message and sends it to the Virtual Controller of the W-IAP network. Once the Virtual Controller receives this message, it draws the certificate content from the message, converts it to the right format and saves it on the RADIUS server.

To load a certificate in Dell PowerConnect W-AirWave:

1. Navigate to **Device Setup > Certificate** and then click **Add** to add a new certificate. The **Certificate** window appears.
2. Enter the certificate **Name**, and click **Choose File** to browse and upload the certificate.

**Figure 100 - Loading Certificate via Dell PowerConnect W-AirWave**

The screenshot shows the 'Certificate' configuration page. The navigation bar includes 'Home', 'Groups', 'APs/Devices', 'Clients', 'Reports', 'System', 'Device Setup', and 'AMP Setup'. Below this is a sub-menu with 'Discover', 'Add', 'Communication', 'Upload Firmware & Files', and 'Certificate'. The main form has the following fields: 'Name' (text input), 'Certificate File' (button 'Choose File' and text 'No file chosen'), 'passphrase' (text input), 'Confirm passphrase' (text input), 'Format' (dropdown menu set to 'DER'), and 'Type' (dropdown menu set to 'Server Cert'). At the bottom are 'Add' and 'Cancel' buttons.

3. Select the appropriate **Format** that matches the certificate file name. Select **Server Cert** certificate **Type**, and provide the passphrase if you want to upload a Server certificate. Select either **Intermediate CA** or **Trusted CA** certificate **Type**, if you want to upload a CA certificate.

**Figure 101 - CA Certificate**

The screenshot shows the 'Certificate' configuration page with the following values: 'Name' is 'Test', 'Certificate File' is 'Root.der', 'Format' is 'DER', and 'Type' is 'Intermediate CA'. The 'passphrase' and 'Confirm passphrase' fields are empty. 'Add' and 'Cancel' buttons are at the bottom.

**Figure 102 - Server Certificate**

The screenshot shows the 'Certificate' configuration page with the following values: 'Name' is 'Test1', 'Certificate File' is 'Server.p12', 'Format' is 'PKCS#12', and 'Type' is 'Server Cert'. The 'passphrase' and 'Confirm passphrase' fields are masked with dots. 'Add' and 'Cancel' buttons are at the bottom.

4. After you upload the certificate, navigate to **Groups**, click on the Instant **Group** and then select **Basic**. The Group name appears only if you have entered the **Organization** name in the Dell W-Series Instant UI. Refer to "[Creating your Organization String](#)" on page 207 for further information.

**Figure 103 - Selecting the Group**

Name	SSTD	Total Devices	Down	Mismatched	Ignored	Clients	Usage	VPI Sessions	Up/Down Status Polling Period	Duplicate
Access Points	-	2	0	2	0	0	-	0	5 minutes	
Karhi	-	3	0	3	0	2	-	0	5 minutes	
S2500	-	1	1	0	0	0	-	0	5 minutes	
SA-ethersphere-india	-	38	0	38	0	115	3.17 Mbps	0	5 minutes	
Test_2	-	3	0	0	0	0	-	0	5 minutes	
Test_2	-	2	0	0	0	1	-	0	5 minutes	

- The Virtual Controller Certificate section displays the certificates (CA cert and Server) as highlighted in the figure below.

**Figure 104 - Virtual Controller Certificate**

Group: Test\_2

**Basic**

Name: Test\_2

Missed SNMP Poll Threshold (1-100): 1

Regulatory Domain: United States

Timezone: AMP system time

Allow One-to-One NAT:  Yes  No

Audit Configuration on Devices:  Yes  No

**SNMP Polling Periods**

Up/Down Status Polling Period: 5 minutes

Override Polling Period for Other Services:  Yes  No

AP Interface Polling Period: 10 minutes

Client Data Polling Period: 10 minutes

Thin AP Discovery Polling Period: 15 minutes

Device-to-Device Link Polling Period: 5 minutes

802.11 Counters Polling Period: 15 minutes

Rogue AP and Device Location Data Polling Period: 30 minutes

CDP Neighbor Data Polling Period: 30 minutes

**Automatic Authorization**

Add New Controllers and Autonomous Devices Location: Use Global Setting

Current Global Setting for Controllers: New Device List

Add New Thin APs Location: Use Global Setting

Current Global Setting for Thin APs: New Device List

**Maintenance Windows**

Add New AP Group Maintenance Window

**Virtual Controller Certificate**

CA Cert: Test

Server Cert: Test1

Save Save and Apply Revert

- Click **Save** to apply the changes only to Dell PowerConnect W-AirWave. Click **Save and Apply** to apply the changes to the Instant AP.



**NOTE:** To unselect the certificate options, click **Revert**.

# Chapter 11

## Encryption

### Encryption Types Supported in Dell W-Instant

Encryption is the process of converting data into an undecipherable format or code when it is transmitted on a network. Encryption prevents unauthorized use of the data. The following encryption types are supported in Dell W-Instant:

#### WEP

Though WEP is an authentication method, it is also an encryption algorithm where all users typically share the same key. WEP is easily broken with automated tools, and should be considered no more secure than an open network. Dell recommends against deploying WEP encryption. Organizations that use WEP are strongly encouraged to move to Advanced Encryption Standard (AES) encryption.

#### TKIP

TKIP uses the same encryption algorithm as WEP, but TKIP is much more secure and has an additional message integrity check (MIC). Recently some cracks have begun to appear in the TKIP encryption methods. Dell recommends that all users migrate from TKIP to AES as soon as possible.

#### AES

The Advanced Encryption Standard (AES) encryption algorithm is now widely supported and is the recommended encryption type for all wireless networks that contain any confidential data. AES in Wi-Fi leverages 802.1X or PSKs to generate per station keys for all devices. AES provides a high level of security, similar to what is used by IP Security (IPsec) clients. Dell recommends that all devices that cannot support AES be upgraded or replaced so that they are capable of AES encryption.



---

**NOTE:** WEP and TKIP are limited to WLAN connection speed of 54 Mbps. For 802.11n connection only AES encryption is supported.

---

### Encryption Recommendations

Dell recommendations for encryption on Wi-Fi networks are as follows:

- WEP —Not recommended
- TKIP— Not recommended
- AES— Recommended for all deployments

## Understanding WPA and WPA2

The Wi-Fi Alliance created the Wi-Fi Protected Access (WPA) and WPA2 certifications to describe the 802.11i standard. The standard was written to replace WEP, which was found to have numerous security flaws. It took longer than expected to complete the standard, so WPA was created based on a draft of 802.11i, which allowed people to move forward quickly to create more secure WLANs. WPA2 encompasses the full implementation of the 802.11i standard. [Table 18](#) summarizes the differences between the two certifications. WPA2 is a superset that encompasses the full WPA feature set. WPA and WPA2 can be further classified as follows:

- **Personal** — Personal is also called Pre-Shared Key (PSK). In this type, a unique key is shared with each client in the network. Users have to use this key to securely log in to the network. The key remains the same until it is changed by authorized personnel. Key change intervals can also be configured.
- **Enterprise** — Enterprise is more secure than WPA Personal. In this type, every client automatically receives a unique encryption key after securely logging on to the network. This key is long and automatically updated regularly. While WPA uses TKIP, WPA2 uses AES algorithm.

**Table 18 - WPA and WPA2 Features**

Certification	Authentication	Encryption
WPA	<ul style="list-style-type: none"> <li>• PSK</li> <li>• IEEE 802.1X with Extensible Authentication Protocol (EAP)</li> </ul>	Temporal Key Integrity Protocol (TKIP) with message integrity check (MIC)
WPA2	<ul style="list-style-type: none"> <li>• PSK</li> <li>• IEEE 802.1X with EAP</li> </ul>	Advanced Encryption Standard -- Counter Mode with Cipher Block Chaining Message Authentication Code (AESCCMP)

## Recommended Authentication and Encryption Combinations

[Table 19](#) summarizes the recommendations for authentication and encryption combinations that should be used in Wi-Fi networks.

**Table 19 - Recommended Authentication and Encryption Combinations**

Network Type	Authentication	Encryption
Employee	802.1X	AES
Guest Network	Captive Portal	None
Voice Network or Handheld devices	802.1X or PSK as supported by the device	AES if possible, TKIP or WEP if necessary (combine with restricted policy enforcement firewall (PEF) user role).



# Chapter 12

## Role Derivation

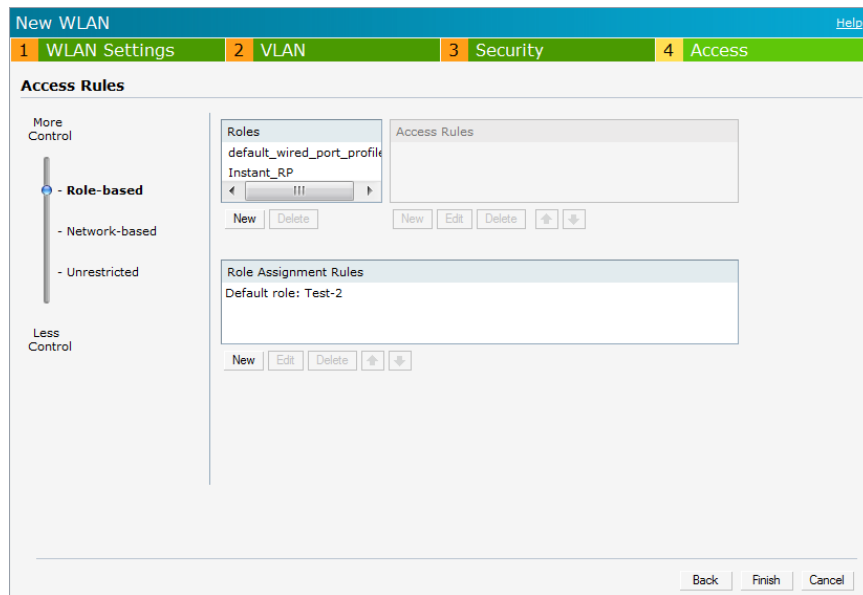
Every client in a Dell W-Instant network is associated with a user role, which determines the client's network privileges, how often it must re-authenticate, and which bandwidth contracts are applicable.

This section describes creating and assigning roles using the Dell W-Series Instant UI.

### User Roles

This section describes how to create a new user role.

**Figure 105 - Access Tab - Instant User Role Settings**



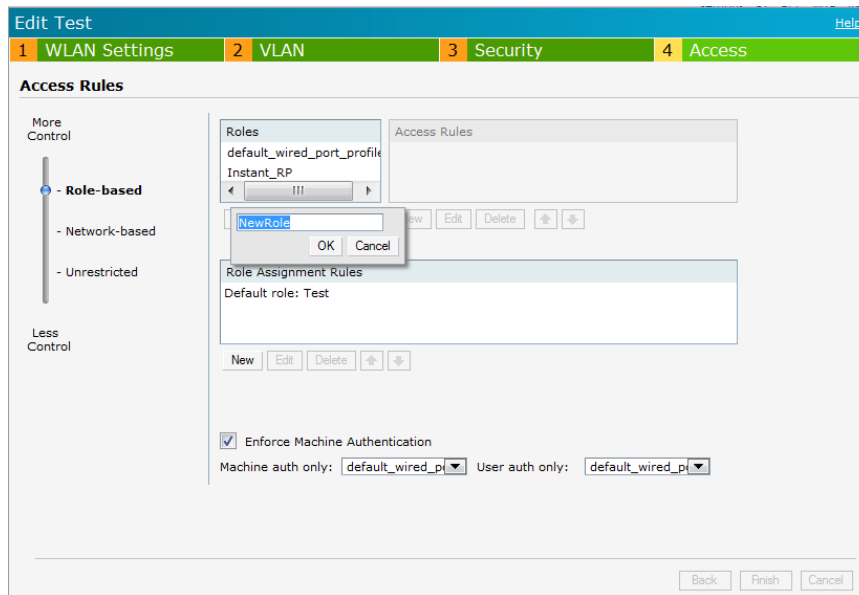
### Creating a New User Role

To create a new user role:

1. Click the **New** link in the **Networks** tab.  
To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **WLAN Settings** tab, enter the appropriate information and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN. Click **Next** to continue.
4. Click **Next** and set appropriate values in the **Security** tab.
5. Click **Next**. The **Access** tab appears.
6. Slide to **Role-based** using the scroll bar on the left.

7. Click **New**. The **New Rule** window appears. Enter the name of the new user role. To delete a user role, select the user role and click **Delete**.

**Figure 106 - Creating a New User Role**



8. Click **OK**. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To create new access rules, see ["Examples for Access Rules" on page 158](#).
9. **Assign pre-authentication role**— Use this option if you want to allow some access to users even before they are authenticated.
10. **Enforce Machine Authentication**— You can assign different rights to clients based on whether their hardware device supports machine authentication. Machine Authentication is only supported on Windows devices, so this can be used to distinguish between Windows devices and other devices such as iPads.
  - **Machine Auth only role** - This indicates a Windows machine with no user logged in. The device supports machine authentication and has a valid RADIUS account, but a user has not yet logged in and authenticated.
  - **User Auth only role** - This indicates a known user or a non-Windows device. The device does not support machine auth or does not have a RADIUS account, but the user is logged in and authenticates.

When a device does both Machine and User authentication, the user obtains the default role or the derived role based on the RADIUS attribute.

To configure Machine Authentication, do the following:

1. In the **Roles** window, create a role for **Machine auth only** and **User auth only**.
2. Configure Access Rules for these roles by selecting the role, and applying the rule. Refer to ["Examples for Access Rules" on page 158](#) for procedures to create access rules.
3. Select **Enforce Machine Authentication** and specify these two roles.
4. Click **Finish** to apply these changes.

## Creating Role Assignment Rules

This section describes the rules for determining the role that is assigned for each authenticated client.

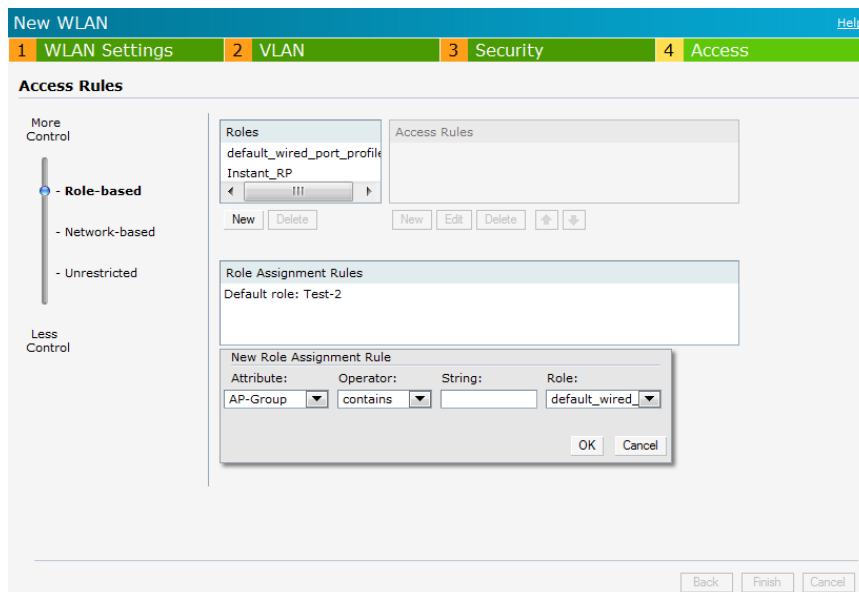


**NOTE:** When Enforce Machine Authentication is enabled, both the device and the user must be authenticated for the role assignment rule to apply.

To create role assignment rules for the user role:

1. Click **New** in the **Role Assignment Rules** section of the window. The default user role is the newly created user role.
2. Select the attribute from the **Attribute** drop-down list that the rule it matches against. The list of supported attributes includes RADIUS attributes (see ["List of Supported VSA" on page 118](#)), DHCP-Option, 802.1X-Authentication-Type, and MAC-Address.
3. Select the operator from the **Operator** drop-down list. The following types of operators are supported:
  - **contains**— To check if the attribute contains the operand value.
  - **Is the role**— To check if the role is same as the operand value.
  - **equals**— To check if the attribute is equal to the operand value.
  - **not-equals**— To check if the attribute is not equal to the operand value.
  - **starts-with**— To check if the attribute the starts with the operand value.
  - **ends-with**— To check if the attribute ends with the operand value.
4. Enter the string to match in the **String** text box.
5. Select the appropriate role from the **Role** drop-down list.
6. Click **OK**.

**Figure 107 - Creating Role Assignment Rules**



## MAC-Address Attribute

The first three octets in a MAC address are known as Organizationally Unique Identifier (OUI), and are purchased from the Institute of Electrical and Electronics Engineers, Incorporated (IEEE)

Registration Authority. This identifier uniquely identifies a vendor, manufacturer, or other organization (referred to by the IEEE as the “assignee”) globally and effectively reserves a block of each possible type of derivative identifier (such as MAC addresses) for the exclusive use of the assignee. IAP uses the OUI part of a MAC address to identify the device manufacturer and assigns a desired role for users who have completed 802.1X authentication and MAC authentication.

## DHCP Option and DHCP Fingerprinting

The DHCP fingerprinting feature allows you to identify the operating system of a device by looking at the options in the DHCP frame. Based on the operating system type, a role can be assigned to the device.

For example, in order to create a role assignment rule with DHCP option, select **equals** from the **Operator** drop-down list and enter 370103060F77FC in the **String** text box. Since 370103060F77FC is the fingerprint for Apple iOS devices such as iPad and iPhone, W-IAP assigns Apple iOS devices to the role that you choose.

**Table 20 - Validated DHCP Fingerprint**

Device	DHCP Option	DHCP Fingerprint
Apple iOS	Option 55	370103060F77FC
Android	Option 60	3C64686370636420342E302E3135
Blackberry	Option 60	3C426C61636B4265727279
Windows 7/Vista Desktop	Option 55	37010f03062c2e2f1f2179f92b
Windows XP(SP3, Home, Professional)	Option 55	37010f03062c2e2f1f21f92b
Windows Mobile	Option 60	3c4d6963726f736f66742057696e646f77732043450-0
Windows 7 Phone	Option 55	370103060f2c2e2f
Apple Mac OSX	Option 55	370103060f775ffc2c2e2f

## 802.1X-Authentication-Type

W-IAP allows you to use client 802.1X authentication to assign a desired role for users who have completed 802.1X authentication.



**NOTE:** When creating more than one role assignment rule based on RADIUS attributes, a DHCP option, and 802.1X-authentication-type, the first matching rule in the rule list is applied.

### User VLAN Derivation

W-Instant allows you to assign a user VLAN based on user attributes. When an external RADIUS authentication server is used for authentication, the user VLAN can be derived from Vendor Specific Attributes (VSAs).

The user VLAN can be derived in 802.1X authentication or MAC authentication using the following rules:

- Vendor Specific Attributes (VSA)
- VLAN derivation rule
- User role
- SSID Profile

The user VLAN cannot be derived in the following scenarios:

- Captive Portal authentication
- Guest SSID network

### Vendor Specific Attributes (VSA)

When an external RADIUS server is used, the user VLAN can be derived from the **Dell-User-Vlan** VSA. The VSA is then carried in an Access-Accept packet from the RADIUS server. The W-IAP can analyze the return message and derive the value of the VLAN which it assigns to the user.

**Figure 108 - RADIUS Access—Accept packets with VSA**

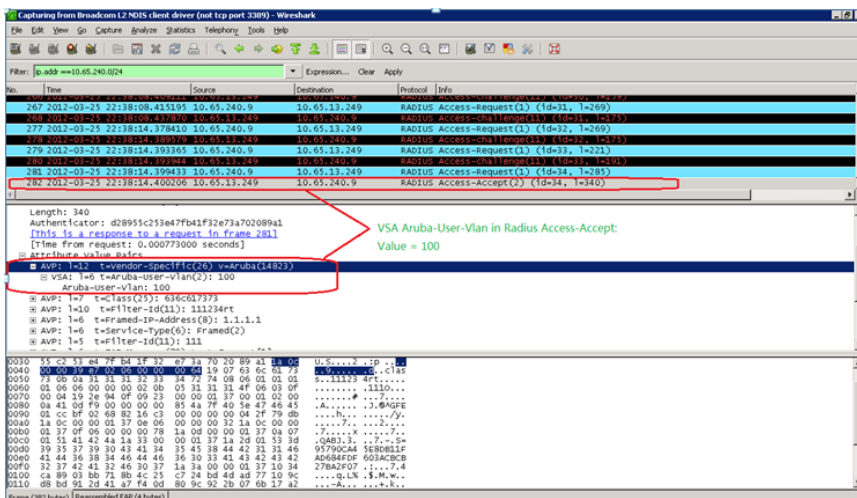
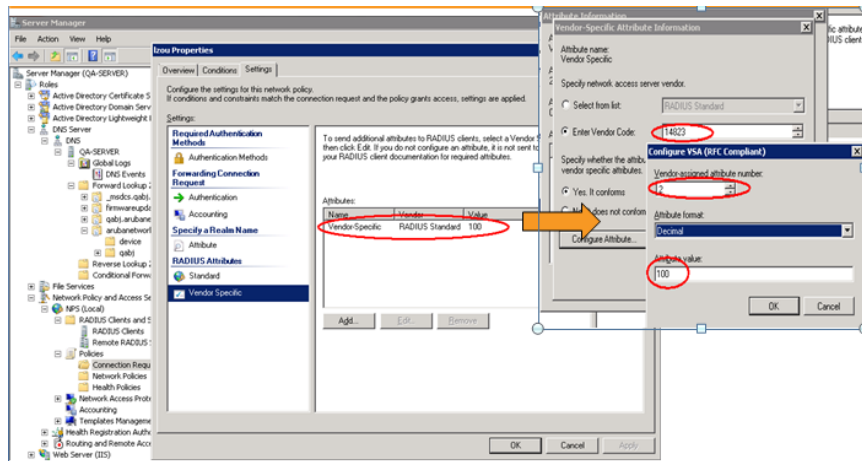


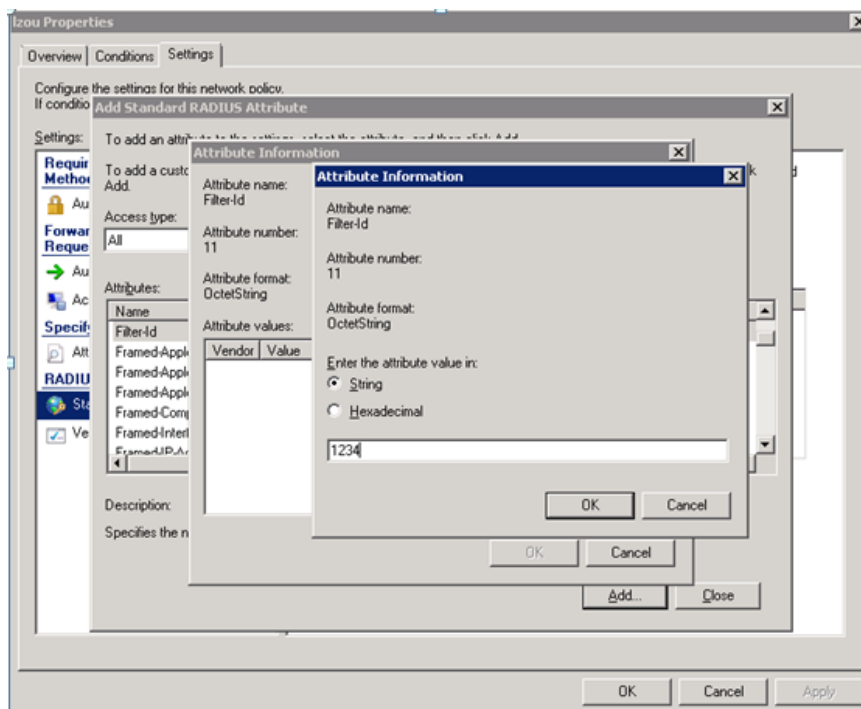
Figure 109 - Configure VSA on a RADIUS Server



## VLAN Derivation Rule

When an external RADIUS server is used for authentication, the RADIUS server may return a reply message for authentication. If the RADIUS server supports return attributes, and sets an attribute value to the reply message, W-IAP can analyze the return message and match attributes with a user pre-defined VLAN derivation rule. If the rule is matched, the VLAN value defined by the rule is assigned to the user.

Figure 110 - Configuring RADIUS Attributes on the RADIUS Server



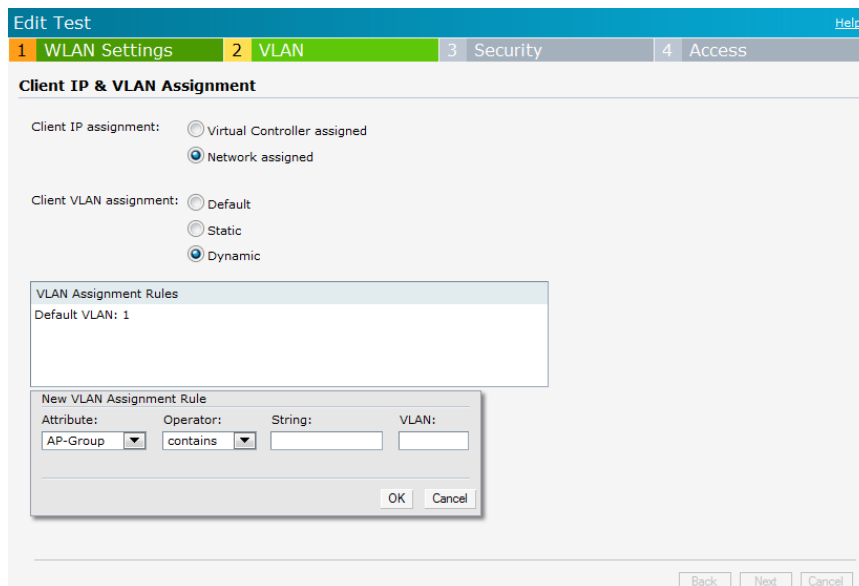
## Configuring VLAN Derivation Rules on a W-IAP

The rule assigns the user to a VLAN based on the attributes returned by the RADIUS server when the user is authenticated and the MAC address of the user.

To configure VLAN derivation rules on a W-IAP:

1. Select a network on the Instant UI and click on the **edit** link.
2. Select the **VLAN** tab and check the Dynamic radio button under the **client VLAN assignment**.
3. Click **New** to assign the user to a VLAN. The **New VLAN Assignment Rule** window appears. Enter the following information:
  - **Attribute**— Select the attribute returned by the RADIUS server during authentication or the MAC-Address.
  - **Operator**— Select an operator for matching the string.
  - **String**— Enter the string to match.
  - **VLAN**— Enter the VLAN to be assigned.
4. Click **OK**.

**Figure 111 - Configuring VLAN Derivation Rules on a W-IAP**



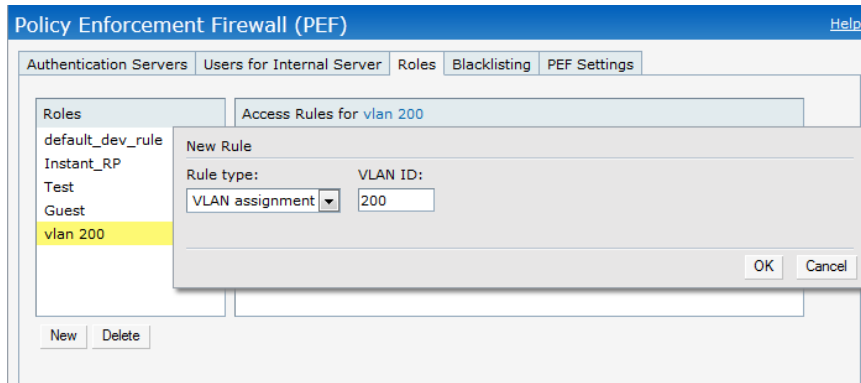
## User Role

If the VSA and VLAN derivation rules are not matching, then the user VLAN can be derived by a user role.

### Configuring a User Role

1. Click the **PEF** link at the top right corner of Dell W-Series Instant UI.
2. Select **Roles** tab.
3. Click the **New** button under roles.
4. Enter the new role in the text box and click **OK**.
5. Click the **New** button under the **Access rules**.
6. Select the **Rule type** as **VLAN assignment**.
7. Enter the ID of the VLAN in the **VLAN id** text box.
8. Click **OK**.

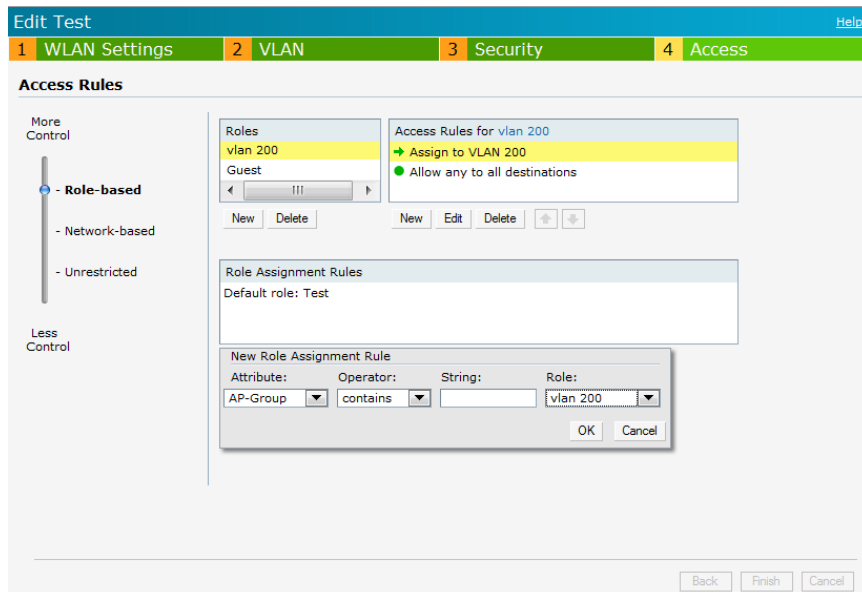
**Figure 112 - Configuring VLAN Derivation using the User Role**



To use a defined user VLAN role:

1. Select a network on the Dell W-Series Instant UI and click on the **edit** link.
2. Select the **Access** tab
3. Under **role-based**, select the defined role.
4. Select the access rule for the defined role from the list of Access rules.
5. Click the **New** button under the **New Role Assignment** window.
6. Select the attribute from the **Attribute** drop-down list.
7. Select the operator to match from the **Operator** drop-down list.
8. Enter the string to match in the **String** text box.
9. Select the role to be assigned from the **Role** text box.
10. Click **OK**.

**Figure 113 - To use a Defined User VLAN Role**



## SSID Profile

If the VSA, VLAN derivation rules are not matching, and the User Role does not contain a VLAN, then the user VLAN can be derived by the SSID profile.



## Configuring VLAN Derivation Rules Using an SSID Profile

To configure VLAN derivation rules on a W-IAP:

1. Select a network on the Dell W-Series Instant UI and click on the **edit** link.
2. Select the **VLAN** tab and check the static radio button under the **client VLAN assignment**.
3. Enter the ID of the VLAN in the **VLAN ID** text box.
4. Click **OK**.

**Figure 114** - *Configuring VLAN Derivation Rules Using an SSID Profile*

Client IP & VLAN Assignment

Client IP assignment:  Virtual Controller assigned  
 Network assigned

Client VLAN assignment:  Default  
 Static  
 Dynamic

VLAN ID:

Back Next Cancel



# Chapter 14

## Instant Firewall

A firewall is a system designed to prevent unauthorized Internet users from accessing a private network connected to the Internet. It defines access rules and monitors all data entering or leaving the network and blocks data that does not satisfy the specified security policies.

Dell W-Instant implements a W-Instant Firewall feature that uses a simplified firewall policy language. An administrator can define the firewall policies on an SSID or wireless LAN such as the Guest network or an Employee network. At the end of the authentication process, these policies are uniformly applied to users connected to that network. The W-Instant Firewall gives you the flexibility to limit packets or bandwidth available to a particular class of users. Instant Firewall manages packets according to the first rule the packet matches.

1. In the **Networks** tab, click the **New** link. The **New WLAN** window appears.
2. Navigate to **Access** tab to specify the access rules for the network.
3. Slide to **Network-based** using the scroll bar and click **New** to add a new rule.

The New Rule window consists of the following options:

- **Rule type**— Select the rule type (Access control, VLAN assignment) from the drop-down list.



---

**NOTE:** This release of W-Instant supports configuration of up to 64 access control rules.

---

- **Action**— Select **Allow**, **Deny**, or **Destination-NAT** from the drop-down list to allow or deny traffic with the specified service type and destination.
- **Log**— Select this check box if you want a log entry to be created when this rule is triggered. Instant firewall supports firewall based logging function. Firewall logs on W-IAP are generated as syslog messages.
- **Blacklist**— Select this check box if you want the client to be blacklisted when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist** time on the Blacklisting tab of the **PEF** window. See "[Client Blacklisting](#)" on page 255 for more information.
- **Classify media**— Select this check box if you want to prioritize video and voice traffic. When enabled, deep packet inspection is performed on all non-NATed traffic, and the traffic is marked as follows:
  - Video: Priority 5 (Critical)
  - Voice: Priority 6 (Internetwork Control)
- **Disable scanning**— Select this check box if you want ARM scanning to be paused when this rule is triggered, to optimize performance.



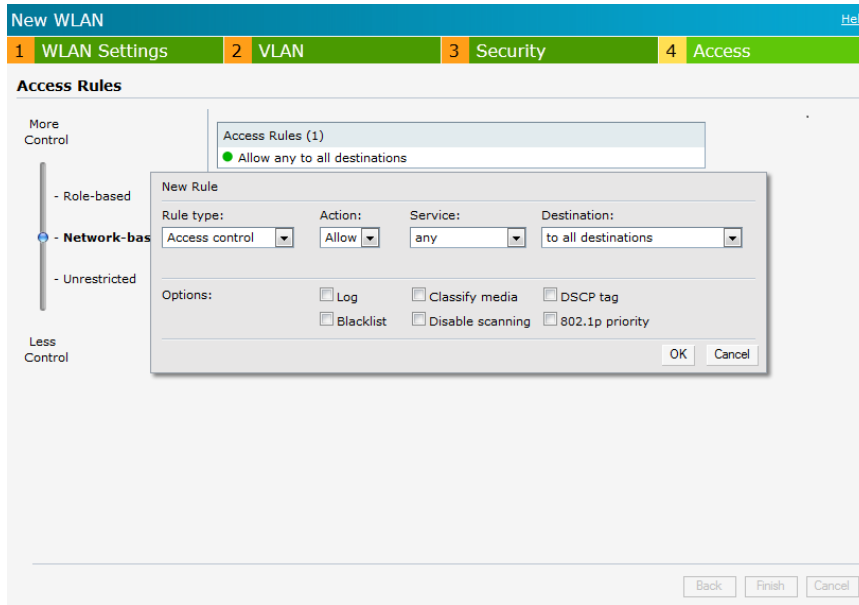
---

**NOTE:** This feature only takes effect if ARM scanning is enabled, from the ARM tab of the RF dialog.

---

- **DSCP tag**— Select this check box if you want to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value between 0 and 63. The higher the value, the higher the priority.
- **802.1p priority**— Select this check box if you want to specify an 802.1p priority. Specify a value between 0 and 7. The higher the value, the higher the priority.

**Figure 115 - Access Tab - Instant Firewall Settings**



## Service Options

[Table 21](#) lists the set of service options available in the Dell W-Series Instant UI. You can allow or deny access to any or all of these services depending on your requirements.

**Table 21 - Network Service Options**

Service	Description
any	Access is allowed or denied to all services.
custom	Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If you select the <b>Other</b> option, enter the appropriate ID.
adp	Application Distribution Protocol
bootp	Bootstrap Protocol
dhcp	Dynamic Host Configuration Protocol
dns	Domain Name Server
esp	Encapsulating Security Payload
ftp	File Transfer Protocol

Service	Description
gre	Generic Routing Encapsulation
h323-tcp	H.323-Transmission Control Protocol
h323-udp	H.323-User Datagram Protocol
http-proxy2	Hypertext Transfer Protocol-proxy2
http-proxy3	Hypertext Transfer Protocol-proxy3
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
icmp	Internet Control Message Protocol
ike	Internet Key Exchange
kerberos	Computer network authentication protocol
l2tp	Layer 2 Tunneling Protocol
lpd-tcp	Line Printer Daemon protocol-Transmission Control Protocol
lpd-udp	Line Printer Daemon protocol-User Datagram Protocol
msrpc-tcp	Microsoft Remote Procedure Call-Transmission Control Protocol
msrpc-udp	Microsoft Remote Procedure Call-User Datagram Protocol
netbios-dgm	Network Basic Input/Output System-Datagram Service
netbios-ns	Network Basic Input/Output System-Name Service
netbios-ssn	Network Basic Input/Output System-Session Service
ntp	Network Time Protocol
papi	Point of Access for Providers of Information
pop3	Post Office Protocol 3
pptp	Point-to-Point Tunneling Protocol
rtsp	Real Time Streaming Protocol
sccp	Skinny Call Control Protocol
sip	Session Initiation Protocol
sip-tcp	Session Initiation Protocol-Transmission Control Protocol
sip-udp	Session Initiation Protocol-User Datagram Protocol

Service	Description
smb-tcp	Server Message Block-Transmission Control Protocol
smb-udp	Server Message Block-User Datagram Protocol
smtp	Simple mail transfer protocol
snmp	Simple network management protocol
snmp-trap	Simple network management protocol-trap
svp	Software Validation Protocol
tftp	Trivial file transfer protocol

## Destination Options

[Table 22](#) lists the destination options available in the Dell W-Series Instant UI. You can allow or deny access to any or all of these destinations depending on your requirements.

**Table 22 - Destination Options**

Destination	Description
To all destinations	Access is allowed or denied to all destinations.
To a particular server	Access is allowed or denied to a particular server. You have to specify the IP address of the server.
Except to a particular server	Access is allowed or denied to servers other than the specified server. You have to specify the IP address of the server.
To a network	Access is allowed or denied to a network. You have to specify the IP address and netmask for the network.
Except to a network	Access is allowed or denied to networks other than the specified network. You have to specify the IP address and netmask for the network.

## Examples for Access Rules

This section provides procedures to create the following access rules.

- ["Allow TCP Service to a Particular Network" on page 158](#)
- ["Allow POP3 Service to a Particular Server" on page 159](#)
- ["Deny FTP Service except to a Particular Server" on page 160](#)
- ["Deny bootp Service except to a Particular Network" on page 161](#)

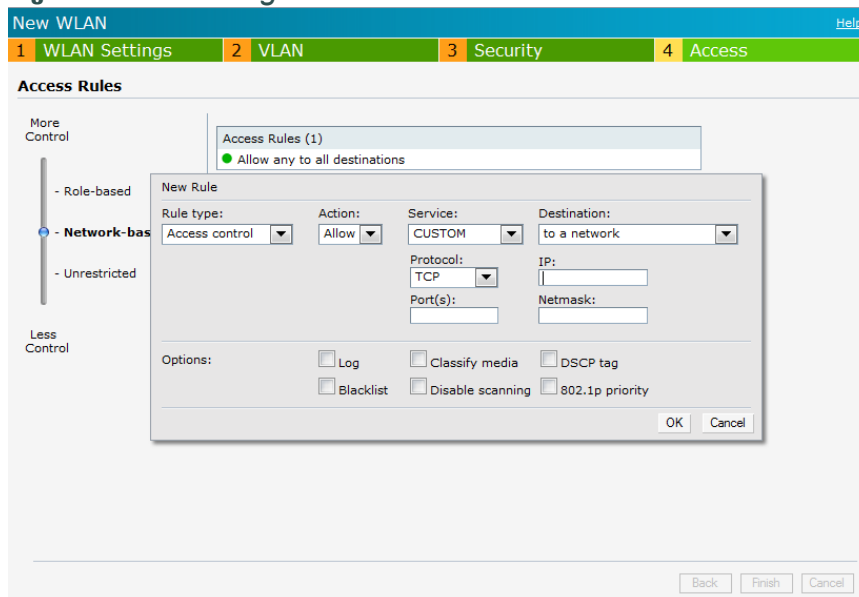
### Allow TCP Service to a Particular Network

1. Click the New link in the Networks tab.

To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.

2. In the **WLAN Settings** tab, enter the appropriate information. and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN. Click **Next** to continue.
4. Click **Next** and set appropriate values in the **Security** tab.
5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define allow TCP service access rule to a particular network:
  - a. Click **New**, the **New Rule** window appears.
  - b. Select **Allow** from the **Action** drop-down list.
  - c. Select **custom** from the **Service** drop-down list.
    - Select **TCP** from the **Protocol** drop-down list.
    - Enter appropriate port number in the **Port(s)** text box.
  - d. Select **to a network** from the **Destination** drop-down list.
    - Enter appropriate IP address in the **IP** text box.
    - Enter appropriate netmask in the **Netmask** text box.

**Figure 116 - Defining Rule — Allow TCP Service to a Particular Network**



- e. Click **OK**.
6. Click **Finish**.

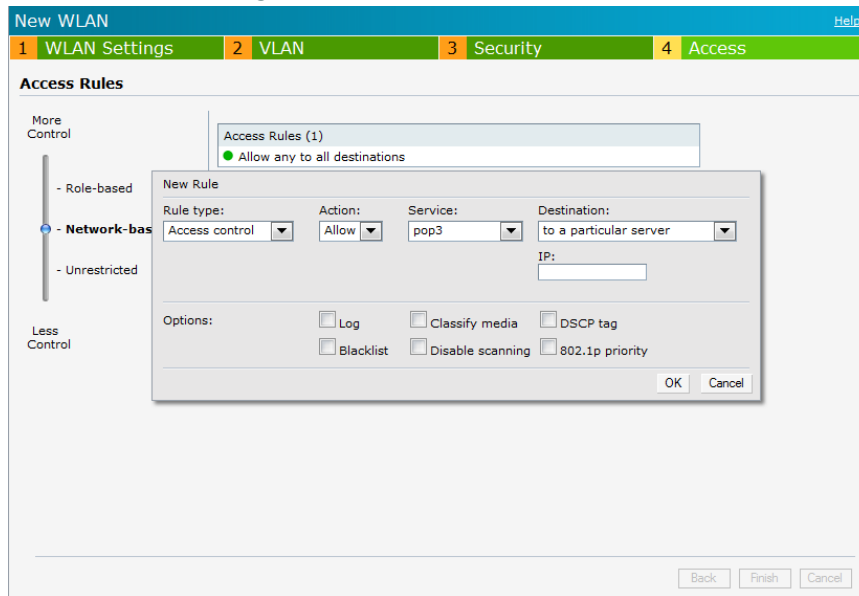
## **Allow POP3 Service to a Particular Server**

1. Click the **New** link in the **Networks** tab.

To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **WLAN Settings** tab, enter the appropriate information and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN. Click **Next** to continue.
4. Click **Next** and slide to set the appropriate security levels in the **Security** tab.

5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define allow POP3 service access rule to a particular server:
  - a. Click **New**, the **New Rule** window appears.
  - b. Select **Allow** from the **Action** drop-down list.
  - c. Select **pop3** from the **Service** drop-down list.
  - d. Select **to a particular server** from the **Destination** drop-down list and enter appropriate IP address in the IP text box.
  - e. Click **OK**.
6. Click **Finish**.

**Figure 117 - Defining Rule — Allow POP3 Service to a Particular Server**



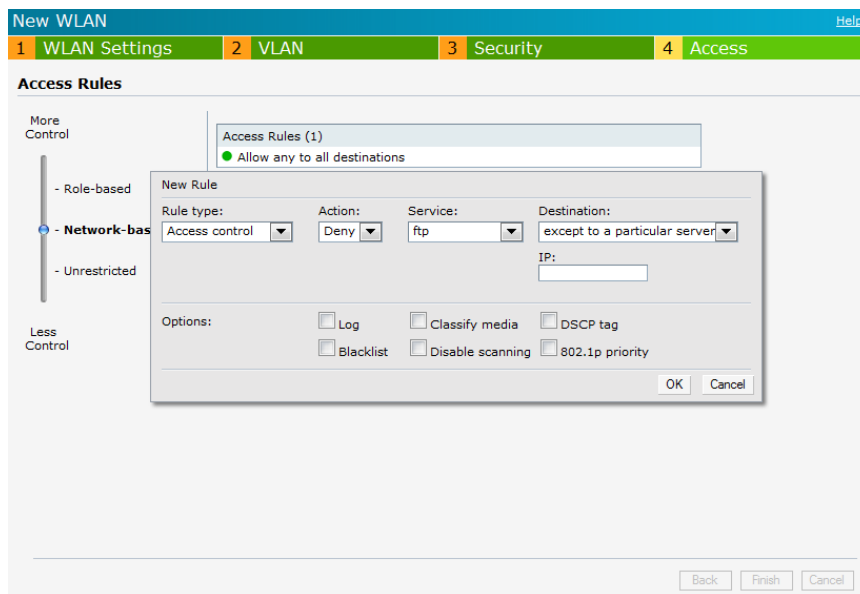
## Deny FTP Service except to a Particular Server

1. Click the **New** link in the **Networks** tab.  
To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **WLAN Settings** tab, enter the appropriate information and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN. Click **Next** to continue.
4. Click **Next** and set appropriate security levels using the slider bar in the **Security** tab.
5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define deny FTP service access rule except to a particular server:
  - a. Click **New**, the **New Rule** window appears.
  - b. Select **Deny** from the **Action** drop-down list.
  - c. Select **ftp** from the **Service** drop-down list.
  - d. Select **except to a particular server** from the **Destination** drop-down list and enter appropriate IP address in the **IP** text box.
  - e. Click **OK**



## 6. Click **Finish**

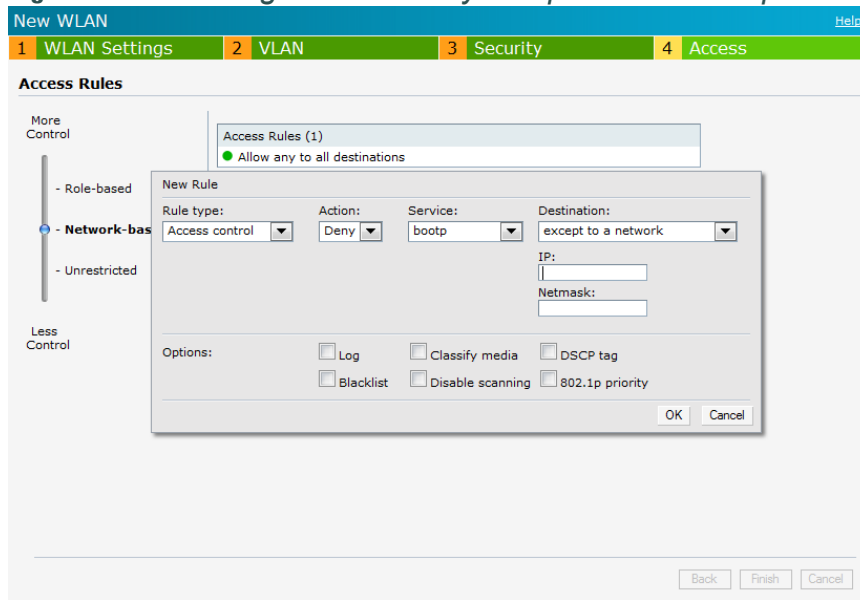
**Figure 118 - Defining Rule — Deny FTP Service Except to a Particular Server**



## Deny bootp Service except to a Particular Network

1. Click the **New** link in the **Networks** tab.  
To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **WLAN Settings** tab, enter the appropriate information, and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN. Click **Next** to continue.
4. Click **Next** and set appropriate security levels using the slider bar in the **Security** tab.
5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define deny bootp service access rule except to a network:
  - a. Click **New**, the **New Rule** window appears.
  - b. Select **Deny** from the **Action** drop-down list.
  - c. Select **bootp** from the **Service** drop-down list.
  - d. Select **except to a network** from the **Destination** drop-down list.
    - Enter the appropriate IP address in the IP text box.
    - Enter the appropriate netmask in the Netmask text box.
  - e. Click **OK**.
6. Click **Finish**.

**Figure 119 - Defining Rule — Deny bootp Service Except to a Network**



# Chapter 15

## Content Filtering

The Content Filtering feature allows you to create Internet access policies that allow or deny user access to websites based on website categories and security ratings. This feature is useful to:

- Prevent known malware hosts from accessing your wireless network.
- Improve employee productivity by limiting access to certain websites.
- Reduce bandwidth consumption significantly.

Content Filtering is based on per SSID, and up to four domain names can be configured manually. When enabled, all DNS requests to non-corporate domains on this wireless network are sent to the open DNS server.



---

**NOTE:** Regardless of whether content filtering is disabled or enabled, [instant.dell-pcw.com](http://instant.dell-pcw.com) is always resolved internally on W-Instant.

---

### Enabling Content Filtering

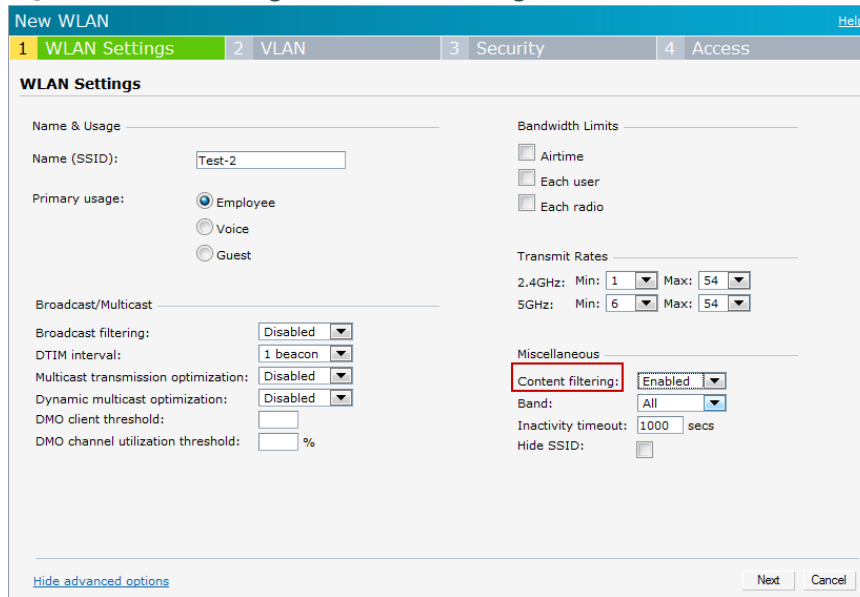
To enable content filtering per SSID:

1. Click **New** in the **Networks** tab and then click **Show advanced options**.
2. Select **Enabled** from the **Content Filtering** drop-down list and click **Next** to continue.

When Content Filtering is enabled, the internal domains check the DNS request of the clients. There are two ways to configure the internal domain.

1. Navigate to **Settings > General > click Show advanced options > DHCP Server > Domain name** to configure a domain name for a Virtual Controller assigned network. This domain name applies for Content Filtering.
2. Navigate to **Settings > General > click Show advanced options > Enterprise Domains** to configure a domain name for Content Filtering.

**Figure 120 - Enabling Content Filtering**

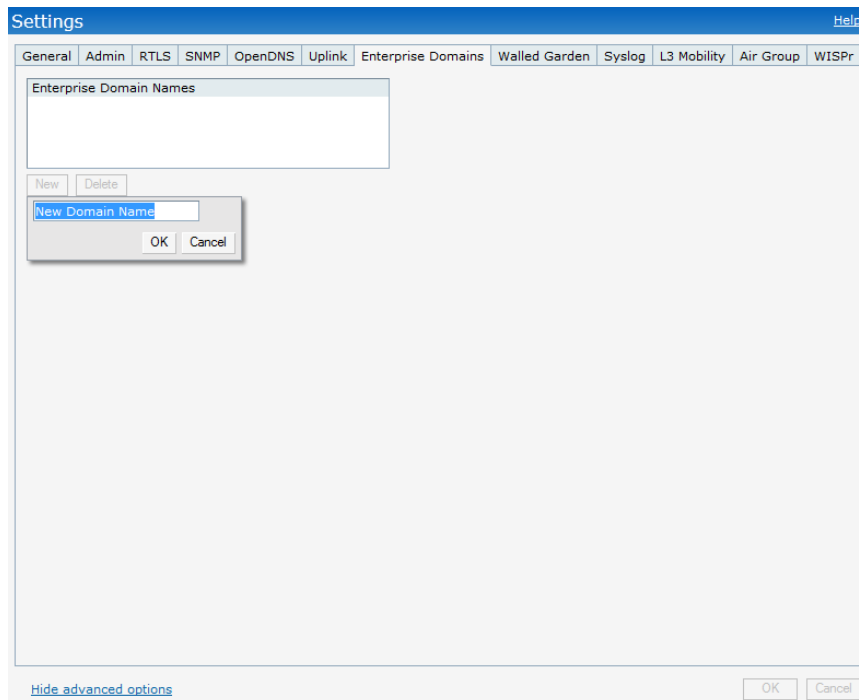


The content filtering configuration applies to all the W-IAPs in the Dell W-Instant network and the service is enabled or disabled globally across all the wireless networks that are configured in the Dell W-Series Instant UI.

## Enterprise Domains

The Enterprise Domain Names list displays all the DNS domain names that are valid on the enterprise network. This list is used to determine how client DNS requests should be routed. When **Content Filtering** is enabled for the wireless network, everything that does not match this list is sent to the open DNS server.

**Figure 121 - Enterprise Domains**



To manually add or delete a domain, perform the following steps.

1. Navigate to **Settings** at the top right corner of the Dell W-Series Instant UI and then select **Enterprise Domains** in the UI.
2. Click **New** and enter a **New Domain Name** or select the domain and click **Delete** to remove the domain name from the list.
3. Click **OK** to apply the changes.



# Chapter 16

## OS Fingerprinting

The OS Fingerprinting feature gathers information about the client that is connected to the Dell W-Instant network to find the operating system that the client is running on. The following is a list of advantages of this feature:

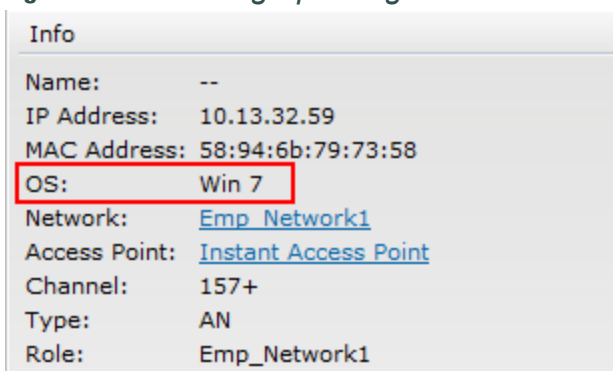
- Identifying rogue clients— Helps to identify clients that are running on forbidden operating systems.
- Identifying outdated operating systems— Helps to locate outdated and unexpected OS in the company network.
- Locating and patching vulnerable operating systems— Assists in locating and patching specific operating system versions on the network that have known vulnerabilities, thereby securing the company network.

OS Fingerprinting is enabled in the Dell W-Instant network by default. The following operating systems are identified by Dell W-Instant:

- Windows 7
- Windows Vista
- Windows Server
- Windows XP
- Windows ME
- OS-X
- iPhone
- iOS
- Android
- Blackberry
- Linux

In the following image, the OS of the client is Windows 7.

**Figure 122 - OS Fingerprinting**



Info	
Name:	--
IP Address:	10.13.32.59
MAC Address:	58:94:6b:79:73:58
OS:	Win 7
Network:	<a href="#">Emp_Network1</a>
Access Point:	<a href="#">Instant Access Point</a>
Channel:	157+
Type:	AN
Role:	Emp_Network1





# Chapter 17

## Adaptive Radio Management

Adaptive Radio Management (ARM) is a radio frequency management technology that optimizes WLAN performance even in the networks with highest traffic by dynamically and intelligently choosing the best 802.11 channel and transmitting power for each W-IAP in its current RF environment. ARM works with all standard clients, across all operating systems, while remaining in compliance with the IEEE 802.11 standards. It does not require any proprietary client software to achieve its performance goals. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. By ensuring the fair distribution of available Wi-Fi bandwidth to mobile devices, ARM ensures that data, voice, and video applications have sufficient network resources at all times. ARM allows mixed 802.11a, b, g, and n client types to inter operate at the highest performance levels.

### ARM Features

This section describes ARM features that are available in Dell W-Instant.

#### Channel or Power Assignment

This feature automatically assigns channel and power settings for all the W-IAPs in the network according to changes in the RF environment. This feature automates many setup tasks during network installation and during ongoing operations when RF conditions change.

#### Voice Aware Scanning

This feature stops a W-IAP supporting an active voice call from scanning for other channels in the RF spectrum. The W-IAP resumes scanning when no more active voice calls are present on that W-IAP. This significantly improves the voice quality when a call is in progress while simultaneously delivering automated RF management functions.

#### Load Aware Scanning

This feature dynamically adjusts scanning behavior to maintain uninterrupted data transfer on resource intensive systems when the network traffic exceeds a predefined threshold. The W-IAPs resume complete monitoring scans when the traffic drops to the normal levels.

#### Band Steering Mode

This feature moves dual-band capable clients to stay on the 5 GHz band on dual-band W-IAPs. This feature reduces co-channel interference and increases available bandwidth for dual-band clients because there are more channels on the 5 GHz band than on the 2.4 GHz band.

Band steering supports the following three different band steering modes:

- **Prefer 5 GHz**— If you configure the W-IAP to use prefer-5 GHz band steering mode, the W-IAP steers the client to 5 GHz band (if the client is 5 GHz capable) but lets the client connect on the 2.4 GHz band if the client persists in 2.4 GHz association attempts.

- **Force 5 GHz**— When the W-IAP is configured in force-5 GHz band steering mode, the W-IAP forces 5 GHz-capable W-IAPs to use that radio band.
- **Balance Bands**— In this band steering mode, the W-IAP tries to balance the clients across the two radios in order to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40MHz while the 2.5 GHz band operates in 20MHz.
- **Disabled**— Disabled means that the clients selects which band to use.

## Airtime Fairness Mode

This feature provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system, thus delivering uniform performance to all clients. This feature prevents some clients from monopolizing resources at the expense of other clients.



**NOTE:** Reboot the W-IAP after configuring the radio profile settings in order for the changes to take effect.

## Airtime Fairness Modes

Navigate to **RF** which is at the top right corner of the Instant UI and click **ARM**.

The Airtime fairness consists of the following modes:

- **Default Access**— Provides access based on the client request. When **Air Time Fairness** is set to default access, per user and per SSID bandwidth limits are not enforced
- **Fair Access**— Allocates Airtime evenly across all the clients
- **Preferred Access**— 11n clients get more airtime than 11a/11g, which get more airtime than 11b. The ratio is 16:4:1.

**Figure 123 - Airtime Fairness Mode**

The screenshot shows the 'RF' configuration window with the 'Radio' tab selected. Under 'Client Control', 'Band steering mode' is set to 'Prefer 5Ghz' and 'Airtime fairness mode' is set to 'Fair Access'. Under 'Access Point Control', 'Customize valid channels' is unchecked, 'Min transmit power' is '18', 'Max transmit power' is 'Max', 'Client aware' is 'Enabled', 'Scanning' is 'Enabled', and 'Wide channel bands' is '5GHz'. There are 'OK' and 'Cancel' buttons at the bottom right, and a 'Hide advanced options' link at the bottom left.

## Access Point Control

### Customize Valid Channels

You can customize **Valid 5 GHz channels** and **Valid 2.4 GHz channels** for 20MHz and 40MHz channels in the W-IAP. Here, the administrator can configure the ARM channels in the channel width window. The valid channels automatically show in the static channel assignment window.

### Min Transmit Power

This indicates the minimum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links. Higher power level settings may be constrained by local regulatory requirements and AP capabilities. In the event that an AP is configured for a Min Tx EIRP setting it cannot support, this value is reduced to the highest supported power setting.

The default value is 18 dBm.

### Max Transmit Power

This indicates the maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. Higher power level settings may be constrained by local regulatory requirements and AP capabilities. In the event that an AP is configured for a Max Tx EIRP setting it cannot support, this value is reduced to the highest supported power setting.

Default value: 127 dBm

### Client Aware

When **Enabled**, Adaptive Radio Management (ARM) does not change channels for the Access points when the clients are active, except for high priority events such as radar or excessive noise. This should be enabled in most deployments for a stable WLAN.

If the Client Aware mode is **Disabled**, the W-IAP may change to a more optimal channel, but this change may also disrupt current client traffic.

The Client Aware option is **Enabled** by default



---

**NOTE:** When the Client Aware ARM is disabled, channels can be changed even when the clients are active on BSSID.

---

### Scanning

When ARM is enabled, the W-IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and reports everything it sees to the W-IAP on each channel it scans. This includes, but is not limited to, data regarding WLAN coverage, interference, and intrusion detection.

### Wide Channel Bands

This feature allows administrators to configure 40 MHz channels in the 2.4 GHz and 5.0 GHz bands. 40 MHz channels are essentially two 20 MHz adjacent channels that are bonded together. 40 MHz channel effectively doubles the frequency bandwidth available for data transmission.

## Monitoring the Network with ARM

When ARM is enabled, a W-IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and provides reports for network (WLAN) coverage, interference, and intrusion detection, to a Virtual Controller.

## ARM Metrics

ARM computes coverage and interference metrics for each valid channel and chooses the best performing channel and transmit power settings for each W-IAP RF environment. Each W-IAP gathers other metrics on its ARM-assigned channel to provide a snapshot of the current RF health state.

## Configuring Administrator Assigned Radio Settings for W-IAP

Adaptive Radio Management (ARM) is enabled on Dell W-Instant by default. It automatically assigns appropriate channel and power settings for the W-IAPs.

To manually configure radio settings:

1. In the **Access Points** tab, click the AP for which you want to enable ARM. The **edit** link appears.
2. Click the **edit** link. The **Edit AP** window appears.
3. Click the **Radio** tab.

**Figure 124 - Configuring Administrator Assigned Radio Settings for W-IAP**

The screenshot shows the 'Edit Access Point' window for the AP with MAC address d8:c7:c8:c4:01:78. The 'Radio' tab is selected. The 'Mode' is set to 'Access'. For the 2.4 GHz band, 'Adaptive radio management assigned' is selected, with a channel of 1 and an empty transmit power field. For the 5 GHz band, 'Adaptive radio management assigned' is also selected, with a channel of 36 and an empty transmit power field. 'OK' and 'Cancel' buttons are at the bottom right.

4. Select the **Mode** from the drop-down list.
  - Access Mode— In Access mode the AP serves clients, while also monitoring for rogue APs in the background.

- **Monitor Mode**— In Monitor mode the AP acts as a dedicated monitor scanning all channels for rogue APs and clients.
- **Spectrum Monitor**— In the Spectrum Monitor mode the AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring APs or from non Wi-Fi devices such as microwaves and cordless phones.

By default the access point's channel and power are optimized dynamically using Adaptive Radio Management (ARM). You can override ARM on the 2.4 GHz and 5 GHz bands and set the channel and power manually if desired.

**Table 23 - Mode, Spectrum and AP Operation**

Mode	Spectrum	AP Operation
Access	Disabled	AP serves clients, while also monitoring for rogue APs in the background.
Access	Enabled	AP monitors all RF interference on its current channel, while simultaneously providing normal access services to clients.
Monitor	Disabled	AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring APs or from non Wi-Fi devices such as microwaves and cordless phones.
Monitor	Enabled	AP does not provide access service to clients.

5. Select **Administrator** assigned in **2.4 GHz** and **5 GHz** band sections.
6. Select appropriate channel number from the **Channel** drop-down list for both **2.4 GHz** and **5 GHz** band sections.
7. Enter appropriate transmit power value in the **Transmit power** text box in **2.4 GHz** and **5 GHz** band sections.
8. Click **OK**.

## Configuring Radio Profiles in Instant

Dell W-Instant supports radio profile configuration. The radio settings are available for both the 2.4-GHz and the 5-GHz radio profiles. You can configure the radios separately, using the parameters described in table on each radio.

Use the following procedure to configure W-Instant's radio attributes for the 2.4 GHz and 5 GHz frequency bands.

Figure 125 - Radio Profile

The screenshot shows the 'RF' configuration window with the 'Radio' tab selected. It is divided into two sections: '2.4 GHz band' and '5 GHz band'. Each section contains the following settings:

- Legacy only: Disabled
- 802.11d / 802.11h: Disabled
- Beacon interval: 100 ms
- Interference immunity level: 2
- Channel switch announcement count: 0
- Channel reuse type: Disabled
- Channel reuse threshold: 0 dB
- Background spectrum monitoring: Disabled

The '5 GHz band' section also includes a 'Standalone spectrum band' setting set to 'Middle'. At the bottom, there is a 'Hide advanced options' link and 'OK' and 'Cancel' buttons.

1. Navigate to **RF** which is at the top right corner of the Dell W-Series Instant UI.
2. Click **Show advanced options** to view the **Radio** tab.
3. Refer to the table below to configure the radio settings for bands 2.4 GHz and 5 GHz.

Table 24 - Radio Profile Configuration Parameters

Parameter	Description
Legacy only	Enable to run the radio in non-802.11n mode. This is disabled by default.
802.11d / 802.11h	Enable the radio to advertise its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This is disabled by default.
Beacon interval	Enter the Beacon period (60ms to 500ms) for the W-IAP in msec. This indicates how often the 802.11 beacon management frames are transmitted by the access point. The default value is 100 msec.
Interference immunity level	Select to increase the immunity level to improve performance in high-interference environments. The default immunity level is 2. <b>NOTE:</b> Increasing the immunity level makes the AP slightly "deaf" to its surroundings, causing the AP to lose a small amount of range.

Parameter	Description
	<ul style="list-style-type: none"> <li>• Level 0— no ANI adaptation.</li> <li>• Level 1— Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet.</li> <li>• Level 2— Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature.</li> <li>• Level 3— Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones.</li> <li>• Level 4— Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference.</li> <li>• Level 5— The AP completely disables PHY error reporting, improving performance by eliminating the time the W-IAP would spend on PHY processing.</li> </ul>
Channel switch announcement count	Indicates the number of channel switching announcements that must be sent prior to switching to a new channel. This allows associated clients to recover gracefully from a channel change.
Channel reuse type	<p>When set to <b>Dynamic</b>, the access point, when busy, automatically adjust its Clear Channel Assessment (CCA) threshold to accommodate transmissions to the most distant associated client.</p> <p>When set to <b>Static</b>, the access point sets its CCA threshold to the value specified in <b>Channel reuse threshold</b>.</p>
Channel reuse threshold	When set to <b>Static</b> , this value specifies the tolerable interference that must be maintained.
Background spectrum monitoring	When background spectrum monitoring is enabled, the APs in access mode continue to provide normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients on.
Standalone spectrum band	For background spectrum monitoring on the 5 GHz band, it is necessary to specify which portion of the channel to monitor: upper, middle, or lower.



**NOTE:** Reboot the W-IAP after configuring the radio profile settings in order for the changes to take effect.





Intrusion Detection System (IDS) is a feature that monitors the network for the presence of unauthorized W-IAPs and clients. It also logs information about the unauthorized W-IAPs and clients, and generates reports based on the logged information.

### Rogue AP Detection and Classification

The most important IDS functionality offered in the Dell W-Instant network is the ability to detect rogue APs, interfering 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. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat since it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

Navigate to **IDS** in the Dell W-Series Instant UI and click the **IDS** link. The built-in IDS scans for access points that are not controller by this Virtual Controller. These are listed below and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

**Figure 126 - Intrusion Detection**

Foreign Access Points Detected							Foreign Clients Detected						
MAC address	Network	Classification	Chan.	Type	Last Seen	Where	MAC address	Network	Classification	Chan.	Type	Last Seen	Where
00:24:6c:82:48:72	docomo	Interfering	1	G	11:31:07		00:26:08:b7:7a:76	ethersphere-voip	Interfering	1	GN 20MHz	11:31:07	
00:0b:86:94:28:21	HTT-SPOT	Interfering	1	G	11:31:07		1c30:94:a1:8a:8b	ethersphere-wpa2	Interfering	1	GN 20MHz	11:31:07	
00:24:6c:80:a4:52	docomo	Interfering	1	G	11:31:07		58:94:5b:57:50:38	ethersphere-wpa2	Interfering	1	GN 20MHz	11:31:07	
00:24:6c:0f:90:42	docomo	Interfering	1	G	11:31:07		2479:037:7a:57:5c	UI_DashBoard	Interfering	1	G	11:31:07	
00:24:6c:b0:bc:62	docomo	Interfering	1	G	11:31:07		00:1e:65:30:7e:09	ethersphere-wpa2	Interfering	1	GN 20MHz	11:30:51	
00:24:6c:8a:9a:09	aruba-ap	Interfering	1	GN 20MHz	11:31:07		04:46:65:8c:50:0a	ethersphere-wpa2	Interfering	1	GN 20MHz	11:30:58	
00:0b:86:94:34:62	docomo	Interfering	1	G	11:31:07		2479:037:7a:57:5c	wpd-alpha	Interfering	1	GN 20MHz	11:30:55	
00:0b:86:94:29:32	docomo	Interfering	1	G	11:31:07		00:37:6d:e2:af:52	ethersphere-voip	Interfering	1	GN 20MHz	11:30:20	
00:24:6c:33:6c:11	HTT-SPOT	Interfering	1	G	11:31:07		00:05:0a:62:3b:b7	advanced	Interfering	1	G	11:30:20	
6c:f3:7f:18:6d:58	hotspot_each	Interfering	157	AN 40MHz	11:31:07		20:02:af:9a:6b:35	ethersphere-wpa2	Interfering	1	GN 20MHz	11:29:34	
00:24:6c:33:6c:12	docomo	Interfering	1	G	11:31:07		84:29:99:11:35:04	midre-voip	Interfering	11	GN 20MHz	11:29:05	
6c:f3:7f:18:6d:20	mnwp1	Interfering	1	GN 20MHz	11:31:07		5c:0a:5b:13:a5:0d	ethersphere-voip	Interfering	11	GN 20MHz	11:28:50	
08:c7:0b:27:33:65	aanip-test	Interfering	11	GN 20MHz	11:31:07		00:17:0a:5e:7a:af	ethersphere-voip	Interfering	1	S	11:29:05	
00:24:6c:00:30:49	75POT	Interfering	1	GN 20MHz	11:31:07		20:64:32:81:d2:37	wpd-alpha	Interfering	1	GN 20MHz	11:27:49	
00:24:6c:06:82:09	75POT	Interfering	1	GN 20MHz	11:31:07		20:64:32:81:d2:37	ethersphere-wpa2	Interfering	1	BN 20MHz	11:23:34	
00:24:6c:00:4b:01	ARUBA-VISITOR	Interfering	1	GN 20MHz	11:31:07		30:84:6b:31:d2:09	midre-roaming	Interfering	11	B	11:21:48	
00:0b:86:70:4b:61	aan-mdns-pk	Interfering	1	GN 20MHz	11:31:07		00:14:0f:31:88:8a	UI_DashBoard	Interfering	6	G	11:18:18	
08:c7:0b:27:33:c2	Millford_Staff	Interfering	1	GN 20MHz	11:31:07		00:26:08:be:68:8b	ethersphere-voip	Interfering	6	GN 20MHz	11:18:18	

### Wireless Intrusion Protection (WIP)

WIP offers a wide selection of intrusion detection and protection features to protect the network against wireless threats. Like most other security-related features of the Dell network, the WIP configuration can be done on the W-IAP.

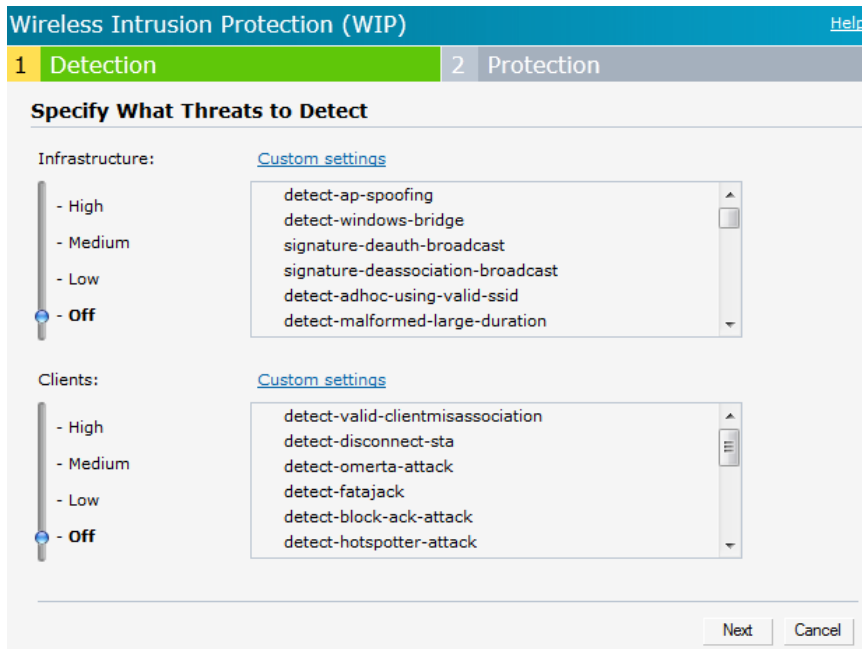
An administrator can configure the following five main options.

- **Infrastructure Detection Policies**— Specifies which wireless attacks on access points to detect
- **Client Detection Policies**— Specifies which wireless attacks on clients to detect
- **Infrastructure Protection Policies**— Specifies which wireless attacks on access points to protect against
- **Client Protection Policies**— Specifies which wireless attacks on clients to protect against
- **Containment Methods**— Prevents unauthorized stations from connecting to your W-Instant network.

In each of these options there are several default levels that enable different sets of policies. An administrator can customize (enable/disable) these options accordingly.

Four levels of detection can be configured in the WIP Detection page— **Off**, **Low**, **Medium**, and **High** (as shown in [Figure 127](#)).

**Figure 127 - Wireless Intrusion Protection— Detection**



The following table describes the detection policies that are enabled in the Infrastructure Detection Custom settings field.

**Table 25 - Infrastructure Detection Policies**

Detection Level	Detection Policy
Off	Rogue Classification
Low	<ul style="list-style-type: none"> <li>• Detect AP Spoofing</li> <li>• Detect Windows Bridge</li> <li>• IDS Signature— Deauthentication Broadcast</li> <li>• IDS Signature— Disassociation Broadcast</li> </ul>
Medium	<ul style="list-style-type: none"> <li>• Detect Adhoc networks using VALID SSID— Valid SSID list is auto-configured based on Instant AP configuration</li> <li>• Detect Malformed Frame— Large Duration</li> </ul>
High	<ul style="list-style-type: none"> <li>• Detect AP Impersonation</li> <li>• Detect Adhoc Networks</li> <li>• Detect Valid SSID Misuse</li> <li>• Detect Wireless Bridge</li> <li>• Detect 802.11 40MHz intolerance settings</li> <li>• Detect Active 802.11n Greenfield Mode</li> <li>• Detect AP Flood Attack</li> </ul>

Detection Level	Detection Policy
	<ul style="list-style-type: none"> <li>• Detect Client Flood Attack</li> <li>• Detect Bad WEP</li> <li>• Detect CTS Rate Anomaly</li> <li>• Detect RTS Rate Anomaly</li> <li>• Detect Invalid Address Combination</li> <li>• Detect Malformed Frame— HT IE</li> <li>• Detect Malformed Frame— Association Request</li> <li>• Detect Malformed Frame— Auth</li> <li>• Detect Overflow IE</li> <li>• Detect Overflow EAPOL Key</li> <li>• Detect Beacon Wrong Channel</li> <li>• Detect devices with invalid MAC OUI</li> </ul>

The following table describes the detection policies that are enabled in the Client Detection Custom settings field.

**Table 26 - Client Detection Policies**

Detection Level	Detection Policy
Off	All detection policies are disabled.
Low	<ul style="list-style-type: none"> <li>• Detect Valid Station Misassociation</li> </ul>
Medium	<ul style="list-style-type: none"> <li>• Detect Disconnect Station Attack</li> <li>• Detect Omerta Attack</li> <li>• Detect FATA-Jack Attack</li> <li>• Detect Block ACK DOS</li> <li>• Detect Hotspotter Attack</li> <li>• Detect unencrypted Valid Client</li> <li>• Detect Power Save DOS Attack</li> </ul>
High	<ul style="list-style-type: none"> <li>• Detect EAP Rate Anomaly</li> <li>• Detect Rate Anomaly</li> <li>• Detect Chop Chop Attack</li> <li>• Detect TKIP Replay Attack</li> <li>• IDS Signature— Air Jack</li> <li>• IDS Signature— ASLEAP</li> </ul>

Three levels of detection can be configured in the WIP Protection page— **Off**, **Low**, and **High** (as shown in [Figure 128](#)).

**Figure 128 - Wireless Intrusion Protection— Detection**



The following table describes the detection policies that are enabled in the Infrastructure Protection Custom settings field.

**Table 27 - Infrastructure Protection Policies**

Detection Level	Detection Policy
Off	All detection policies are disabled
Low	<ul style="list-style-type: none"> <li>Protect SSID – Valid SSID list should be auto derived from Instant configuration</li> <li>Rogue Containment</li> </ul>
High	<ul style="list-style-type: none"> <li>Protect from Adhoc Networks</li> <li>Protect AP Impersonation</li> </ul>

The following table describes the detection policies that are enabled in the Client Protection Custom settings field.

**Table 28 - Client Protection Policies**

Detection Level	Detection Policy
Off	All detection policies are disabled
Low	<ul style="list-style-type: none"> <li>Protect Valid Station</li> </ul>
High	<ul style="list-style-type: none"> <li>Protect Windows Bridge</li> </ul>

## Containment Methods

You can enable wired and wireless containments to prevent unauthorized stations from connecting to your W-Instant network.

W-Instant supports the following types of containment mechanisms:

- Wired containment— When enabled, Dell Access Points generate ARP packets on the wired network to contain wireless attacks.
- Wireless containment— When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified Access Point.
  - None— Disables all the containment mechanisms.
  - Deauthenticate only— With deauthentication containment, the Access Point or client is contained by disrupting the client association on the wireless interface.
  - Tarpit containment— With Tarpit containment, the Access Point is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the Access Point being contained.

Figure 129 - Containment Methods

Wireless Intrusion Protection (WIP) [Help](#)

1 Detection 2 Protection

### Specify What Threats to Protect

Infrastructure: [Custom settings](#)

- High  
● - **Low**  
- Off

- ✓ protect-ssid
- ✓ rogue-containment
- protect-adhoc-network
- protect-ap-impersonation

Clients: [Custom settings](#)

- High  
● - **Low**  
- Off

- ✓ protect-valid-sta
- protect-windows-bridge

Containment Methods

Wired containment: Off ▼

Wireless containment: None ▼

- None
- Deauthenticate only
- Tarpit invalid stations
- Tarpit all stations

[Hide advanced options](#)

The default containment settings are recommended. [Restore defaults](#)

Back Finish Cancel



# Chapter 19

## SNMP

Dell W-Instant supports SNMPv1, SNMPv2c, and SNMPv3 for reporting purposes only. An W-IAP cannot use SNMP to set values in an Dell system.

### SNMP Parameters for W-IAP

You can configure the following parameters for W-IAP.

**Table 29 - SNMP Parameters for W-IAP**

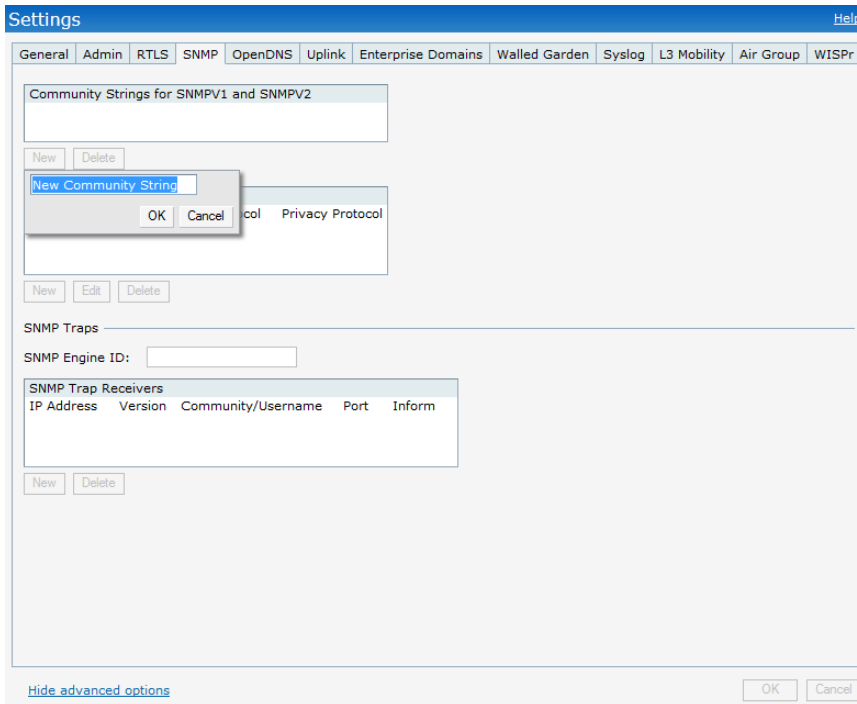
Field	Description
Community Strings for SNMPV1 and SNMPV2	An SNMP Community string is a text string that acts as a password, and is used to authenticate messages sent between the Virtual Controller and the SNMP agent.
If you are using SNMPv3 to obtain values from the Dell W-Instant, you can configure the following parameters:	
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).
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.

Follow the steps below to create community strings for SNMPV1 and SNMPV2.

1. In the Settings tab, click the **SNMP** tab.
2. Click **New** in the Community Strings for SNMPV1 and SNMPV2 box.
3. Enter the string in the **New Community String** text box.
4. Click **OK**.

To delete a community string, select the string and click **Delete**.

**Figure 130 - Creating Community Strings for SNMPV1 and SNMPV2**



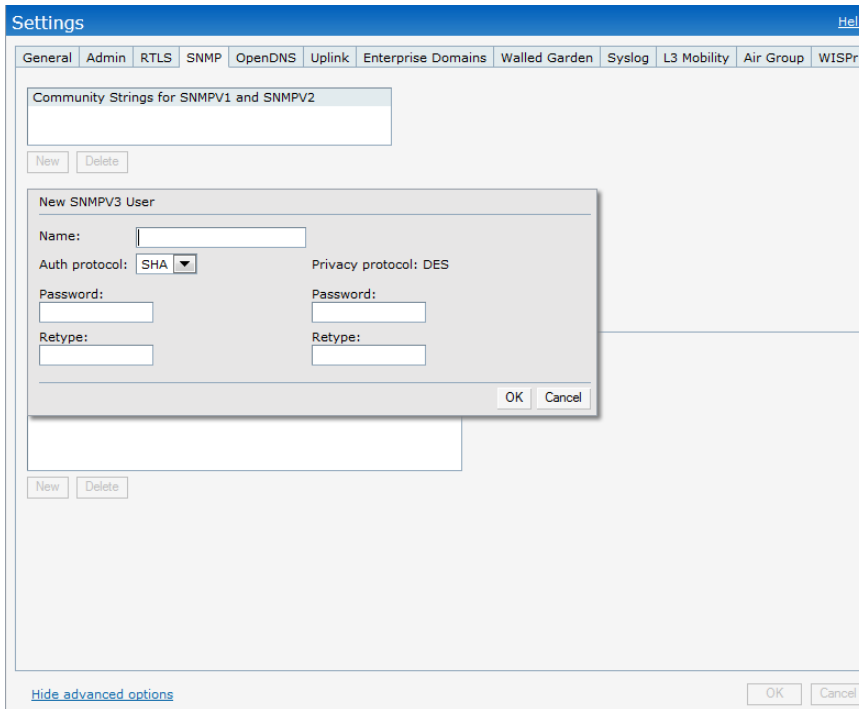
Follow the procedure below to create, edit, and delete users for SNMPV3.

1. In the **Settings** tab, click the **SNMP** tab.
2. Click **New** in the **Users for SNMPV3** box.
3. Enter the name of the user in the **Name** text box.
4. Select the type of authentication protocol from the **Auth protocol** drop-down list.
5. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box.
6. Select the type of privacy protocol from the **Privacy protocol** drop-down list.
7. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box.
8. Click **OK**.

To edit the details for a particular user, select the user and click **Edit**. To delete a particular user, select the user and click **Delete**.



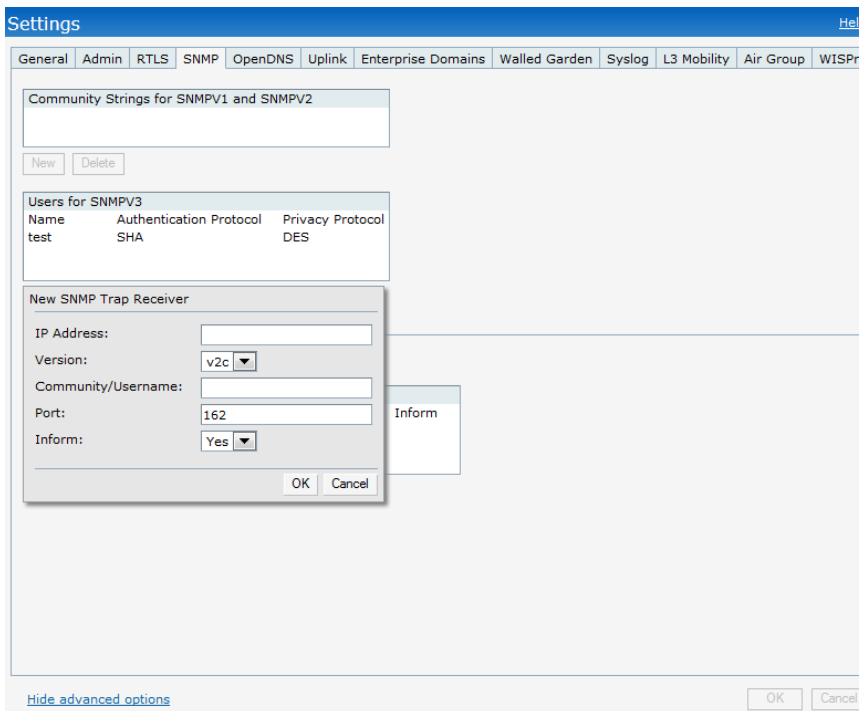
**Figure 131 - Creating Users for SNMPV3**



## SNMP Traps

Dell W-Instant supports the configuration of external trap receivers in the Dell W-Series Instant UI. Only the W-IAP acting as the Virtual Controller generates traps. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

**Figure 132 - SNMP Traps**



To configure an SNMP trap receiver:

1. Enter a name in the **SNMP Engine ID** text box. It indicates the name of the SNMP agent on the access point. SNMPV3 agent has an engine ID that uniquely identifies the agent in the device and is unique to that internal network.
2. Click **New** and update the following fields:
  1. **IP Address**— Enter the **IP Address** of the new SNMP Trap receiver.
  2. **Version**— Select the SNMP version— **v1**, **v2c**, **v3** from the drop-down list. The version specifies the format of traps generated by the access point.
  3. **Community/Username**— Specify the community string for SNMPV1 and SNMPV2c traps and a username for SNMPV3 traps.
  4. **Port**— Enter the port to which the traps are sent. The default value is 162.
  5. **Inform**— When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPV3 only. The default value is **Yes**.
3. Click **OK** to view the trap receiver information in the **SNMP Trap Receivers** window.



---

**NOTE:** Dell-specific management Information bases (MIBs) describe the objects that can be managed using SNMP. See the *Dell PowerConnect W-Series Instant Access Point 6.2.0.0-3.2.0.0 MIB Reference Guide* for information about the Dell MIBs and SNMP traps.

---

# Chapter 20

## Ethernet Downlink

### Ethernet Downlink Overview

The Ethernet downlink ports allow third party devices such as VoIP phones or printers (which support only wired connections) to connect to the wireless network. Additionally, an Access Control List (ACL) can be configured for added security on the Ethernet downlink.



---

**NOTE:** This release of W-Instant supports only the OpenAuth mechanism.

---

### Ethernet Downlink Profile Parameters

To create a new Ethernet downlink profile:

1. Click on the **Wired** link on the top right corner of the W-Instant.
2. Click on the **New** button below the **Wired Networks** window and enter the following information in the **Wired** tab.

**Table 30 - Ethernet Downlink Profile Parameters - Wired Tab**

Field	Description
Name	Name of the Ethernet downlink profile.
Primary Usage	<ul style="list-style-type: none"><li>• <b>Employee</b> — Employee access.</li><li>• <b>Guest</b> — Guest access.</li></ul>
Speed/Duplex	Only experienced network administrators should change the speed and duplex parameters manually.
POE	When enabled, the system passes electric power along with the data on the Ethernet cable. <b>NOTE:</b> The Power Sourcing Equipment (PSE) functionality is available only for the Ethernet port2 on W-IAP3WNP.
Admin Status	Displays the status of the admin.

The following figure displays the wired parameters of the Ethernet profile configuration:

**Figure 133 - Ethernet Profile Configuration - Wired Tab**

3. Click the **VLAN** tab or click **Next** and enter the following information:

**Table 31 - Ethernet Downlink Profile Parameters - VLAN Tab**

Field	Description
Mode	<ul style="list-style-type: none"> <li>In <b>Access mode</b> the port carries a single VLAN, specified as the Native VLAN.</li> <li>In <b>Trunk mode</b> the port carries packets for multiple VLANs, specified as the Allowed VALN.</li> </ul>
Native VLAN	Specifies the VLAN carried by the port in Access mode.
Allowed VLANs	Specifies the VLAN carried by the port in Trunk mode.

The following figure displays the VLAN parameters of the Ethernet profile configuration:

**Figure 134 - Ethernet Profile Configuration — VLAN Tab**

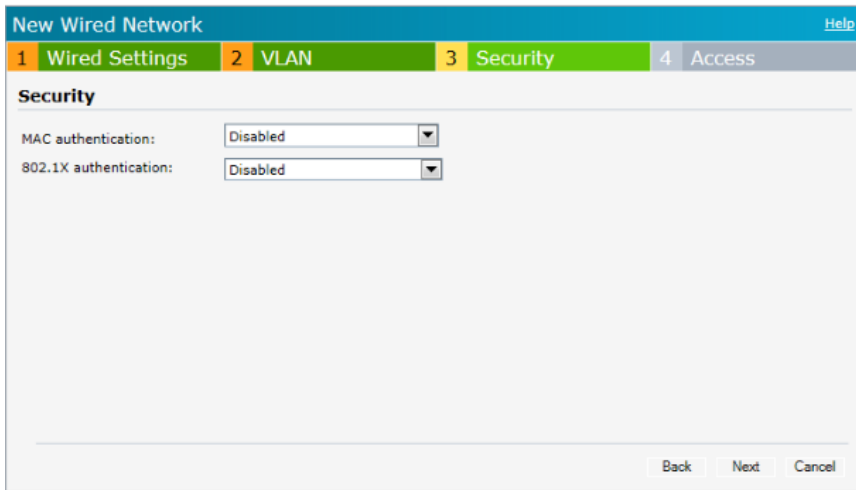
4. Click on **Security** tab or click on **Next** and enter the following information:

**Table 32 - Ethernet Downlink Profile Parameters - Security Tab**

Field	Description
MAC authentication	<ul style="list-style-type: none"> <li>• <b>Disable</b>— Disable MAC Authentication on the profile (default).</li> <li>• <b>Enable</b>— Enable MAC Authentication on the profile.</li> </ul>

The following figure displays the security parameters of the Ethernet profile configuration:

**Figure 135 - Ethernet Profile Configuration - Security Tab**



5. Click the **Access** tab and configure the access rule for the profile.

**Table 33 - Ethernet Downlink Profile Parameters - Access Tab**

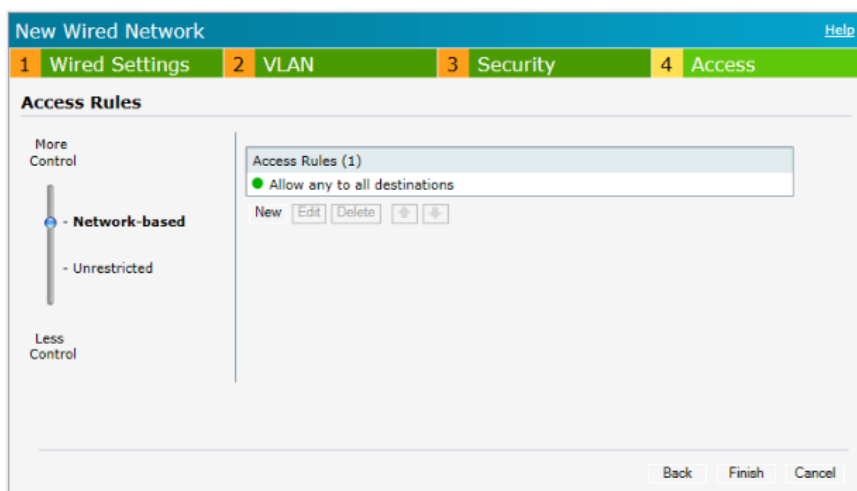
Field	Description
Access Rules	<ul style="list-style-type: none"> <li>• <b>Unrestricted</b>— User obtains unrestricted access on the port.</li> <li>• <b>Network-based</b>— User is authenticated using the access rules defined here.</li> </ul>



**NOTE:** This release of W-Instant supports configuration of up to 64 access rules.

The following figure displays the access parameters of the Ethernet profile configuration:

**Figure 136 - Ethernet Profile Configuration - Access Tab**



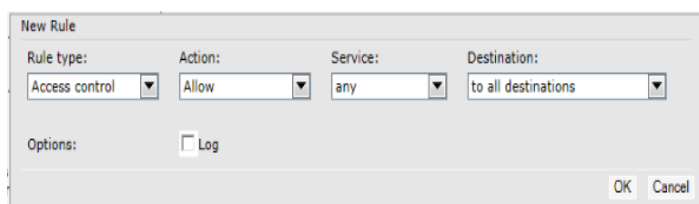
6. Click **New** in the **Access Rules** window to create a new rule and enter the following:

**Table 34 - Access Rule Parameters**

Field	Description
Rule type	<b>Access Control</b>
Action	<ul style="list-style-type: none"> <li>• <b>Allow</b>— Allow users based on the access rule.</li> <li>• <b>Deny</b>— Deny users based on the access rule.</li> </ul>
Service	Type of service.
Destination	Specify the destination.
Options	Disable or enable logging.

The following figure displays the parameters of the access rule configuration:

**Figure 137 - Access Rule Parameters**



7. Click **Finish** to configure the new network profile.
8. To edit an Ethernet downlink profile, select the configured Ethernet downlink profile and click the **Edit** button below the **Wired Networks** window.
9. To delete an Ethernet downlink profile, select the configured Ethernet downlink profile and click the **Delete** button below the **Wired Networks** window.

## Assigning a Profile to the Ethernet Port

You can assign the configured profiles to the Ethernet ports under the **Network Assignments** window.

- To assign an Ethernet downlink profile to Ethernet 0 port:

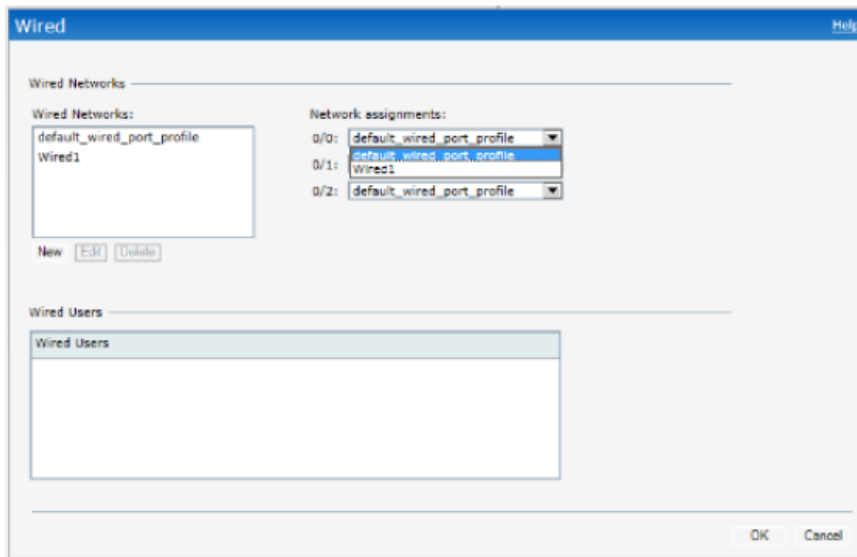
1. Enable wired bridging on the port. See "Configuring Wired Bridging on Ethernet 0" on page 79.
2. Select and assign a profile from the 0/0 drop down list.



**NOTE:** Wired bridging must be enable on Ethernet 0 (0/0) port before you can assign a Ethernet downlink profile.

- To assign an Ethernet downlink profile to Ethernet 1 port, select the profile from the 0/1 drop down list.
- To assign an Ethernet downlink profile to Ethernet 2 port, select the profile from the 0/2 drop down list.

**Figure 138 - Assigning a Profile to the Ethernet Ports**







# Chapter 21

## Hierarchical Deployment

In earlier releases of Dell W-Instant, a W-IAP could be connected to another W-IAP via the uplink port through a wired switch. If there is no wired infrastructure (Ethernet connection with a L3 NAT router), then multiple W-IAPs could not be deployed.

A W-IAP-130 series or W-IAP3WN AP (with more than one wired port) can now be connected to the downlink wired port of another W-IAP (ethX). You can provision a W-IAP with a single Ethernet port (like W-IAP-90 or W-IAP-100 series devices) to use `enet0_bridging`, so that Eth0 is converted to a downlink wired port. In such single Ethernet port platform deployments, the root AP must use the 3G uplink.

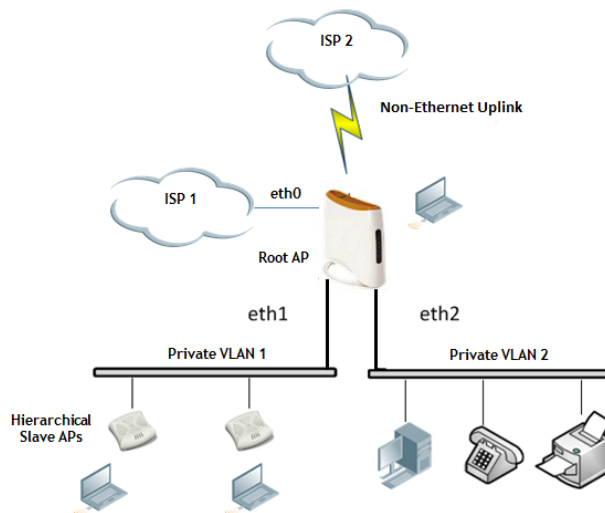
In this release of Dell W-Instant, you can form a W-IAP network by connecting the downlink port of an AP to other APs. Only one AP in the network uses its downlink port to connect to the other APs. This AP (called the root AP) acts as the wired device for the network, provides DHCP service and an L3 connection to the ISP uplink with NAT. The root AP is always the master of the Instant network. On a single Ethernet port platform, you can use `enet0_bridging` so that Eth0 is converted to a downlink wired port and the root AP must have the 3G uplink configured.

### Deployment

A typical hierarchical deployment is comprised of the following:

- A direct wired ISP connection and/or wireless uplink.
- One or more DHCP pools for private VLANs.
- One downlink port configured on a private VLAN without authentication for connecting to slave APs. This port should not be used for any wired client connection. Other downlink ports can be used for connecting to wired clients.

**Figure 139 - Hierarchical Deployment**





# Chapter 22

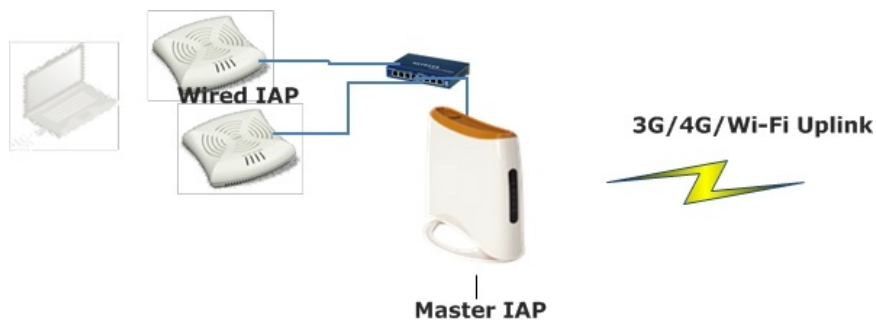
## Uplink Configuration

The Dell W-Instant network supports Ethernet and 3G/4G USB modems and the Wi-Fi uplink for the corporate Instant network. The 3G/4G USB modems and the Wi-Fi uplink can be used to extend the connectivity to places where an Ethernet uplink cannot be configured, allowing the client traffic to reach the Internet and the corporate network. It also provides a reliable backup link for the Ethernet based Instant network.

### Uplink Interface Configuration

The following figure describes the W-IAP when the Ethernet connection is not configurable on a W-IAP network. The other W-IAPs also join the Virtual Controller as slave W-IAPs through a wired or mesh Wi-Fi uplink.

**Figure 140 - Uplink Types**



The following types of uplinks are supported on Instant:

- Ethernet
  - PPPoE
  - DHCP
  - Static IP
- 3G/4G LTE modem
- Wi-Fi

### Ethernet Uplink

The Ethernet 0 port on a W-IAP is enabled as an uplink port by default.



**NOTE:** Instant does not support configuration of an Eth0 uplink.

View the type of uplink and the status of the uplink in the Dell W-Series Instant UI in the **Info** tab.

Figure 141 - Uplink Status

Info	
Name:	Instant-C4:01:78
Country code:	IN
Virtual Controller IP:	0.0.0.0
Band:	All
Master:	10.17.115.1
OpenDNS status:	Not connected
MAS integration:	Enabled
Uplink type:	Ethernet
Uplink status:	Up

### 3G/4G Uplink

W-Instant supports the use of 3G/4G USB modems to provide Internet backhaul to an W-Instant network. The 3G/4G USB modems extend client connectivity to places where an Ethernet uplink is not feasible. This enables the IAP3WN to choose the available network in an area automatically.



NOTE: The 3G and 4G LTE USB modems can be provisioned on IAP3WN and W-IAP108/109.

### Types of Modems

W-Instant supports the following three types of 3G modems:

- **True Auto Detect**— Modems of this type can be used only in one country and for a specific ISP. The parameters are configured automatically and hence no configuration is necessary (Plug and Play).
- **Auto-detect + ISP/country**— Modems of this type require the user to specify the Country and ISP. The same modem is used for different ISPs with different parameters configured for each of them.
- **No Auto-detect**—Modems of this type are used where the modems share the same Device-ID, Country, and ISP, but need to configure different parameters for each of them. These modems work with W-Instant provided the correct parameters are configured. All the new auto-detected modems falls under this category as the parameter necessary to automatically configure them are unknown.

The following table lists the types of supported 3G modems:

Table 35 - List of Supported 3G Modems

Modem Type	Supported 3G Modems
True Auto Detect	<ul style="list-style-type: none"><li>• USBConnect 881 (Sierra 881U)</li><li>• Quicksilver (Globetrotter ICON 322)</li><li>• UM100C (UTstarcom)</li><li>• Icon 452</li><li>• Aircard 250U (Sierra)</li><li>• USB 598 (Sierra)</li></ul>

Modem Type	Supported 3G Modems
	<ul style="list-style-type: none"> <li>• U300 (Franklin wireless)</li> <li>• U301 (Franklin wireless)</li> <li>• USB U760 for Virgin (Novatel)</li> <li>• USB U720 (Novatel/Qualcomm)</li> <li>• UM175 (Pantech)</li> <li>• UM150 (Pantech)</li> <li>• UMW190(Pantech)</li> <li>• SXC-1080 (Qualcomm)</li> <li>• Globetrotter ICON 225</li> <li>• UMG181</li> <li>• NTT DoCoMo L-05A (LG FOMA L05A)</li> <li>• NTT DoCoMo L-02A</li> <li>• ZTE WCDMA Technologies MSM (MF668?)</li> <li>• Fivespot (ZTE)</li> <li>• c-motech CNU-600</li> <li>• ZTE AC2736</li> <li>• SEC-8089 (EpiValley)</li> <li>• Nokia CS-10</li> <li>• NTT DoCoMo L-08C (LG)</li> <li>• NTT DoCoMo L-02C (LG)</li> <li>• Novatel MC545</li> <li>• Huawei E220 for Movistar in Spain</li> <li>• Huawei E180 for Movistar in Spain</li> <li>• ZTE-MF820</li> <li>• Huawei E173s-1</li> <li>• Sierra 320</li> <li>• Longcheer WM72</li> <li>• U600 (3G mode)</li> </ul>
Auto-detect + ISP/country	<ul style="list-style-type: none"> <li>• Sierra USB-306 (HK CLS/1010 (HK))</li> <li>• Sierra 306/308 (Telstra (Aus))</li> <li>• Sierra 503 PCIe (Telstra (Aus))</li> <li>• Sierra 312 (Telstra (Aus))</li> <li>• Aircard USB 308 (AT&amp;T's Shockwave)</li> <li>• Compass 597(Sierra) (Sprint)</li> <li>• U597 (Sierra) (Verizon)</li> <li>• Tstick C597(Sierra) (Telecom(NZ))</li> <li>• Ovation U727 (Novatel) (Sprint)</li> <li>• USB U727 (Novatel) (Verizon)</li> <li>• USB U760 (Novatel) (Sprint)</li> <li>• USB U760 (Novatel) (Verizon)</li> <li>• Novatel MiFi 2200 (Verizon Mifi 2200)</li> <li>• Huawei E272, E170, E220 (ATT)</li> <li>• Huawei E169, E180,E220,E272 (Vodafone/SmarTone (HK))</li> <li>• Huawei E160 (O2(UK))</li> <li>• Huawei E160 (SFR (France))</li> <li>• Huawei E220 (NZ and JP)</li> <li>• Huawei E176G (Telstra (Aus))</li> <li>• Huawei E1553, E176 (3/HUTCH (Aus))</li> <li>• Huawei K4505 (Vodafone/SmarTone (HK))</li> <li>• Huawei K4505 (Vodafone (UK))</li> <li>• ZTE MF656 (Netcom (norway))</li> <li>• ZTE MF636 (HK CSL/1010)</li> <li>• ZTE MF633/MF636 (Telstra (Aus))</li> </ul>

Modem Type	Supported 3G Modems
	<ul style="list-style-type: none"> <li>• ZTE MF637 (Orange in Israel)</li> <li>• Huawei E180, E1692, E1762 (Optus (Aus))</li> <li>• Huawei E1731 (Airtel-3G (India))</li> <li>• Huawei E3765 (Vodafone (Aus))</li> <li>• Huawei E3765 (T-Mobile (Germany))</li> <li>• Huawei E1552 (SingTel)</li> <li>• Huawei E1750 (T-Mobile (Germany))</li> <li>• UGM 1831 (TMobile)</li> <li>• Huawei D33HW (EMOBILE(Japan))</li> <li>• Huawei GD01 (EMOBILE(Japan))</li> <li>• Huawei EC150 (Reliance NetConnect+ (India))</li> <li>• KDDI DATA07(Huawei) (KDDI (Japan))</li> <li>• Huawei E353 (China Unicom)</li> <li>• Huawei EC167 (China Telecom)</li> <li>• Huawei E367 (Vodafone (UK))</li> <li>• Huawei E352s-5 (T-Mobile (Germany))</li> </ul>
No auto-detect	<ul style="list-style-type: none"> <li>• Huawei D41HW</li> <li>• ZTE AC2726</li> </ul>

**Table 36 - 4G Supported Modem**

Modem Type	Supported 4G Modem
True Auto Detect	<ul style="list-style-type: none"> <li>• Pantech UML290</li> </ul>



NOTE: When UML290 runs in auto detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

### Provisioning 3G/4G Uplink Manually

To provision a 3G/4G uplink manually, configure the modem parameters. The W-IAP has to be rebooted if you configure USB modem parameter from the Dell W-Series Instant UI.

Use the following procedure to provision 3G/4G uplink manually:

1. In the **settings** tab, click the **show advanced settings** link.
2. Select the **Uplink** tab. Under **3G/4G** tab, enter the parameters:
  - a. Enter the type of the 3G/4G modem driver type:
    - To provision 3G modem, enter the type of 3G modem in the **USB type** text box.
    - To provision 4G modem, enter the type of 4G modem in the **4G USB type** text box.
  - b. Enter the identifier of the modem device in the **USB dev** text box.
  - c. Enter the TTY port of the modem in the **USB tty** text box.
  - d. Enter the parameter to initialize the modem in the **USB init** text box.
  - e. Enter the parameter to dial the cell tower in the **USB dial** text box.
  - f. Enter the username used to dial the ISP in the **USB user** text box.

- g. Enter the password used to dial the ISP in the **USB password** text box.
- h. Enter the parameter used to switch modem from storage mode to modem mode in the **USB mode switch** text box.



**NOTE:** The parameter details are available from the manufacturer of your modem or from your IT administrator.

**Figure 142 - Provisioning 3G/4G Uplink— Manually**

3G/4G			
Country:	None	ISP:	None
USB type:	option	USB dial:	
4G USB type:		USB mode switch:	
USB dev:		USB user:	
USB tty:		USB password:	
USB init:			



**NOTE:** You must reboot the W-IAP after manually provisioning the W-IAP.

### Provisioning 3G Uplink Automatically

To provision a 3G uplink automatically, select only the **Country** and **ISP**. The W-IAP finds the parameters automatically.

**Figure 143 - Provisioning 3G Uplink— Automatically**

3G/4G			
Country:	India	ISP:	Verizon



**NOTE:** In the Dell W-Series Instant UI, you can view the list of country or ISP in the country and ISP drop-down lists. You can either use the country or ISP to configure the modem, or configure the individual modem parameters manually. If you cannot view the list of country or ISP from the drop-down list, then configure the modem parameters manually.

### Provisioning a 3G/4G Switch Network

To provision a 3G/4G switch network, provide the driver type for the 3G modem in the **USB type** text box and the driver type for 4G modem in the **4G USB type** text box and click **OK**.

**Figure 144 - 3G/4G Switch Network**

3G/4G			
Country:	None	ISP:	None
USB type:	pantech-3g	USB dial:	
4G USB type:	pantech-lte	USB mode switch:	
USB dev:		USB user:	
USB tty:		USB password:	
USB init:			

## Wi-Fi Uplink

The Wi-Fi uplink is supported for all the W-IAP models but only the master W-IAP uses this uplink. The Wi-Fi allows uplink to open, PSK-CCMP, and PSK-TKIP SSIDs.

- For single radio W-IAPs, the radio serves wireless clients and the Wi-Fi uplink.
- For dual radio W-IAPs, both radios can be used to serve clients but only one of them can be used for the Wi-Fi uplink.



**NOTE:** When the Wi-Fi uplink is in use, the client IP is assigned by the internal DHCP server.

You can provision an Instant AP to support the Wi-Fi uplink.

- To bind or unbind the Wi-Fi uplink on the 5 GHz band, you must reboot the W-IAP.
- If the Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two are mutually exclusive.
- As of DelLOS 6.2, APs do not support forming a Wi-Fi uplink with a W-IAP.

### Provisioning Wi-Fi Uplink

To provision the Wi-Fi Uplink:

1. Navigate to **Settings > Show advanced options > Uplink**.
2. Under WiFi, enter the name of the wireless network that is used for the Wi-Fi uplink in the Name (SSID) text box.
3. Select the type of key for uplink encryption and authentication from the **Key management** drop-down list. If the uplink wireless router uses mixed encryption, WPA-2 is suggested for Wi-Fi uplink.
4. Select the band in which the Virtual Controller is operating from the **band** drop-down list. Available options are:
  - 2.4GHz (default)
  - 5 GHz
5. Select a passphrase format from the **Passphrase format** drop-down list. Available options are:
  - 8 - 63 alphanumeric characters
  - 64 hexadecimal characters



**NOTE:** Ensure that the hexadecimal password string is exactly 64 digits in length.

6. Enter a pre-shared key (PSK) passphrase in the **Passphrase** text box.
7. Click OK.

**Figure 145-** *Provisioning Wi-Fi Uplink*

The screenshot shows a configuration window for WiFi. It has a title bar 'WiFi'. Below the title bar, there are five fields arranged in two columns. The first column contains 'Name (SSID):' with a text box containing 'test\_ssid', and 'Band:' with a dropdown menu showing '2.4GHz'. The second column contains 'Key management:' with a dropdown menu showing 'WPA-2 Personal', 'Passphrase format:' with a dropdown menu showing '8-63 chars', and 'Passphrase:' with an empty text box.

### Provisioning 3G/4G and Wi-Fi Uplink with Factory Setting

Once the W-IAP is rebooted with the factory setting:

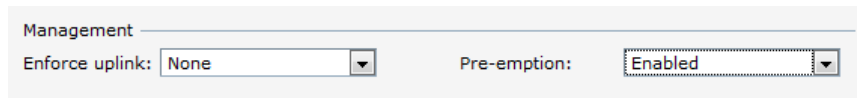


1. Plug an Ethernet cable to allow the W-IAP to get the IP address.
2. Provision the W-IAP for 3G/4G or Wi-Fi uplink (Refer to the above sections).

## Uplink Management

W-Instant allows you to set preferences for uplink preemption and switchover. The following figure shows the fields in the Dell W-Series Instant UI, which can be used for configuring the uplink preferences.

**Figure 146 - Uplink Preference**



Management

Enforce uplink:  Pre-emption:

### Enforce Uplink

This feature forces the W-IAP to use a specific uplink. For example, to enforce a 3G/4G uplink, select 3G/4G from the Enforce uplink drop-down list.



---

**NOTE:** Preemption is disabled when the Ethernet, 3G/4G or Wi-Fi uplink is enforced.

---

### Uplink Preemption

With this feature, the W-IAP tries to get a higher priority link every ten minutes even if the current uplink is up. This does not affect the current uplink connection. If the higher uplink is usable, the W-IAP switches over to that uplink. Preemption is enabled by default.

### Uplink Switchover

The default priority for uplink switchover is Ethernet and then 3G/4G. The W-IAP has the ability to switch to the lower priority uplink if the current uplink is down.



---

**NOTE:** A W-IAP reboot is not required for uplink switchover process.

---

### Uplink Switching Based on VPN Status

W-Instant supports switching uplinks based on the VPN status when deploying mixed uplinks (Eth0, 3G/4G, Wi-Fi). When VPN is used with multiple backhaul options, the W-IAP switches to an uplink connection based on the VPN connection status instead of only using Eth0, the physical backhaul link. The behavior of the uplink switching is described as follows:

- If the current uplink is Eth0 and the VPN connection is down, the W-IAP will retry to connect to VPN. This retry time depends on the configuration of primary/backup and fast-failover for VPN. If all the possibilities fail, then the W-IAP waits for a vpn-failover-timeout and then a different uplink (3G, Wi-Fi) is selected.
- If the current uplink is 3G or Wi-Fi, and Eth0 has a physical link, the W-IAP periodically suspends user traffic to try and connect to the VPN on the Eth0. If the W-IAP succeeds, then the W-IAP switches to Eth0. If the W-IAP does not succeed, then the W-IAP restores the VPN connection to the current uplink.



---

**NOTE:** This feature is automatically enabled when a VPN is configured in the W-IAP. When this feature is enabled, the W-IAP monitors the VPN status. When VPN status is down for 3 minutes, the uplink switches over (if low priority uplink is detected, and the uplink preference is set to none).

---

## Uplink Switching Based on Internet Connectivity Status

W-Instant supports switching uplinks based on Internet connectivity status.

With this feature enabled, the W-IAP continuously sends ICMP packets to some well known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, the W-IAP switches to a different connection.

To enable this feature, perform the following steps:

1. Navigate to **Settings > Show advanced options > Uplink**.
2. Under Management, select **Enabled** from the **Internet failover** drop-down list.
3. Specify the required values for Failover detection Count and Failover detection frequency.
4. Click **OK**.



---

**NOTE:** When this feature is enabled, the W-IAP ignores the VPN status, although uplink switching based on VPN status is enabled.

---

## PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a method of connecting to the Internet typically used with DSL services where the client connects to the DSL modem. You can use PPPoE for your uplink connectivity in both normal W-IAP and VPN W-IAP deployments. PPPoE is supported only in a single AP deployment.



---

**NOTE:** Uplink redundancy with the PPPoE link is not supported.

---

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. Once the PPPoE settings are configured, PPPoE has the highest priority for the uplink. The W-IAP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP). Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After you configure PPPoE, you have to reboot the W-IAP for the configuration to take effect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during bootup and if found incorrect, Ethernet is used for the uplink connection.



---

**NOTE:** When you use PPPoE, do not configure the IP address of the Virtual Controller. When you use PPPoE, do not use Dynamic RADIUS Proxy. An SSID created with default VLAN is not supported with PPPoE.

---

## Configuring PPPoE

To configure the PPPOE settings:

1. Click the **Settings** link at the upper right corner of the Dell W-Series Instant UI.
2. Click the **Show advanced options** link.
3. In the **Uplink** tab, perform the following steps in the **PPPoE** section:

- a. Enter the **PPPoE service name** provided to you by your service provider in the **Service name** field.
  - b. In the **CHAP secret** and **Retype** fields, enter the CHAP secret and confirm it.
  - c. Enter the user name for the PPPoE connection in the **User** field.
  - d. In the **Password** and **Retype** fields, enter the PPPoE password and confirm it.
4. Click **OK**.
  5. Reboot the IW-IAP for the configuration to take effect.

**Figure 147 - PPPoE Settings**

PPPoE			
Service name:	<input type="text"/>	User:	<input type="text"/>
CHAP secret:	<input type="text"/>	Password:	<input type="text"/>
Retype:	<input type="text"/>	Retype:	<input type="text"/>



## Dell PowerConnect W-AirWave Integration and Management

Dell PowerConnect W-AirWave is a powerful and easy-to-use network operations system that manages Dell wireless, wired, and remote access networks, as well as wired and wireless infrastructures from a wide range of third-party manufacturers. With its easy-to-use interface, Dell PowerConnect W-AirWave provides real-time monitoring, proactive alerts, historical reporting, and fast, efficient troubleshooting. It also offers tools that manage RF coverage, strengthen wireless security, and demonstrate regulatory compliance.

Dell W-IAPs communicate with Dell PowerConnect W-AirWave using the HTTPS protocol. This allows an Dell PowerConnect W-AirWave server to be deployed in the cloud across a NAT device, such as a router.

## Dell PowerConnect W-AirWave Features

This section describes the Dell PowerConnect W-AirWave features that are available in the Dell W-Instant network.

### Image Management

Dell PowerConnect W-AirWave allows you to manage firmware updates on WLAN devices by defining a minimum acceptable firmware version for each make and model of a device. It remotely distributes the firmware image to the WLAN devices that require updates, and it schedules the firmware updates such that updating is completed without requiring you to manually monitor the devices.

The following models can be used to upgrade the firmware:

- Automatic— In this model, the Virtual Controller (VC) periodically checks for newer updates from a configured URL and automatically initiates upgrade of the network.
- Manual— In this model, the user can manually start a firmware upgrade on a VC-by-VC basis or set the desired firmware preference per group of devices.

### W-IAP and Client Monitoring

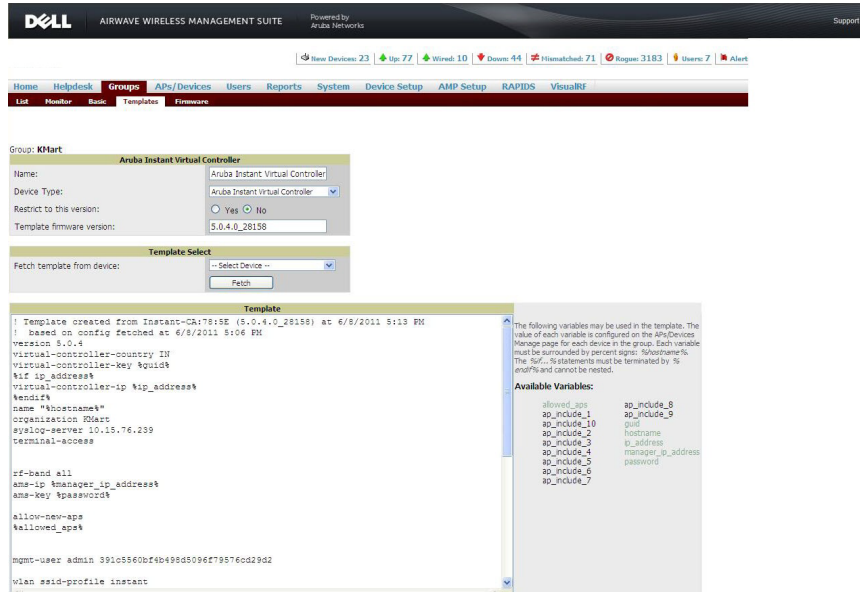
Dell PowerConnect W-AirWave allows you to find any W-IAP or client on the wireless network and to see real-time monitoring views. These monitoring views can be used to aggregate critical information and high-end monitoring information.

### Template-based Configuration

Dell PowerConnect W-AirWave automatically creates a configuration template based on any of the existing W-IAPs, and it applies that template across the network as shown in [Figure 148](#). It audits every device on an ongoing basis to ensure that configurations never vary from the

enterprise policies. It alerts you whenever a violation is detected and automatically repairs the misconfigured device.

**Figure 148 - Template-based Configuration**



## Trending Reports

Dell PowerConnect W-AirWave saves up to 14 months of actionable information, including network performance data and user roaming patterns, so you can analyze how network usage and performance trends have changed over time. It also provides detailed capacity reports with which you can plan the capacity and appropriate strategies for your organization.

## Intrusion Detection System

Dell PowerConnect W-AirWave provides advanced, rules-based rogue classification. It automatically detects rogue APs irrespective of their location in the network and prevents authorized W-IAPs from being detected as rogue W-IAPs. It tracks and correlates the IDS events to provide a complete picture of network security.

## Wireless Intrusion Detection System (WIDS) Event Reporting to Dell PowerConnect W-AirWave

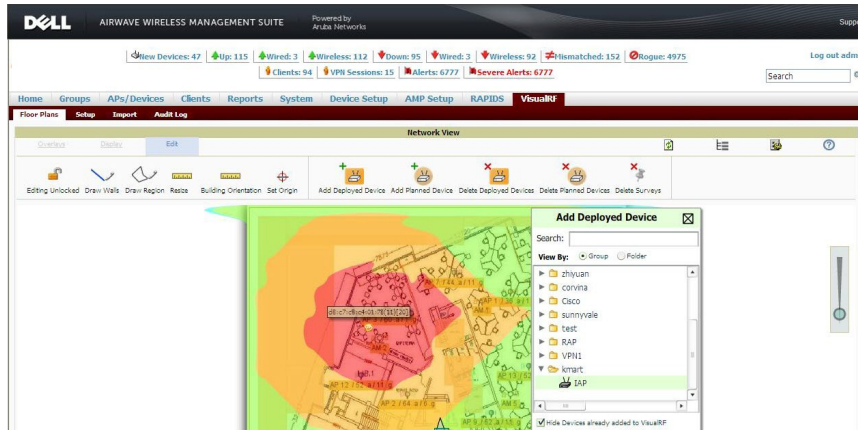
Dell PowerConnect W-AirWave supports Wireless Intrusion Detection System (WIDS) Event Reporting, which is provided by Dell W-Instant. This includes WIDS classification integration with the RAPIDS (Rogue Access Point Detection Software) module. RAPIDS is a powerful and easy-to-use tool for automatic detection of unauthorized wireless devices. It supports multiple methods of rogue detection and uses authorized wireless APs to report other devices within range.

The WIDS report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours and provides links to support additional analysis or configuration in response.

## RF Visualization Support for Dell W-Instant

Dell PowerConnect W-AirWave supports RF visualization for Dell W-Instant. The VisualRF module provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. VisualRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every Instant device in range. VisualRF provides graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network.

**Figure 149 - Adding a W-IAP in VisualRF**



## Configuring Dell PowerConnect W-AirWave

This section describes how to configure Dell PowerConnect W-AirWave integration. Before configuring the Dell PowerConnect W-AirWave, you need the following:

- IP address of the Dell PowerConnect W-AirWave server.
- Shared key for service authorization— This is assigned by the Dell PowerConnect W-AirWave administrator.

## Creating your Organization String

The Organization String is a set of colon-separated strings created by the Dell PowerConnect W-AirWave administrator to accurately represent the deployment of each Dell W-Instant system. This string is entered into the Dell W-Series Instant UI by the on-site installer.

- AMP Role— "Org Admin" (initially disabled)
- AMP User— "Org Admin" (assigned to the role "Org Admin")
- Folder— "Org" (under the Top folder in AMP)
- Configuration Group— "Org"

Additional strings in the Organization String are used to create a hierarchy of sub folders under the folder named "Org":

- subfolder1 would be a folder under the "Org" folder
- subfolder2 would be a folder under subfolder1

## About Shared Key

The Shared Secret key is used by the administrator to manually authorize the first Virtual Controller for an organization. Any string is acceptable.

### Entering the Organization String and AMP Information into the W-IAP

1. Click the Dell PowerConnect W-AirWave Set Up Now link in the bottom-middle region of the Dell W-Series Instant UI window. The Settings window with the Dell PowerConnect W-AirWave tab selected appears.

Figure 150 - Configuring Dell PowerConnect W-AirWave

Settings Help

General Admin

Local

Authentication: Internal

Username: admin

Password: ●●●●

Retype: ●●●●

AirWave

Organization:

AirWave IP:

AirWave backup IP:

Shared key:

Retype:

[Show advanced options](#) OK Cancel

2. Enter the name of your organization in the **Organization** name text box. This name automatically appears in Dell PowerConnect W-AirWave under Groups list.
3. Enter the IP address of the Dell PowerConnect W-AirWave server in the **Dell PowerConnect W-AirWave IP** text box.
4. Enter the IP address of a backup Dell PowerConnect W-AirWave server in the **Dell PowerConnect W-AirWave backup IP** text box. The backup server provides connectivity when the primary server is down. If the W-IAP cannot send data to the primary server, the Virtual Controller switches to the backup server automatically.
5. Enter the shared key in the **Shared key** text box and reconfirm. This shared key is used for configuring the first AP in the Dell W-Instant network.
6. Click OK.

### Dell PowerConnect W-AirWave Discovery through DHCP Option

The Dell PowerConnect W-AirWave configuration can also be performed on the DHCP option that is configured on the DHCP server. You can configure this only if Dell PowerConnect W-AirWave was not configured earlier or if you have deleted the precedent configuration.

On the DHCP server, the format for option 60 is "DellInstantAP", and the format for option 43 is "ams-ip,ams-key".

### Standard DHCP option 60 and 43 on Windows Server 2008

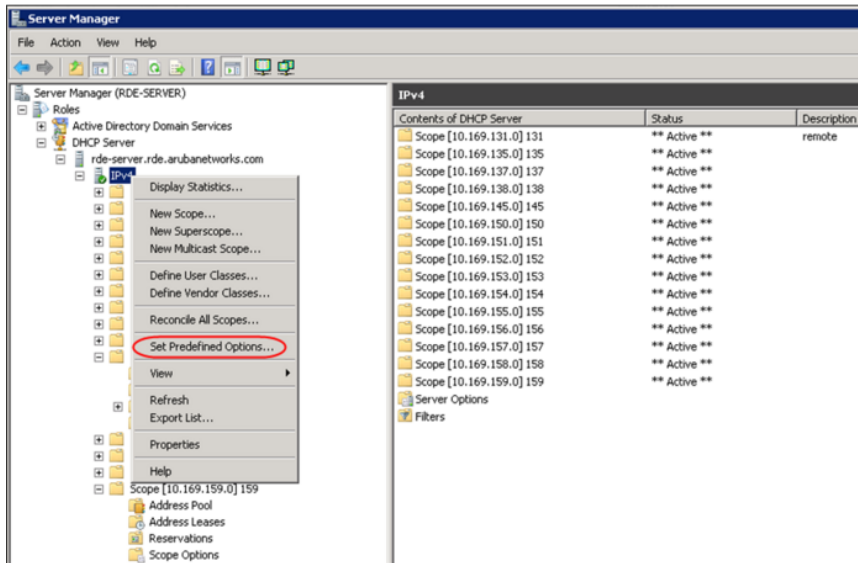
In networks that are not using DHCP option 60 and 43, it is easy to use the standard DHCP options 60 and 43 for Dell AP or Dell W-Instant AP. For Dell APs these options can be used to



indicate the, master controller or the local controller. For W-IAP, this can be used to define the Dell PowerConnect W-AirWave IP, group and password.

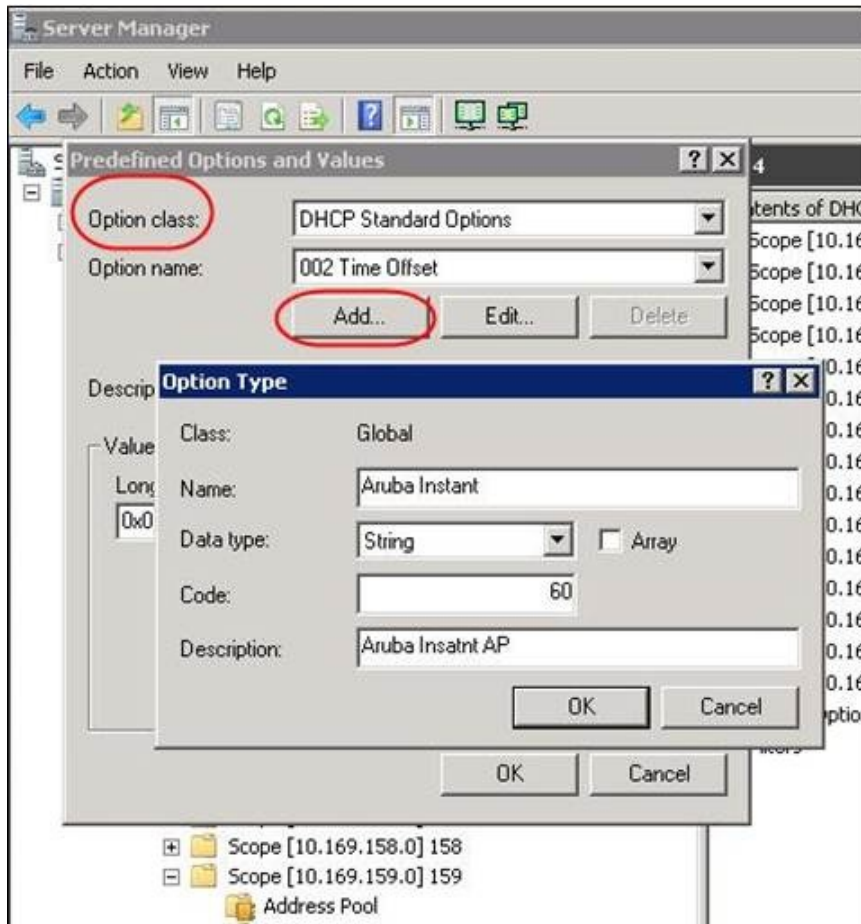
1. From a server running Windows Server 2008 navigate to **Server Manager > Roles > DHCP sever > domain DHCP Server > IPv4**.
2. Right-click on **IPv4** and select **Set Predefined Options**.

**Figure 151 - Instant and DHCP options for Dell PowerConnect W-AirWave— Set Predefined Options**



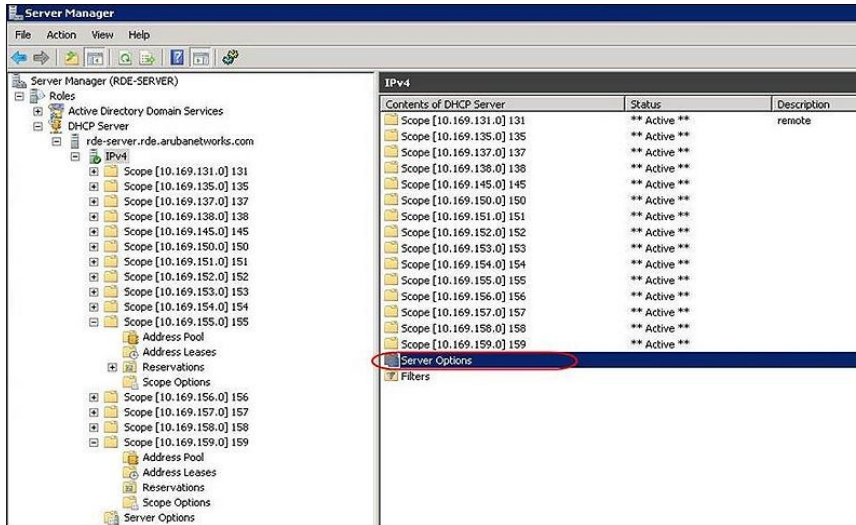
3. Select **DHCP Standard Options** in the **Option** class drop-down list and then click **Add**. Enter the following information:
  - Name— Dell W-Instant
  - Data Type— String
  - Code— 60
  - Description— Dell W-Instant AP

**Figure 152 - W-Instant and DHCP options for Dell PowerConnect W-AirWave— Predefined Options and Values**



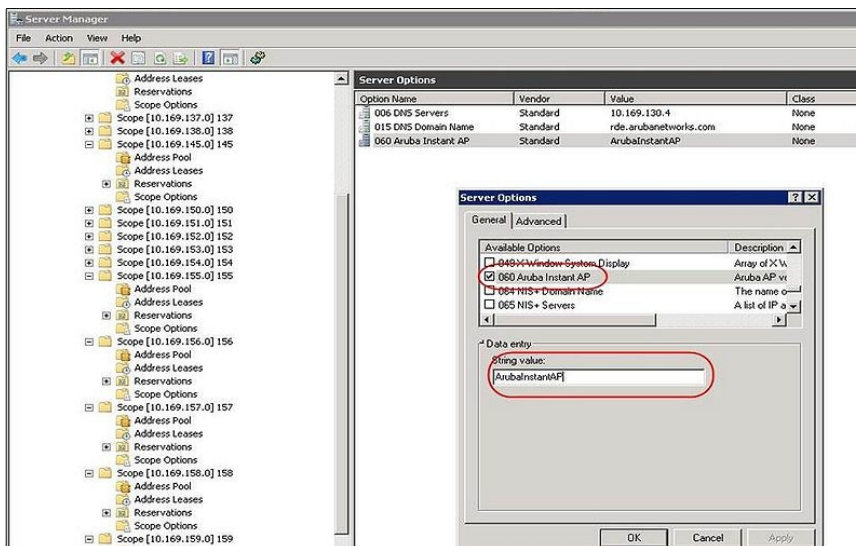
4. Navigate to **Server Manager** and select **Server Options** in the **IPv4** window. (This sets the value globally. Use options on a per-scope basis to override the global options.)
5. Right-click on **Server Options** and select the configuration options.

**Figure 153 - W-Instant and DHCP options for Dell PowerConnect W-AirWave— Server Options**



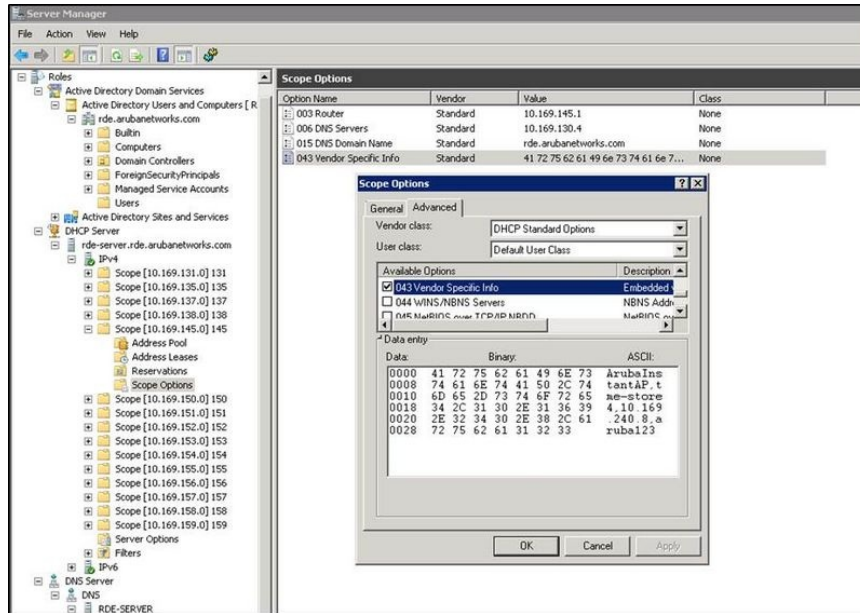
6. Select 060 Dell W-Instant AP in the Server Options window and enter DellInstantAP in the String Value.

**Figure 154 - W-Instant and DHCP options for Dell PowerConnect W-AirWave—060 Dell W-Instant AP in Server Options**



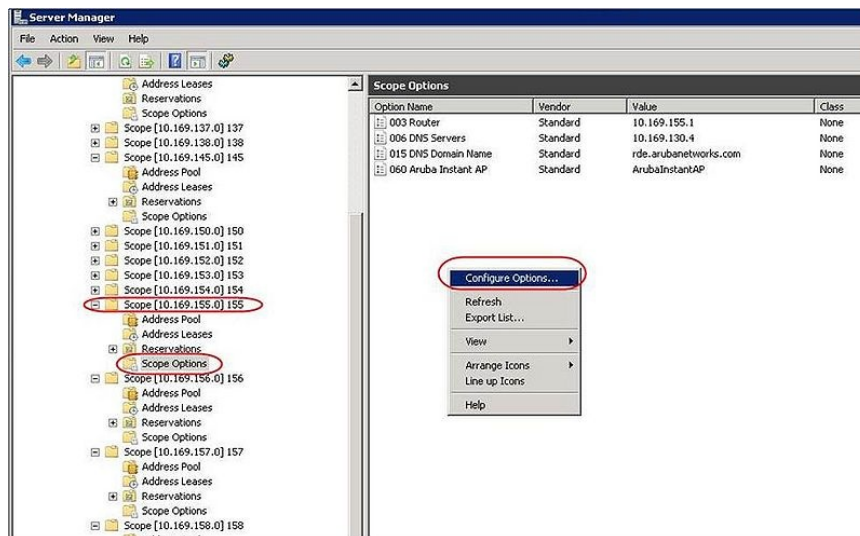
7. Select 043 Vendor Specific Info and enter a value for airwave-orgn, airwave-ip, airwave-key in the ASCII field (for example: tme-instant-store1,10.169.240.8, Dell123).

**Figure 155 - W-Instant and DHCP options for Dell PowerConnect W-AirWave— 043 Vendor Specific Info**



This creates a DHCP option 60 and 43 on a global basis. You can do the same on a per-scope basis. The per-scope option overrides the global option.

**Figure 156 - W-Instant and DHCP options for Dell PowerConnect W-AirWave— Scope Options**



## Alternate Method for Defining Vendor-Specific DHCP Options

This section describes how to add vendor-specific DHCP options for Dell W-Instant APs in a network that already uses DHCP options 60 and 43 for other services. Some networks use DHCP standard options 60 and 43 to give the DHCP clients info about certain services such as PXE to the DHCP clients. In such an environment, it is not possible to use the standard DHCP options 60 and 43 for Dell APs.

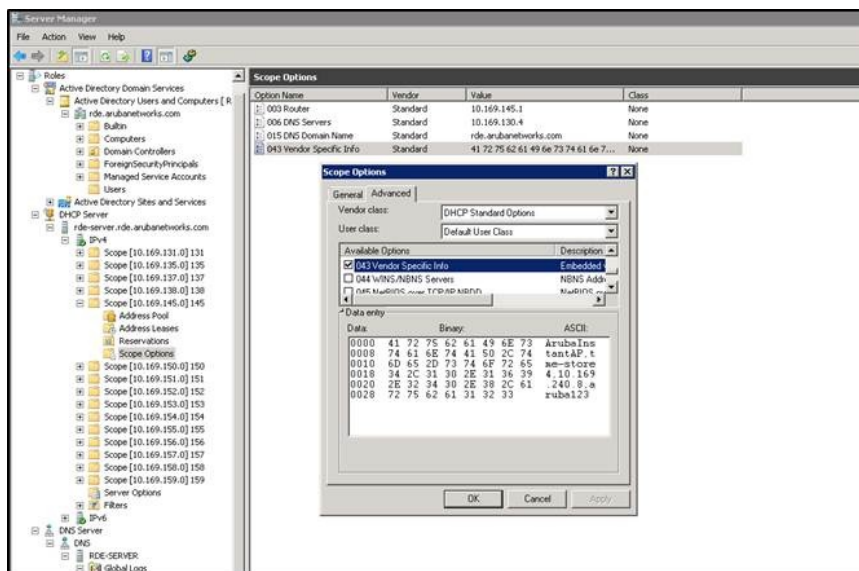
This method describes how to set up a DHCP server to send option 43 with Dell PowerConnect W-AirWave information to Dell W-Instant W-IAP. This section assumes that option 43 is sent per scope because option 60 is being shared by other devices as well.



**NOTE:** This scope should be specific to Instant, and the PXE devices that use options 60 and 43 should not connect to the subnet defined by this scope. This is because you can specify only one option 43 for a scope, and if other devices that use option 43 connect to this subnet, they are presented with Instant-specific information.

1. In server 2008, navigate to **Server Manager > Roles > DHCP Server > Domain DHCP Server > IPv4**.
2. Select a scope (subnet). Scope (10.169.145.0)145 is selected in the example shown in the figure below.
3. Right click and select **Advanced**, and then specify the following options:
  - Vendor class— DHCP Standard Options
  - User class— Default User Class
  - Available options— Select 043 Vendor-Specific Info
  - String Value— DellInstantAP, tme-store4, 10.169.240.8, Dell123 (which is the AP description, organization string, Dell PowerConnect W-AirWave IP address, Pre-shared key for Dell PowerConnect W-AirWave)

**Figure 157 - Vendor Specific DHCP options**

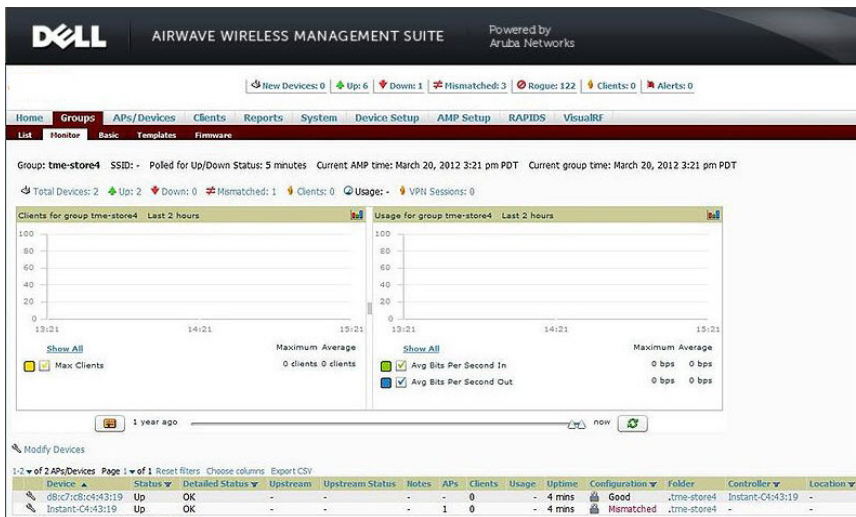


Upon completion, the W-IAP shows up as a new device in Dell PowerConnect W-AirWave, and a new group called **tme-store4** is created. Navigate to **APs/Devices > New > Group** to view this group.

Figure 158 - Dell PowerConnect W-AirWave — New Group



Figure 159 - Dell PowerConnect W-AirWave — Monitor



# Chapter 24

## AirGroup

### Introducing AirGroup

AirGroup™ capabilities are available as a feature in Dell WLANs where Wi-Fi data is distributed among W-Instant APs. AirGroup is a unique enterprise-class capability that leverages zero configuration networking to enable Bonjour® services like Apple® AirPrint and AirPlay from mobile devices in an efficient manner. Bonjour, the trade name for the zeroconf implementation introduced by Apple, is the most common example. Apple AirPlay and AirPrint services are based on the Bonjour protocol are essential services in campus Wi-Fi networks.

AirGroup solution supports both wired and wireless devices. Wired devices which support the Bonjour services are made part of the AirGroup when the VLANs of the devices are terminated on the Virtual Controller.

AirGroup also supports Dell PowerConnect W-ClearPass Policy Manager (CPPM).

With CPPM:

- Users, such as students in dorm rooms can register their personal devices and define a group of users who are allowed to share the users' registered devices.
- Administrators can register and manage an organization's shared devices like printers and conference room Apple TVs. An administrator can grant global access to each device, or restrict access according to the username, role, or user location.



---

NOTE: Dell AirGroup is a technology which is made available as part of the Dell W-Instant 6.2.0.0-3.2.0.0 version. See ["Enabling or Disabling AirGroup" on page 220](#) to enable AirGroup after you have upgraded to Dell W-Instant 6.2.0.0-3.2.0.0 version.

---

### What is Bonjour and Zero Configuration Networking?

Zero configuration networking enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home. Bonjour, the trade name for the zeroconf implementation introduced by Apple, is the most common example. It is supported by most of the Apple product lines, including the Mac OS X operating system, iPhone, iPod Touch, iPad, Apple TV and AirPort Express.

Bonjour can be installed on computers running Microsoft Windows® and is supported by most new network-capable printers. Bonjour is also included with popular software programs such as Apple iTunes, Safari, and iPhoto.

Bonjour uses multicast DNS (mDNS) to locate devices and the services that those devices offer. Since the addresses used by the protocol are link-scope multicast addresses, each query or advertisement can only be forwarded on its respective VLAN, but not across different VLANs.

## WLANs and Bonjour

In large universities and enterprise networks, it is common for Bonjour-capable devices to connect to the network across VLANs. As a result, user devices such as an iPad on a specific VLAN cannot discover the Apple TV that resides on another VLAN.

Broadcast and multicast traffic are usually filtered out from a wireless LAN network to preserve the airtime and battery life. This inhibits the performance of Bonjour services as they rely on multicast traffic.

## AirGroup Solution

Dell addresses this multicast DNS (mDNS) challenge with the introduction of patent-pending AirGroup technology. AirGroup leverages key elements of Dell's solution portfolio including operating system software for Dell W-Instant and Dell PowerConnect W-ClearPass Policy Manager.

AirGroup maintains seamless connectivity between clients and services across VLANs and SSIDs. The mDNS packet traffic is minimized thereby preserving valuable wired network bandwidth and WLAN airtime.

AirGroup also enables context awareness for services across the network:

- AirGroup is aware of personal devices. For example, an Apple TV in a dorm room can be associated with the student who owns it.
- AirGroup is aware of shared resources. This might be an Apple TV in a meeting room or a printer in a supply room that is available to certain users, such as the marketing department. Or, in a classroom, teachers can use AirPlay to wirelessly project a laptop screen onto an HDTV monitor using an Apple TV.
- AirGroup is aware of the location of services through Dell CPPM (Dell PowerConnect W-ClearPass Policy Manager) support. For example, depending on proximity, an iPad would be presented with the closest printer instead of all the printers in the building. Another example is a user in a conference room who wants to use AirPlay to project a MacBook screen on an HDTV monitor using an Apple TV receiver. When that users' device queries the network for a list of available Apple TVs, the location-aware W-IAP only shows the Apple TV closest to the user.

All of these above filtering options require Dell PowerConnect W-ClearPass Policy Manager (CPPM).

- In addition, the W-IAP supports Bonjour services' filtering options based on VLANs and roles for which Dell PowerConnect W-ClearPass Policy Manager is not required.

The following table summarizes the filtering options which are described above.

**Table 37- AirGroup Features**

Features	Dell W-Instant Deployment Models	
	Integrated	Integrated with CPPM
Allow mDNS to propagate across subnets/VLANs	Yes	Yes



Features	Dell W-Instant Deployment Models	
Limit multicast mDNS traffic on the network	Yes	Yes
VLAN based mDNS service policy enforcement	Yes	Yes
User-role based mDNS service policy enforcement	Yes	Yes
Portal to self register personal leaves	No	Yes
Device owner based policy enforcement	No	Yes
Location based policy enforcement	No	Yes
Shared user list based policy enforcement	No	Yes
Shared role list based policy enforcement	No	Yes

## AirGroup Features

- AirGroup sends unicast responses to mDNS queries and reduces mDNS traffic footprint.
- Ensure cross-VLAN visibility and availability of mDNS devices and services.
- Allow or block mDNS services for all users.
- Allow or block mDNS services based on user roles.
- Allow or block mDNS services based on VLANs.
- Match users' devices, such as iPads, to their closest Bonjour devices, such as printers. This requires CPPM support.

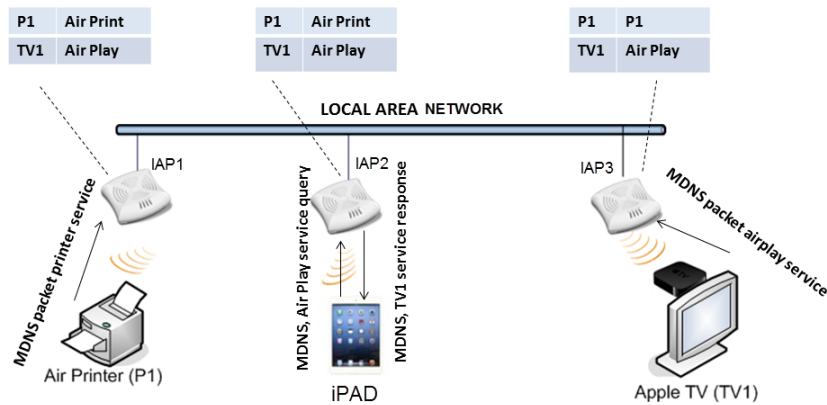
## Dell PowerConnect W-ClearPass Policy Manager and ClearPass Guest Features

- Registration portal for WLAN users to register their personal devices, such as Apple TVs and printers.
- Registration portal for WLAN administrators to register shared devices, such as conference room Apple TVs and printers.
- Operator-defined “personal AirGroups” to specify a list of other users who can share devices with the operator.
- Administrator defined username, user role, and location attributes for shared devices.

## AirGroup Architecture

The distributed AirGroup architecture allows each W-IAP to handle Bonjour queries and responses individually instead of over loading a Virtual controller with these tasks. This results in a scalable AirGroup solution.

**Figure 160- AirGroup Architecture**



As seen in the image above, the W-IAP1 discovers Air Printer (P1) and W-IAP3 discovers Apple TV (TV1). W-IAP1 advertises information about its connected P1 device to the other W-IAPs i.e W-IAP2 and W-IAP3. Similarly, W-IAP3 advertises TV1 device to W-IAP1 and W-IAP2. This type of distributed architecture allows any W-IAPs to respond to its connected devices locally. In this example, the iPad connected to W-IAP2 obtains direct response from the same W-IAP about the other Bonjour-enabled services in the network.

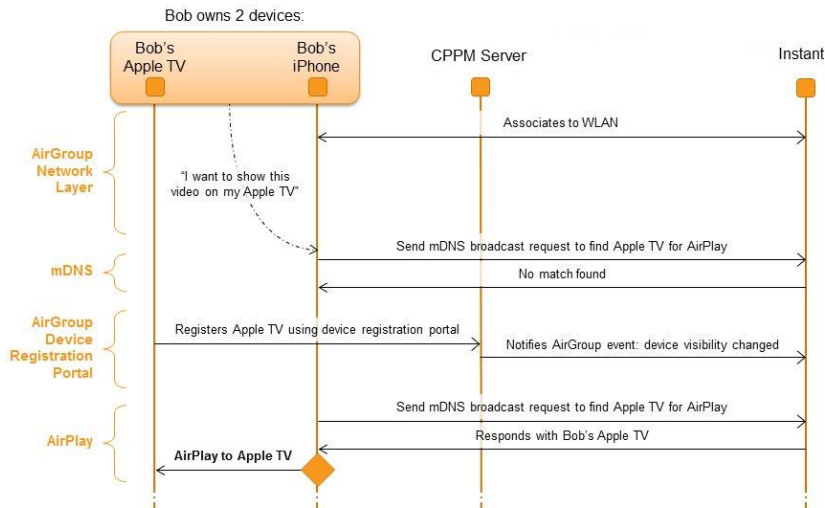
## How Does AirGroup Work?

AirGroup functionality is described in the steps below. This flow occurs when an Dell WLAN is powered by an Dell W-Instant and Dell PowerConnect W-ClearPass Policy Manager.

A device can be registered by an administrator or a guest user.

1. The AirGroup administrator gives an end user the AirGroup operator role which authorizes the user to register the users device—such as an Apple TV on the Dell PowerConnect W-ClearPass Policy Manager platform.
2. Dell W-Instant maintains state information for all mDNS services. Dell W-Instant queries Dell PowerConnect W-ClearPass Policy Manager to map each device's access privileges to available services.
3. Dell W-Instant responds back to the query made by a device based on contextual data – user role, username, and location.

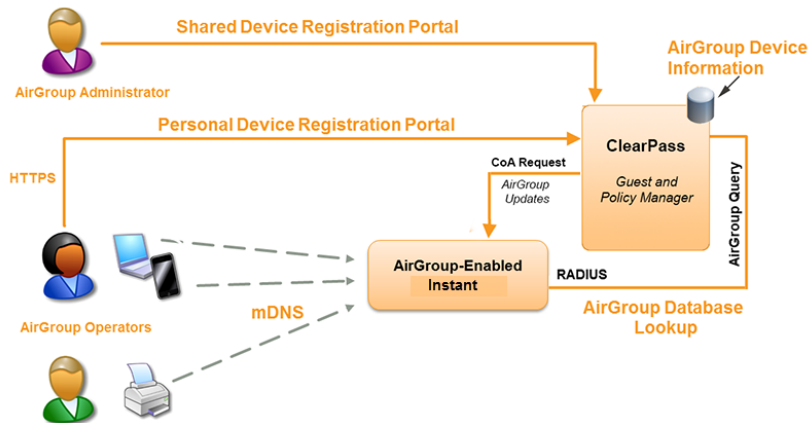
**Figure 161- AirGroup Enables Personal Device Sharing**



### Use Case: Higher Education Wireless LAN

Figure 162 shows a higher-education environment with shared, local, and personal services available to mobile devices. With AirGroup, context-based policies determine which Bonjour services are visible to an end-user's mobile device.

**Figure 162- AirGroup in a Higher-Education Environment**



### The AirGroup Solution Components

The components that make up the AirGroup Solution include the Dell W-Instant, Dell PowerConnect W-ClearPass Policy Manager, and Dell PowerConnect W-ClearPass Guest. The version requirements are described below:

**Table 38- Dell W-Instant, Dell PowerConnect W-ClearPass Policy Manager, and Dell PowerConnect W-ClearPass Guest Requirements**

Component	Minimum Version
Dell W-Instant	6.2.0.0-3.2.0.0
Dell PowerConnect W-ClearPass Guest software	3.9.7
AirGroup Services plugin	0.8.7
Dell PowerConnect W-ClearPass Policy Manager software	5.2

## Configuring AirGroup on W-Instant

Configuring AirGroup and its service requires that you enable the AirGroup feature. W-IAP AirGroup supports two default services i.e. AirPlay and AirPrint.

### Using the Dell W-Series Instant UI

#### Enabling or Disabling AirGroup

As the first step in configuring AirGroup services, you must enable AirGroup in the Dell W-Series Instant UI.

1. Go to **Settings > Air Group** to enable this feature.
2. Select **Enable Air Group** to view the AirGroup Settings.

W-Instant supports two types deployment models:

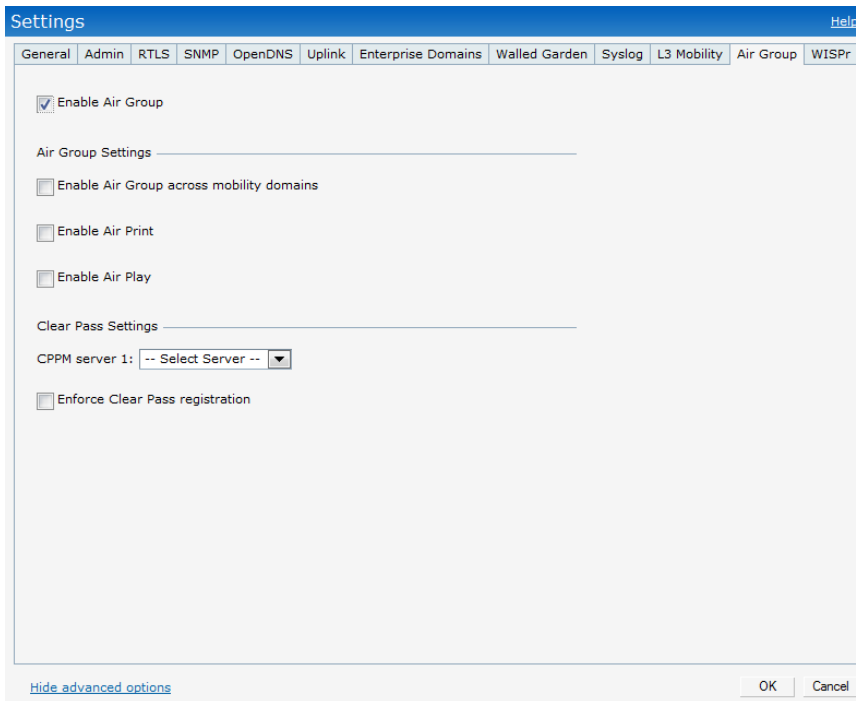
- Intra Cluster
- Inter Cluster

In the Intra Cluster model, the W-IAP does not share the mDNS database information with the other clusters. In the Inter Cluster model, the W-IAP shares the mDNS database information with the other clusters.

- **Enable Air Group across mobility domains**— Select **Enable Air Group across mobility domains** to enable Inter cluster. By default, this feature is disabled. Navigate to **L3 Mobility** tab of **Settings** to define a set of clusters.
- **Enable Air Print**— When enabled, the following two options are made available:
  - Air Print disallowed roles— Clients with these roles will not have access to AirPrint devices.
  - Air Print disallowed VLANs — No AirPrint servers will be seen on these VLANs.
- **Enable Air Play**— When enabled, the following two options are made available:
  - Air Play disallowed roles— Clients with these roles will not have access to AirPlay devices.
  - Air Play disallowed VLANs — No AirPlay servers will be seen on these VLANs.
- **Clear Pass Settings**— Use this section to configure the CPPM server, CoA server and enforce Clear Pass registering.
  - **CPPM server 1**— Indicates the Dell PowerConnect W-ClearPass Policy Manager server information for AirGroup policy. Refer to "[Configuring AirGroup-CPPM Interface in W-Instant](#)" on page 223 for more information.

- **Enforce Clear Pass registering**— When enabled, only devices registered with CPPM will be discovered by Bonjour devices, based on the CPPM policy.

**Figure 163- Enabling AirGroup**

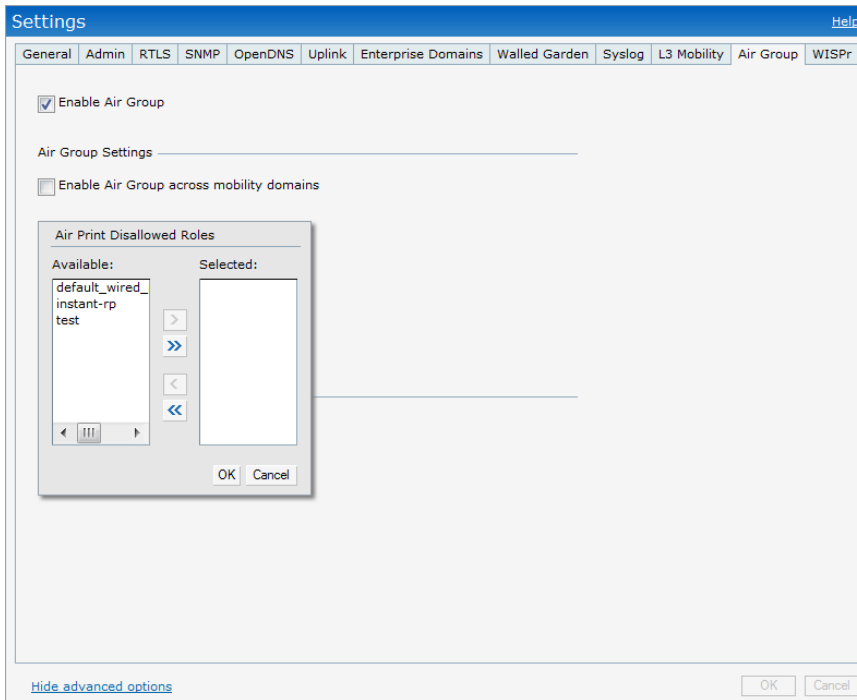


## Disallow Role

By default, an AirGroup service is accessible by all user roles configured in your W-IAP cluster. The **disallow role** option selectively prevents specified user roles from accessing AirGroup services.

Perform the following steps to configure disallow role from accessing AirPrint servers and disallow learning of AirPrint servers on the configured VLAN as shown in [Figure 164](#) and [Figure 165](#).

**Figure 164 - AirPrint Disallowed Roles**

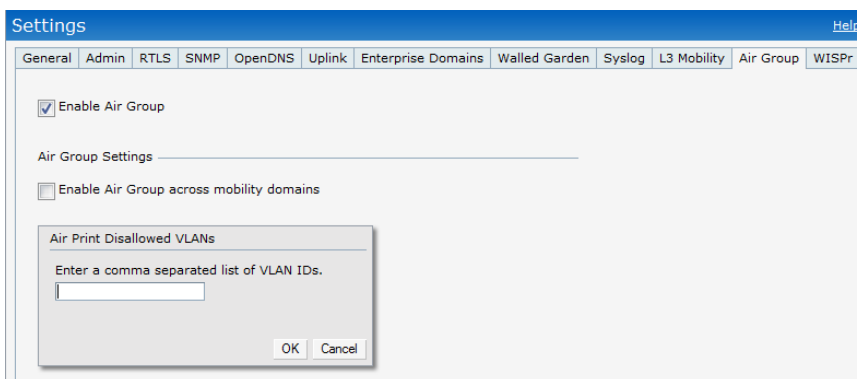


1. In the **Enable Air Print** section of the Instant UI, select **Edit** . The **Air Print Disallowed Roles** window appears.
2. Use the arrow keys to move the available roles to the selected window and vice versa.
3. Click **OK** to apply the selected roles as disallowed roles.

## Disallow VLAN

By default, an AirGroup service is accessible by users or devices in all VLANs configured in your W-IAP cluster. You can enable or disable learning of AirGroup services in a specific VLAN using the **Air Print Disallowed VLANs** configuration window.

**Figure 165 - AirPrint Disallowed VLANs**



1. Select **Edit** (the field next to Air Print disallowed VLANs). The **Air Print Disallowed VLANs** window appears.
2. Enter the VLANs on which you want to disallow learning of AirGroup services.
3. Click **OK** to apply these changes.

## Configuring AirGroup-CPPM Interface in W-Instant

Configure the AirGroup and CPPM interface to allow an AirGroup W-IAP and CPPM to exchange information regarding device sharing, and location. The configuration options define the RADIUS server that is used by the AirGroup RADIUS client. The following steps are required for this configuration:

1. Create a RADIUS server.
2. Assign a server to AirGroup.
3. Configure CPPM to enforce registration.

### Creating a RADIUS Server

Navigate to the **PEF** link at the top right corner of the Dell W-Series Instant UI to configure an external RADIUS server for a wireless network.

**Figure 166- New Authentication Server**

The screenshot shows the 'New Authentication Server' dialog box within the 'Policy Enforcement Firewall (PEF)' configuration tool. The 'RADIUS' option is selected, and the 'CoA only' checkbox is not checked. The fields are filled with the following values: Name (empty), IP address (empty), Auth port (1812), Accounting port (1813), Shared key (empty), Retype key (empty), Timeout (5 sec), Retry count (3), RFC 3576 (Enabled), Air Group CoA port (5999), NAS IP address (optional, empty), and NAS identifier (optional, empty). The dialog has 'OK' and 'Cancel' buttons at the bottom.

1. Click New and update the following fields to configure an external RADIUS server for a wireless network.
  - Name— Enter the name of the new external RADIUS server. The maximum length is 32 characters.
  - IP address— Enter the IP address of the external RADIUS server.
  - Auth port— Enter the authorization port number of the external RADIUS server. The port number is set to 1812 by default.
  - Accounting port— Enter the accounting port number. This port is used to send accounting records to the RADIUS server. The port number is set to 1813 by default
  - Shared key— Enter a shared key for communicating with the external RADIUS server.
  - Timeout— Indicates the timeout for one RADIUS request. The W-IAP retries to send the request several times (as configured in the "Retry count") before the user gets disconnected. e.g. If the "Timeout" is 5 sec, "Retry counter" is 3, user is disconnected after 20 sec ("Timeout" x "Retry counter" + 1). The default value is 5 seconds. Specify a number between 1 and 30 (seconds).

- Retry count— Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to server group, and the default value is 3 requests.
- RFC 3576— When enabled, the Access Points process RFC 3576-compliant Change of Authorization (CoA) messages from the RADIUS server.
- Air Group CoA port— Indicates that the AirGroup CoA is sent on a different port than the standard CoA port. The default value is 5999.
- NAS IP address— Enter the Virtual Controller IP address. The NAS IP address is the Virtual Controller IP address that is sent in data packets. Note: If you do not enter the IP address, the Virtual Controller IP address is used by default when Dynamic RADIUS Proxy is enabled.
- NAS identifier— Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.

2. Click **OK** to apply the changes.



**NOTE:** Alternatively, you can also create a RADIUS server in the **Air Group** window of the Dell W-Series Instant UI. Navigate to **Settings > Show advanced options > AirGroup > Clear Pass Settings > CPPM server 1>** and select **New** from the drop-down menu.

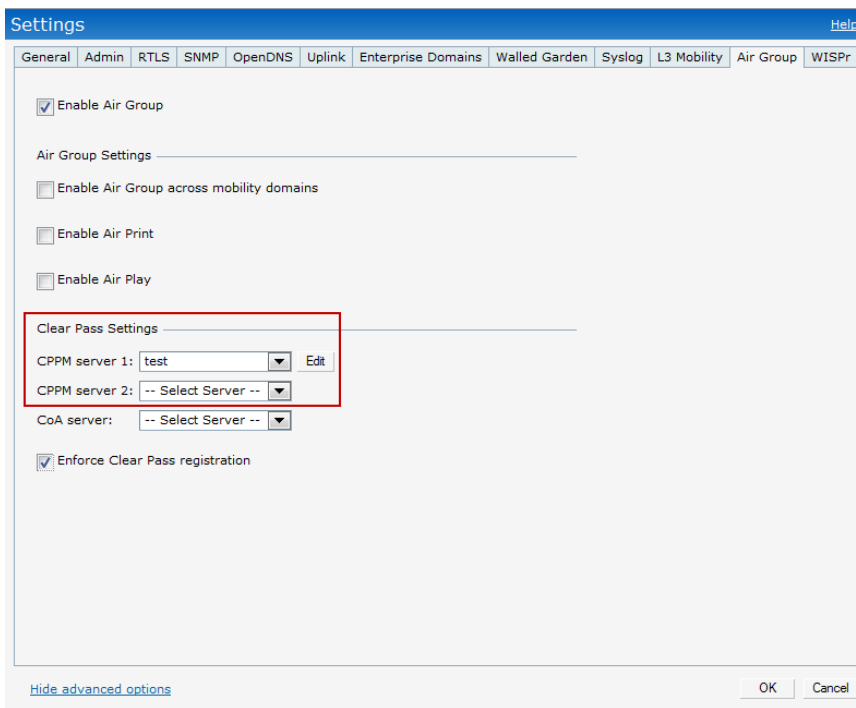
## Assign a Server to AirGroup

After configuration is complete, the server that you configured will appear in the **CPPM server** option section. To view this server go to **Settings > AirGroup > ClearPass Settings** and assign the server for AirGroup policy.



**NOTE:** The CPPM server 1 acts as a primary server and the CPPM server 2 is optional and acts as a backup server.

**Figure 167- CPPM Server**





## Configure CPPM to Enforce Registration

When enabled, only devices registered with CPPM will be discovered by Bonjour devices, based on the CPPM policy.

### Change of Authorization (CoA)

CoA only server is Dell PowerConnect W-ClearPass Guest server which allows guest users to register their devices.

To configure the CoA only server follow the steps below:

1. Navigate to the **PEF** link at the top right corner of the Dell W-Series Instant UI and click **New**.



**NOTE:** Ensure to configure CPPM server and the AirGroup W-IAP with the same AirGroup RFC-3576 UDP port. By default the AirGroup CoA port is 5999 on W-IAP as well as the CPPM server. For more information on how to configure the CPPM server refer to "[Enabling Support for Dynamic Notifications](#)" on page 1.

2. Select CoA only and update the following fields to enable change of authorization.

**Figure 168- Change of Authorization**

The screenshot shows the 'Policy Enforcement Firewall (PEF)' configuration interface. A 'New Authentication Server' dialog box is open, with the 'RADIUS' radio button selected and the 'CoA only' checkbox checked. The dialog box contains the following fields: Name, IP address, Air Group CoA port (with a default value of 5999), Shared key, and Retype key. There are 'OK' and 'Cancel' buttons at the bottom right of the dialog box. Below the dialog box, there are 'New', 'Edit', and 'Delete' buttons.

- Name— Enter the name of the new external RADIUS server. The maximum length is 32 characters.
  - IP address— Specify the IP address of the external RADIUS server
  - Air Group CoA port— Indicates that the AirGroup CoA is sent on a different port than the standard CoA port. The default value is 5999.
  - Shared key— Enter a shared key for communicating with the external RADIUS server.
3. Click **OK** to apply the changes.



**NOTE:** Alternatively, you can also create a **CoA only server** in the **Air Group** window of the Dell W-Series Instant UI. Navigate to **Settings > Show advanced options > AirGroup > Clear Pass Settings > CoA server >** and select **New**.

After configuration is complete, this particular server will appear in the CoA server option. To view this server go to **Settings > AirGroup > ClearPass Settings > CoA server**.

# AirGroup Monitoring

This link provides an overall view of your AirGroup Bonjour services. Click on each of the features to view or edit the settings.

**Figure 169- AirGroup Link**



MAC	IP	Host Name	Service	VLAN	Wired/Wireless	Role	Username	AP Name	CPPM
9c:2b:76:45:48:10	172.16.22.240	sws022	printer	21	Wireless			d8:c7:c8:c4:01:78	
9c:2b:76:45:48:14	172.16.22.240	Power-Mgmt-Apple-TV-10107		21	Wireless			d8:c7:c8:c4:01:78	
9c:2b:76:45:48:16	172.16.22.240	IPHONE0000000000	printer	21	Wireless			d8:c7:c8:c4:01:78	

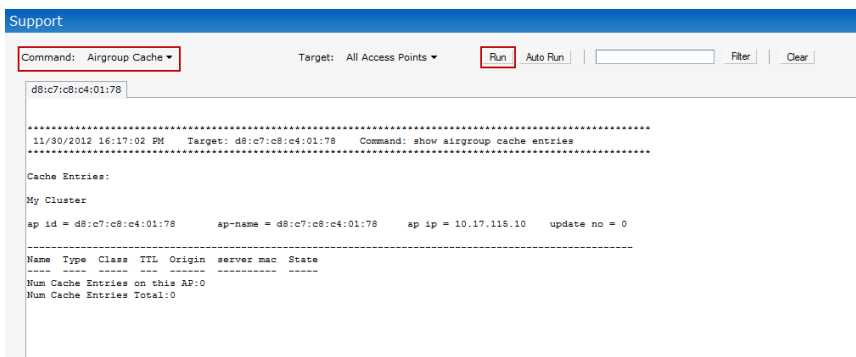
AirGroup consists of the following fields:

- **MAC** — Displays the MAC address of the AirGroup server.
- **IP** — Displays the IP address of the AirGroup Server's.
- **Host Name** — Displays the machine name or hostname of the AirGroup server.
- **Service**— Displays the type of the service offered by the AirGroup server like AirPlay or printer.
- **Wired/Wireless** — Displays if the AirGroup server is connected via wired or wireless interface.
- **Role** — Indicates the role assigned to the specified AirGroup server. Normally it is the SSID name, in case of a wireless client.
- **Username** — If the server is connected using 802.1x, this field displays the user name. If the server is connected via PSK or open auth, this field will be blank.
- **AP-NAME**— Displays the MAC address of the W-IAP where the server is connected.
- **Update no/hash**— This is used for debugging issues. Use this to identify the internal database of AirGroup.
- **CPPM**— By clicking on this, you get details of the registered rules in Dell PowerConnect W-ClearPass Policy Manager (CPPM) for this server.
- **MDNS Cache**— By clicking on this, you receive MDNS record details of a particular server.

## Troubleshooting and Log Messages

Navigate to the Support window at the top right corner of the Dell W-Series Instant UI. Select the required AirGroup command from the **Command** drop-down list and click **Run**.

**Figure 170- AirGroup Support Commands**



You can view the following AirGroup commands in the Command drop-down list.

- **AP AirGroup Cache**— Displays the Bonjour mDNS records for the selected W-IAP(s).
- **AP AirGroup CPPM Entries**— Displays the AirGroup CPPM policies of the registered devices.
- **AP AirGroup CPPM Servers**— Displays the AirGroup CPPM server information.

- AP AirGroup Debug Statistics— Displays the debug statistics for the selected W-IAP(s).
- AP AirGroup Servers— Displays information about the Bonjour devices which supports AirPrint and AirPlay services for the selected W-IAP(s).
- AP AirGroup User— Displays IP/MAC address, device name, VLAN, type of connection of the Bonjour devices for the selected W-IAP(s).
- VC AirGroup Service— Displays the Bonjour services supported for the selected W-IAP(s).
- VC AirGroup Status— Displays the enable/disable status of the AirGroup and the parameters of the CPPM servers for the selected W-IAP(s).
- VC AirGroup vlan— Displays the AirGroup status information for a VLAN of the selected W-IAP(s).



# Chapter 25

## Monitoring

Monitor the Dell W-Instant network, W-IAPs, Wi-Fi networks, and clients in the network using one or all of the following views:

- "Virtual Controller View" on page 229
- "Network View" on page 232
- "Dell W-Instant Access Point View" on page 235
- "Client View" on page 243

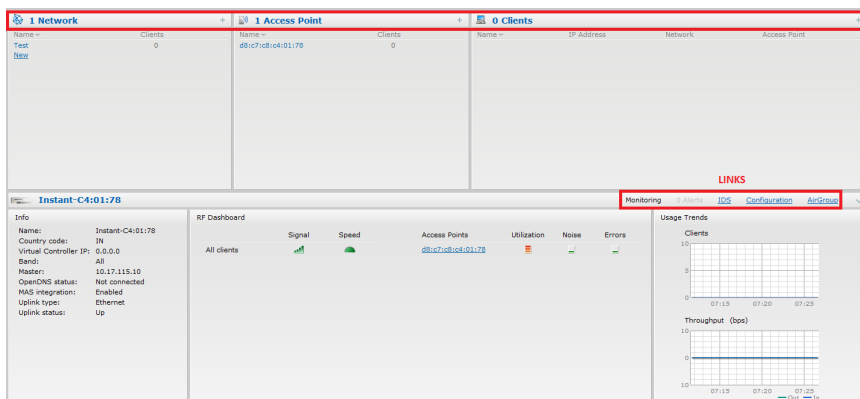
This section provides information about the parameters that can be monitored using these views. It also provides procedures to monitor these parameters. For information on AirGroup monitoring, see "AirGroup Monitoring" on page 226.

### Virtual Controller View

The Virtual Controller view is the default view. This view allows you to monitor the Dell W-Instant network. The following Dell W-Series Instant UI elements are available in this view:

- Tabs— Contains three tabs— Networks, Access Points, and Clients. For detailed information about the tabs, see "Dell W-Instant User Interface" on page 23.
- Links— Contains three links— Monitoring, Client Alerts, and IDS. The Spectrum link is visible if you have configured the W-IAP as a spectrum monitor. These links allow you to monitor the Dell W-Instant network. For detailed information about the sections in these links and how they can be used to monitor the network, see "Monitoring Link" on page 230, "IDS Link" on page 232, "Client Alerts Link" on page 232, Configuration Link sections. For detailed information about spectrum monitoring, see "Spectrum Monitor" on page 97.

Figure 171 - Virtual Controller View



## Monitoring Link

This link is selected by default and the following sections are displayed. These sections provide information about the Virtual Controller and allow you to monitor the network.

- Info
- RF Dashboard
- Usage Trends

### Info

The **Info** section displays the following information about the Virtual Controller:

- **Name**— Displays the Virtual Controller name.
- **Country Code**— Displays the Country in which the Virtual Controller is operating.
- **Virtual Controller IP address**— Displays the IP address of the Virtual Controller.
- **Dell PowerConnect W-AirWave IP**— Displays the IP address of the Dell PowerConnect W-AirWave server.
- **Band**— Displays the band in which the Virtual Controller is operating— 2.4 GHz band, 5 GHz band, or both.
- **Master**— Displays the IP address of the Access Point acting as a Virtual Controller.
- **OpenDNS Status**— Displays the OpenDNS status. If the OpenDNS is **Not connected**, make sure you have provided the correct credentials on the **OpenDNS** tab of the **Settings** window. In addition, please check if the Internet connection is up.
- **Uplink type**— Displays the type of uplink— Ethernet and 3G
- **Uplink status**— Displays whether the uplink is up or down.

### RF Dashboard

The **RF Dashboard** section displays the following information:

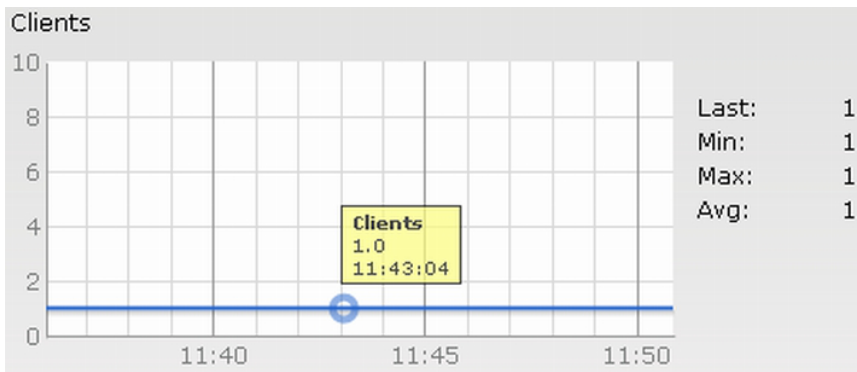
- IP address, Signal, and Speed information about the clients in the Dell W-Instant network. If the speed or signal strength of a client is low, IP address of the client appears as a link. Click the link to monitor the client. For more information, see "[Client View](#)" on page 243.
- Instant Access Points, Utilization, Noise, and Errors information about the W-IAPs in the Dell W-Instant network. If utilization, noise or errors of a W-IAP are not within the specified threshold, the W-IAP name appears as a link. Click the link to monitor the W-IAP. For more information, see "[Dell W-Instant Access Point View](#)" on page 235.

### Usage Trends

The **Usage Trends** section displays the following graphs for the Virtual Controller:

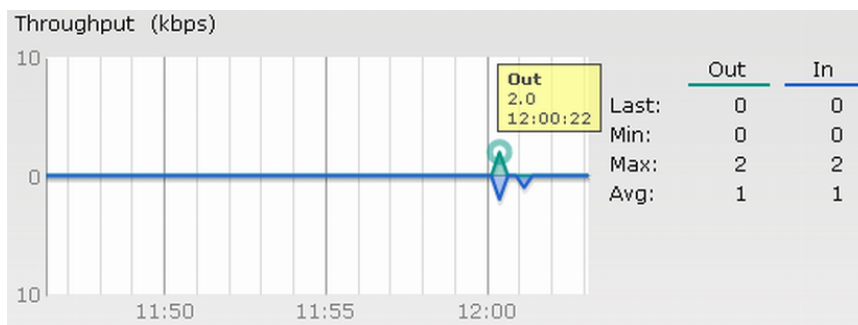
- Clients Graph

**Figure 172 - Clients Graph**



- Throughput Graph

**Figure 173 - Throughput Graph**



For more information about the graphs in the Virtual Controller view and for monitoring procedures, see [Table 39](#).

**Table 39 - Virtual Controller View — Graphs and Monitoring Procedures**

Graph Name	Description	Monitoring Procedure
Clients	<p>The Clients graph shows the number of clients associated with the Virtual Controller for the last 15 minutes. To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>• The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the Virtual Controller for the last 15 minutes.</li> <li>• To see the exact number of clients in the Dell W-Instant network at a particular time, hover the cursor over the graph line.</li> </ul>	<p>To check the number of clients associated with the Virtual Controller for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. Study the Clients graph in the <b>Usage Trends</b> pane. For example, the graph shows that one client is associated with the Virtual Controller at 11:43 hours.</li> </ol>
Throughput	<p>The Throughput graph shows the throughput of all networks and W-IAPs associated with the Virtual Controller for the last 15 minutes.</p> <ul style="list-style-type: none"> <li>• Outgoing traffic — Throughput for</li> </ul>	<p>To check the throughput of the networks and W-IAPs associated with the Virtual Controller for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series</li> </ol>

Graph Name	Description	Monitoring Procedure
	<p>outgoing traffic is displayed in green. Outgoing traffic is shown above the median line.</p> <ul style="list-style-type: none"> <li>Incoming traffic — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line.</li> </ul> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the Virtual Controller for the last 15 minutes.</li> </ul> <p>To see the exact throughput of the Dell W-Instant network at a particular time, hover the cursor over the graph line.</p>	<p>Instant UI. The Virtual Controller view appears. This is the default view.</p> <ol style="list-style-type: none"> <li>Study the Throughput graph in the <b>Usage Trends</b> pane. For example, the graph shows 2.0 kbps outgoing traffic throughput at 12:00 hours. It also shows some incoming traffic throughput at the same time.</li> </ol>

### Client Alerts Link

For information about the Client Alerts link, see ["Clients Tab" on page 25](#) and ["Alert Types and Management" on page 249](#) sections.

### IDS Link

For information about the IDS link, see ["IDS" on page 39](#).

## Network View

All Wi-Fi networks in the Dell W-Instant network are listed in the **Networks** tab. Click the network that you want to monitor. Network View for the selected network appears.

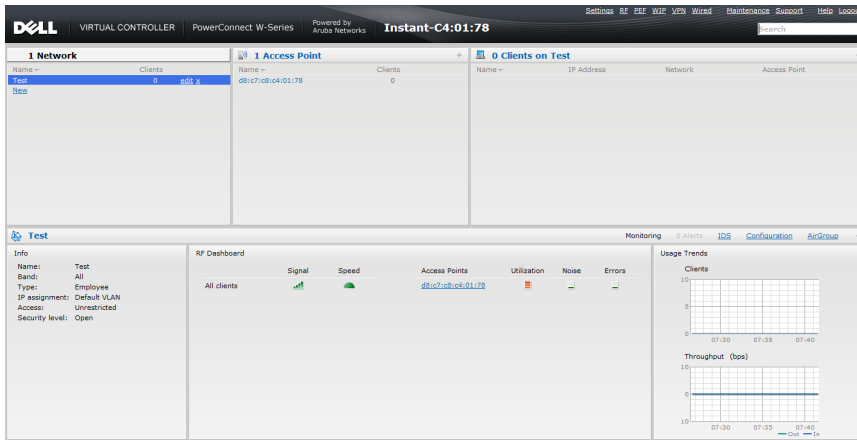
Similar to the Virtual Controller view, the Network view also has three tabs— Networks, Access Points, and Clients.

The following sections in the Dell W-Series Instant UI, provide information about the selected network:

- Info
- Usage Trends



**Figure 174 - Network View**



## Info

The **Info** section displays the following information about the selected network:

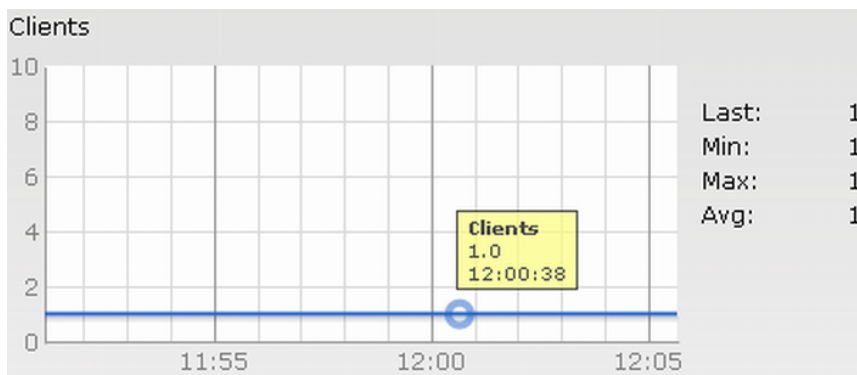
- **Name**— Name of the network.
- **Band**— Band in which the network is broadcast: 2.4 GHz band, 5 GHz band, or both.
- **Type**— Network type: Employee, Guest, or Voice.
- **IP Assignment**— Source of IP address for the client.
- **Access**— The level of access control for this network.
- **Security level**— The type of user authentication and data encryption for this network.

## Usage Trends

The **Usage Trends** section displays the following graphs for the selected network:

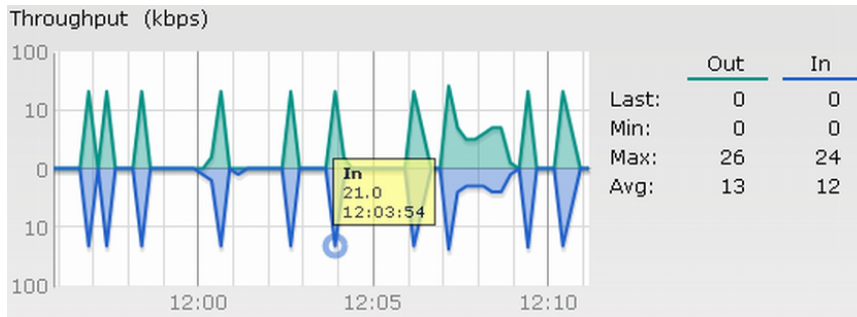
- Clients

**Figure 175 - Clients Graph**



- Throughput

**Figure 176 - Throughput Graph**



For more information about the graphs in the network view and for monitoring procedures, see [Table 40](#).

**Table 40 - Network View – Graphs and Monitoring Procedures**

Graph Name	Description	Monitoring Procedure
Clients	<p>The Clients graph shows the number of clients associated with the network for the last 15 minutes.</p> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the Virtual Controller for the last 15 minutes.</li> <li>To see the exact number of clients in the Dell W-Instant network at a particular time, hover the cursor over the graph line.</li> </ul>	<p>To check the number of clients associated with the network for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the <b>Networks</b> tab, click the network for which you want to check the client association. The Network view appears.</li> <li>Study the Clients graph in the <b>Usage Trends</b> pane. For example, the graph shows that one client is associated with the selected network at 12:00 hours</li> </ol>
Throughput	<p>The Throughput graph shows the throughput of the selected network for the last 15 minutes.</p> <ul style="list-style-type: none"> <li>Outgoing traffic — Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line.</li> <li>Incoming traffic — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line.</li> </ul> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the network for the last 15 minutes.</li> </ul> <p>To see the exact throughput of the selected network at a particular time, hover the cursor over the graph line.</p>	<p>To check the throughput of the selected network for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the <b>Networks</b> tab, click the network for which you want to check the client association. The Network view appears.</li> <li>Study the Throughput graph in the <b>Usage Trends</b> pane. For example, the graph shows 22.0 kbps incoming traffic throughput for the selected network at 12:03 hours.</li> </ol>

## Dell W-Instant Access Point View

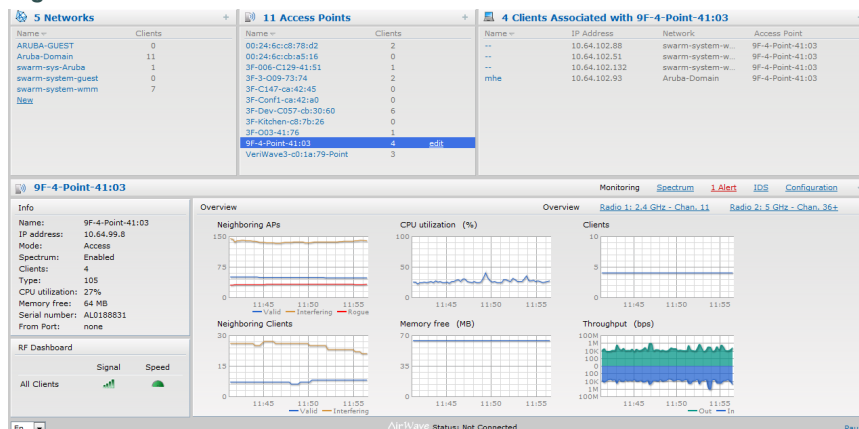
All W-IAPs in the Dell W-Instant network are listed in the **Access Points** tab. Click the W-IAP that you want to monitor. Access Point view for that W-IAP appears.

Similar to the Virtual Controller view, the Access Point view also has three tabs— **Networks**, **Access Points**, and **Clients**.

The following sections in the Dell W-Series Instant UI provide information about the selected W-IAP:

- Info
- RF Dashboard
- Overview

**Figure 177 - Dell W-Instant Access Point View**



### Info

The **Info** section provides the following information about the selected W-IAP:

- **Name**— Displays the name of the selected W-IAP.
- **IP Address**— Displays the IP address of the W-IAP.
- **Mode**— Displays the mode type. In **Access** mode the W-IAP serves clients, while also monitoring for rogue APs in the background. In **Monitor** mode, the W-IAP acts as a dedicated monitor, scanning all channels for rogue APs and clients.
- **Spectrum**— Displays the status of the spectrum monitor.
- **Clients**— Number of clients associated with the W-IAP.
- **Type**— Displays the model number of the W-IAP.
- **CPU Utilization**— Displays the CPU utilization in percentage.
- **Memory Free**— Displays the memory availability of the W-IAP in Mega Bytes (MB).
- **Serial number**— Displays the serial number of the W-IAP.
- **From Port**— Displays the port from where the slave W-IAP is learned in hierarchy mode.

### RF Dashboard

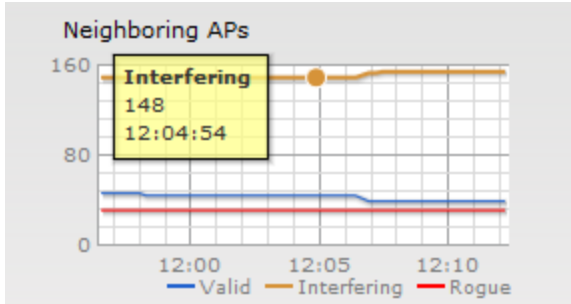
In the Instant Access Point view, the **RF Dashboard** section is moved below the **Info** section. It lists the IP address of the clients that are associated with the selected W-IAP if the signal strength or the data transfer speed of the client is low.

## Overview

The Overview section displays the common RF metrics for the selected access point over the last 15 minutes. The following graphs are displayed for the selected W-IAP:

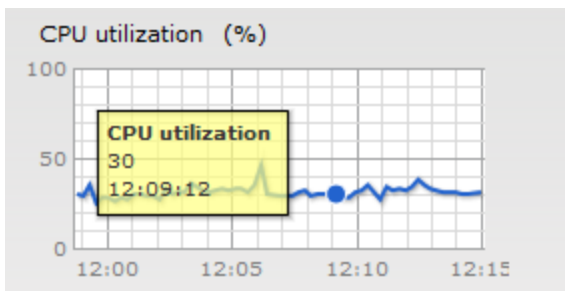
- Neighboring APs

**Figure 178 - Neighboring APs Graph**



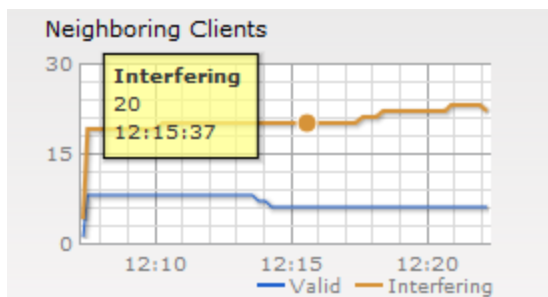
- CPU Utilization

**Figure 179 - CPU Utilization Graph**



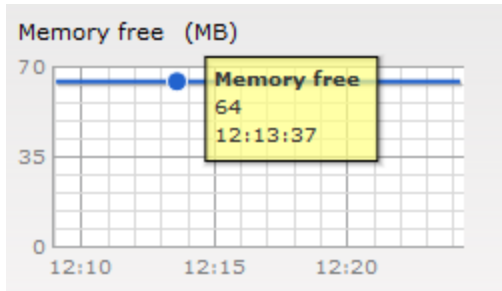
- Neighboring Clients

**Figure 180 - Neighboring Clients Graph**



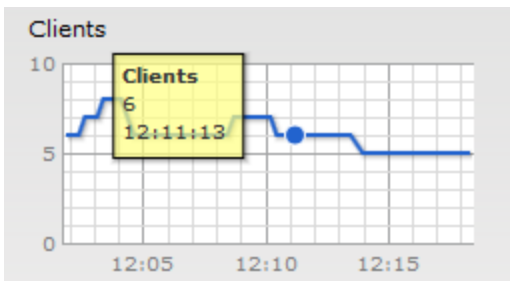
- Memory Free (MB)

**Figure 181 - Memory free Graph**



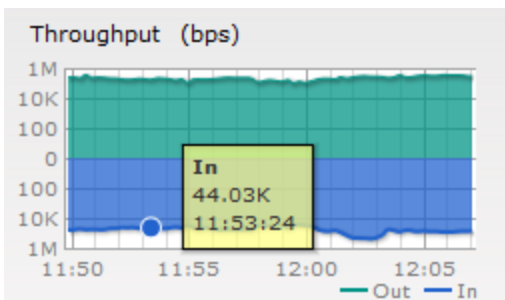
- Clients

**Figure 182 - Clients Graph**



- Throughput (bps)

**Figure 183 - Throughput Graph**



For more information about the graphs in the instant access point view and or monitoring procedures, see [Table 41](#).

**Table 41 - Dell W-Instant Access Point View — Usage Trends and Monitoring Procedures**

Graph Name	Description	Monitoring Procedure
Neighboring APs	The Neighboring APs graph shows the number of APs heard by the selected IAP: Valid APs: An AP that is part of the enterprise providing WLAN service. Interfering APs: An AP that is seen in the RF environment but is not	To check the neighboring APs detected by the W-IAP for the last 15 minutes, 1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.

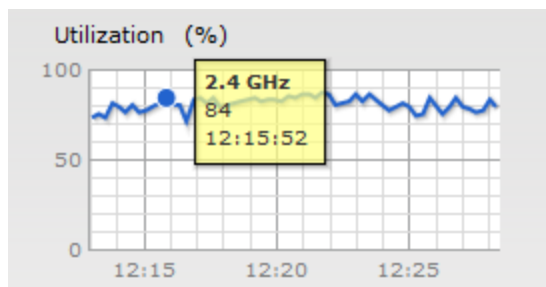
Graph Name	Description	Monitoring Procedure
	<p>connected to the network.  <b>Rogue APs:</b> An unauthorized AP that is plugged into the wired side of the network.            To see the number of different types of neighboring APs for the last 15 minutes, hover the cursor over the respective graph lines.</p>	<ol style="list-style-type: none"> <li>In the <b>Access Points</b> tab, click the W-IAP for which you want to monitor the client association. The W-IAP view appears.</li> <li>Study the Neighboring APs graph in the <b>Overview</b> section. For example, the graph shows that 148 interfering APs are detected by the W-IAP at 12:04 hours.</li> </ol>
CPU Utilization	<p>The CPU Utilization graph displays the utilization of CPU for the selected IAP. To see the CPU utilization of the W-IAP, hover the cursor over the graph line.</p>	<p>To check the CPU utilization of the W-IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the <b>Access Points</b> tab, click the W-IAP for which you want to monitor the client association. The W-IAP view appears.</li> <li>Study the CPU Utilization graph in the <b>Overview</b> pane. For example, the graph shows that the CPU utilization of the W-IAP is 30% at 12:09 hours.</li> </ol>
Neighboring Clients	<p>The Neighboring Clients graph shows the number of clients not connected to the selected AP, but heard by it:  <b>Valid:</b> Any client that successfully authenticates with a valid AP and passes encrypted traffic is classified as a valid client.  <b>Interfering:</b> A client associated to any AP and is not valid.            To see the number of different types of neighboring clients for the last 15 minutes, hover the cursor over the respective graph lines.</p>	<p>To check the neighboring clients detected by the W-IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the <b>Access Points</b> tab, click the W-IAP for which you want to monitor the client association. The W-IAP view appears.</li> <li>Study the Neighboring Clients graph in the <b>Overview</b> pane. For example, the graph shows that 20 interfering clients were detected by the W-IAP at 12:15 hours.</li> </ol>
Memory free (MB)	<p>The memory free graph displays the memory availability of the W-IAP in Mega Bytes (MB). To see the free memory of the W-IAP, hover the cursor over the graph line.</p>	<p>To check the free memory of the W-IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the <b>Access Points</b> tab, click the W-IAP for which you want to monitor the client association. The W-IAP view appears.</li> <li>Study the Memory free graph in the <b>Overview</b> pane. For example, the graph shows that the free memory of the W-IAP is 64 MB at 12:13 hours.</li> </ol>

Graph Name	Description	Monitoring Procedure
Clients	<p>The Clients graph shows the number of clients associated with the selected W-IAP for the last 15 minutes.</p> <p>To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the W-IAP for the last 15 minutes.</p> <p>To see the exact number of clients associated with the selected W-IAP at a particular time, hover the cursor over the graph line.</p>	<p>To check the number of clients associated with the W-IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the <b>Access Points</b> tab, click the W-IAP for which you want to monitor the client association. The W-IAP view appears.</li> <li>3. Study the Clients graph. For example, the graph shows that six clients are associated with the W-IAP at 12:11 hours.</li> </ol>
Throughput	<p>The Throughput graph shows the throughput for the selected W-IAP for the last 15 minutes.</p> <ul style="list-style-type: none"> <li>• Outgoing traffic — Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown about the median line.</li> <li>• Incoming traffic — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line.</li> </ul> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>• The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the W-IAP for the last 15 minutes.</li> </ul> <p>To see the exact throughput of the selected W-IAP at a particular time, hover the cursor over the graph line.</p>	<p>To check the throughput of the selected W-IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the <b>Access Points</b> tab, click the W-IAP for which you want to monitor the throughput. The W-IAP view appears.</li> <li>3. Study the Throughput graph. For example, the graph shows 44.03 kbps incoming traffic throughput at 12:08 hours.</li> </ol>

The Overview section also has two links— 2.4 GHz and 5 GHz. The following graphs are displayed for each band:

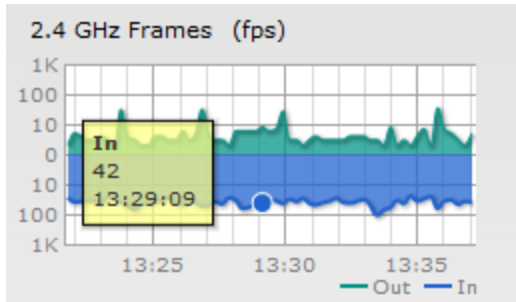
- Utilization

**Figure 184 - Utilization Graph**



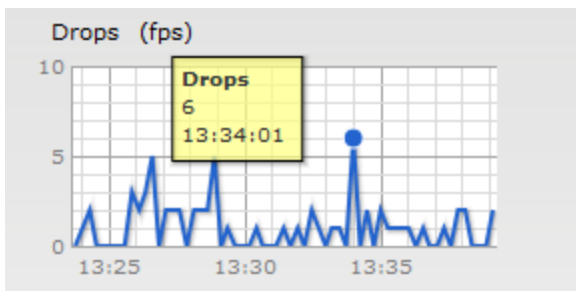
- 2.4 GHz Frames (fps)

**Figure 185 - 2.4 GHz Management Frames (fps) Graph**



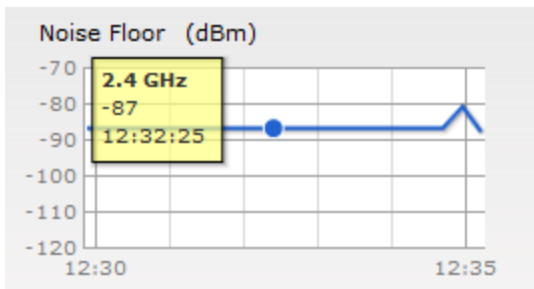
- Drops (fps)

**Figure 186 - Drops (fps) Graph**



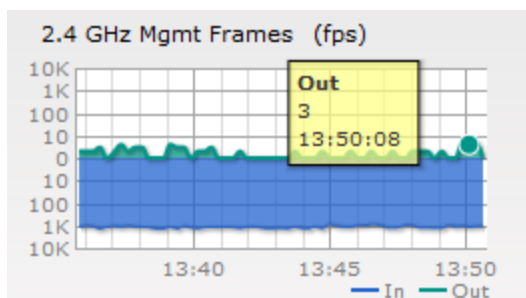
- Noise Floor (dBm)

**Figure 187 - Noise Floor (dBm) Graph**



- 2.4 GHz Mgmt Frames

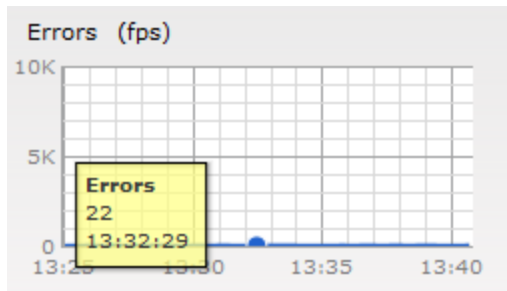
**Figure 188 - 2.4 GHz Management Frames (fps) Graph**





- Errors (fps) Graph


**Figure 189 - Errors (fps) Graph**





To see the graphs for the 5 GHz band, click the **5 GHz** link.

For more information about the graphs in the instant access point view and for monitoring procedures, see [Table 42](#).

**Table 42 - Dell W-Instant Access Point View — RF Trends Graphs and Monitoring Procedures**

Graph Name	Description	Monitoring Procedure
Utilization	<p>The Utilization graph shows the radio utilization percentage of the access point for the last 15 minutes. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average radio utilization statistics for the W-IAP for the last 15 minutes. To see the exact utilization percent at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the utilization of the selected W-IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the <b>Access Points</b> tab, click the W-IAP for which you want to monitor the utilization. The W-IAP view appears.</li> <li>3. Study the Utilization graph in the RF Trends pane. For example, the graph shows 84% W-IAP radio utilization for the 2.4 GHz band at 12:15 hours.</li> </ol> <p><b>NOTE:</b> You can also click the rectangle icon under the Utilization column in the <b>RF Dashboard</b> pane to see the Utilization graph for the selected W-IAP. The rectangle icon is seen as follows:</p> 
2.4 GHz Frames	<p>The 2.4 GHz Frames graph shows the In and Out frame rate per second for the radio in 2.4 GHz band for the last 15 minutes.</p> <ul style="list-style-type: none"> <li>• Outgoing frames — Outgoing frame traffic is displayed in green. It is</li> </ul>	<p>To monitor the In and Out frame rate per second for the radio in 2.4 GHz band, for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default</li> </ol>

Graph Name	Description	Monitoring Procedure
	<p>shown above the median line.</p> <ul style="list-style-type: none"> <li>Incoming frames — Incoming frame traffic is displayed in blue. It is shown below the median line.</li> </ul> <p>To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing frames.</p> <p>To see the exact utilization percent at a particular time, hover the cursor over the graph line.</p>	<p>view.</p> <ol style="list-style-type: none"> <li>In the <b>Access Points</b> tab, click the name link of the W-IAP for which you want to monitor the frame rate. The W-IAP view appears.</li> <li>Study the 2.4 GHz Frames graph. For example, the graph shows 42 incoming frames at 13:29 hours.</li> </ol>
Drops	<p>The Drops graph shows dropped frames over the last 15 minutes.</p> <p>To see the number of frames dropped at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the number of frames dropped for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the <b>Access Points</b> tab, click the name link of the W-IAP for which you want to monitor the frame rate. The W-IAP view appears.</li> <li>Study the Drops graph. For example, the graph shows that 6 frames per second were dropped at 13:34 hours.</li> </ol>
Noise Floor	<p>The Noise Floor graph shows the signals created by all the noise sources and unwanted signals in the network. Noise floor is measured in decibels/metre. Too many unwanted signals hamper the performance of the W-IAP. Monitor the noise floor regularly for optimal performance of the W-IAP.</p> <p>To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In and Out frames.</p> <p>To see the exact utilization percent at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the noise floor for the W-IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the <b>Access Points</b> tab, click the name link of the W-IAP for which you want to monitor the noise floor. The W-IAP view appears.</li> <li>Study the Noise Floor graph. For example, the graph shows that the noise floor for the W-IAP at 22:38 hours is —82.0 dBm.</li> </ol> <p><b>NOTE:</b> You can also click the rectangle icon the Noise column in the <b>RF Dashboard</b> pane to see the Noise graph for the selected W-IAP. The rectangle icon is seen as follows:</p> 
2.4 GHz Mgmt	<p>The 2.4 GHz Mgmt Frames graph shows the rate for management frames</p>	<p>To monitor the rate of management frames in and out of the radio for the</p>

Graph Name	Description	Monitoring Procedure
Frames	<p>in and out of the radio in the 2.4 GHz band for the last 15 minutes. Note that the scale for the Y-axis is logarithmic. To see the exact number of management frames per second at a particular time, hover the cursor over the graph lines.</p>	<p>last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the <b>Access Points</b> tab, click the name link of the W-IAP for which you want to monitor the noise floor. The W-IAP view appears.</li> <li>3. Study the 2.4 GHz Mgmt Frames graph. For example, the graph shows that 3 management frames were out of the radio at 13:50 hours.</li> </ol>
Errors	<p>The Errors graph shows the errors that occurred while receiving the frames for the last 15 minutes. The errors are measured in frames per second. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In and Out frames. To see the exact utilization percent at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the errors for the W-IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the <b>Access Points</b> tab, click the name link of the W-IAP for which you want to monitor the errors. The W-IAP view appears.</li> <li>3. Study the Errors graph. For example, the graph shows that the errors for the W-IAP at 13:32 hours is 22 frames per second.</li> </ol> <p><b>NOTE:</b> You can also click the rectangle icon under the Errors column in the <b>RF Dashboard</b> pane to see the Errors graph for the selected W-IAP.</p> 

## Client View

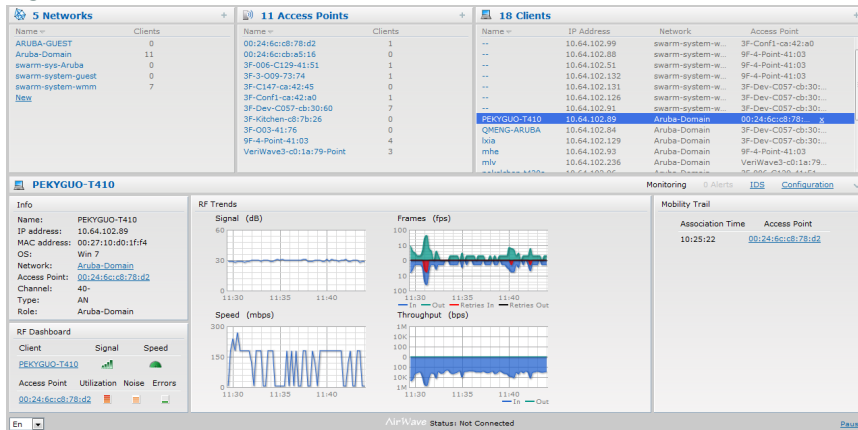
In the Virtual Controller view, all clients in the Dell W-Instant network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor. Client view for that client appears.

The Client view has three tabs— Networks, Access Points, and Clients.

The following sections in the Dell W-Series Instant UI provide information about the selected client:

- Info
- RF Dashboard
- RF Trends
- Usage Trends

Figure 190 - Client View



## Info

The **Info** section provides the following information about the selected W-IAP:

- **Name**— Name of the selected client.
- **IP Address**— IP address of the client.
- **MAC Address**— MAC Address of the client.
- **OS**— Operating System that is running on the client.
- **Network**— Network to which the client is connected to.
- **Access Point**— W-IAP to which the client is connected to.
- **Channel**— Channel that the client is using.
- **Type**— Channel type that the client is broadcasting on.

## RF Dashboard

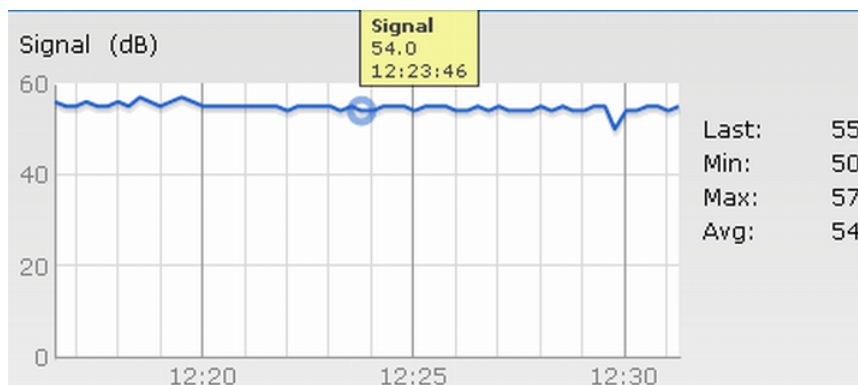
In the Client view, the **RF Dashboard** section is moved below the **Info** section. The **RF Dashboard** section in the client view shows the speed and the signal information for the client and the RF information for the W-IAP to which the client is connected to.

## RF Trends

The **RF Trends** section displays the following graphs for the selected client:

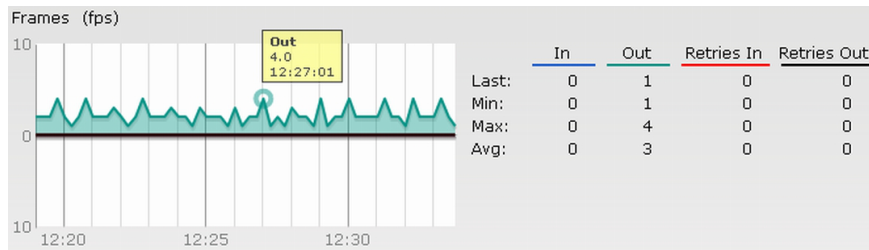
- Signal

Figure 191 - Signal Graph



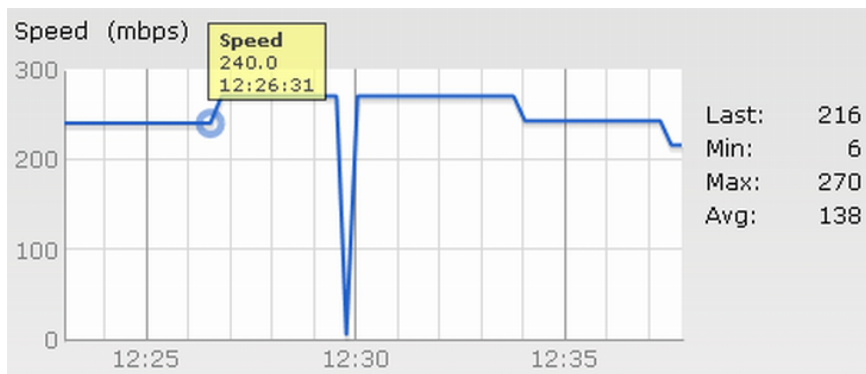
- Frames

**Figure 192 - Frames Graph**



- Speed

**Figure 193 - Speed Graph**



- Throughput

**Figure 194 - Throughput Graph**



For more information about RF trends graphs in the client view and for monitoring procedures, see [Table 43](#).

**Table 43 - Client View — RF Trends Graphs and Monitoring Procedures**

Graph Name	Description	Monitoring Procedure
Signal	<p>The Signal graph shows the signal strength of the client for the last 15 minutes. It is measured in decibels. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average signal statistics for the client for the last 15 minutes.</p> <p>To see the exact signal strength at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the signal strength of the selected client for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the <b>Clients</b> tab, click the IP address of the client for which you want to monitor the signal strength. The client view appears.</li> <li>3. Study the Signal graph in the RF Trends pane. For example, the graph shows that signal strength for the client is 54.0 dB at 12:23 hours.</li> </ol>
Frames	<p>The Frames Graph shows the In and Out frame rate per second for the client for the last 15 minutes. It also shows data for the Retry In and Retry Out frames.</p> <ul style="list-style-type: none"> <li>• Outgoing frames — Outgoing frame traffic is displayed in green. It is shown above the median line.</li> <li>• Incoming frames — Incoming frame traffic is displayed in blue. It is shown below the median line.</li> <li>• Retry Out — Retries for the outgoing frames is displayed in black and is shown above the median line.</li> <li>• Retry In — Retries for the incoming frames is displayed in red and is shown below the median line.</li> </ul> <p>To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In, Out, Retries In, and Retries Out frames.</p> <p>To see the exact frames at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the In and Out frame rate per second and retry frames for the In and Out traffic, for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the <b>Clients</b> tab, click the IP address of the client for which you want to monitor the frames. The client view appears.</li> <li>3. Study the Frames graph in the RF Trends pane. For example, the graph shows 4.0 frames per second for the client at 12:27 hours.</li> </ol>
Speed	<p>The Speed graph shows the data transfer speed for the client. Data transfer is measured in Mega bits per second (mbps).</p> <p>To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics for the client for the last 15 minutes.</p> <p>To see the exact speed at a particular time, hover the cursor over the graph</p>	<p>To monitor the speed for the client for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the <b>Clients</b> tab, click the IP address of the client for which you want to monitor the speed. The client view appears.</li> <li>3. Study the Speed graph in the RF</li> </ol>

Graph Name	Description	Monitoring Procedure
	line.	Trends pane. For example, the graph shows that the data transfer speed at 12:26 hours is 240 Mbps.
Throughput	<p>The Throughput Graph shows the throughput for the selected client for the last 15 minutes.</p> <ul style="list-style-type: none"> <li>• <b>Outgoing traffic</b> — Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line.</li> <li>• <b>Incoming traffic</b> — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line.</li> </ul> <p>To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the client for the last 15 minutes. To see the exact throughput at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the errors for the client for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Dell W-Series Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the <b>Clients</b> tab, click the IP address of the client for which you want to monitor the throughput. The client view appears.</li> <li>3. Study the Throughput graph in the RF Trends pane. For example, the graph shows 1.0 kbps outgoing traffic throughput for the client at 12:30 hours.</li> </ol>

## Mobility Trail

The **Mobility Trail** section displays the following mobility trail information for the selected client:

- **Association Time**— The time at which the selected client was associated with a particular W-IAP.  
The Dell W-Series Instant UI shows the client-W-IAP association over the last 15 minutes.
- **Access Point**— W-IAP name with which the client was associated.




---

**NOTE:** Mobility information about the client is reset each time it roams from one W-IAP to another.

---





# Chapter 26

## Alert Types and Management

### Alert Types

Alerts are generated when a user encounters problems accessing or connecting to the Wi-Fi network. These alerts enable you to troubleshoot the problems. The alerts that are generated on Dell W-Instant can be categorized as follows:

- 802.11 related association and authentication failure alerts.
- 802.1X related mode and key mismatch, server, and client time-out failure alerts.
- IP address related failure - Static IP address or DHCP related alerts.

[Table 44](#) displays a list of alerts that are generated on the Dell W-Instant network.

**Table 44 - Alerts List**

Type Code	Description	Details	Corrective Actions
100101	Internal error	The W-IAP has encountered an internal error for this client.	Contact the Dell customer support team.
100102	Unknown SSID in association request	The W-IAP cannot allow this client to associate because the association request received contains an unknown SSID.	Identify the client and check its Wi-Fi driver and manager software.
100103	Mismatched authentication/encryption setting	The W-IAP cannot allow this client to associate because its authentication or encryption settings do not match W-IAP's configuration.	Ascertain the correct authentication or encryption settings and try to associate again.
100104	Unsupported 802.11 rate	The W-IAP cannot allow this client to associate because it does not support the 802.11 rate requested by this client.	Check the configuration on the W-IAP to see if the desired rate can be supported; if not, consider replacing the W-IAP with another model that can support the rate.
100105	Maximum capacity reached on W-IAP	The W-IAP has reached maximum capacity and cannot accommodate any more clients.	Consider expanding capacity by installing additional W-IAPs or balance load by relocating W-IAPs.
100206	Invalid MAC Address	The W-IAP cannot	This condition may be

Type Code	Description	Details	Corrective Actions
		authenticate this client because the client's MAC address is not valid.	indicative of a misbehaving client. Try to locate the client device and check its hardware and software.
100307	Client blocked due to repeated authentication failures	The W-IAP is temporarily blocking the 802.1X authentication request from this client because the credentials provided have been rejected by the RADIUS server too many times.	Identify the client and check its 802.1X credentials.
100308	RADIUS server connection failure	The W-IAP cannot authenticate this client using 802.1X because the RADIUS server did not respond to the authentication request.	If the W-IAP is using the internal RADIUS server, recommend checking the related configuration as well as the installed certificate and passphrase.  If the W-IAP is using an external RADIUS server, check if there are any issues with the RADIUS server and try connecting again.
100309	RADIUS server authentication failure	The W-IAP cannot authenticate this client using 802.1X because the RADIUS server rejected the authentication credentials (password, etc) provided by the client.	Ascertain the correct authentication credentials and log in again.
100410	Integrity check failure in encrypted message	The W-IAP cannot receive data from this client because the integrity check of the received message (MIC) has failed.	Check the encryption setting on the client and on the W-IAP.
100511	DHCP request timed out	This client did not receive a response to its DHCP request in time.	Check the status of the DHCP server in the network.

# Chapter 27

## Policy Enforcement Firewall

Dell's Policy Enforcement Firewall (PEF) module for Dell W-Instant provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks.

The PEF window displays the external/internal authentication servers, currently defined roles for all the networks, blacklisted clients and to enable or disable the protocols for ALG.

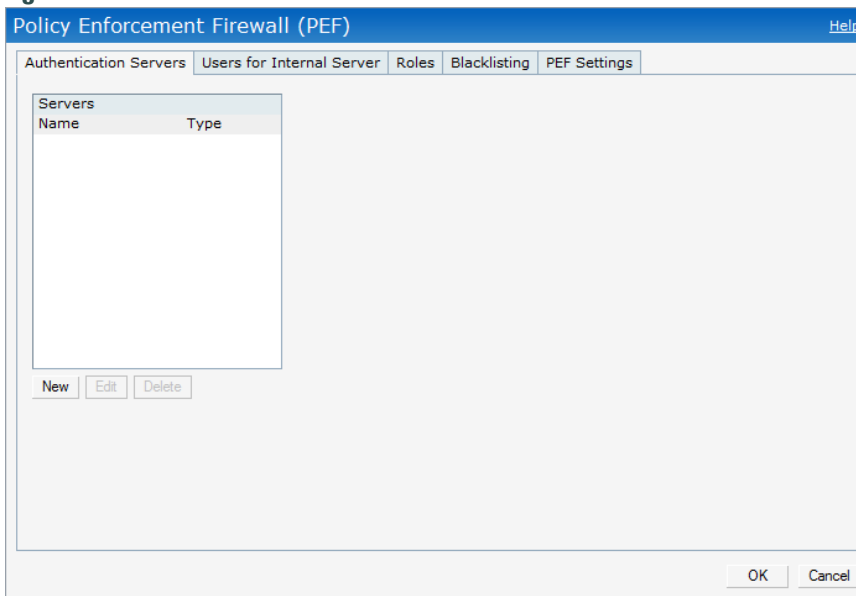
Navigate to the **PEF** link at the top right corner of the Dell W-Series Instant UI to view the following features.

### Authentication Servers

This section displays the currently defined external authentication servers.

- **Name**— Indicates the name of the external authentication server.
  - **Type**— Indicates the type of the authentication server-RADIUS or LDAP.
1. Click **New** to configure an external RADIUS server for a wireless network. See "[External RADIUS Server](#)" on page 112 for more information.
  2. Click **OK** to apply the changes.

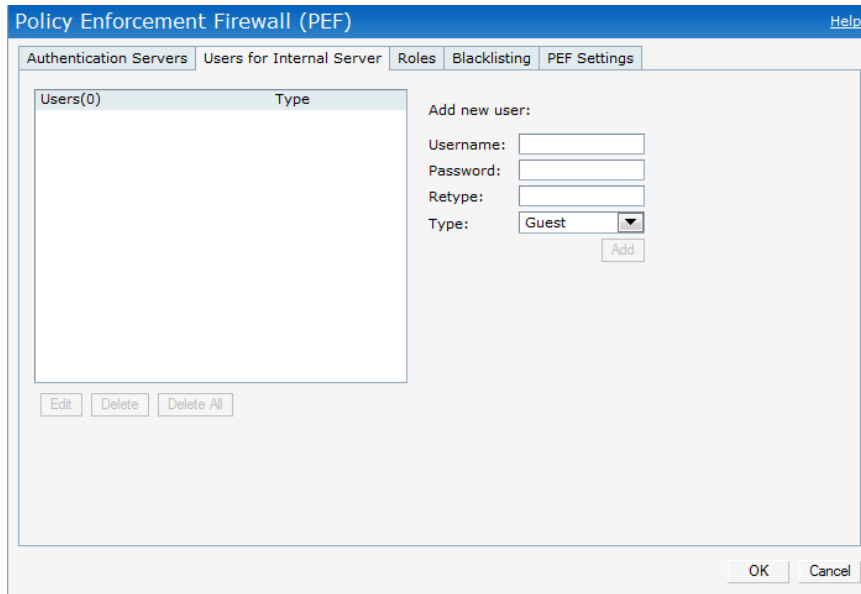
**Figure 195 - Authentication Server**



### Users for Internal Server

This section displays the currently defined users for the internal authentication server.

**Figure 196 - Users for Internal Server**



To add a user:

1. Enter the username in the **Username** text box.
2. Enter the password in the **Password** text box and reconfirm
3. Select appropriate network type from the **Type** drop-down list.
4. Click **Add** and click **OK**. The users are listed in the **Users** list.

See "[User Database](#)" on page 269 for more information.

## Roles

This window consists of the following options:

- **Roles**— This table displays all the roles defined for all the networks. See "[User Role](#)" on page 151 for more information.



---

**NOTE:** A special default role with the same name as the network is automatically defined for each network. These roles cannot be deleted or renamed.

---

- **Access Rules**— This table lists the permissions for each Role. See "[Role Derivation](#)" on page 145 for more information.

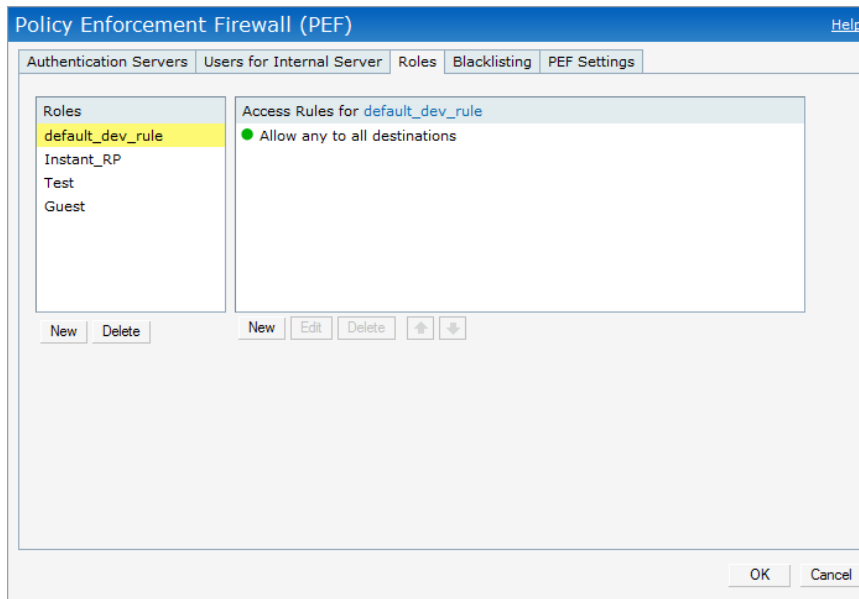


---

**NOTE:** This release of W-Instant supports configuration of up to 64 access rules.

---

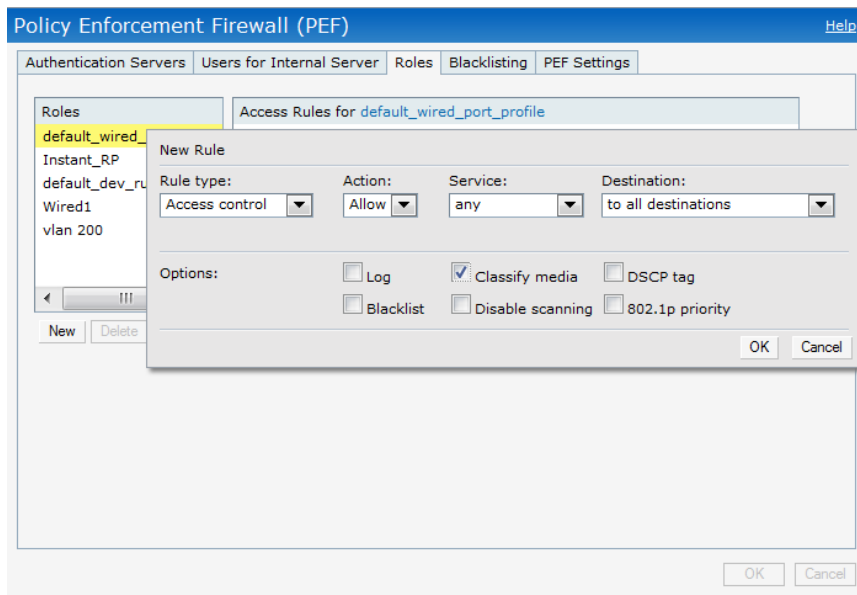
**Figure 197 - Roles**



## Extended Voice and Video Functionalities

W-Instant has the added ability to identify and prioritize voice and video traffic from applications like Microsoft Office Communications Server (OCS) and Apple Facetime.

**Figure 198 - Classify Media**



## QoS for Microsoft Office OCS and Apple Facetime

Voice and video devices use a signaling protocol to establish, control, and terminate voice and video calls. These control or signaling sessions are usually permitted using pre-defined ACLs. If, however, the control signaling packets are encrypted, the W-IAP cannot determine which dynamic ports are used for voice or video traffic. In these cases, the W-IAP has to use an ACL with the

classify-media option enabled to identify the voice or video flow based on a deep packet inspection and analysis of the actual traffic.

### Microsoft OCS

Microsoft Office Communications Server (OCS) uses Session Initiation Protocol (SIP) over TLS to establish, control, and terminate voice and video calls.

### Apple Facetime

When an Apple device starts a Facetime video call, it initiates a TCP session to the Apple Facetime server over port 5223, then sends SIP signaling messages over a non-default port. When media traffic starts flowing, audio and video data are sent through that same port using RTP. (The audio and video packets are interleaved in the air, though individual the sessions can be uniquely identified using their payload type and sequence numbers.) The RTP header and payload also get encapsulated under the TURN ChannelData Messages. The Facetime call is terminated with a SIP BYE message that can be sent by either party.

The following table lists the ports used by Apple Facetime. Facetime users need to be assigned a role where traffic is allowed on these ports.

**Table 45 - Ports Used by the Apple Facetime Application**

Port	Packet Type
53	TCP/UDP
443	TCP
3478-3497	UDP
5223	TCP
16384-16387	UDP
16393-16402	UDP

The following screenshots are configuration examples for Microsoft OCS and Apple Facetime applications.

Figure 199 - Classify Media —Microsoft Lync

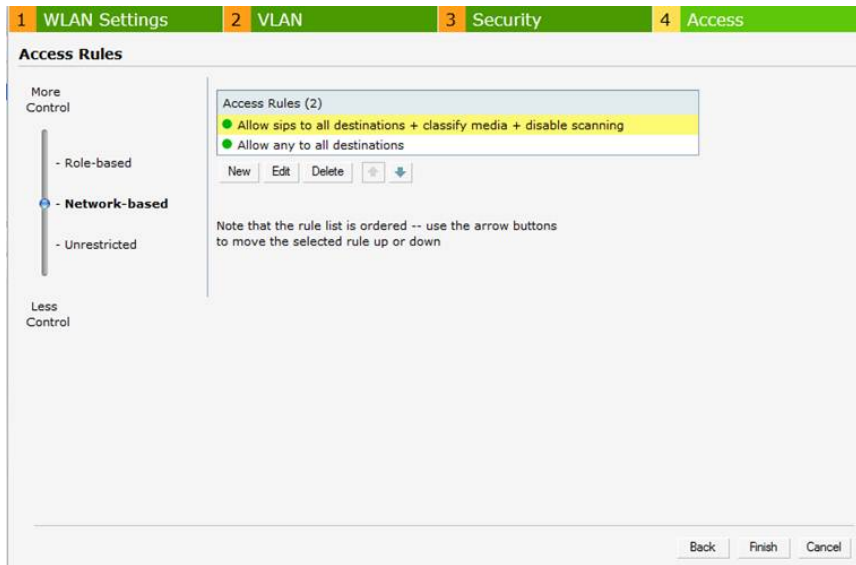


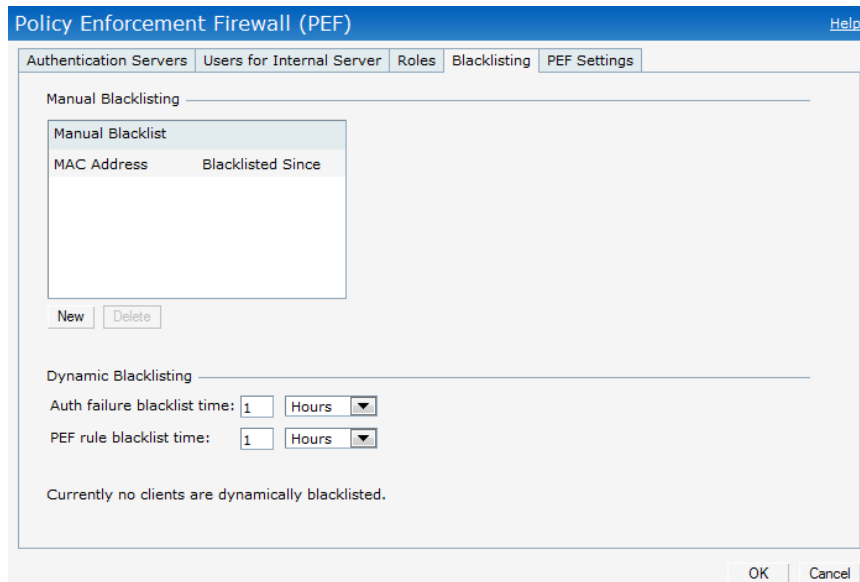
Figure 200 - Classify Media —Apple Facetime



## Client Blacklisting

The client blacklisting denies connectivity to the blacklisted clients. When a client is blacklisted in an Dell W-IAP, the client is not allowed to associate with the W-IAP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force the client to disconnect.

**Figure 201 - Client Blacklisting**



## Types of Client Blacklisting

- The following types of client blacklisting can be generated in an W-Instant:
- Manual Blacklisting
- Dynamic Blacklisting
  - Authentication Failure Blacklisting
  - Session Firewall Based Blacklisting

### Manual Blacklisting

Manual blacklisting is the simplest way to add a client to the blacklist. In manual blacklisting, the MAC address of the client has to be known to the user. These clients would be added into a permanent blacklist. These clients are not allowed to connect to the network unless they are removed from the blacklist.

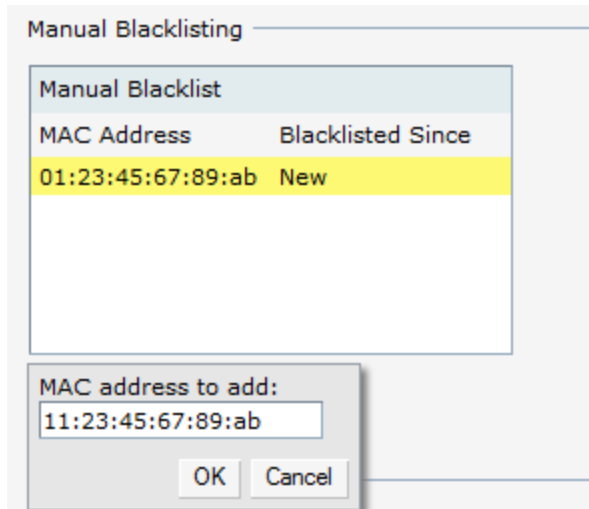
### Adding a Client to the Manual Blacklist

To add a client to the blacklist manually using the MAC address of the client:

1. Click on the **PEF** link and then select **Blacklisting** tab.
2. Click on the **New** button under the **Manual Blacklisting** window.
3. Enter the MAC address of the client to be blacklisted in the **MAC address to add** text box.



**Figure 202 - Manual Blacklisting**



4. Click **Ok**.

The **Blacklisted Since** tab displays the time at which the current blacklisting started for the client.

5. To delete a client from the manual blacklist, select the **MAC Address** of the client under the **Manual Blacklisting** window and then click **Delete**.

## Dynamic Blacklisting

The clients can be blacklisted dynamically when they exceed the authentication failure threshold or a blacklisting rule was triggered as part of the authentication process.

### Authentication Failure Blacklisting

When the time taken by a client fails to authenticate exceeds the configured threshold, the client is automatically blacklisted by a W-IAP.

### Session Firewall Based Blacklisting

In session firewall based blacklisting, an ACL rule is used to enable the option for automation blacklisting. when the ACL rule is hit, it would send out blacklist information and the client would be blacklisted.

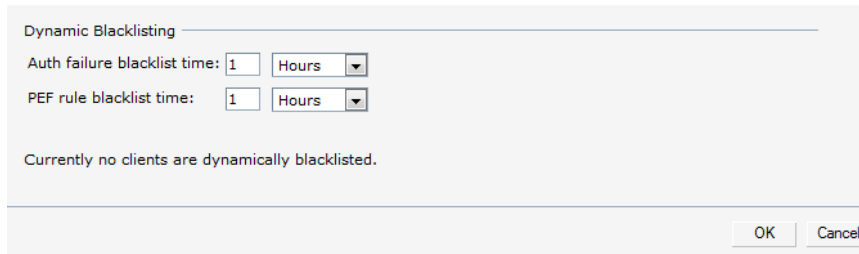
To set the blacklist duration:

1. Select the **PEF** link and then select **Blacklisting** tab.
  - **Auth failure blacklist time**— Enter the duration since the blacklisting has been triggered when the authentication failure threshold is exceeded.
  - **PEF rule blacklisted time**— Enter the duration since the blacklisting has been triggered when a blacklisting rule has been triggered.



**NOTE:** In the **Networks** tab, click the **New** link and navigate to **New WLAN > VLAN > Security** page to enable Blacklisting. Set a value between 1 to 10 in the max authentication failures field for the selected SSID. To enable session firewall based blacklisting, click **New** and navigate to **WLAN Settings > VLAN > Security > Access** window and enable the **Blacklist** option of the corresponding ACL rule.

**Figure 203 - Dynamic Blacklisting**



## PEF Settings

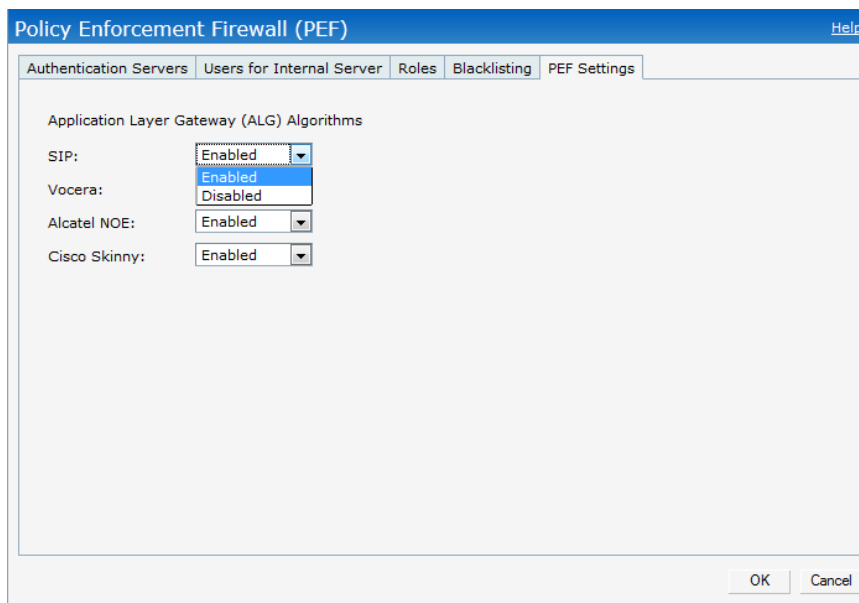
### Firewall ALG Configuration

Instant firewall now supports the ALG (Application Layer Gateway) functions such as SIP, Vocera, Alcatel NOE, and Cisco Skinny protocols.

To enable or disable the protocols for ALG in Dell W-Instant perform the following steps:

1. Select **PEF** from the top right of the Dell W-Series Instant UI.
2. Select **PEF Settings** tab.
3. Select **Enabled** from the corresponding drop-down list to enable SIP, VOCERA, Alcatel NOE, and Cisco skinny protocols.

**Figure 204 - Enabling ALG Protocols**



4. Click **OK**.



**NOTE:** When the protocols for ALG are **Disabled** the changes do not take effect until the existing user sessions expire. Reboot the W-IAP and the client, or wait for few minutes to ensure the changes take effect.

## Firewall-based Logging

W-Instant firewall now supports firewall based logging function. The firewall logs on the W-Instant APs are generated as syslog messages.



# Chapter 28

## VPN Configuration

The W-IAP supports termination of a VPN tunnel on the Dell controller.

VPN features are ideal for:

- enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
- branch offices that require multiple APs.
- individuals working from home, connecting to the VPN.

This new architecture and form factor seamlessly adds the survivability feature of W-Instant APs with the VPN connectivity of RAPs — providing corporate connectivity to non-corporates.

### VPN Configuration

The VPN configuration functionality enables the W-IAP to create a single VPN tunnel from the Virtual Controller to a Dell PowerConnect W-Series Mobility Controller in your corporate office. Here, the VPN tunnels from the Instant APs terminate on the Dell PowerConnect W-Series Mobility Controller. The controller solely acts as a VPN end-point and does not supply the W-Instant AP with any configuration.

To create a VPN tunnel from the Virtual Controller to the Dell PowerConnect W-Series Mobility Controller:

**Figure 205 - Tunneling— Controller**

The screenshot shows a configuration window titled "Tunneling" with a "Help" link in the top right corner. Below the title bar are three tabs: "1 Controller" (highlighted in green), "2 Routing", and "3 DHCP Server". The "Controller" tab is active, displaying the following configuration fields:

- Protocol:
- Primary host:
- Backup host:
- Preemption:
- Fast failover:
- Connection Test Frequency:
- Test Packet count:

At the bottom right of the configuration area are two buttons: "Next" and "Cancel".

1. Navigate to the **VPN** link at the top right corner of the Dell W-Series Instant UI. The **Tunneling** window appears.
2. Select **IPSec** from the **Protocol** drop-down list.
3. If you select **GRE** from the **Protocol** drop-down list then the packets are sent and received without encryption.
  - a. **GRE type** — Enter the value for GRE type parameter.
  - b. **Per-AP tunnel** — Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. The user can create GRE tunnels from all of the APs instead of creating tunnels only from the AP that is acting as the Virtual Controller. The traffic going to the corporate is sent via L2 GRE tunnel from the AP itself and does not have to be forwarded through the Virtual Controller.



---

**NOTE:** By default, the **Per-AP tunnel** option is disabled.

---

4. Enter the IP address or fully qualified domain name for the main VPN/GRE endpoint in the **Primary host** field.
5. Enter the IP address or fully qualified domain name for the backup VPN endpoint in the **Backup host** field. This entry is optional.
6. Select **Enabled** from the **Preemption** drop-down list to switch back to the primary host when and if it becomes available again. This step is optional.
7. Select **Enabled** or **Disabled** from the **Fast failover** drop-down list.
8. Enter **Connection test frequency** at which packets are sent to the controller. The unit is seconds per packet and the default value is 10 seconds which means that every 10 seconds the W-IAP will send one packet to the controller.



---

**NOTE:** This value should be less than L3 user time out value in the Dell Controller. For example, if L3 user timeout in the Dell Controller is 5 minutes, the Connection test frequency should be less than 300 seconds.

---

9. Enter **Test packet count** which is the number of lost packets and after which the W-IAP will make the tunnel down. The default value is 2.
10. Click **Next** to continue.

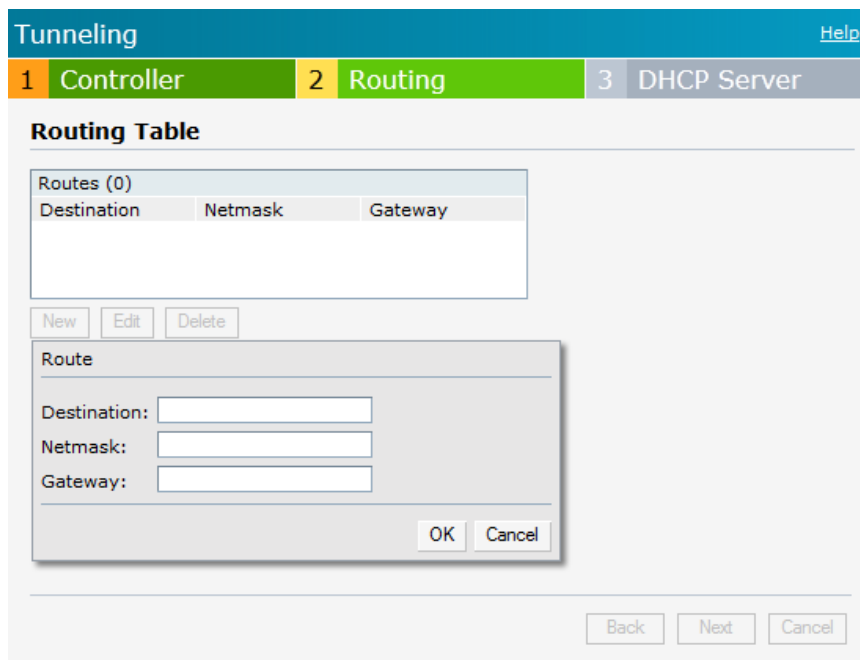
## Fast Failover

Enabling the fast failover feature allows the W-IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnel separately. If the primary tunnel fails, the W-IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

## Routing Profile Configuration

W-Instant can terminate a single VPN connection on an Dell PowerConnect W-Series Mobility Controller. The Routing profile defines the corporate subnets which need to be tunneled through the IPSec tunnel.

Figure 206 - Tunneling— Routing



Use the **Routing Table** to specify policy based on routing into the VPN tunnel. Each routing table entry has a destination, network mask, and default gateway.

1. Click **New** and update the following parameters.
  - **Destination**— Specify the destination network to be routed into the VPN tunnel.
  - **Netmask**— Specify the network mask of the network to be routed into the VPN tunnel.
  - **Gateway**— Specify the gateway to which traffic should be routed. This IP address should be the 'controller-ip' of the controller on which the VPN connection is terminated. See "[Controller Configuration for VPN](#)" on page 277 for more information.
2. Click **Next** to continue.
3. The **DHCP Server** window appears. Use this table to define DHCP pools of different types based on your deployment modes as described in the following section.

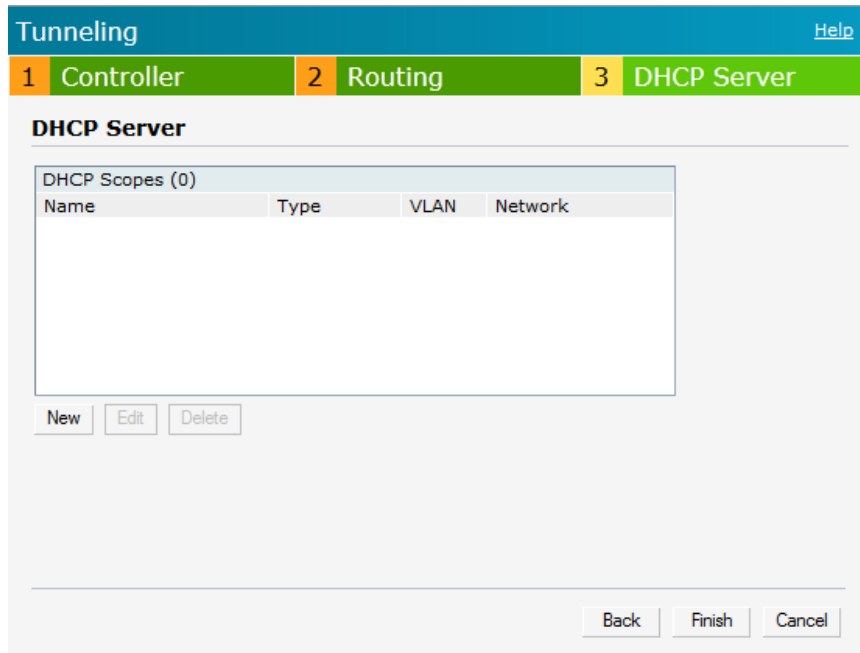
## DHCP Server Configuration

The Virtual Controller (VC) on an W-Instant AP enables different DHCP pools (various deployment models) in addition to allocating IP subnets to each branch. The following modes of DHCP server are supported:

- **Local Subnet**— In this mode, the VC assigns an IP address from a configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. This is achieved by appropriately translating the network address (NAT) and forwarding the packet through the IPsec tunnel or through the uplink.
- **L2 Switching Mode**— In this mode, W-Instant supports the following two types to support L2 switching mode of connection to corporate:
  - **Distributed L2**— In this mode, the VC assigns an IP address from a configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The VC adds the VLAN configured in this subnet to the controller VLAN multicast table enabling the L2 subnet to act as an extension of the VLAN on the controller. Corporate traffic is sent on the IPsec tunnel and non-corporate traffic is sent on the uplink.

- Centralized L2— In this mode, the VC does not assign an IP address to the client, but the DHCP traffic is directly forwarded to the controller over the IPsec tunnel and obtains an IP address from either the controller or a DHCP server behind the controller serving the VLAN of the client. However, W-Instant AP does forward client traffic in the same way as the **Distributed L2** mode.
  - L3 Routing Mode— In this mode, W-Instant supports L3 routing mode of connection to corporate. VC assigns an IP addresses from the configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. W-Instant AP takes care of routing on the subnet and also adds a route on the controller after the VPN tunnel is set up during the registration of the subnet.

**Figure 207 - Tunneling— DHCP Server**



## NAT DHCP Configuration

In NAT mode, the scope of the subnet is local to the W-IAP and forwards traffic through the IPsec tunnel or through the uplink.

- Click **New** in the **DHCP Server** window and select **Local** to configure the following parameters for NAT mode DHCP pool.
  - Name**— Name of the subnet (must be unique).
  - Type**— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Local** implies that this is a NAT mode DHCP subnet.
  - VLAN**— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
  - Network**— Network to be used for this subnet.
  - Netmask**— Net mask of the subnet. This along with Network determines the size of the subnet.
  - DNS server**— An optional field which defines the DNS server.
  - Domain name**— An optional field which defines the domain name.



- Lease time— An optional field which defines the lease time for client.

**Figure 208 - NAT DHCP Configuration**

The screenshot shows the 'Corporate Access' configuration interface. At the top, there are three tabs: '1 Controller', '2 Routing', and '3 DHCP Server'. The '3 DHCP Server' tab is selected. Below the tabs, the 'DHCP Server' section is visible. A 'New DHCP Scope' dialog box is open, containing the following fields:

- Name: nat
- Type: Local (dropdown menu)
- VLAN: 10
- Network: 172.16.10.0
- Netmask: 255.255.255.0
- DNS server: 10.1.1.1
- Domain name: dell.com
- Lease time: 720 min.

At the bottom of the dialog box are 'OK' and 'Cancel' buttons. Below the dialog box, in the main window, are 'Back', 'Finish', and 'Cancel' buttons.

2. Click **OK** to apply these changes.

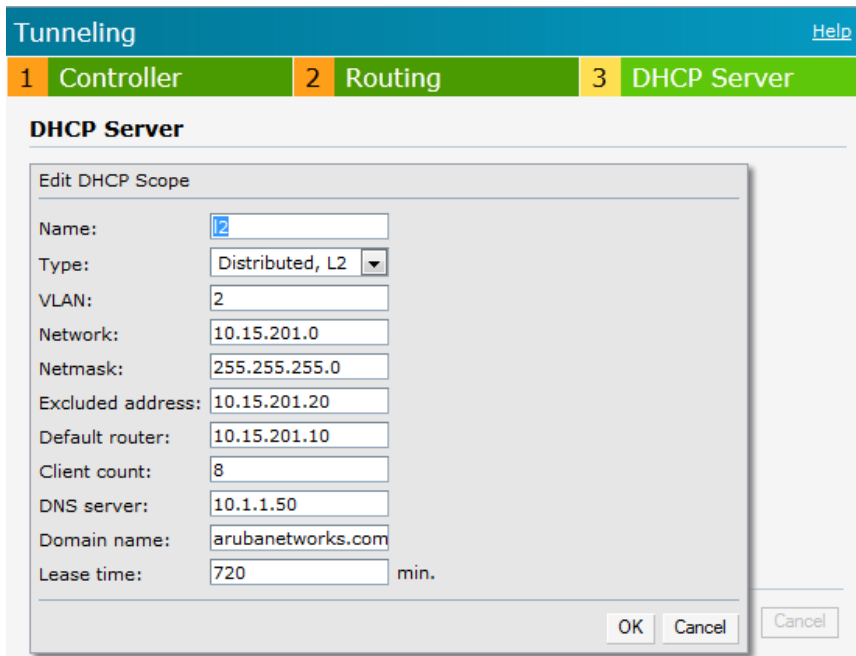
### **Distributed L2 DHCP Configuration**

In Distributed L2 mode, the Virtual Controller acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel.

1. Click **New** in the **DHCP Server** window and select **Distributed, L2** to configure the following parameters for Distributed L2 mode DHCP pool:
  - Name— Name of the subnet (must be unique).
  - Type— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Distributed, L2** implies that this is a Distributed mode L2 DHCP subnet.
  - VLAN— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
  - Network— Network to be used for this subnet.
  - Netmask— Net mask of the subnet. This along with Network determines the size of the subnet.
  - Excluded address— This determines the exclusion range of the subnet. Based on the size of the subnet and value configured here (location within the subnet scope), this is used to either exclude IP addresses before this IP or after this IP. This is an optional field.
  - Default router— Default router for the subnet. This is an IP address on/behind the controller in the same subnet.
  - Client count— This along with network and mask determines how many branches can be supported. For the current phase of W-IAP, it is important that this value is configured consistent across all branches.
  - DNS server— An optional field which defines the DNS server.

- Domain name— An optional field which defines the domain name.
  - Lease time— An optional field which defines the lease time for client.
2. Click **OK** to apply these changes.

**Figure 209 - Distributed L2 DHCP Configuration**



### Distributed L3 DHCP Configuration

In Distributed L3 mode, the Virtual Controller acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel.

1. Click **New** in the **DHCP Server** window and select **Distributed, L3** to configure the following parameters for Distributed L3 mode DHCP pool:
  - Name — Name of the subnet (must be unique).
  - Type— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Distributed, L3** implies that this is a Distributed mode L3 DHCP subnet.
  - VLAN— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
  - Network— Network to be used for this subnet.
  - Netmask— Net mask of the subnet. This along with Network determines the size of the subnet.
  - Client count— This along with network and mask determines how many branches can be supported. For the current phase of W-IAP, it is important that this value is configured consistent across all branches.
  - DNS server— An optional field which defines the DNS server.
  - Domain name— An optional field which defines the domain name.
  - Lease time— An optional field which defines the lease time for client
2. Click **OK** to apply these changes.

Figure 210 - Distributed L3 DHCP Configuration

The screenshot shows a software interface for configuring a DHCP Server. At the top, there is a 'Tunneling' header with a 'Help' link. Below it are three tabs: '1 Controller', '2 Routing', and '3 DHCP Server'. The 'DHCP Server' tab is active. The main window is titled 'DHCP Server' and contains an 'Edit DHCP Scope' dialog box. The dialog box has the following fields: 'Name' (text input), 'Type' (dropdown menu set to 'Distributed, L3'), 'VLAN' (text input set to '3'), 'Network' (text input set to '10.15.202.0'), 'Netmask' (text input set to '255.255.255.0'), 'Client count' (text input set to '8'), 'DNS server' (text input set to '10.1.1.50'), 'Domain name' (text input set to 'arubanetworks.com'), and 'Lease time' (text input set to '720' with 'min.' next to it). At the bottom of the dialog box are 'OK' and 'Cancel' buttons. Below the dialog box are 'Back', 'Finish', and 'Cancel' buttons.

### Centralized L2 DHCP Configuration

In Centralized L2 mode, both the DHCP server and default gateway are in the data center, on the other side of the VPN tunnel.

1. Click **New** in the **DHCP Server** window and select **Centralized, L2** to configure the following parameters for the Distributed L3 mode DHCP pool:
  - **Name** — Name of the subnet (must be unique).
  - **Type**— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Centralized, L2** implies that this is a Centralized mode L2 DHCP subnet.
  - **VLAN**— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
  - **DHCP Relay Agent and Option 82**— Select to enable or disable these features.

When a DHCP server is configured with a DHCP Relay agent, the client's Broadcast DHCP Discover packet is not sent to the corporate network, instead the Virtual Controller acts as the DHCP Relay and unicasts DHCP packets to the corporate DHCP server. Enable DHCP Option 82 to allow clients to send DHCP packets with the Option 82 string.

The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following:

- Remote Circuit IDi X AP-MAC; SSID; SSID-Type
- Remote Agenti X IDUE-MAC



**NOTE:** The Option 82 is specific to Alcatel and is not configurable in this version of W-Instant.

The following table describes the behavior of DHCP Relay Agent and Option 82 in the W-IAP.

**Table 46 - DHCP Relay and Option 82**

DHCP Relay	Option 82	Behavior
Enabled	Enabled	DHCP packet relayed with the ALU-specific Option 82 string
Enabled	Disabled	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	Enabled	DHCP packet not relayed, but broadcasted with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcasted without the ALU-specific Option 82 string

2. Click **OK** to apply these changes.

**Figure 211 - Centralized L2 DHCP Configuration**

The screenshot shows a configuration window titled "Tunneling" with a "Help" button in the top right corner. Below the title bar are three tabs: "1 Controller", "2 Routing", and "3 DHCP Server". The "DHCP Server" tab is active. The main content area is titled "DHCP Server" and contains a "New DHCP Scope" dialog box. The dialog box has the following fields and options:

- Name:** An empty text input field.
- Type:** A dropdown menu with "Centralized, L2" selected.
- VLAN:** An empty text input field.
- DHCP relay:** A dropdown menu with "Enabled" selected.
- DHCP server:** An empty text input field.
- Option 82:** A dropdown menu with "None" selected.

At the bottom right of the dialog box are "OK" and "Cancel" buttons. At the bottom of the main configuration window are "Back", "Finish", and "Cancel" buttons.

# Chapter 29

## User Database

In Dell W-Instant, the user database consists of a list of guest and employee users. Addition of a user involves specifying a username and password for the user. The login credentials for these users are provided outside the Dell W-Instant system.

A guest user can be a visitor who is temporarily using the enterprise network to access the Internet. However, you may not want to share the internal network and the intranet with them. To segregate the guest traffic from the enterprise traffic, you can create a Guest WLAN, specify the required authentication, encryption, and access rules and allow the guest user to use the enterprise network.

An employee user is the employee who is using the enterprise network for various official tasks. You can create Employee WLANs, specify the required authentication, encryption and access rules and allow the employees to use the enterprise network.



**NOTE:** The User Database is also used when Instant is employed as an internal RADIUS server.

### Adding a User

To add a user:

1. At the top right corner of the Dell W-Series Instant UI, click the **PEF** link and click **Users for Internal Server**.

**Figure 212 - Adding a User**

The screenshot shows the 'Users for Internal Server' configuration page in the Policy Enforcement Firewall (PEF) interface. The page has a blue header with 'Policy Enforcement Firewall (PEF)' and a 'Help' link. Below the header are several tabs: 'Authentication Servers', 'Users for Internal Server', 'Roles', 'Blacklisting', and 'PEF Settings'. The 'Users for Internal Server' tab is active. On the left, there is a table with the following structure:

Users(0)	Type
----------	------

Below the table are three buttons: 'Edit', 'Delete', and 'Delete All'. To the right of the table is the 'Add new user' section, which contains the following fields:

- Username:
- Password:
- Retype:
- Type:  (dropdown menu)

Below these fields is an 'Add' button. At the bottom right of the window are 'OK' and 'Cancel' buttons.

2. Enter the username in the **Username** text box.
3. Enter the password in the **Password** text box and reconfirm.

4. Select appropriate network type from the **Type** drop-down list.
5. Click **Add** and click **OK**. The users are listed in the **Users** list.

## Editing User Settings

To edit user settings:

1. At the top right corner of the Instant UI, click the **Users** link. The **Users** window appears.
2. In the **Users** section, select the username for which you want to edit the settings and click **Edit**. The user's details appear on the right side.
3. Edit as required and click **OK**.

## Deleting a User

To delete a user:

1. At the top right corner of the Dell W-Series Instant UI, click the **Users** link. The **Users** window appears.
2. In the **Users** section, select the username that you want to delete and click **Delete**.  
To delete all users or multiple users at a time, select the usernames that you want to delete, and click **Delete All**.



---

**NOTE:** Deleting a user only removes the user record from the user database, and won't disconnect the online user associated with this username.

---

# Chapter 30

## Regulatory Domain

The IEEE 802.11/b/g/n Wi-Fi networks operate in the 2.4 GHz spectrum and IEEE 802.11a/n operate in the 5.0 GHz spectrum. These spectrums are divided into channels. The 2.4 GHz spectrum is divided into 14 overlapping, staggered 20 MHz wireless carrier channels. These channels are spaced 5 MHz apart. The 5 GHz spectrum is divided into more channels. The channels that can be used in a particular country differ based on the regulations of that country.

The initial Wi-Fi setup requires you to specify the country code for the country in which the Dell W-Instant operates. This configuration sets the regulatory domain for the radio frequencies that the W-IAPs use. Within the regulated transmission spectrum, a high-throughput 802.11a, 802.11b/g, or 802.11n radio setting can be configured. The available 20 MHz and 40 MHz channels are dependent on the specified country code.

You cannot change the country code for the W-IAPs designated for US and Japan. Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions on operators of wireless networks with devices set to improper country codes. "[Country Codes List](#)" on page 271 shows the list of country codes.

**Figure 213 - Specifying a Country Code**



### Country Codes List

**Table 47- Country Codes List**

Code	Country Name
US	United States
CA	Canada

Code	Country Name
JP3	Japan
DE	Germany
NL	Netherlands
IT	Italy
PT	Portugal
LU	Luxembourg
NO	Norway
FI	Finland
DK	Denmark
CH	Switzerland
CZ	Czech Republic
ES	Spain
GB	United Kingdom
KR	Republic of Korea (South Korea)
CN	China
FR	France
HK	Hong Kong
SG	Singapore
TW	Taiwan
BR	Brazil
SA	Saudi Arabia
LB	Lebanon
AE	United Arab Emirates
ZA	South Africa
AR	Argentina
AU	Australia
AT	Austria



<b>Code</b>	<b>Country Name</b>
BO	Bolivia
CL	Chile
GR	Greece
IS	Iceland
IN	India
IE	Ireland
KW	Kuwait
LI	Liechtenstein
LT	Lithuania
MX	Mexico
MA	Morocco
NZ	New Zealand
PL	Poland
PR	Puerto Rico
SK	Slovak Republic
SI	Slovenia
TH	Thailand
UY	Uruguay
PA	Panama
RU	Russia
KW	Kuwait
LI	Liechtenstein
LT	Lithuania
MX	Mexico
MA	Morocco
NZ	New Zealand
PL	Poland

<b>Code</b>	<b>Country Name</b>
PR	Puerto Rico
SK	Slovak Republic
SI	Slovenia
TH	Thailand
UY	Uruguay
PA	Panama
RU	Russia
EG	Egypt
TT	Trinidad and Tobago
TR	Turkey
CR	Costa Rica
EC	Ecuador
HN	Honduras
KE	Kenya
UA	Ukraine
VN	Vietnam
BG	Bulgaria
CY	Cyprus
EE	Estonia
MU	Mauritius
RO	Romania
CS	Serbia and Montenegro
ID	Indonesia
PE	Peru
VE	Venezuela
JM	Jamaica
BH	Bahrain

<b>Code</b>	<b>Country Name</b>
OM	Oman
JO	Jordan
BM	Bermuda
CO	Colombia
DO	Dominican Republic
GT	Guatemala
PH	Philippines
LK	Sri Lanka
SV	El Salvador
TN	Tunisia
PK	Islamic Republic of Pakistan
QA	Qatar
DZ	Algeria



# Appendix A

## Controller Configuration for VPN

On the controller, the following configuration is needed to setup a W-IAP.

### Whitelist DB Configuration

If you decide to use the Controller as the whitelist entry to configure the whitelist database, use the following CLI command:

```
(Dell3400) #local-userdb-ap add mac-address 00:11:22:33 44:55 ap-group test  
(Dell3400) #
```

The ap-group parameter is not used for any configuration, but needs to be configured. The parameter can be any valid string. If an external whitelist is being used, the AP MAC address needs to be saved in the RADIUS server as a lower-case entry without any delimiter.

The screenshot shows the configuration page for RADIUS Whitelist. The table contains the following data:

AP MAC Address	User Name	AP Group	AP Name	Description	Revoked	IP-Address
<input type="checkbox"/> 48-c7-cb-cb-08-00	naven	naven	naven			10.10.207.200
<input type="checkbox"/> 48-c7-cb-cb-08-06	naven	naven2	naven2			10.10.207.201
<input type="checkbox"/> 48-c7-cb-cb-08-08	santa	santa	santa			10.10.207.202
<input type="checkbox"/> 48-c7-cb-cb-08-0e	santa	santa2	santa2			10.10.207.203
<input type="checkbox"/> 00-24-6c-c9-27-c5	anupam	anupam	anupam			10.10.207.205
<input type="checkbox"/> 00-24-6c-c9-27-f7	anupam	anupam2	anupam2			10.10.207.206
<input type="checkbox"/> 00-24-6c-c9-18-04	naven-test	test1	naven-test			10.10.207.207
<input type="checkbox"/> 48-c7-cb-cb-08-08	sandep	sandep	sandep			10.10.207.204
<input type="checkbox"/> 00-24-6c-c9-18-1a	naven-test	test2	naven-test			10.10.207.208
<input type="checkbox"/> 00-1a-1a-00-23-04	defaul	00:1a:1a:00:23:04	defaul			0.0.0.0
<input type="checkbox"/> 00-24-6c-c9-01-f2	defaul	00:24:6c:c9:01:f2	defaul			0.0.0.0
<input type="checkbox"/> 48-c7-cb-cb-03-16	naven-test	test3	naven-test			0.0.0.0

At the bottom, there is an 'Add' button and a 'Cancel' button. The 'Add' button is currently disabled.

### VPN Local Pool Configuration

This pool is used to assign an IP Address to the W-IAP after successful VPN authentication.

```
(Dell3400) # ip local pool "rapngpool" <startip> <endip>  
(Dell3400) #
```

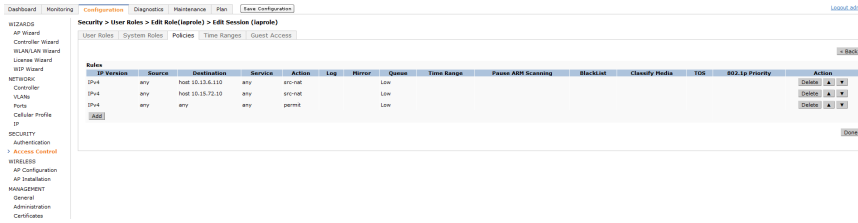
The screenshot shows the configuration page for VPN Services > IPSEC > Add Address Pool. The configuration fields are as follows:

Field	Value
Pool Name	rapngpool
Start Address	172.15.10.1
End Address	172.15.10.100

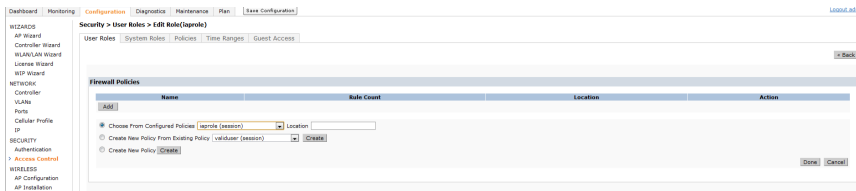
# W-IAP VPN Profile Configuration

This defines the server used to authenticate the W-IAP (internal or an external server) and the role for W-IAP user. This role is used to define the src-nat rule to RADIUS server to allow Dynamic RADIUS proxy.

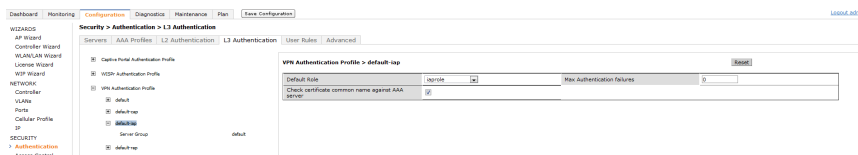
```
(Dell3400) (config) #ip access-list session iaprole
(Dell3400) (config-sess-iaprole)#any host <radius-server-ip> any src-nat
(Dell3400) (config-sess-iaprole)#any any any permit
(Dell3400) (config-sess-iaprole)#!
```



```
(Dell3400) (config) #user-role iaprole
(Dell3400) (config-role) #session-acl iaprole
(Dell3400) (config-role) #
```



```
(Dell3400) (config) #aaa authentication vpn default-iap
(Dell3400) (VPN Authentication Profile "default-iap") #server-group default
(Dell3400) (VPN Authentication Profile "default-iap") #default-role iaprole
(Dell3400) (VPN Authentication Profile "default-iap") #!
(Dell3400) (config) #
```



# Appendix B

## Dell PowerConnect W-ClearPass Configuration for AirGroup

The purpose of this chapter is to help you configure AirGroup with Dell PowerConnect W-ClearPass 6.0.1.

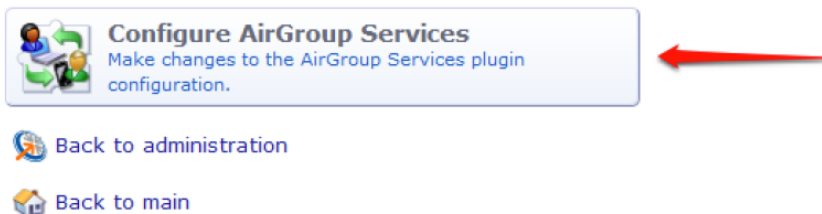
### Dell PowerConnect W-ClearPass Setup

1. On Dell PowerConnect W-ClearPass Guest, navigate to **Administration > AirGroup Services**.
2. Click **Configure AirGroup Services**.

Figure 214- Configure AirGroup Services

#### AirGroup Services

Use the commands below to configure AirGroup services on your network.



3. Click **Add a new controller**.

Figure 215- Add a New Controller for AirGroup Services

#### AirGroup Services 6.0.1-22806 Configuration

Set the configuration options for AirGroup Services 6.0.1-22806.

Configure AirGroup Services 6.0.1-22806													
* AirGroup Logging:	Standard (Recommended) – log basic information Select an option for logging events related to AirGroup Services.												
* Controllers:	<table border="1"><thead><tr><th>Use</th><th>Hostname</th><th>Port</th><th>Shared Secret</th></tr></thead><tbody><tr><td colspan="4">There are no items to display.</td></tr><tr><td colspan="4"><a href="#">Add a new controller</a></td></tr></tbody></table> <p>Define the Aruba controllers that should receive AirGroup asynchronous information updates.</p>	Use	Hostname	Port	Shared Secret	There are no items to display.				<a href="#">Add a new controller</a>			
Use	Hostname	Port	Shared Secret										
There are no items to display.													
<a href="#">Add a new controller</a>													
* Timeout:	5 seconds Timeout for sending an AirGroup message.												
* Attempts:	3 Maximum number of attempts to use when sending an AirGroup message.												
<a href="#">Save Configuration</a>													

\* required field

4. Update the fields with the appropriate information.



NOTE: Ensure that the port configured matches the CoA port ([RFC 3576](#)) set on the W-IAP configuration.

**Figure 216- Configure AirGroup Services Controller Settings**

AirGroup Services 6.0.1-22806 Configuration

Set the configuration options for AirGroup Services 6.0.1-22806.

Use	Hostname	Port	Shared Secret
<input checked="" type="checkbox"/>	10.1.1.10	21234	••••••••

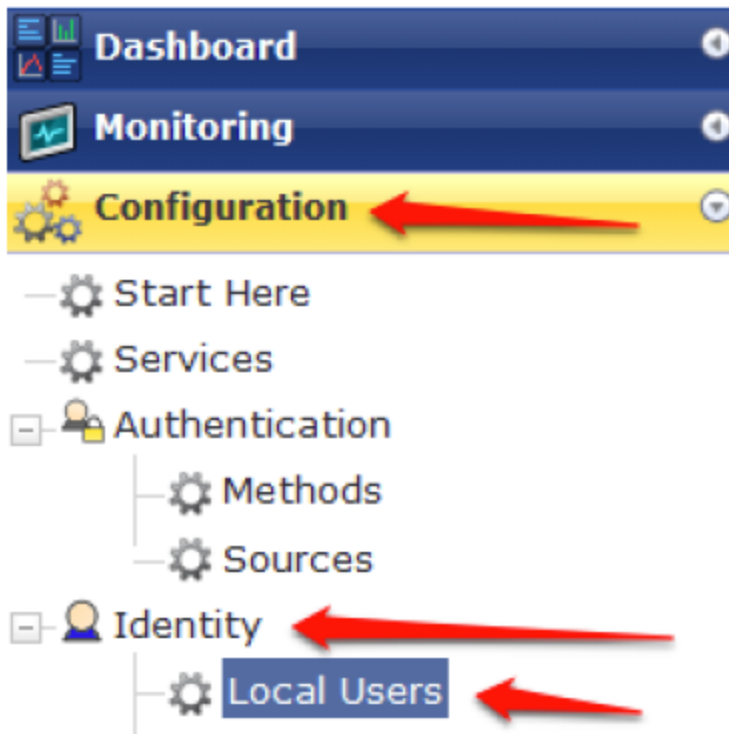
\* required field

5. Click Save Configuration.

In order to demonstrate AirGroup, either an AirGroup Administrator or an AirGroup Operator account must be created.

1. Navigate to the Dell PowerConnect W-ClearPass Policy Manager UI, and navigate to Configuration > Identity > Local Users.

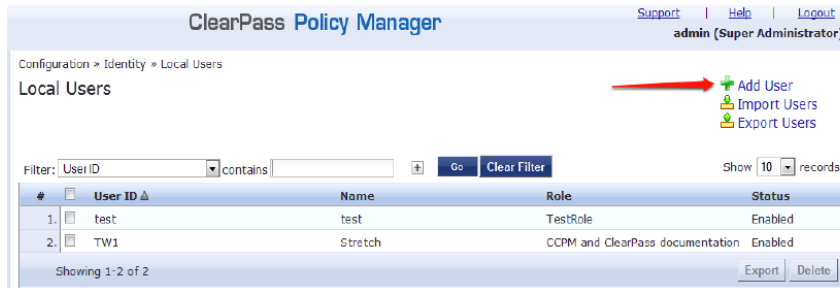
**Figure 217- Configuration > Identity > Local Users Selection**



2. Click Add User.

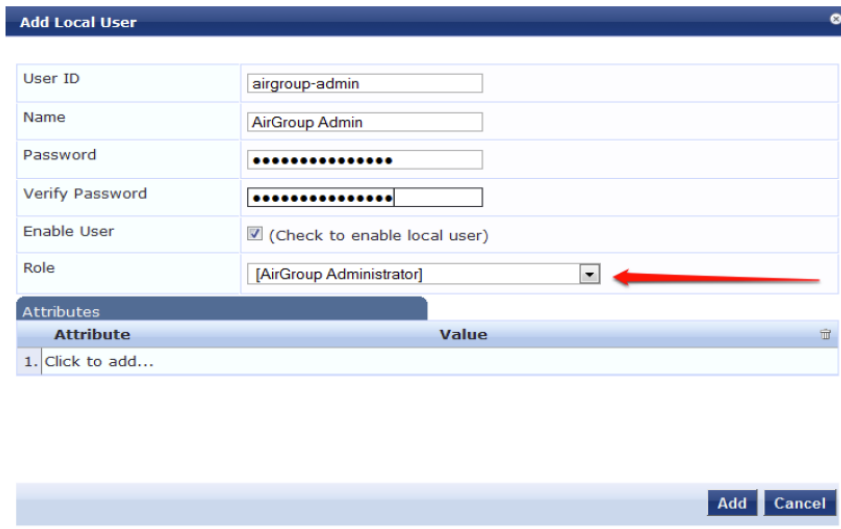


**Figure 218- Adding a New Local User in CPPM**



3. Create an AirGroup Administrator.

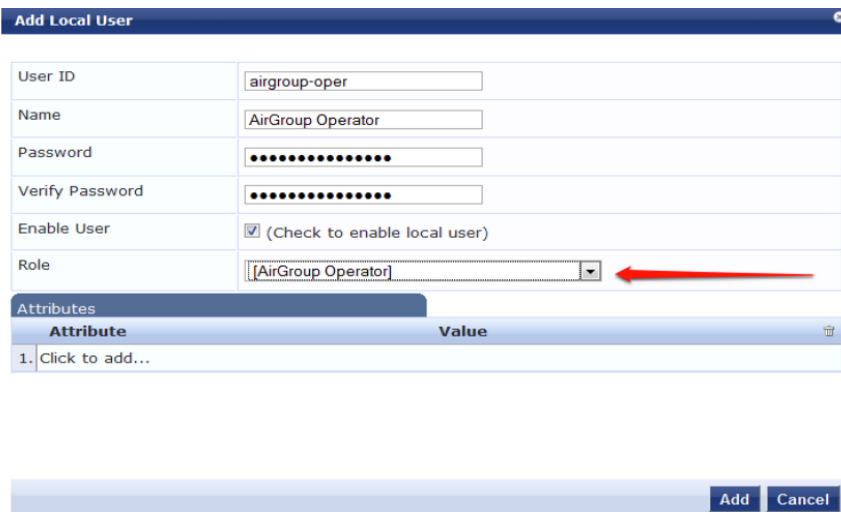
**Figure 219- Create an AirGroup Administrator**



4. In this example, the password used is test123. Click Add.

5. Now click Add User, and create an AirGroup Operator.

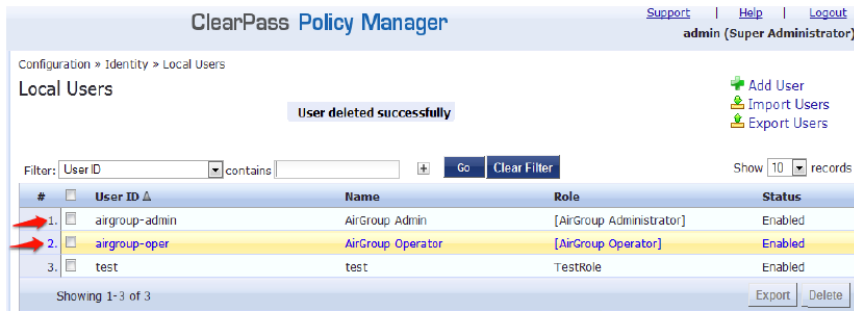
**Figure 220- Create an AirGroup Operator**



6. Click Add to save the user with an AirGroup Operator role.

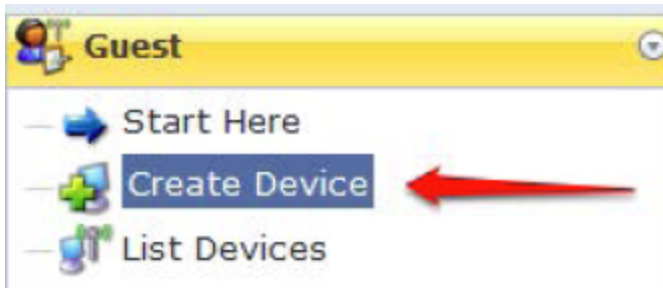
- The AirGroup Administrator and AirGroup Operator IDs will be displayed in the Local Users UI screen.

**Figure 221- Local Users UI Screen**



- Navigate to the Dell PowerConnect W-ClearPass Guest UI and click **Logout**. The ClearPass Guest Login page appears. Use the AirGroup admin credentials to log in.
- After logging in, click **Create Device**.

**Figure 222- Create a Device**



The following page is displayed.

**Figure 223- Register Shared Device**

**Register Shared Device**

\* Device Name:   
Enter a name to identify the device.

\* MAC Address:   
Enter the MAC address of the device.

Shared Locations:   
Enter a list of location IDs where this device will be shared.  
Use a comma-separated list of tag=value pairs; tag may be AP-Name, AP-Group, or FQLN.  
A fully qualified location name is '<ap-name>.floor<N>.<building-name>.<campus>',  
Leave blank to share with all locations.

Shared With:   
Enter up to 10 usernames that will be able to use this device.  
Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.

Shared Roles:   
List the user roles that will be able to use this device.  
Use a comma-separated list, e.g. role1,role2,role3, or blank for all roles.

- For this test, add your AppleTV device name and MAC address but leave all other fields empty.
- Click **Register Shared Device**.

## Testing

1. Disconnect your AppleTV and OSX Mountain Lion/iOS 6 devices if they were previously connected to the wireless network. Remove their entries from the controller's user table using these commands:
  - Find the MAC address— `show user table`
  - Delete the address from the table— `aaa user delete mac 00:aa:22:bb:33:cc`
2. Reconnect both devices. To limit access to the AppleTV, access the Dell PowerConnect W-ClearPass Guest UI using either the AirGroup admin or the AirGroup operator credentials. Next, navigate to **List Devices > Test Apple TV > Edit**. Add a username that is not used to log in to the Apple devices in the **Shared With** field.
3. Disconnect and remove the OSX Mountain Lion/iOS 6 device from the controller's user table. Reconnect the device by not using the username that you added to the **Shared With** field. The AppleTV should not be available to this device.
4. Disconnect the OSX Mountain Lion/iOS 6 device and delete it from the controller's user table. Reconnect using the username that was added to the **Shared With** field. The OSX Mountain Lion/iOS 6 device should once again have access to the AppleTV.

## Troubleshooting

**Table 48- Troubleshooting**

Problem	Solution
Limiting devices has no effect.	Ensure IPv6 is disabled.
Apple Macintosh running Mountain Lion can use AirPlay but iOS devices cannot.	Ensure IPv6 is disabled.



# Appendix C

## IAP-VPN

The IAP-VPN functionality on the controller release provides the ability to terminate VPN and GRE tunnels from the W-Instant AP and provides corporate connectivity to the branch W-Instant AP network.

VPN features are ideal for:

- enterprises with many branches that do not have a dedicated VPN connection to the HQ.
- branch offices that require multiple APs.
- individuals working from home, connecting to the VPN.

This new architecture and form factor seamlessly adds the survivability feature of W-Instant APs with the VPN connectivity of RAPs — providing corporate connectivity to branches.

All Dell controllers that are supported on the DellOS 6.2.0 release will work on IAP-VPN 6.1.3.1.

### Licensing Requirements

The following table lists the licensing requirements for IAP-VPN functionality:

**Table 49-** *Licensing Requirements for IAP-VPN*

License Name	Supported Functionality	Limitations
Base OS (Without license)	IPSec tunnel works with both internal and external DBs.	<ul style="list-style-type: none"><li>• IPSec tunnel does not work with internal DB for version 6.1.3.1. A minimum of one AP license is required to add a W-IAP MAC address in localDB.</li><li>• No support for DRP.</li><li>• Roles cannot be edited.</li></ul>
Only PEF-V license	You can edit the default-role inside aaa auth VPN default-iap. A new user role can be created with src-nat rule and applied to default-iap VPN profile.	—
Only NG-PEF license	You can edit the user-role logon.	default-role in default-iap VPN profile cannot be edited. However, the W-IAP is assigned with a default-vpn-role, which can be edited to include the src-NAT rule.

## VPN Configuration

The following VPN configuration steps on the controller, enable W-IAPs to terminate their VPN connection on the controller:

### Creating a W-IAP Whitelist

#### Controller Whitelist DB

W-IAP whitelist is the list of approved AP's that can be provisioned on your controller. To create a W-IAP whitelist:

1. Navigate to **Configuration > AP Installation (under Wireless)** and then click the **RAP Whitelist** tab on the right side.
2. Click the **New** button and provide the following details:
  - a. **AP MAC Address** — Mandatory parameter. Enter the MAC address of the AP.
  - b. **Username** — Enter a username that will be used when the AP is provisioned.
  - c. **AP Group** — Select a group to add the AP.
  - d. **AP Name** — Enter a name for the AP. If an AP name is not entered, the MAC address will be used instead.
  - e. **Description** — Enter a text description for the AP.
  - f. **IP-Address** — Enter an IP address for the AP.
3. Click the **Add** button to add the instant AP to the whitelist.

The `ap-group` parameter is not used for any configuration, but needs to be configured. The parameter can be any valid string. If an external whitelist is being used, the MAC address of the AP needs to be saved in the Radius server as a lower case entry without any delimiter.

#### External Whitelist DB

The external whitelist functionality enables you to configure the RADIUS server to use an external whitelist for authentication of MAC addresses of RAPs.

If you are using Windows 2003 server, perform the following steps to configure external whitelist on it. There are equivalent steps available for Windows Server 2008 and other RADIUS servers.

1. Add the MAC addresses for all the RAPs in the Active Directory of the Radius server:
  - a. Open the **Active Directory and Computers** window, add a new user and specify the MAC address (without the colon delimiter) of the RAP for the user name and password.
  - b. Right-click the user that you have just created and click **Properties**.
  - c. In the **Dial-in** tab, select **Allow access in the Remote Access Permission** section and click **OK**.
  - d. Repeat Step a through Step b for all RAPs.
2. Define the remote access policy in the Internet Authentication Service:
  - a. In the **Internet Authentication Service** window, select **Remote Access Policies**.
  - b. Launch the wizard to configure a new remote access policy.
  - c. Define filters and select **grant remote access permission** in the **Permissions** window.
  - d. Right-click the policy that you have just created and select **Properties**.
  - e. In the **Settings** tab, select the policy condition, and **Edit Profile....**
  - f. In the **Advanced** tab, select **Vendor Specific**, and click **Add** to add new vendor specific attributes.

- g. Add new vendor specific attributes and click **OK**.
- h. In the **IP** tab, provide the IP for the RAP and click **OK**.

## VPN Local Pool Configuration

To configure the VPN Local Pool:

1. Navigate to the **Configuration > Advanced Services > VPN Services > IPsec** page.
2. Select (check) **Enable L2TP**.
3. Make sure that only **PAP** (Password Authentication Protocol) is selected for Authentication Protocols.
4. To configure the L2TP IP pool, click **Add** in the **Address Pools** section. Configure the L2TP pool from which the APs will be assigned addresses, then click **Done**.



---

**NOTE:** The size of the pool should correspond to the maximum number of APs that the controller is licensed to manage.

---

5. To configure an Internet Security Association and Key Management Protocol (ISAKMP) encrypted subnet and preshared key, click **Add** in the **IKE Shared Secrets** section and configure the preshared key. Click **Done** to return to the IPsec page.
6. Click **Apply**.

## VPN Profile Configuration

The VPN profile configuration defines the server used to authenticate the W-IAP (internal or an external server) and the role for W-IAP user. This role is used to define `src-nat` rule to Radius server to get Dynamic Radius proxy working.

1. Navigate to the **Configuration > Security > Authentication > L3 Authentication** page.
2. In the Profiles list, select the **VPN Authentication Profile > default-iap**.
3. For Default Role, enter the user role you created previously (for example, InstantAP).
4. Click **Apply**.
5. In the **Profile** list, under **VPN Authentication Profile**, select **Server Group**.
6. Select the server group from the drop-down menu.
7. Click **Apply**.

For more information on VPN profile configuration, see ["VPN Configuration" on page 261](#).

## Radius Proxy for VPN Connected IAPs

The Radius proxy for VPN connected W-IAPs functionality defines the server used to authenticate the W-IAP (internal or an external server) and the role for W-IAP user. This role is used to define `src-nat` rule to Radius server to get Dynamic Radius proxy working.

1. Navigate to the **Configuration > Security > Access Control > User Roles** page. Click **Add** to create the sysadmin role.
2. For Role Name, enter `sysadmin`.
3. Under Firewall Policies, click **Add**. In Choose from Configured Policies, select the predefined allowall policy. Click **Done**.
4. Click **Apply**.

For more information on VPN profile configuration, see ["VPN Configuration" on page 261](#).

## Viewing Branch Status

To view the details of the branch information connected to the controller, issue the `show iap table` command.

### Example

This example shows the details of the branches connected to the controller.

```
(Dell3400) (config) #show iap table
Branch Key                               Index  Status  Inner IP           MAC Address
-----
d8f6095a01f89b7aea4340c080c3e3c8bd062758461c32c92d  8      DOWN   0.0.0.0           d8:c7:c8:c0:01:6c
4619fa8b014ff058d99e9fe63286c19851e61466627d054968  16     DOWN   0.0.0.0           00:1a:1e:08:21:e1
0e26e65a01732247f98b5d463f1fb56c0200d0944fab521e57   3      DOWN   0.0.0.0           d8:c7:c8:c0:01:6c
cc0b838d014df7db3eb453ef4f513204df4d74bb4063e46587   7      DOWN   0.0.0.0           d8:c7:c8:c0:b8:d0
6bccde5901997e534d14b10580371792ef4c13ca868c929150  15     DOWN   0.0.0.0           d8:c7:c8:c0:01:6c
764f6038018f2c2765292911e55fedc0c98f86cf79331d8905  6      UP     10.15.207.206    00:24:6c:c9:27:cf
c2b46b530119844dcdbb55ddb94ff308d1f08ec7cb4eda113c   0      DOWN   0.0.0.0           d8:c7:c8:c0:b8:d6
9deb828c0106f4562b50c8141cfa28ad5c1a3f89b3e171efcc  14     DOWN   0.0.0.0           00:1a:1e:08:23:f4
be5ffcfc801eedd92a76b978ceee53f4e2284c8e8f3dbd84457  5      DOWN   0.0.0.0           00:24:6c:c9:27:cf
b5d279460166c39a5fb9462a65559eb91266b9ac9f8e2356a0  13     DOWN   0.0.0.0           d8:c7:c8:c0:01:6c
0f7057990174cde7901a0c8779baeb7393b26d974a45eb8602  10     DOWN   0.0.0.0           00:24:6c:c0:41:f2
a1e23c1201cfb76a50fb3328e58c9825e716a259dd71874c67  4      UP     10.15.207.207    00:24:6c:c9:18:64
47f930fc019317069d04fd1c2ffdf6a49a6e51c148c2164ed0  9      DOWN   0.0.0.0           d8:c7:c8:c0:01:6c
0c478ce101df81e3c0a46fe4f3ab6eca9bb012151dea99a82f   1      DOWN   0.0.0.0           d8:c7:c8:c0:01:6c
747c20ac0155736c3b11bd972c967ebdf7c9883e69ec2a01fb   2      DOWN   0.0.0.0           d8:c7:c8:c0:b8:d0
0e40138601b34eb33fb57d94208848b0f8e37bba0a6a0d43ca  12     DOWN   0.0.0.0           00:24:6c:c9:18:64
de293919019196d7c8ac8f04a50fbd5b96c2af3d3576aa1dc2  11     DOWN   0.0.0.0           d8:c7:c8:c0:b8:d8
208c416e01e1cfaf0fdc11190349ad43334879f39ba9e19188  17     DOWN   0.0.0.0           d8:c7:c8:c0:01:6c

(Aruba3400) (config) #
```

The output of this command includes the following parameters:

**Table 50- show iap table Parameters**

Parameter	Description
Branch Key	Key for the branch, which is unique to each branch.
Index	Index assigned to the branch.
Status	Current status of the branch (UP/DOWN).
Inner IP	VPN inner IP of the branch.
MAC Address	MAC address of the VC of the branch.



# Appendix D

## Troubleshooting

The Support module Dell W-Instant provides CLI commands to view logs for APs.

### Viewing Logs

To view the log information for APs:

1. At the top right corner of Dell W-Series Instant UI, click **Support**. The **Support** window appears.
2. Select the required option from the **Command** drop-down list. For example, **AP ARM Configuration**.
3. Select **All Access Points** or a specific W-IAP from the **Target** drop-down list for which you want to view the **AP ARM Configuration**.
4. Click **Run**.

### Support Commands

You can view the following information for each access point in the Dell W-Instant network using the support window:

- **AP 3G/4G Status**—Displays the cellular status of the W-IAPs.
- **AP 802.1X Statistics**— Displays the 802.1X statistics of the selected W-IAP.
- **AP Access Rule Table**— Displays all the ACL rules of the selected W-IAP.
- **AP Active**— Displays all the APs of Instant.
- **AP Airgroup Cache**— Displays the Bonjour mDNS records for the selected W-IAP(s).
- **AP Airgroup CPPM Entries** —Displays the AirGroup CPPM policies of the registered devices.
- **AP Airgroup CPPM Servers**— Displays the AirGroup CPPM server information.
- **AP Airgroup Debug Statistics**— Displays the debug statistics for the selected W-IAP(s).
- **AP Airgroup Servers**— Displays information about the Bonjour devices which supports Airprint and Airplay services for the selected W-IAP(s).
- **AP Airgroup User**— Displays the IP/MAC address, device name, VLAN, type of connection of the Bonjour devices for the selected W-IAP(s).
- **AP Allowed Channels**— Displays information of the allowed channels for the selected W-IAP.
- **AP All Supported Timezones**— Displays all the supported time zones of Instant.
- **AP ARM Bandwidth Management**— Displays bandwidth management information for the selected W-IAP.
- **AP ARM Channels**— Displays channels of ARM in the selected W-IAP.
- **AP ARM Configuration**— Displays configuration of ARM in the selected W-IAP.

- **AP ARM History**— Displays the channel history and power changes due to Adaptive Radio Management (ARM) for the selected W-IAP.
- **AP ARM Neighbors**— Displays the ARM settings for the selected W-IAP's neighbors.
- **AP ARM RF Summary**— Displays the state and statistics for all channels being monitored by the selected W-IAP.
- **AP ARM Scan Times**— Displays AM channel scan times for the selected W-IAP.
- **AP ARP Table**— Displays the ARP table of the selected W-IAP.
- **AP Association Table**— Displays information of the selected W-IAP association.
- **AP Authentication Frames**— Displays the authentication trace buffer information of the selected W-IAP.
- **AP BSSID Table**— Displays the Basic Service Set (BSS) table of the selected W-IAP.
- **AP Country Codes**— Displays country code for the selected W-IAP.
- **AP CPU Utilization**— Displays utilization of CPU for the selected W-IAP.
- **AP Crash Info**— Displays crash log information (if it exists) for the selected W-IAP. The stored information is cleared from the flash after the AP reboots.
- **AP Current Time**— Displays current time of the selected W-IAP.
- **AP Current Timezone**— Displays current time zone of the selected W-IAP.
- **AP Datapath ACL Table Allocation**
- **AP Datapath ACL Tables**
- **AP Datapath Bridge Table**— Displays bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for the selected W-IAP.
- **AP Datapath DMO Session**
- **AP Datapath Multicast Table**— Displays datapath multicast table statistics for the selected W-IAP.
- **AP Datapath Route Table**— Displays datapath route table statistics for the selected W-IAP.
- **AP Datapath Session Table**— Displays the datapath session table statistics for the selected W-IAP.
- **AP Datapath Statistics**— Displays the hardware packet statistics for the selected W-IAP.
- **AP Datapath User Table**— Displays datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length for the selected W-IAP.
- **AP Datapath VLAN Table**— Displays the VLAN table information such as VLAN memberships inside the datapath including L2 tunnels for the selected W-IAP.
- **AP Daylight Saving Time**
- **AP Driver Configuration**— Displays driver configuration details of the selected W-IAP.
- **AP Election Statistics**
- **AP ESSID Table**— Displays networks of the selected W-IAP.
- **AP Flash Configuration**— Displays statistics of the selected W-IAP in flash.
- **AP IGMP Group Table**
- **AP Interface Counters**— Displays the package counters of bond0 of the selected W-IAP.
- **AP Interface Status**— Displays the status of br0 of the selected W-IAP.
- **AP Internal DHCP Status**
- **AP IP Interface**

- **AP IP Route Table**— Displays the route table of the selected W-IAP.
- **AP L3 Mobility Datapath**
- **AP L3 Mobility Events Log**
- **AP L3 Mobility Status**
- **AP Log All**— Displays all logs of the selected W-IAP.
- **AP Log AP-Debug**— Displays logs about the selected W-IAP.
- **AP Log Conversion**
- **AP Log Driver**
- **AP Log Network**— Displays network logs of the selected W-IAP.
- **AP Log PPPd**
- **AP Log Rapper**
- **AP Log Sapd**
- **AP Log Security**— Displays security logs of the selected W-IAP.
- **AP Log System**— Displays system logs of the selected W-IAP.
- **AP Log Tunnel Status Management**
- **AP Log Upgrade**
- **AP Log User-Debug**— Displays user-debug logs of the selected W-IAP.
- **AP Log User**— Displays user logs of the selected W-IAP.
- **AP Log VPN Tunnel Log**
- **AP Log Wireless**— Displays wireless logs of the selected W-IAP.
- **AP Management Frames**— Displays the traced 802.11 management frames for the selected W-IAP.
- **AP Memory Allocation State Dumps** — Displays the Malloc State dump details.
- **AP Memory Utilization**— Displays memory utilization of the selected W-IAP.
- **AP Mesh Counters**— Displays the mesh counters of the selected W-IAP.
- **AP Mesh Link**— Displays the mesh link of the selected W-IAP.
- **AP Mesh Neighbors**— Displays the mesh link neighbors of the selected W-IAP.
- **AP Monitor Active Laser Beams**
- **AP Monitor AP Table**— Displays the list of monitored APs of the selected W-IAP.
- **AP Monitor ARP Cache**
- **AP Monitor Client Table**— Displays the list of monitored clients of the selected W-IAP.
- **AP Monitor Containment Information**
- **AP Monitor Potential AP Table**— Displays the list of potential AP of the selected W-IAP.
- **AP Monitor Potential Client Table**— Displays the list of potential AP of the selected W-IAP.
- **AP Monitor Router**
- **AP Monitor Scan Information**
- **AP Monitor Status**— Displays the configuration and status of monitor information of the selected W-IAP.
- **AP Persistent Clients**— Displays the persistent clients of the selected W-IAP.
- **AP PPPoE uplink debug**
- **AP PPPoE uplink status**

- **AP Processes**— Displays the processes of the selected W-IAP.
- **AP Radio 0 Stats**— Displays aggregate debug statistics of the selected W-IAP Radio 0.
- **AP Radio 1 Stats**— Displays aggregate debug statistics of the selected W-IAP Radio 1.
- **AP RADIUS Statistics**— Displays the RADIUS statistics of the selected W-IAP.
- **AP Shaping Table**— Displays the VAP statistics of the selected W-IAP.
- **AP Sockets**— Displays the using sockets of the selected W-IAP.
- **AP STM Configuration**— Displays the SSID configuration in STM of the selected W-IAP.
- **AP System Status**— Displays detailed system status information for the selected W-IAP.
- **AP System Summary**— Displays the W-IAP configuration.
- **AP Tech Support Dump**— Displays the technical support dump logs of the selected W-IAP.
- **AP Uplink Status**
- **AP User Table**
- **AP Valid Channels**— Displays valid channels of the selected W-IAP.
- **AP Version**— Displays the version number of the selected W-IAP.
- **AP VPN Status**
- **AP Wired Port Settings**
- **AP Wired User Table**
- **VC 802.1x Certificate**— Displays the CA certificate and server certificate of the selected W-IAP.
- **VC About**— Displays some info of the selected W-IAP, including AP type, build time of image, image version.
- **VC Active Configuration**— Displays the active configuration of Virtual Controller.
- **VC Airgroup Service**— Displays the Bonjour services supported for the selected W-IAP(s).
- **VC Airgroup Status**— Displays the enable/disable status of the AirGroup and the parameters of the CPPM servers for the selected W-IAP(s).
- **VC Airgroup vlan**— Displays the AirGroup status information for a VLAN of the selected W-IAP(s).
- **VC Allowed AP Table**— Displays allowed AP enable/disable status and allowed AP list of the selected W-IAP.
- **VC AMP Current State Data**
- **VC AMP Current Stats Data**
- **VC AMP Data Sent**
- **VC AMP Events Pending**
- **VC AMP Last Configuration Received**
- **VC AMP Single Sign-on Key**
- **VC Application Services**— Displays the details of application services of the selected W-IAP, which includes protocol number, port number.
- **VC Auth-Survivability cache**— Displays the list of 802.1X cached user's information for the selected W-IAP(s).
- **VC DHCP Option 43 Received**
- **VC Global Alerts**— Displays all the alerts about client of the selected W-IAP.
- **VC Global Statistics**— Displays the flow information and signal strength of the selected W-IAP.

- **VC IDS AP List**— Displays the list of W-IAPs monitored by the selected W-IAP.
- **VC IDS Client List**— Displays the IDS detected client list of the selected W-IAP.
- **VC Internal DHCP Server Configuration**— Displays the configuration of internal DHCP server of the selected W-IAP.
- **VC Local User Database**— Displays the user configuration of the selected W-IAP.
- **VC OpenDNS Configuration and Status**— Displays configuration and status about OpenDNS server.
- **VC Radius Attributes**— Displays the RADIUS attributes of the selected W-IAP.
- **VC Radius Servers**— Displays the RADIUS servers' configuration of the selected W-IAP.
- **VC Saved Configuration**— Displays the saved configuration of Virtual Controller.
- **VC Scanning Statistics**
- **VC SNMP Configuration**— Displays the SNMP configuration of the selected W-IAP.
- **VC Uplink 3G/4G Configuration**
- **VC Uplink Management Configuration**
- **VC WISPr Configuration** — Displays the WISPr configuration details.



**NOTE:** Use the support commands under the supervision of Dell technical support.

**Figure 224-** *Support Commands*

The screenshot shows a web-based interface for running support commands. The command 'show ap debug dot1x-statistics' has been executed on the target 'IAP'. The output displays statistics for 802.1X authentication.

```

*** 9/21/2011 10:10:11 PM Target: IAP Command: show ap debug dot1x-statistics ***

802.1X Statistics
-----
Mac      Name  AP  Auth-Succes  Auth-Fails  Auth-Tmout  Re-Auths  Supp-Name  USKeyRot  MKeyRot
-----
Total:   0      0      0            0            0            0            0            0
802.1X Counters
  
```



# Appendix E

## Abbreviations

### Abbreviations

The following table lists the abbreviations used in this user guide.

**Table 51** - *List of abbreviations*

Abbreviation	Expansion
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
BSS	Basic Server Set
BSSID	Basic Server Set Identifier
CA	Certification Authority
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
W-IAP	Instant Access Point
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
Instant UI	Instant User Interface
LEAP	Lightweight Extensible Authentication Protocol
MX	Mail Exchanger
MAC	Media Access Control
NAS	Network Access Server

<b>Abbreviation</b>	<b>Expansion</b>
NAT	Network Address Translation
NS	Name Server
NTP	Network Time Protocol
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial In User Service
VC	Virtual Controller
VSA	Vendor-Specific Attributes
WLAN	Wireless Local Area Network