Dell PowerConnect W-Series Instant Access Point 6.1.2.3-2.0.0.0

User Guide

Contents

Figures

Tables

Dell PowerConnect W-Instant Access Point Overview

Dell PowerConnect 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, as long there is an Ethernet port with a link is the network infrastructures required to deploy the Dell Instant wireless network. Dell PowerConnect W-Instant is specifically designed for easy deployment, and proactive management of networks for small customers or remote locations without an on-site IT administrator.

A Dell Instant network can support up to 16 IAPs and 256 users. Dell PowerConnect W-Instant consists of at least one Instant Access Point (IAP) and a Virtual Controller (VC). The Virtual Controller resides within one of the access points. In an Dell PowerConnect W-Instant deployment only the first IAP needs to be configured. After the first IAP is deployed, the subsequent IAPs will inherit all the required information from the Virtual Controller.

Supported Devices

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

- W-IAP105
- W-IAP92
- W-IAP93
- W-IAP134
- W-IAP135

Objective

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

Intended Audience

This guide is intended for Dell Instant customers who will be configuring and using Dell Instant to set up the Dell PowerConnect W-Instant wireless network infrastructure.

Conventions

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

Table 1 *Conventions*

Type Style	Description
Italics	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: • Screen output • On screen system prompt • Filenames, software devices, and specific commands
Bold	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.

Website Contact

Table 2 *Website Support*

Web Site Support	
Main Website	dell.com
Support Website	support.dell.com
Documentation Website	support.dell.com/manuals

Chapter 1

Initial Configuration

This chapter provides information that is required to setup Dell Instant and access the Instant User Interface.

Initial Setup

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

Pre-Installation Checklist

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

- Ethernet cable of required length to connect the IAP to the home router.
- One of the following power sources:
  - IEEE 802.3af-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 two ways:

Endspan: The switch that the IAP is connected to can provide power.
Midspan: A device can sit between the switch and the IAP.

The choice of endspan or midspan depends on the capabilities of the switch that the IAP is connected to. 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.

NOTE: 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 the IAP to a Power Source” on page 18
2. “Assigning an IP Address to the IAP” on page 18
3. “Connecting to a Provisioning Wi-Fi Network” on page 18

4. "Login into Instant User Interface" on page 19
5. "Specifying the Country Code" on page 20—Skip this step, if you are installing the IAP in United States, Japan or Israel.

Connecting the IAP to a Power Source

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

- PoE switch—Connect the ENET port of the IAP to the appropriate port on the PoE switch.
- PoE midspan—Connect the ENET port of 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 IAP

The IAP needs an IP address for network connectivity. When you connect the IAP to a network, the IAP receives an IP address from a DHCP server. To get an IP address for an IAP, perform the following steps:

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

NOTE: After the IAP starts up, it will try to do a DHCP if the static IP configuration is not available. If DHCP times out, a default IP within 169.254.x.y/16 subnet will be configured on the IAP. The DHCP client will be still running so that when the DHCP service recovers the IAP will get a valid IP address and then reboots.

Connecting to a Provisioning Wi-Fi Network

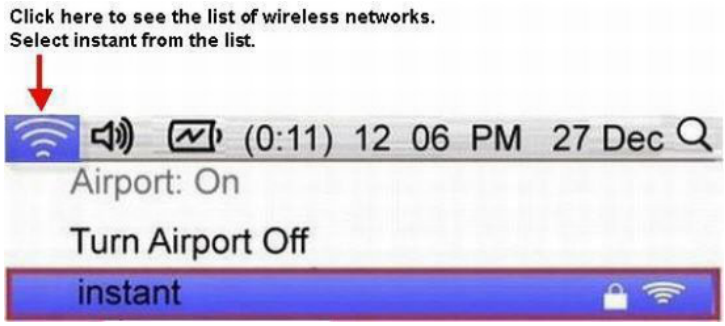
To connect to a provisioning Wi-Fi network:

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** box appears.
3. Click on the **instant** network and click **Connect.**
4. In the Mac operating system, click the AirPort icon. A list of available Wi-Fi networks is displayed.
5. Click on the **instant** network.

NOTE: While connecting to a 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*

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

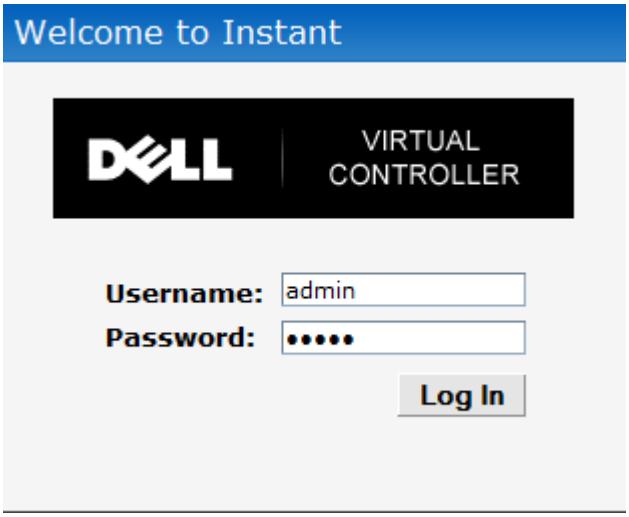


Login into Instant User Interface

Launch a web browser and navigate to instant.dell-pcw.com (or any URL or web address). In the login screen, enter the following credentials:

- Username—admin
- Password—admin

Figure 3 *Instant User Interface Login Screen*



When you use a provisioning Wi-Fi network to connect to the internet, all browser requests are directed to the Instant user interface. For example, if you enter www.example.com in the address field, you will be directed to the Instant user interface. You can change the default login credentials after your first login.

Specifying the Country Code

NOTE: Skip this section, if you are installing the IAP in United States, Japan or Israel.

Dell PowerConnect W-Instant Access Points are shipped in four variants:

- IAP—US (United States)
- IAP—JP (Japan)
- IAP—IL (Israel)
- IAP—ROW (Rest of World)

After you successfully login to the Instant user interface, a **Country Code** box appears, if IAP-ROW APs are installed. Select the country code for the IAP-ROW APs installed.

For the complete list of the countries that are supported in the IAP-ROW variant type, see "Regulatory Domain" on page 153.

Figure 4 *Specifying the Country Code*

The 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 Instant UI.

Supported browsers are:

- Internet Explorer 7 or higher
- Safari
- Google Chrome
- Mozilla Firefox

NOTE: The Instant UI logs out automatically if the window is inactive for fifteen minutes.

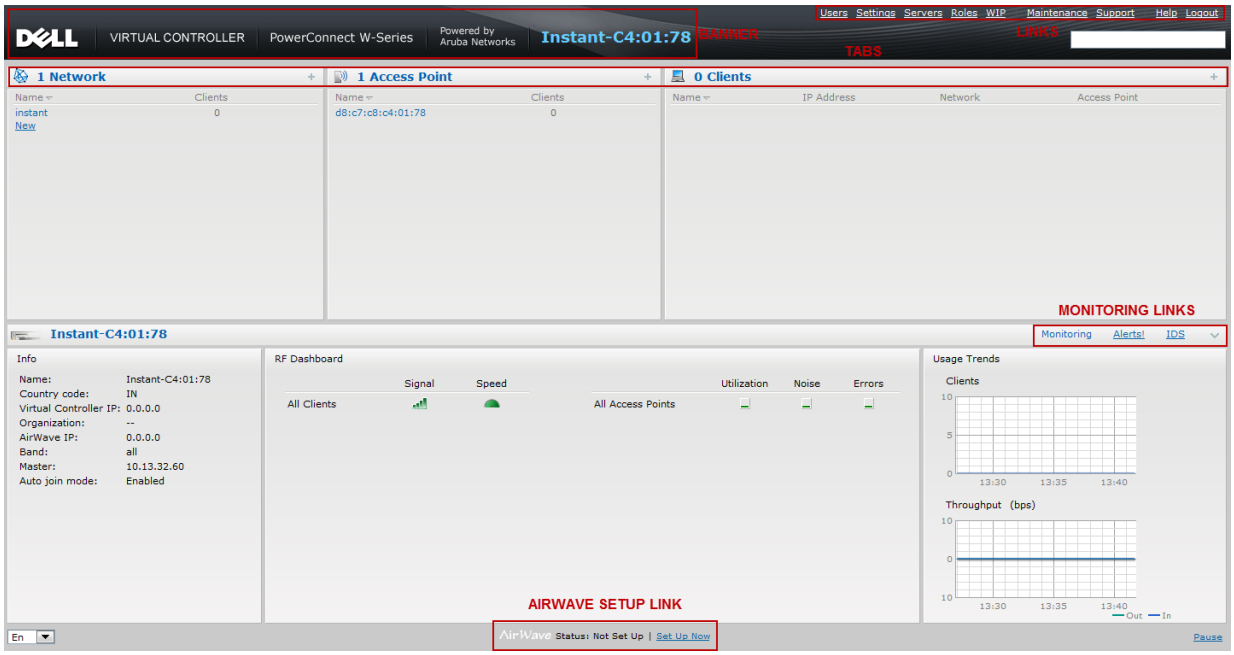
Understanding the Instant UI Layout

The Instant UI consists of the following elements:

- Banner
- Search
- Tabs
- Links
- Views

These elements are explained in the following sections.

Figure 5 *Instant UI Interface*



Banner

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

Search

Administrators can search an IAP, client, or a network using a simple **Search** dialog box in the Instant UI. This Search option helps fill in the blank when you type in a word and suggested matches will be 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 Instant UI consists of the following tabs:

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

Each tab appears in a compressed view by default. A number, specifying the number of networks, 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

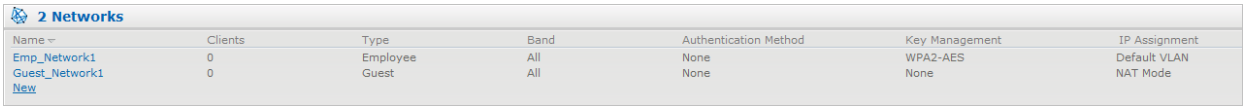
This tab displays a list of Wi-Fi networks that are configured in the Dell Instant network. The network names appear as links. The expanded view displays the following information about each Wi-Fi network:

- **Name**—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, 5.4 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 Chapter 3, “Wireless Network” on page 39.

An **edit** link appears on clicking the network name in the **Networks** tab. For information about editing a wireless network, see “Editing a Network” on page 53. To delete a network, click **x** on the right side of the **edit** link.

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



Access Points Tab

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

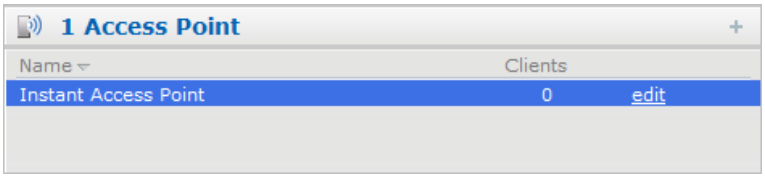
If the Auto Join Mode feature is disabled, a **New** link appears. Click on this link to add a new IAP to the network. If an IAP is configured and not active, its Mac Address is displayed in red.

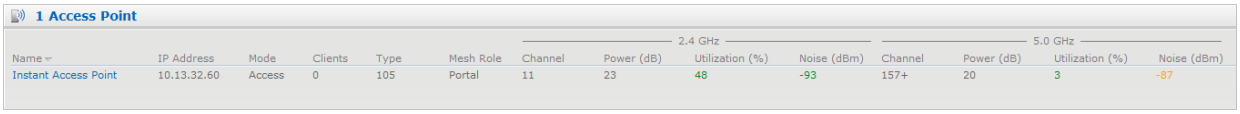
The expanded view displays the following information about each IAP:

- **Name**—Name of the access point.
- **IP Address**—IP address of the IAP.
- **Mode—**Mode of the IAP.
- **Clients**—Number of clients that are connected to the IAP.
- **Type**—Model number of the IAP.
- **Mesh Role—**Role of the mesh IAP
- **Channel**—Channel the IAP is currently broadcasting on.
- **Power (dB)**—Maximum transmit EIRP of the radio.
- **Utilization (%)**—Utilization percentage of the IAP radios.
- **Noise (dBM)**—Noise floor of the IAP.

An **edit** link appears on clicking the IAP name. For details about editing IAP settings see, "Editing IAP Settings" on page 64.

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



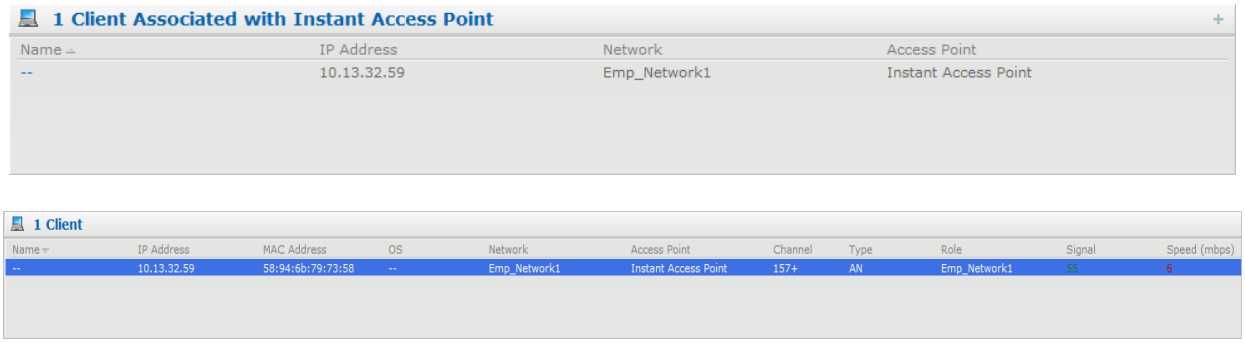


Clients Tab

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

- **Name**—Name of the client.
- **IP Address**—IP address of the client.
- **Mac Address**—Mac address of the client.
- **OS**—Operating system that the client is running on.
- **Network**—Network that the client is connected to.
- **Access Point**—IAP to which the client is connected.
- **Channel**—Channel that the client is currently broadcasting on.
- **Type**—Wi-Fi type of the client: A, G, AN, or GN.
- **Role—**Role assigned to the client.
- **Signal—**Indicates Signal strength.
- **Speed (mbps)**—Data transfer speed.

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



Links

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

- New version available
- Users
- Settings
- Servers
- Roles
- Support
- Help
- Logout
- Monitoring
- Alerts
- IDS
- Language
- AirWave Setup
- Pause/Resume

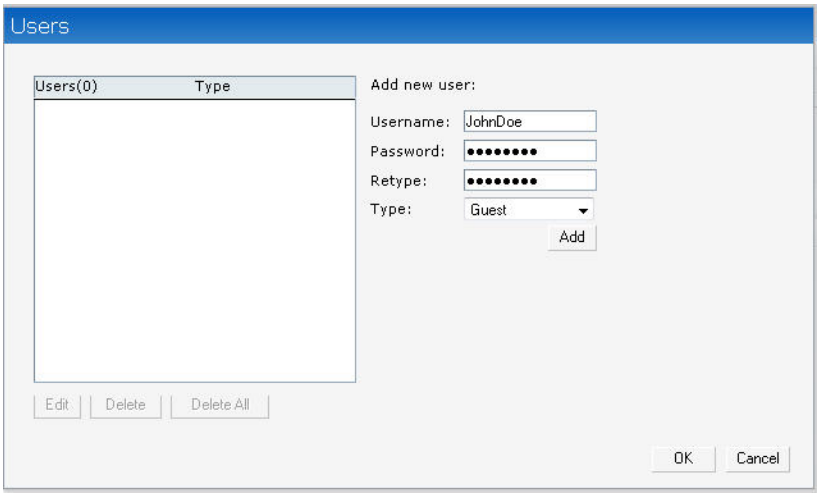
New version available

This link appears in the Instant UI only if a new image version is available on the image server and 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 69.

Users

This link displays the **Users** box. This box contains fields that are required to add, edit, or delete a user or users. You can also specify the user type. Two types of users, employee and guest, will be using the Dell Instant network. For more information about users, see Chapter 20, "User Database" .

Figure 9 *Users Box*

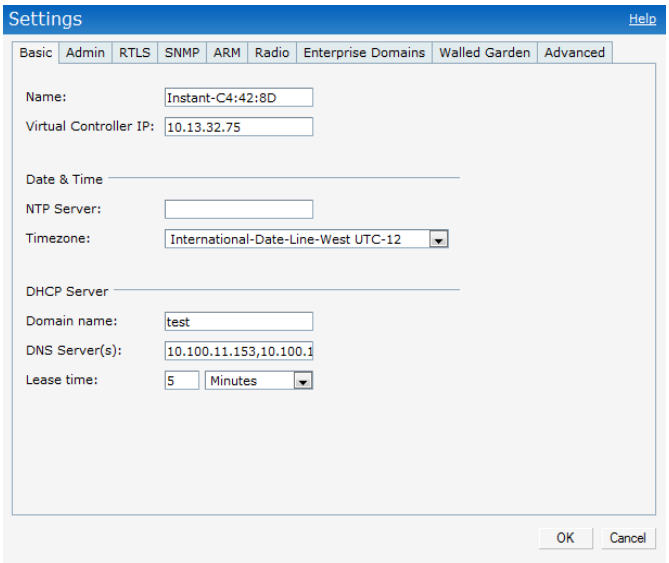


Settings

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

- **Basic**—View or edit the Virtual Controller's name, IP address, NTP Server and DHCP server settings. For information about Virtual Controller settings and NTP Server, see Chapter 7, "Virtual Controller" and Chapter 6, "NTP Server" .
- **Admin**—View or edit the admin credentials.
- **RTLS**—View or edit the RTLS server settings.
- **SNMP**—View or specify SNMP agent settings. For information see Chapter 16, "SNMP" .
- **ARM**—View or assign channel and power settings for all the IAPs in the network. For information about ARM (Adaptive Radio Management), see Chapter 14, "Adaptive Radio Management" .
- **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 119.
- **Enterprise Domains**—This indicates all the DNS domain names 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, the names that don't match this list is sent to OpenDNS.
- **Walled Garden**—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 93.
- **Advanced**—View or edit the preferred band for the network, dynamic RADIUS Proxy, and Auto join mode settings. For information about dynamic RADIUS Proxy and Auto join mode, see "External RADIUS Server" on page 78 and "Auto Join Mode" on page 59.

Figure 10 *Settings Link—Default View*



Servers

This link displays the **RADIUS Server** box. This box allows you to add new server. To add a new radius server, see "Configuring an External RADIUS Server" on page 79.

Roles

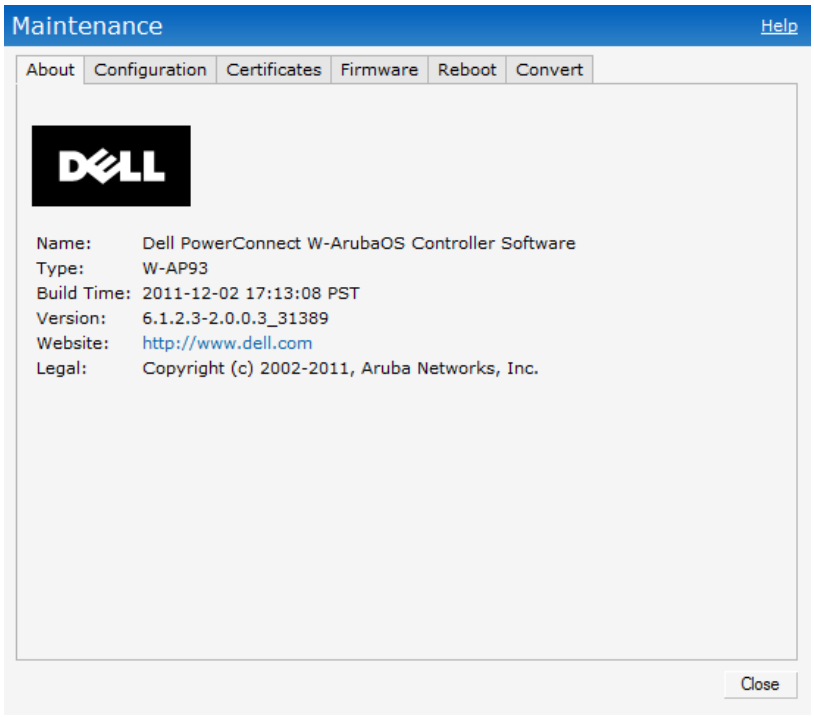
This link displays the **Roles** box. You can create new user roles and new rules for the users. For more information, see "User Roles" on page 99.

Maintenance

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

- **About**—Displays the Build Time, IAP model name, Dell Instant OS version, Web address of Dell Inc., and Copyright information.
- **Configuration**—Displays the current configuration of the network. The Clear Configuration function allows you to delete or clear the current configuration of the network and reset to provisioning configuration.
- **Certificates**—Displays information about current certificate installed in the network. Provides interface to upload new certificates and to set a passphrase for the certificates. For more information, see "Certificates" on page 94.
- **Firmware**—Displays the current firmware version and provides options to upgrade to a new firmware version. For more information, see"Manual Firmware Image Check and Upgrade" on page 71.
- **Reboot**—Displays the IAPs in the network and provides an option to reboot the required access point or all access points. For more information, see "Rebooting the IAP" on page 68.
- **Convert**—Provides an option to change the Virtual Controller managed network to an Dell Mobility Controller managed network. For more information, see "Migrating from a Virtual Controller Managed Network to Mobility Controller Managed Network" on page 66.

Figure 11 *Maintenance Link—Default View*

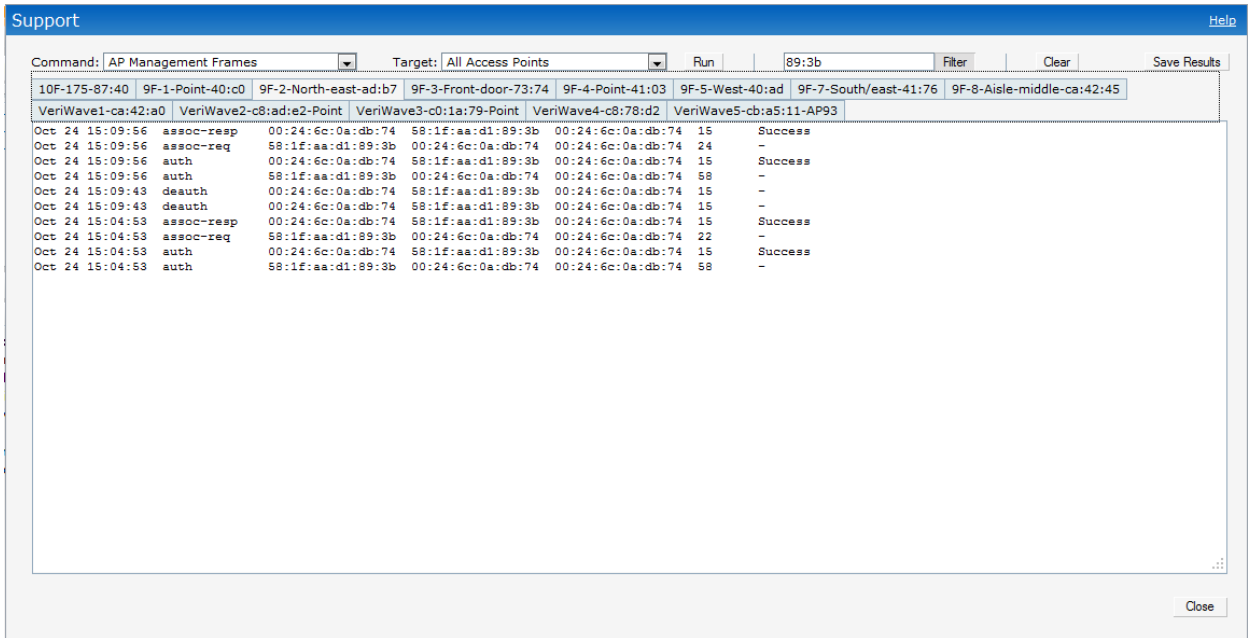


Support

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 IAPs in the network.
- **Run**—Click this to generate the support log for the selected option and IAP.
- **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.

Figure 12 *Support Window*



To view the log information, perform the following steps:

1. At the top right corner of 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 IAP from the **Target** drop-down list for which you want to view the **AP ARM Configuration**.
4. Click **Run**.

NOTE: Use the support commands under the supervision of Dell technical support.

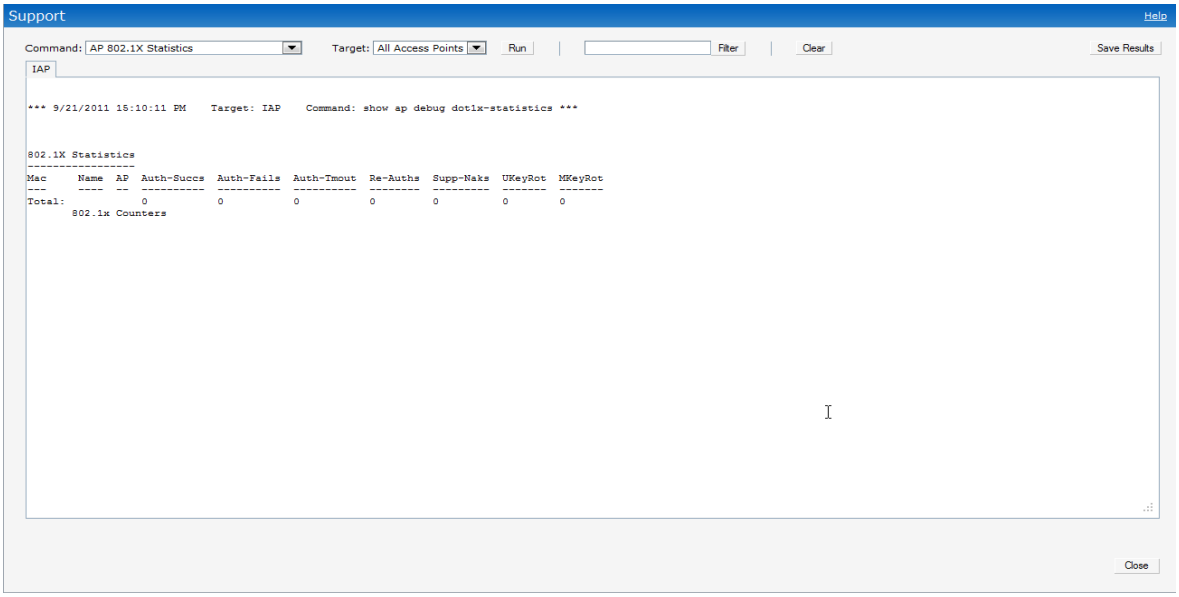
You can view the following information for each access point in the Dell Instant network using the support box:

- **AP Access Rule Table**—Displays all the ACL rules of the selected IAP.
- **AP Active**—Displays all the APs of Instant.
- **AP All Supported Timezones**—Displays all the supported time zones of Instant.
- **AP ARM Channels**—Displays channels of ARM in the selected IAP.
- **AP ARM Configuration**—Displays configuration of ARM in the selected IAP.
- **AP Country Codes**—Displays country code for the selected IAP.
- **AP CPU Utilization**—Displays utilization of CPU for the selected IAP.
- **AP Current Time**—Displays current time of the selected IAP.
- **AP Current Timezone**—Displays current time zone of the selected IAP.
- **AP Log All**—Displays all logs of the selected IAP.
- **AP Log Debug**—Displays logs about the selected IAP.
- **AP Log Network**—Displays network logs of the selected IAP.
- **AP Log Security**—Displays security logs of the selected IAP.
- **AP Log System**—Displays system logs of the selected IAP.
- **AP Log User-Debug**—Displays user-debug logs of the selected IAP.
- **AP Log User**—Displays user logs of the selected IAP.
- **AP Log Wireless**—Displays logs about wireless of the selected IAP.
- **AP Log Wireless**—Displays logs about wireless of the selected IAP.
- **AP Driver Configuration**—Displays driver configuration details of the selected IAP.
- **AP Essid Table**—Displays networks of the selected IAP.
- **AP Flash Configuration**—Displays statistics of the selected IAP in flash.
- **AP Memory Utilization**—Displays memory utilization of the selected IAP.
- **AP Mesh Counters**—Displays the mesh counters of the selected IAP.
- **AP Mesh Link**—Displays the mesh link of the selected IAP.
- **AP Mesh Neighbors**—Displays the mesh link neighbors of the selected IAP.
- **AP Monitor AP Table**—Displays the list of monitored APs of the selected IAP.
- **AP Monitor Client Table**—Displays the list of monitored clients of the selected IAP.
- **AP Monitor Potential AP Table**—Displays the list of potential AP of the selected IAP.
- **AP Monitor Potential Client Table**—Displays the list of potential AP of the selected IAP.
- **AP Monitor Status**—Displays the configuration and status of monitor information of the selected IAP.
- **AP Persistent Clients**—Displays the persistent clients of the selected IAP.

- **AP Process**—Displays the processes of the selected IAP.
- **AP Shaping Table**—Displays the VAP statistics of the selected IAP.
- **AP Sockets**—Displays the using sockets of the selected IAP.
- **AP STM Configuration**—Displays the SSID configuration in STM of the selected IAP.
- **AP Valid Channels**—Displays valid channels of the selected IAP.
- **AP Version**—Displays the version number of the selected IAP.
- **IDS Client List**—Displays clients list IDS checked of the selected IAP.
- **Interface Counters**—Displays the package counters of bond0 of the selected IAP.
- **Interface Port Status**—Displays the status of br0 of the selected IAP.
- **IP ARP Table**—Displays the ARP table of the selected IAP.
- **IP DHCP Database**—Displays the configuration of internal DHCP server of the selected IAP.
- **IP Route Table** —Displays the route table of the selected IAP.
- **VC 802.1x Certificate**—Displays the CA certificate and server certificate of the selected IAP.
- **VC About**—Displays some info of the selected IAP, including AP type, build time of image, image version.
- **VC Allowed AP Table** —Displays allowed AP enable/disable status and allowed AP list of the selected IAP.
- **VC Application Services**—Displays the details of application services of the selected IAP, which includes protocol number, port number.
- **VC Global Alerts**—Displays all the alerts about client of the selected IAP.
- **VC Global Statistics**—Displays the flow information and signal strength of the selected IAP.
- **VC Local User Database**—Displays the user configuration of the selected IAP.
- **VC Radius Attributes**—Displays the radius attributes of the selected IAP.
- **VC Radius Servers**—Displays the radius servers' configuration of the selected IAP.
- **VC Saved Configuration**—Displays the saved configuration information of the selected IAP.
- **VC SNMP Configuration**—Displays the SNMP configuration of the selected IAP.
- **AP Summary**—Displays the IAP configuration.
- **Debug Logs**—Displays debug logs of the selected IAP.
- **Driver Logs**—Displays the driver logs of the selected IAP.
- **Tech Support Dump**—Displays the technical support dump logs of the selected IAP.
- **Active Configuration**—Displays the active configuration of Virtual Controller.
- **Saved Configuration**—Displays the saved configuration of Virtual Controller.
- **AP Management Frames**—Displays the traced 802.11 management frames of the selected IAP.
- **AP Authentication Frames**—Displays the authentication trace buffer information of the selected IAP.
- **AP System Status**—Displays detailed system status information for the selected IAP.
- **AP Crash Info**—Displays crash log information (if it exists) for the selected IAP. The stored information is cleared from the flash after the AP reboots.
- **AP 802.1X Statistics**—Displays the 802.1X statistics of the selected IAP.
- **AP RADIUS Statistics**—Displays the RADIUS statistics of the selected IAP.
- **AP System Status**—Displays the system status of the selected IAP.
- **AP Client Table**—Displays information of the client connected to the selected IAP.
- **AP Association Table**—Displays information of the selected IAP association.
- **AP Allowed Channels**—Displays information of the allowed channels for the selected IAP.
- **AP Radio 0 Stats**—Displays aggregate debug statistics of the selected IAP Radio 0.

- **AP Radio 1 Stats**—Displays aggregate debug statistics of the selected IAP Radio 1.
- **Bridge Table**—Displays bridge table entry statistics including Mac address, VLAN, assigned VLAN, Destination and flag information for the selected IAP.
- **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 IAP.
- **Session Table**—Displays the datapath session table statistics for the selected IAP.
- **Route Table**—Displays datapath route table statistics for the selected IAP.
- **Datapath Statistics**—Displays the hardware packet statistics for the selected IAP.
- **VLAN Table**—Displays the VLAN table information such as VLAN memberships inside the datapath including L2 tunnels for the selected IAP.
- **BSSID Table**—Displays the Basic Service Set (BSS) table of the selected IAP.
- **IDS Status**—Displays WLAN Interface, Data Structures, WLAN Interface Switch Status and RTLS Configuration tables for the selected IAP.
- **IDS AP Table**—Displays the Monitored IAP Table, which lists all the IAPs monitored by the selected IAP.
- **ARM Bandwidth Management**—Displays bandwidth management information for the selected IAP.
- **ARM History**—Displays the channel history and power changes due to Adaptive Radio Management (ARM) for the selected IAP.
- **ARM Neighbors**—Displays the ARM settings for the selected IAP's neighbors.
- **ARM RF Summary**—Displays the state and statistics for all channels being monitored by the selected IAP.
- **ARM Scan Times**—Displays AM channel scan times for the selected IAP.

Figure 13 *Support commands*

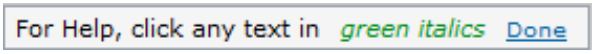


Help

The **Help** link at the top right corner of the Instant UI allows you to view a short description or definition of selected terms and fields in the Instant UI. To activate the context-sensitive help, perform the following steps:

1. At the top right corner of Instant UI, click the **Help** link. The following box appears below the **Help** link.

Figure 14 *Help Link*



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

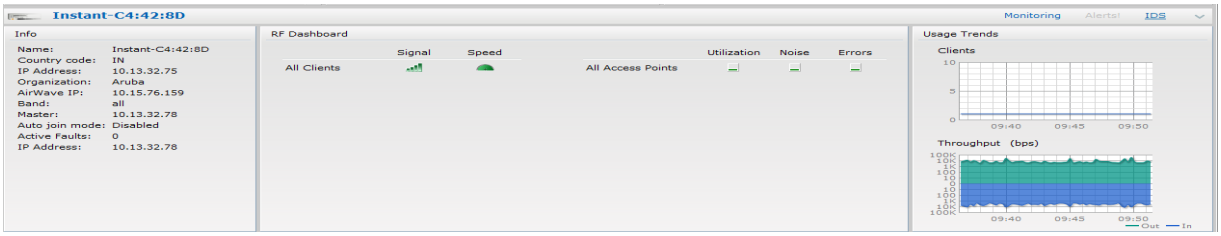
Use this link to logout of the Instant UI.

Monitoring

This link displays the Monitoring pane. This pane can be used to monitor the Dell 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
- RF Dashboard
- Usage Trends

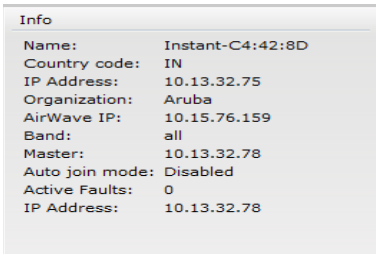
Figure 15 *Monitoring on Instant UI*



Info

Displays the configuration information of the Virtual Controller by default. In a Network View, this section displays configuration information of the selected network. Similarly, in an Instant Access Point View or Client View, this section displays the configuration information of the selected IAP or the client.

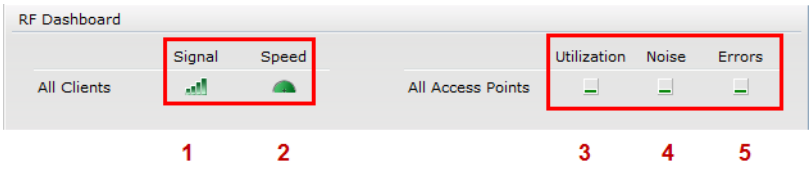
Figure 16 *Info Section in the Monitoring Pane*



RF Dashboard

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

Figure 17 *RF Dashboard in the Monitoring Pane*



The following table lists the icons in the RF Dashboard.

Table 3 *RF Dashboard icons*

Icon	Name
1	Signal bar
2	Speed icon
3	Utilization icon
4	Noise icon
5	Errors icon

- Clients—Lists the clients with low speed or signal strength in the network.
  - Signal—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 > Orange > Red.
    - Green—Signal strength is more than 20 decibels.
    - Orange—Signal strength is between 15-20 decibels.
    - Red—Signal strength is less than 15 decibels.

To view the signal graph for a client, click on the signal bar against the client in the **Signal** column.

  - Speed—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 > Orange > Red.
    - Green—Data transfer speed is more than 50 percent of the maximum speed supported by the client.
    - Orange—Data transfer speed is between 25 - 50 percent of the maximum speed supported by the client.
    - Red—Data transfer speed is less than 25 percent of the maximum speed supported by the client.

To view the data transfer speed graph of a client, click on the speed icon against the client in the Speed column.

- Access Points—Lists the IAPs whose utilization, noise, or errors are not within the specified threshold. The IAP names appear as links. When the IAP is clicked, the IAP configuration information is displayed in the Info section. The RF Dashboard section is pushed to the bottom left corner of the 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 Chapter 18, “Monitoring” .
  - Utilization—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 > Orange > Red.
    - Green—Utilization is less than 50 percent.
    - Orange—Utilization is between 50 - 75 percent.
    - Red—Utilization is more than 75 percent.

To view the utilization graph of an IAP, click on the Utilization icon against the IAP in the Utilization column.

  - Noise—Displays the noise floor of the IAPs. Noise is measured in decibels/meter. Depending on the noise floor, the color of the lines on the Noise icon changes from Green > Orange > Red.
    - Green—Noise floor is more than 87dBm.
    - Orange—Noise floor is between 80 dBm - 87 dBm.
    - Red—Noise floor is less than 80 dBm.

To view the noise floor graph of an IAP, click on the noise icon against the IAP in the Noise column.

- Errors—Displays the errors for the IAPs. Depending on the errors, color of the lines on the Errors icon changes from Green > Yellow > Red.
  - Green—Errors are less than 5000 frames per second.
  - Orange—Errors are between 5000 - 10000 frames per second.
  - Red—Errors are more than 10000 frames per second.

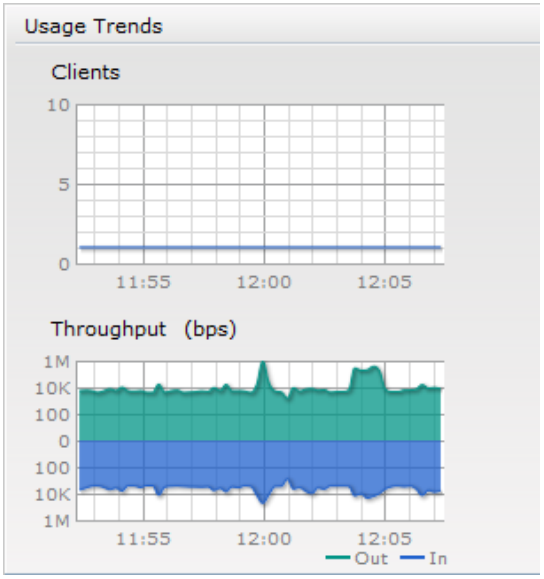
To view the errors graph of an IAP, click on the Errors icon against the IAP in the Errors column.

Usage Trends

Displays the following graphs:

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

Figure 18 *Usage Trends Section in the Monitoring Pane*



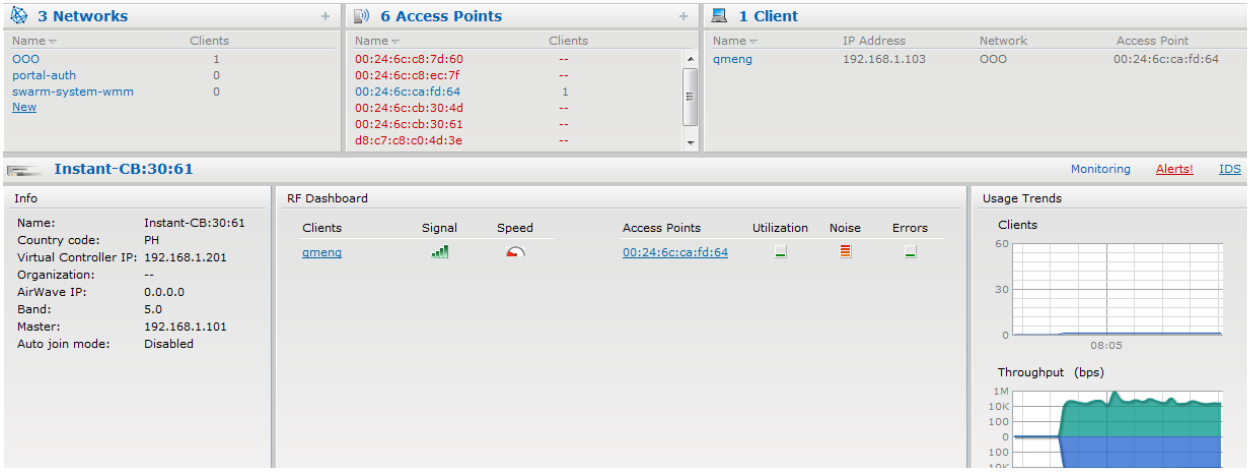
For more information about the graphs and monitoring procedures, see Chapter 18, “Monitoring” .

Alerts

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

NOTE: New alerts will be generated for an incomplete DHCP transaction of a client.

Figure 19 *Alerts Link*

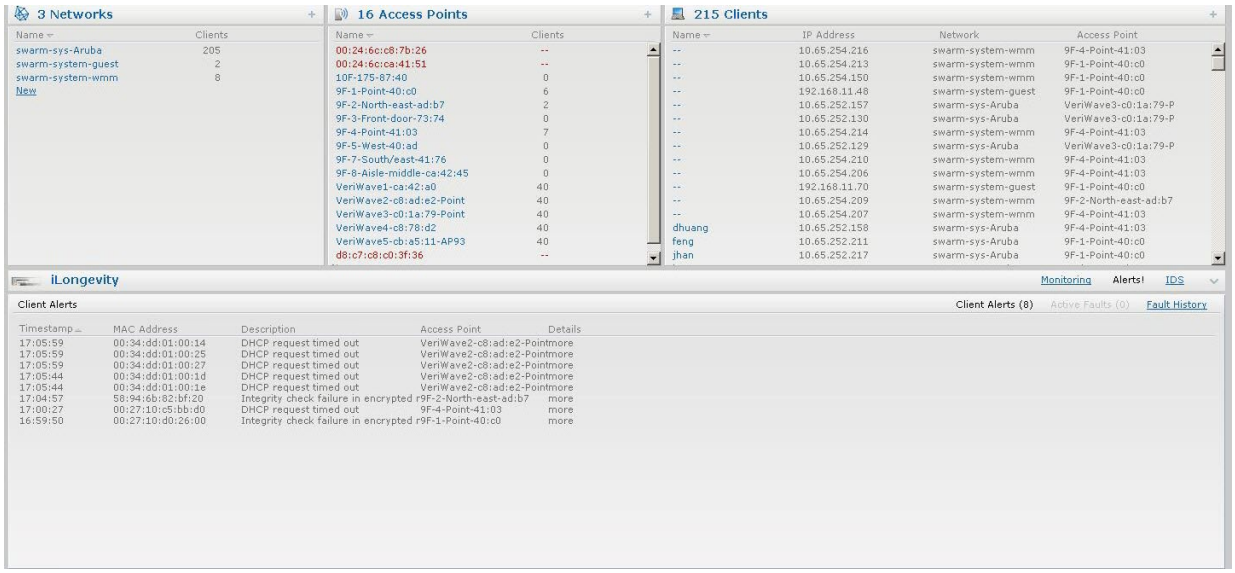


Client Alerts

These alerts occur when clients are connected to the 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 IAP to which the client is connected.
- Details—Provides complete details of the alert.

Figure 20 *Client Alerts*

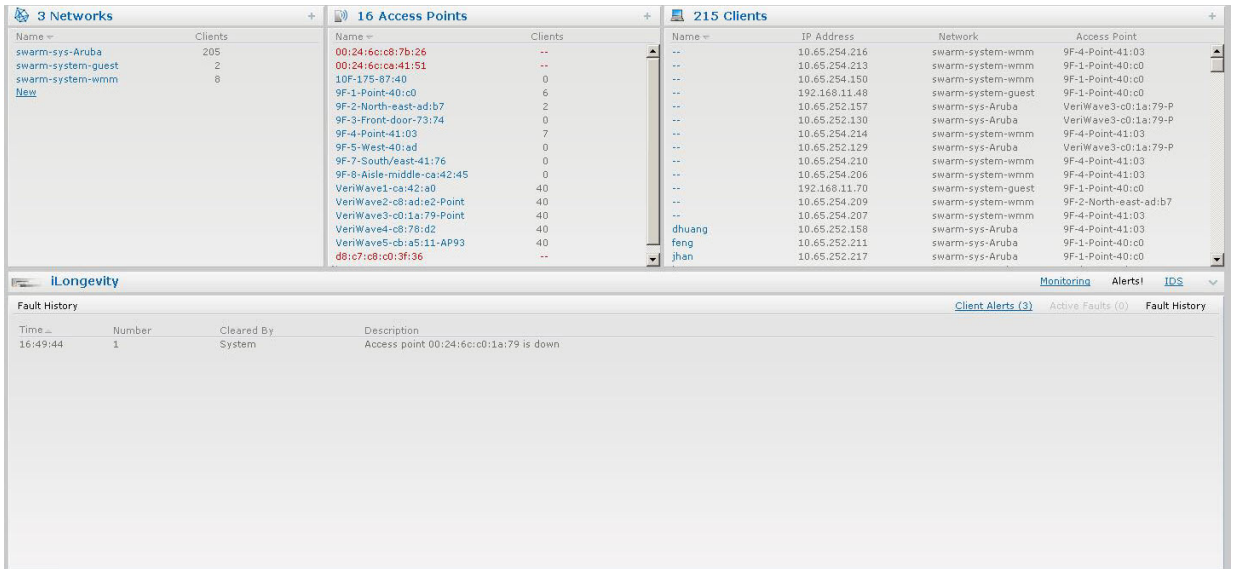


Fault History

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 21 *Fault History*

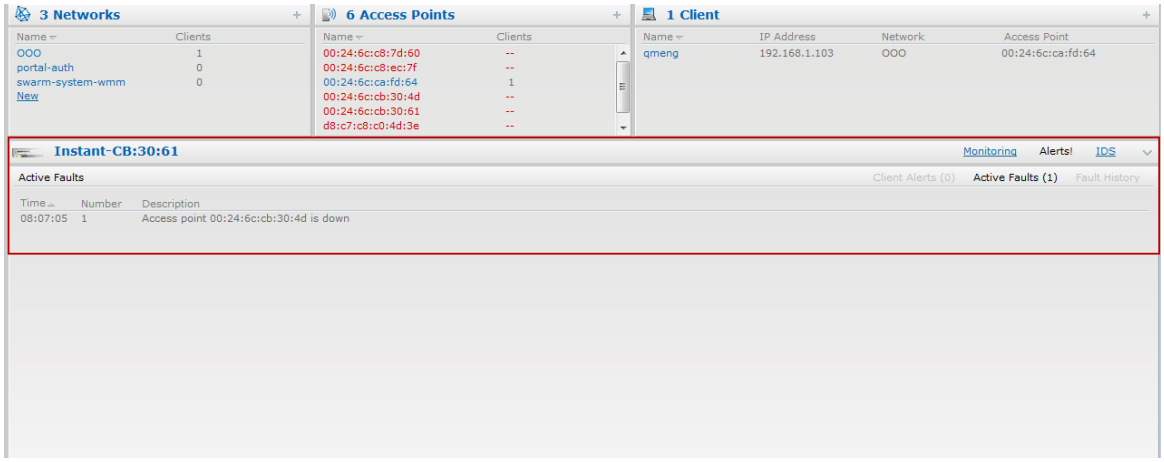


Active Faults

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 22 *Active Faults*



For more information about alerts, see Chapter 19, “Alert Types and Management” .

IDS

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

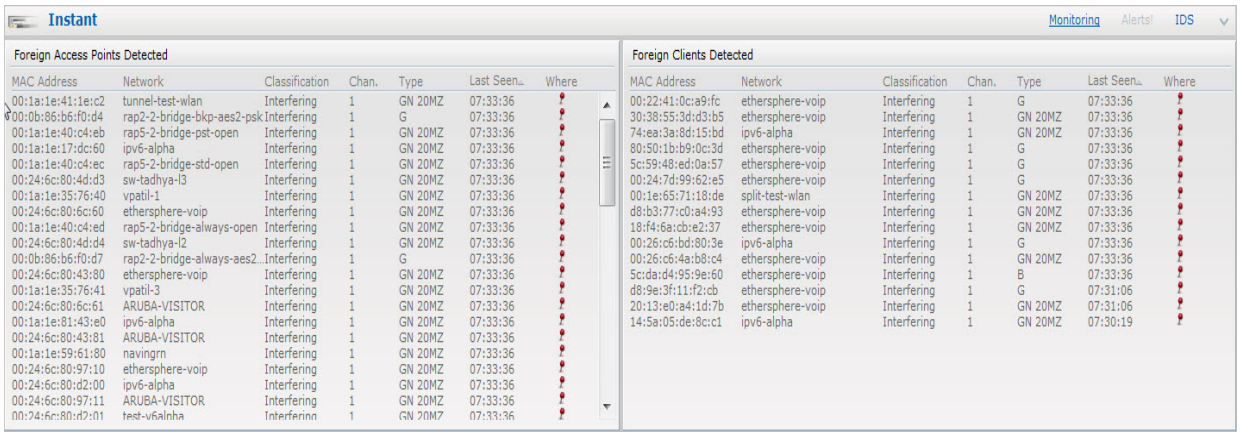
- Foreign Access Points Detected—Lists the APs that are not controlled by the Virtual Controller. The following information is displayed for each foreign AP:
  - Mac address—Displays the Mac address of the foreign AP.
  - Network—Displays the name of the network to which the foreign AP is connected.
  - Classification—Displays the classification of the foreign AP - Interfering IAP or Rogue 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 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 IAP that detected the foreign client. Click the pushpin icon to view the information.

For more information on the intrusion detection feature, see Chapter 15, “Intrusion Detection System” .

Figure 23 *Intrusion Detection on Instant UI*



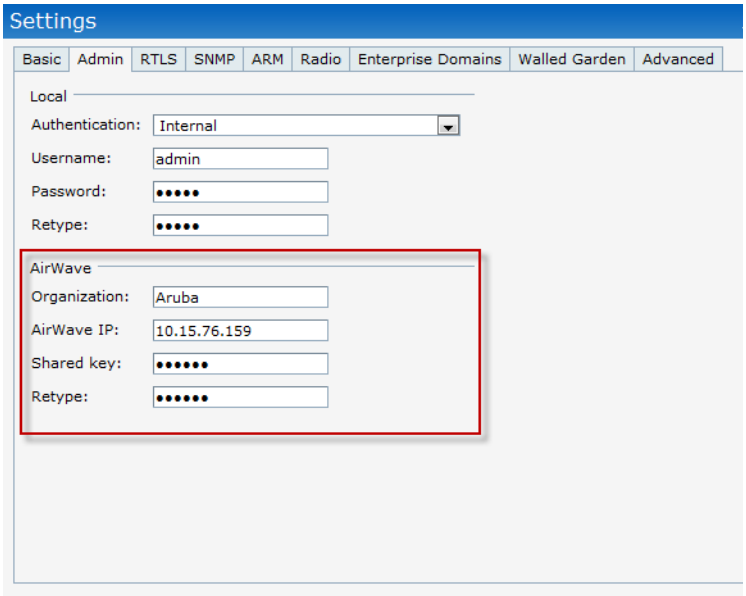
Language

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

AirWave Setup

AirWave is a solution for managing rapidly changing wireless networks. When enabled, AirWave allows you to manage the Instant network. For more information on AirWave, see Chapter 17, “Airwave Integration and Management” on page 131. The AirWave status is displayed on the right side of the language links in the Instant UI. If the AirWave status is **Not Set Up**, click the **Set Up Now** link to set up the AirWave. The Settings box appears with **Admin** tab selected. For information to configure AirWave, see “Configuring AirWave” on page 133.

Figure 24 *AirWave Setup Link – AirWave Configuration*



Pause/Resume

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

Click the **Pause** link to pause the automatic refreshing of the Instant UI. When the automatic 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 Instant UI displays information about the Virtual Controller, Wi-Fi networks, IAPs, or the clients in the Info section. The views on the 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 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 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.
- Instant Access Point view—The Instant Access Point view provides information that is necessary to monitor a selected IAP. All IAPs in the Dell Instant network are listed in the Access Points tab. Click the name of the IAP that you want to monitor. Access Point view for that IAP appears.
- Client view—The Client view provides information that is necessary to monitor a selected client. In the Virtual Controller view, all clients in the Dell 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 Chapter 18, “Monitoring” .

Chapter 3

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 IAP. After locating the IAP, the following transactions take place between the client and the IAP:

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

Network Types

Dell Instant wireless networks are categorized as:

- Employee Network
- Voice Network
- Guest Network

NOTE: When a client is associated to the Voice network, all data traffic will be 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

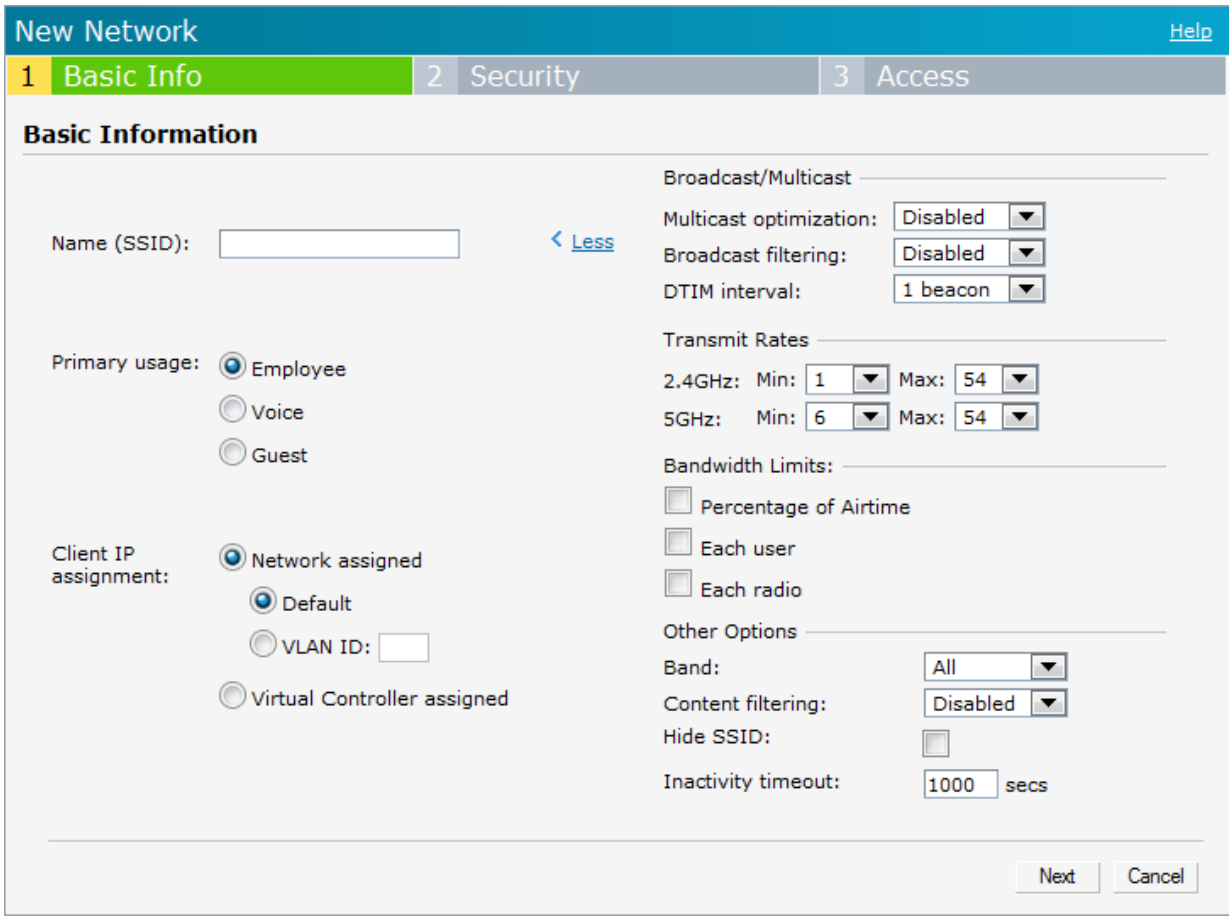
An Employee network is a classic Wi-Fi network. This network type is supported with full customization on Dell Instant. It will be used by the employees in the organization. Passphrase based or 802.1X based authentication methods are supported on this network type. Employees can access the protected 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 Network** box appears.

Figure 25 *Adding an Employee Network—Basic Info Tab*



2. In the **Basic Info** 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.
   c. **Client IP assignment:** Select the required **Client IP assignment** option. Available options for an Employee network are **Network assigned—Default, Network assigned—VLAN ID,** and **Virtual Controller assigned.** The following table describes these options.

Table 5 *Conditions for Adding an Employee Network—Basic Info Tab*

If	then,
You select the Network assigned—Default option	The client gets the IP address in the same subnet at the IAPs.
You select the Network assigned – VLAN ID option	The client gets the IP address from the specified VLAN. Enter the ID of the VLAN in the VLAN ID text box.

Table 5 *Conditions for Adding an Employee Network—Basic Info Tab (Continued)*

If	then,
You select Virtual Controller assigned option	The client gets the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the 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 Chapter 7, "Virtual Controller" on page 76 for configuring the DHCP server.

d. **Bandwidth Limits:** You can specify three types of bandwidth limits.
   - Percentage of 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.

3. Click the **More** link and perform the following steps (These steps are optional).
   a. **Broadcast/Multicast**
      - **Multicast optimization:** When **Enabled**, the IAP will choose 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 2.4GHz and 6 mbps for 5.0GHz bands. Multicast traffic can be sent at upto 24 mbps when this option is enabled. This option is disabled by default.
      - **Broadcast filtering:** When set to **All**, the IAP will drop all broadcast and multicast frames except for DHCP and ARP. When set to **ARP**, in addition to the above, the IAP will convert 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 number of beacons. You can configure this option for every WLAN SSID profile. The default value is 1, which means the client will check for buffered data on the IAP at every beacon. You may choose to configure a larger DTIM value for power saving.

   b. **Transmit Rates:** Indicates the ability to configure the basic and supported rates per SSID for Dell Instant. Select to set the minimum and maximum legacy (non-802.11n) transmit rates for each band -2.4GHz and 5GHz.

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

   d. **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.

4. Click **Next** and set appropriate security levels using the slider button in the **Security** tab. Default selection is **Personal.** Available options are **Enterprise, Personal,** and **Open.**

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

If	then,
You select the Enterprise security level	Perform the following steps: 1. Select the required key options from the Key management drop-down list. Available options are: • WPA-2 Enterprise • WPA Enterprise • Both (WPA-2 & WPA) • Dynamic WEP with 802.1x • Use Session Key for LEAP: Use the Session Key for LEAP 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 Disabled by default. For more information on encryption and recommended encryption type, see Chapter 9, "Encryption" . 2. Termination: Enable this option to terminate the EAP portion of 802.1x authentication on the IAP instead of the RADIUS server. For more information, see "External RADIUS Server" on page 78. 3. Select the required Authentication server option from the Authentication server 1drop-down list. Available options are: • New—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 Chapter 8, "Authentication" . • InternalServer- 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 "Adding a User" on page 151. 4. Reauth interval: When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients. 5. For Internal users: • Users: Click to populate the system's internal auth server with users. For information about adding a user, see "Adding a User" on page 151. • Certificates: Click to display information about current certificates installed in the network. It also provides interface to upload new certificates and to set passphrase for the certificates. For more information, see "Certificates" on page 94.

Table 6 *Conditions for Adding an Employee Network—Security Tab (Continued)*

If	then,
You want to use the default security level, Personal	Perform the following steps: 1. Select the required key options from the Key management drop-down list. Available options are: • WPA-2 Personal • WPA Personal • Both (WPA-2 & WPA) • Static WEP If you have selected Static WEP, then do the following: • Select appropriate WEP key size from the WEP key size drop-down list. Available options are 64-bit and 128-bit. • Select appropriate Tx key from the Tx Key drop-down list. Available options are 1, 2, 3,and 4. • Enter an appropriate WEP key and reconfirm. For more information on encryption and recommended encryption type, see Chapter 9, "Encryption" . 2. Select a passphrase format from the Passphrase format drop-down list. Available options are: • 8-63 alphanumeric chars • 64 hexadecimal chars 3. Enter a passphrase in the Passphrase text box and reconfirm. 4. Select the required option from the Mac authentication drop-down list. Available options are • Enabled and Disabled When Enabled, user must configure at least one RADIUS server for authentication server. See "Mac Authentication" on page 91 for further details
You select the Open security level	Select the required Mac authentication from the Mac authentication drop-down list. Available options are: • Enabled and Disabled When Enabled, user must configure at least one RADIUS server for authentication server. See "Mac Authentication" on page 91 for further details.

Figure 26 *Security Tab—Enterprise*

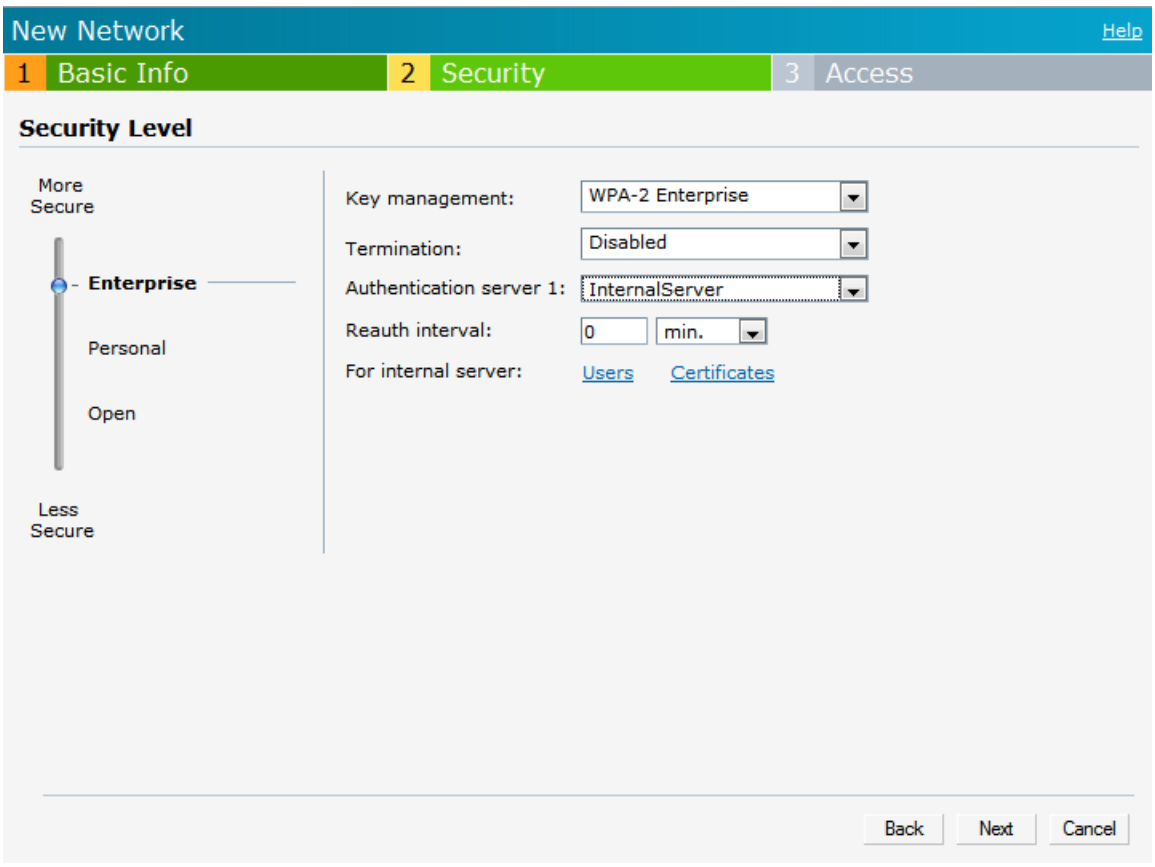


Figure 27 *Security Tab—Personal*

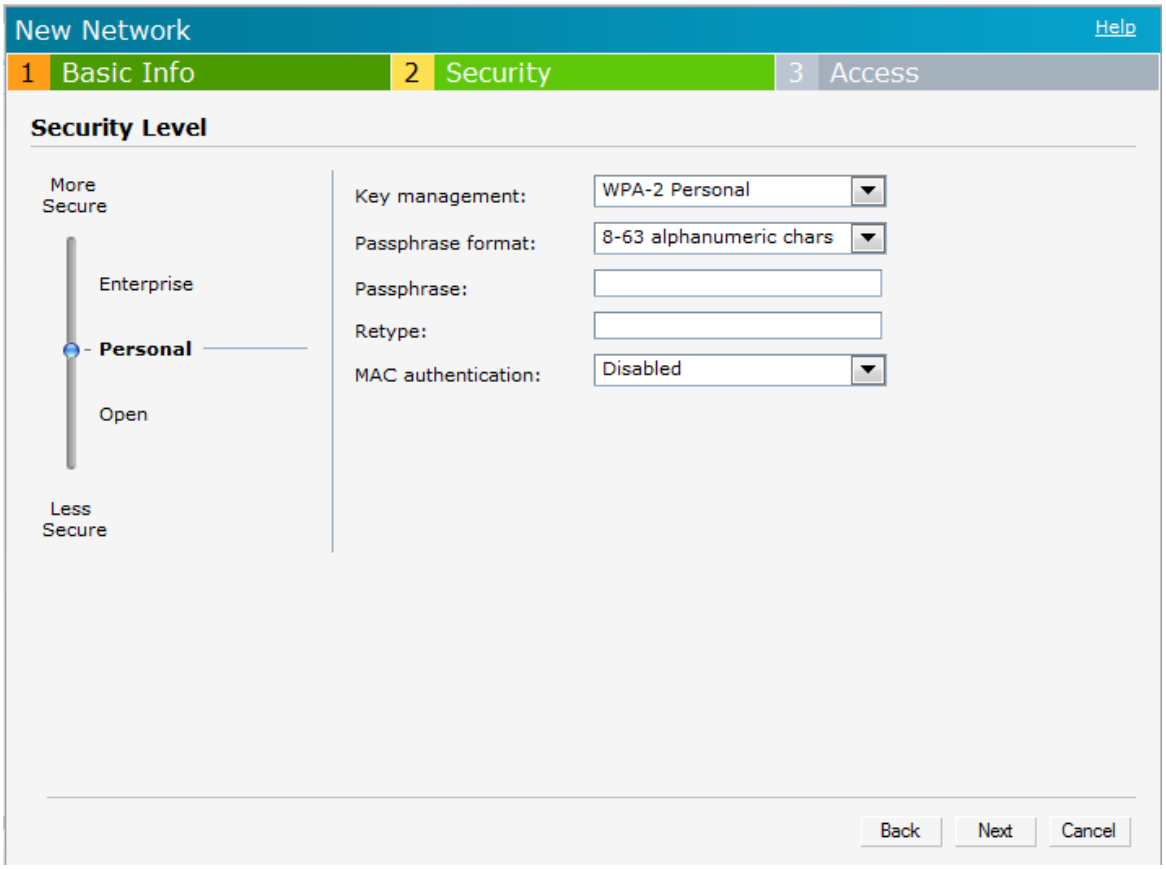
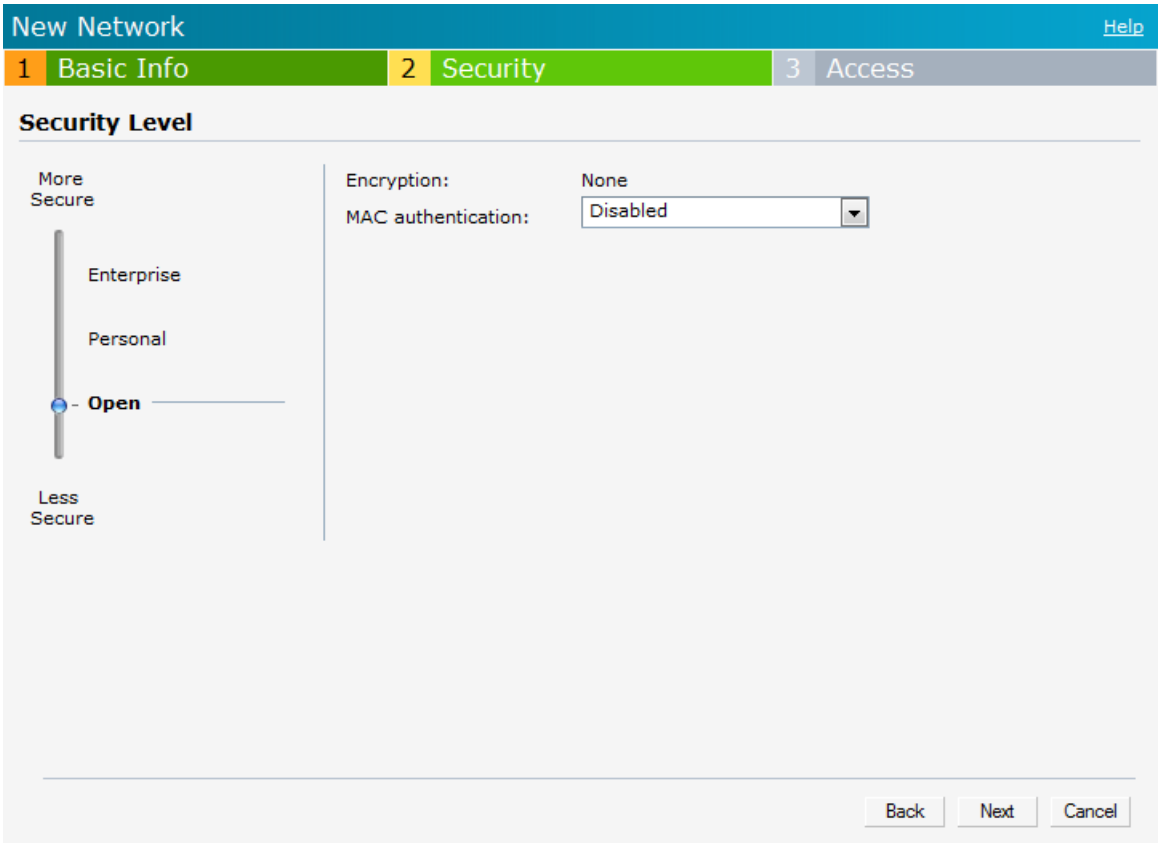


Figure 28 *Security Tab—Open*



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. Instant Firewall treats packets based on the first rule matched. For more information, see Chapter 11, "Instant Firewall" .

To edit the default rule, perform the following steps:

a. Select the rule and then click **Edit**.

b. Select appropriate options in the **Edit Rule** box and click **OK.**

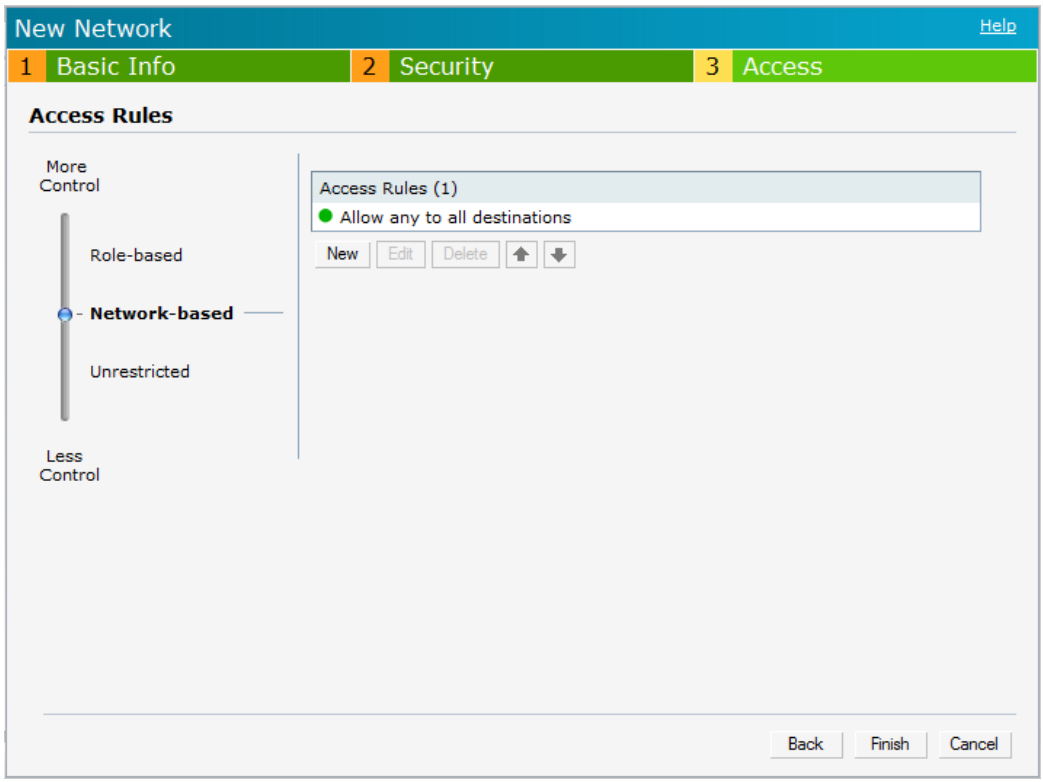
To define an access rule, perform the following steps:

a. Click **New**.

b. Select appropriate options in the **New Rule** box.

c. Click **OK.**

Figure 29 *Adding an Employee Network—Access Rules Tab—Network*



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

Voice Network

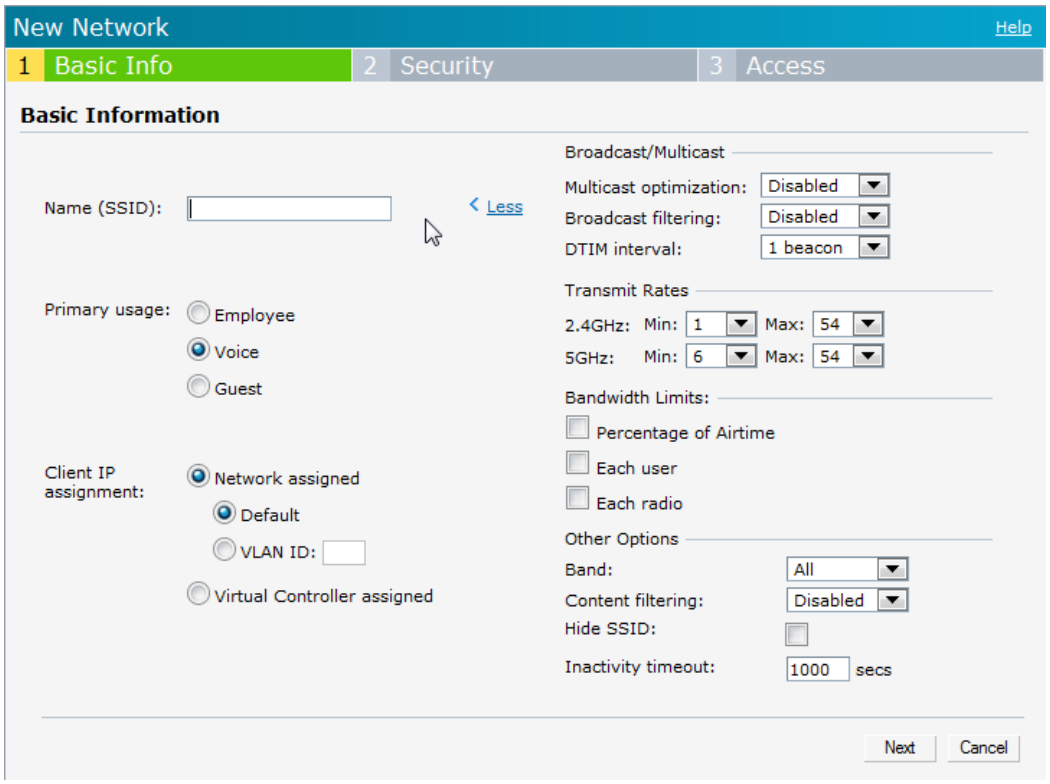
Use the Voice network type when you want devices that provide only voice services like handsets or only applications that require voice-like prioritization need connectivity.

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 Network** box appears.

Figure 30 *Adding a Voice Network—Basic Info Tab*



In the **Basic Info** tab, perform the following steps:

a. Type a name for the network in the **Name (SSID)** text box.

b. Select **Voice** from the **Primary usage** options. This selection determines the primary usage of the network being added.

c. Select the required **Client IP assignment** option. Available options for a Voice network are **Network assigned—Default**, **Network assigned—VLAN ID,** and **Virtual Controller assigned.**

d. Select the band from the **Band** drop-down list at which the wireless network will transmit radio signals. Available options are **All, 2.4 GHz,** and **5 GHz.** The **All** option is selected by default. It is also the recommended option.

Table 7 *Conditions for Adding a Voice Network—Basic Info Tab*

If	then,
You select the Network assigned – Default option	The client gets the IP address in the same subnet at the IAPs.
You select the Network assigned – VLAN ID option	The client gets the IP address from the specified VLAN. Enter the ID of the VLAN in the VLAN ID text box.
You select Virtual Controller assigned option	The client gets the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN for the IAPs and 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.

2. Click the **More** link and perform the following steps (These steps are optional).
   a. **Broadcast/Multicast**
      - **Multicast optimization—**When **Enabled**, the IAP will choose 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 2.4GHz and 6 mbps for 5.0GHz bands. Multicast traffic can be sent at upto 24 mbps when this option is enabled. This option is disabled by default.
      - **Broadcast filtering—**When set to **All**, the IAP will drop all broadcast and multicast frames except for DHCP and ARP. When set to **ARP**, in addition to the above, the IAP will convert ARP requests to unicast and send 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 number of beacons. This option is configurable for each WLAN SSID profile. The default value is 1, which means the client will check for buffered data on the IAP at every beacon. You may choose to configure a larger DTIM value for power saving.
   b. **Transmit Rates—**Indicates the ability to configure the basic and supported rates per SSID for Dell Instant. Select to set the minimum and maximum legacy (non-802.11n) transmit rates for each band - 2.4GHz and 5GHz.
   c. **Hide SSID—**Select this check box if you do not want the SSID (network name) to be visible to users.
3. **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.
4. Click **Next** and set appropriate security levels using the slider button in the **Security** tab. Default selection is **Personal.** Available options are **Enterprise, Personal,** and **Open.**

Table 8 *Conditions for Adding a Voice Network—Security Tab*

If	then,
You select the Enterprise security level	Perform the following steps: 1. Select the required key options from the Key management drop-down list. Available options are: • WPA-2 Enterprise • WPA Enterprise • Both (WPA-2 & WPA) • Dynamic WEP with 802.1x For more information on encryption and recommended encryption type, see Chapter 9, "Encryption" . 2. Select the required RADIUS server option from the RADIUS Server drop-down list. Available options are: • External—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 "Configuring an External RADIUS Server" on page 79. • Internal—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 about adding a user, see "Adding a User" on page 151.

Table 8 *Conditions for Adding a Voice Network—Security Tab (Continued)*

If	then,
You want to use the default security level, Personal,	Perform the following steps: 1. Select the required key options from the Key management drop-down list. Available options are: • WPA-2 Personal • WPA Personal • Both (WPA-2 & WPA) • Static WEP If you selected Static WEP, then do the following: • Select appropriate WEP key size from the WEP key size drop-down list. Available options are 64-bit and 128-bit. • Select appropriate Tx key from the Tx Key drop-down list. Available options are 1, 2, 3, and 4. • Enter an appropriate WEP key in the WEP Key text box and reconfirm. For more information on encryption and recommended encryption type, see Chapter 9, "Encryption" . 2. Enter a passphrase in the Passphrase text box and reconfirm. 3. Select the required option from the Mac authentication drop-down list. Available options are: • None—This option provides open authentication. Any client that requests association is allowed to connect to the network. Open authentication is not recommended unless you want users to gain quick access to the network. • External RADIUS Server—For information on configuring an external RADIUS server, see "Configuring an External RADIUS Server" on page 79.
You select the Open security level	Select the required Mac authentication from the Mac authentication drop-down list. Available options are: • None—This option provides open authentication. Any client that requests association is allowed to connect to the network. Open authentication is not recommended unless you want users to gain quick access to the network. • External RADIUS Server—For information on configuring an external RADIUS server, see "Configuring an External RADIUS Server" on page 79.

4. 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. Instant Firewall treats packets based on the first rule matched. For more information, see Chapter 11, "Instant Firewall" .

To edit the default rule, perform the following steps:

a. Select the rule and click **Edit**.

b. Select appropriate options in the **Edit Rule box** and click **OK**.

To define an access rule, perform the following steps:

a. Click **New**.

b. Select appropriate options in the **New Rule** box.

c. Click **OK**.

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

Guest Network

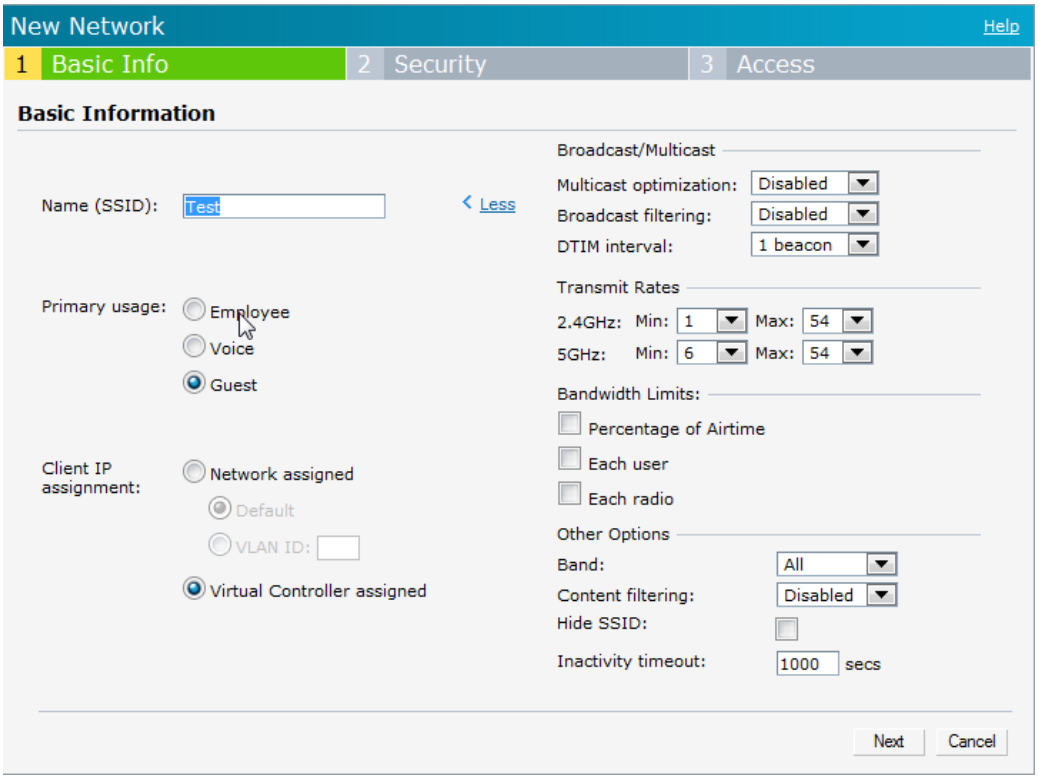
The Guest wireless network is created for guests, visitors, contractors, and any non-employee users who will use the enterprise Wi-Fi network. The Virtual Controller assigns the IP address for the guest clients. Captive portal or passphrase based authentication methods can be set for this wireless network. Typically, a guest network is an un-encrypted network. However, you can specify encryption settings in the **Security** tab step 9 of the following procedure).

Adding a Guest Network

This section provides the procedure to add a guest network.

1. In the **Networks** tab, click the **New** link. The **New Network** box appears.

Figure 31 *Adding a Guest Network—Basic Info Tab*



2. In the **Basic Info** tab, perform the following steps:
   a. Type a name for the network in the **Name (SSID)** text box.
   b. Select **Guest** from the **Primary usage** options. This selection determines the primary usage of the network being added.
   c. The **Client IP assignment** selection automatically changes to **Virtual Controller assigned**. The Virtual Controller creates a private subnet and VLAN for the IAPs and the wireless clients. The Virtual Controller NATs all traffic out of this interface.
3. Click the **More** link and perform the following steps (These steps are optional).
   a. Broadcast/Multicast
   - **Multicast optimization:** When **Enabled**, the IAP will choose 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 2.4GHz and 6 mbps for 5.0GHz bands. Multicast traffic can be sent at upto 24 mbps when this option is enabled. This option is disabled by default.
   - **Broadcast filtering:** When set to **All**, the IAP will drop all broadcast and multicast frames except for DHCP and ARP. When set to **ARP**, in addition to the above, the IAP will convert ARP requests to

unicast and send 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 number of beacons. This option is configurable for each WLAN SSID profile. The default value is 1, which means the client will check for buffered data on the IAP at every beacon. You may choose to configure a larger DTIM value for power saving.

b. **Transmit Rates:** Indicates the ability to configure the basic and supported rates per SSID for Dell Instant. Select to set the minimum and maximum legacy (non-802.11n) transmit rates for each band -2.4GHz and 5GHz.

c. **Bandwidth Limits:** Here, you can specify three types of bandwidth limits.

- **Percentage of Airtime:** The aggregate amount of airtime that all clients on this Network can use to send/receive data.
- **Each User:** The throughput for any single user on this network.
- **Each Radio:** The amount of throughput each radio (some models of AP have multiple radios) is allowed to provide for all clients in aggregate connected to that radio.

d. **Band:** Set the band at which the network will transmit radio signals. Available options are All, 2.4 GHz, and 5 GHz. The All option is selected by default. It is also the recommended option.

e. **Content Filtering:** When enabled, all DNS requests to non-corporate domains on this wireless network are sent to OpenDNS.

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

g. **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.

4. Click **Next**. The **Security** tab appears. This tab allows you to configure the captive portal page for the Guest network. Select one of the following splash page type:

Table 9 *Conditions for Adding a Guest Network—Basic Info Tab*

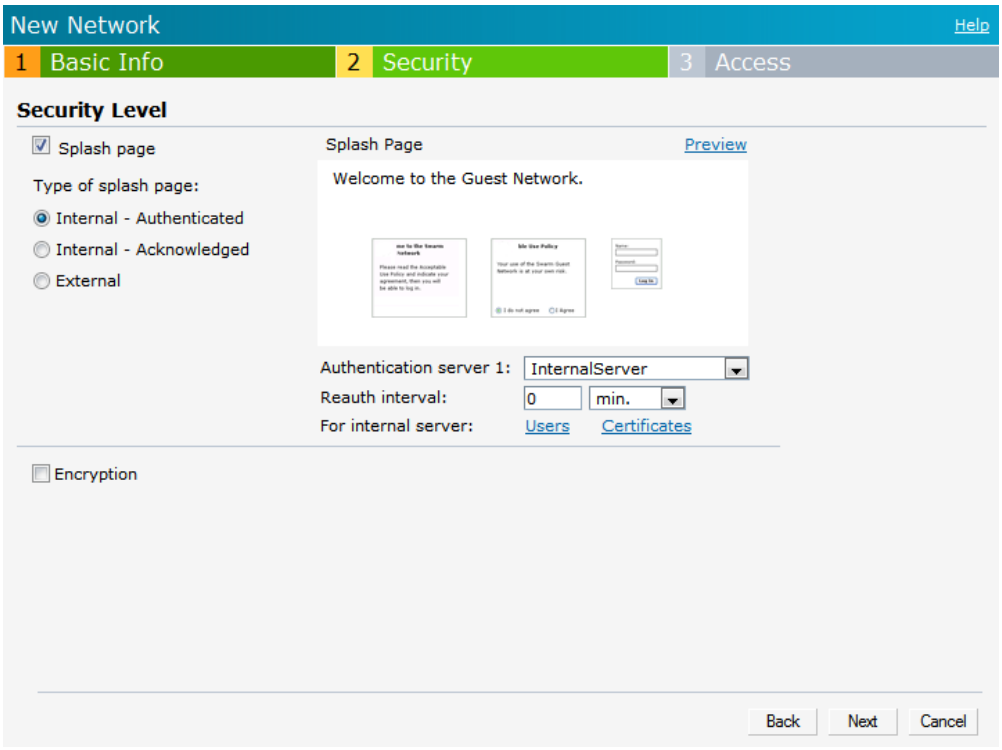
Splash Page Type	Description and steps to set up
Internal—Authenticated	A user has to accept the terms and conditions and enter a username and password on the captive portal page. If this option is selected, then add the users who are required to use the captive portal authentication to the user database. Click the Users link to add the users. For information about adding a user, see "Adding a User" on page 151. For information on customizing the splash page, see "Customizing a Splash Page" on page 87.
Internal—Acknowledged	A user has to accept the terms and conditions for this splash page type. For information on customizing the splash page, see "Customizing a Splash Page" on page 87.

Table 9 *Conditions for Adding a Guest Network—Basic Info Tab (Continued)*

Splash Page Type	Description and steps to set up
External	An external server will be used to display the splash page to the user. If this option is selected, then do the following: 1. Enter the IP or hostname of the external server in the IP or hostname text box. 2. Enter the URL of the captive portal page in the URL text box. 3. Enter the number of the port to be used for communicating with the external server in the Port text box. 4. In the Authentication text box, enter the unique signature that the external server will return in the response after a successful user authentication. 5. Select the required Authentication server 1 option from the drop-down list. Available options are: • New—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 "Configuring an External RADIUS Server" on page 79. 6. Reauth interval—When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients. 7. Accounting—When enabled, the Access Points will post accounting information as RADIUS START and RADIUS STOP accounting records to the RADIUS server. 8. Accounting interval—When set to a value greater than zero, the IAP will periodically post accounting information as RADIUS INTERIM accounting records to the RADIUS server.

If you do not want to set the captive portal authentication, clear the **Splash page** check box.

Figure 32 *Adding a Guest Network—Splash Page Settings*

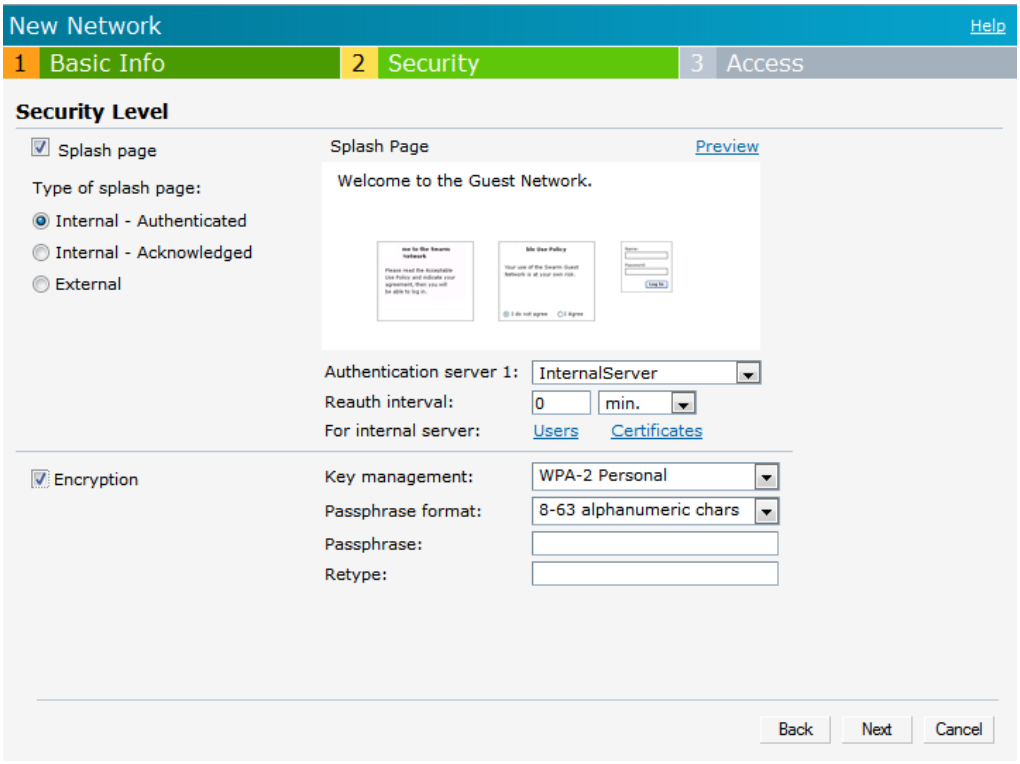


9. Select the **Encryption** check box and perform the following steps (These steps are optional):
   a. Select the required key management option from the **Key management** drop-down list. Available options are:
      - WPA-2 Personal
      - WPA Personal
      - Both (WPA-2 & WPA)

- Static WEP. If you selected Static WEP, then do the following:

1. Select the appropriate WEP key size from the **WEP key size** drop-down list. Available options are **64-bit** and **128-bit.**
2. Select the appropriate Tx key from the **Tx Key** drop-down list. Available options are **1,2,3,** and **4.**
3. Enter an appropriate WEP key in the **WEP Key** text box and reconfirm.

Figure 33 *Configuring a Splash Page—Encryption Settings*



10. 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. Instant Firewall treats packets based on the first rule matched. For more information, see Chapter 11, “Instant Firewall” .

To edit the default rule, perform the following steps:

a. Select the rule and click **Edit**.

b. Select appropriate options in the **Edit Rule** box and click **OK.**

To define an access rule, perform the following steps:

a. Click **New**.

b. Select appropriate options in the **New Rule** box.

c. Click **OK.**

11. Click **Finish**.

Editing a Network

To edit a network, perform the following steps:

1. In the **Networks** tab, click the network of the network which you want to edit. The **edit** link appears.
2. Click the **edit** link. The **Edit network** box 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, perform the following steps:

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

Chapter 4

Mesh Network

The Dell PowerConnect W-Instant secure enterprise mesh solution is an effective way to expand network coverage for outdoor and indoor enterprise environments without any wires. As traffic traverses across mesh IAPs, the mesh network automatically reconfigures around broken or blocked paths. This self-healing feature provides increased reliability and redundancy: the network continues to operate if an IAP stops functioning or a connection fails.

NOTE: A mesh network is always enabled on IAP-105/134/135. The 5Ghz radio is also by default enabled on the mesh network.

This chapter describes the Dell Instant secure enterprise mesh architecture, in the following topics:

Mesh Instant Access Points

Mesh IAPs learn about their environment when they boot up. Mesh IAPs are either configured as a mesh portal (MPP), an IAP that uses its wired interface to reach the controller, or a mesh point (MP), an IAP that establishes an all-wireless path to the mesh portal. Mesh IAPs locate and associate with their nearest neighbor, which provides the best path to the mesh portal. Mesh portals and mesh points are also known as mesh nodes, a generic term used to describe IAPs configured for mesh.

A mesh radio's bandwidth can be shared between mesh-backhaul traffic and client traffic. You can, however, configure a radio for mesh services only. If you have a dual-radio IAP, a mesh node can be configured to deliver client services on one radio and both mesh and WLAN services to clients on the other. If you configure a single-radio IAP to deliver mesh services only (by disabling the mesh radio in its 802.11a or 802.11g radio profile) that mesh node will not deliver WLAN services to its clients.

By default, IAPs operate as thin IAPs, which means their primary function is to receive and transmit electromagnetic signals; other WLAN processing is left to the controller. When planning a mesh network, you manually configure IAPs to operate in mesh portal or mesh point roles. Unlike a traditional WLAN environment, local mesh nodes provide encryption and traffic forwarding for mesh links in a mesh environment. Virtual IAPs are still applied to non-mesh radios.

Mesh Portals

The mesh portal (MPP) is the gateway between the wireless mesh network and the enterprise wired LAN. You configure an IAP to perform the mesh portal role, which uses its wired interface to establish a link to the wired LAN. You can deploy multiple mesh portals to support redundant mesh paths (mesh links between neighboring mesh points that establish the best path to the mesh portal) from the wireless mesh network to the wired LAN.

The mesh portal broadcasts the configured mesh service set identifier (MSSID/mesh cluster name), and advertises the mesh network service to available mesh points. Neighboring mesh points that have been provisioned with the same MSSID authenticate to the portal and establish a secure mesh link over which traffic is forwarded. The authentication process requires secure key negotiation, common to all IAPs, and the mesh link is established and secured using Advanced Encryption Standard (AES) encryption. Mesh portals also propagate channel information, including CSAs.

Mesh Points

The mesh point (MP) is an IAP configured for mesh and assigned the mesh point role. Depending on the IAP model, configuration parameters, and how it was provisioned, the mesh point can perform multiple tasks. The

mesh point provides traditional WLAN services (such as client connectivity, intrusion detection system (IDS) capabilities, user role association, and Quality of Service (QoS) for LAN-to-mesh communication) to clients and performs mesh backhaul/network connectivity. A mesh radio can be configured to carry mesh-backhaul traffic only. Mesh points use one of their wireless interfaces to carry traffic and reach the controller.

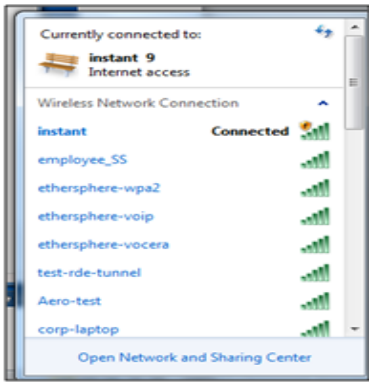
NOTE: Any provisioned IAP that has an ethernet link is a mesh portal, and the IAP without an ethernet link is a mesh point.

Instant Mesh Setup

This section provides instructions on how to create a simple mesh network on Instant. To setup a mesh network, perform the following steps:

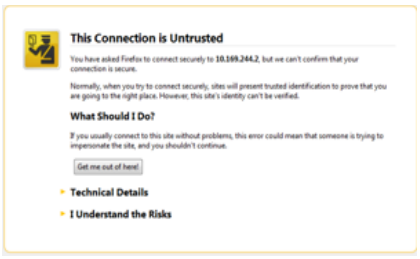
1. Connect all the IAPs to a DHCP server so that the IAPs get their IP addresses in the same subnet.
2. For over-the-air provisioning: Connect one IAP to the switch to form the mesh portal. All the other IAPs are provisioned over-the-air. Ensure that only one Virtual Controller (one subnet) is available over-the-air and all the IAPs are connected to a DHCP server and get their IP addresses in the same subnet.
3. An open SSID, **instant** will be listed. Connect a laptop to the default, open **instant** SSID.

Figure 34 *Open Instant SSID*



4. Type instant.dell-pcw.com in the browser.
5. Click **I understand the risks** and **Add exception** to ignore the certificate warnings that the client does not recognize the certificate authority.

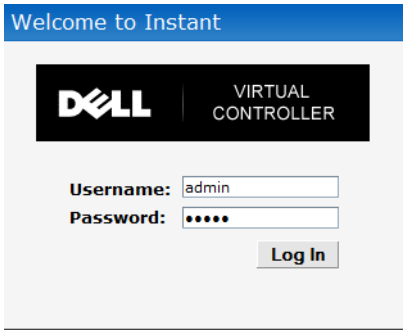
Figure 35 *Untrusted Connection Window*



6. In the login screen as shown in Figure 36, enter the following credentials:

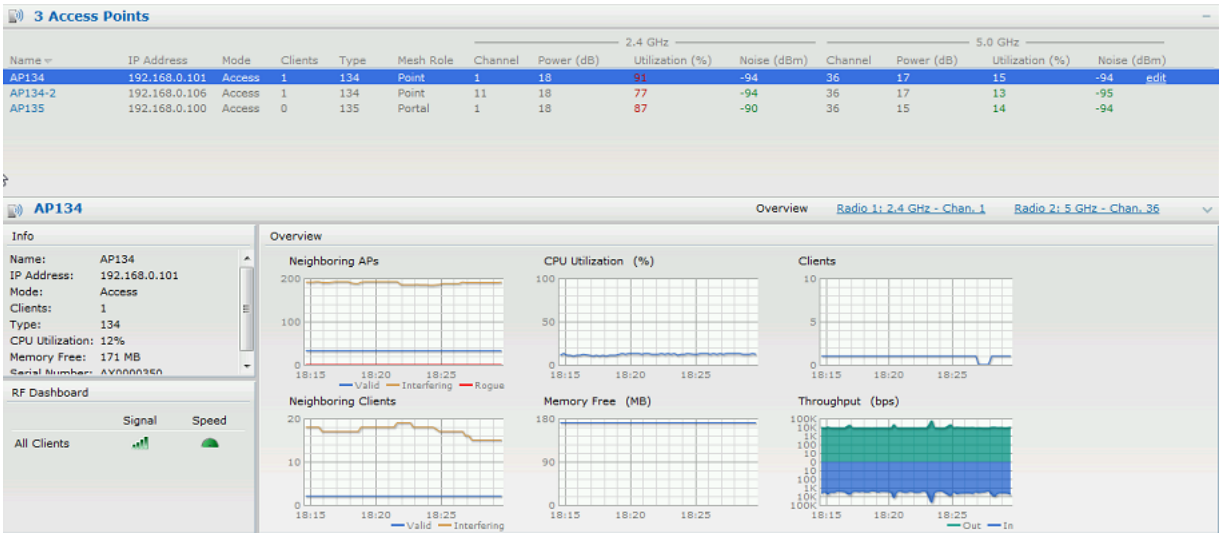
- Username—admin
- Password—admin

Figure 36 *Login Window*



7. Create a new SSID and wpa-2 personal keys with **unrestricted** or **network based** access rules. Select **any permit** for basic connectivity.
8. Connect a client to the new SSID and disconnect from the **instant** SSID.
9. All the IAPs will show up on the Virtual Controller as shown in the figure below. Disconnect the IAPs that you want to deploy as Mesh Points from the switch and place the IAPs at the desired location. The wired IAPs are Mesh Portals.

Figure 37 *Mesh Portal*



NOTE: The IAPs in US, JP, or IL regulatory domain which are in factory default state will scan for several minutes after booting. An IAP mesh point in factory default state will automatically join the portal if only a single Instant mesh network is found. In addition, the auto-join feature must be enabled in the existing network.

NOTE: The IAP mesh point will get an IP address from the same DHCP pool as the portal, and this DHCP request goes through the portal.

The Dell Instant network supports up to 16 IAPs. This chapter describes the auto join mode, Terminal Access, LED display, and Syslog server features in Dell Instant. In addition, the chapter provides procedures for adding and removing IAPs, editing the IAP settings, and upgrading the firmware on the IAP using the Instant UI.

Auto Join Mode

The Auto Join Mode feature allows 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 IAPs to the network. For more information, see "Adding an IAP to the Network" on page 63. Also, when this feature is disabled, IAPs that are configured but not active appear in red.

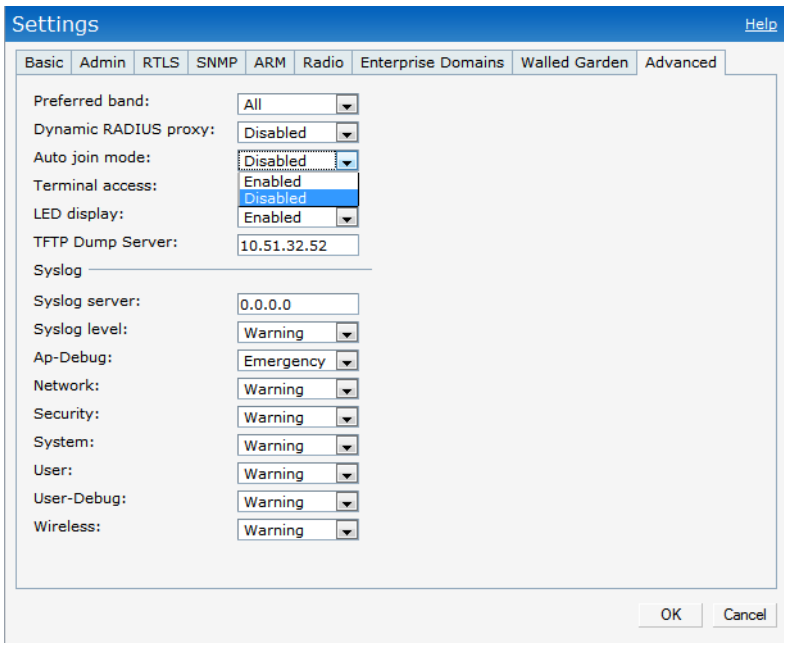
Disabling Auto Join Mode

To disable Auto Join Mode, perform the following steps:

At the top right corner of Instant UI, click the **Settings** link. The **Settings** box appears.

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

Figure 38 *Disabling Auto Join Mode*

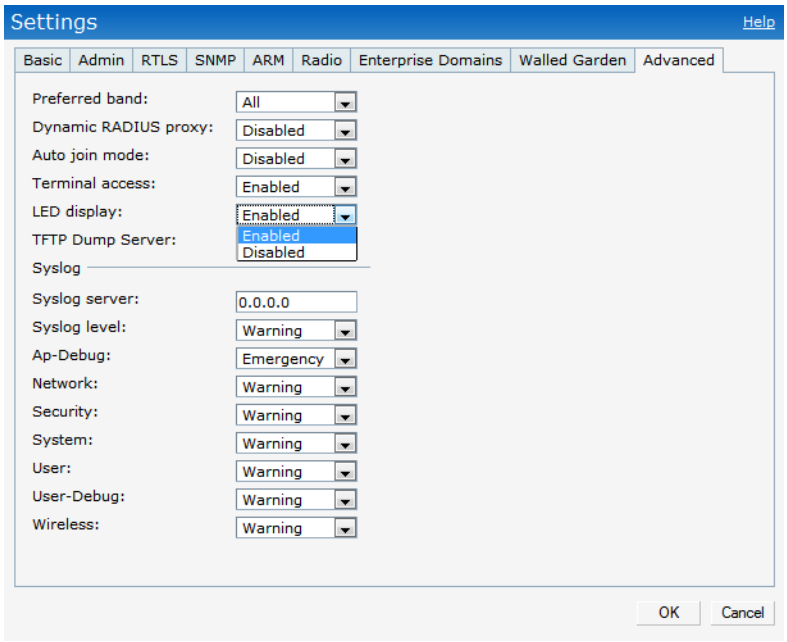


3. Click **OK.**

LED Display

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

Figure 39 *LED Display*

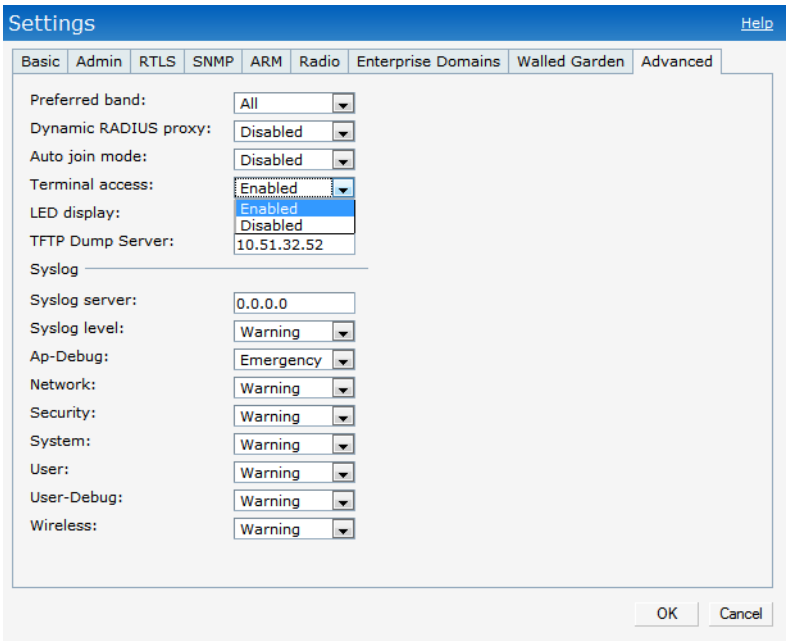


NOTE: The LED display will be always in Enabled mode while rebooting the IAP.

Terminal Access

To enable or disable the telnet access to the IAP's CLI, go to **Settings** > **Advanced** > **Terminal access**.

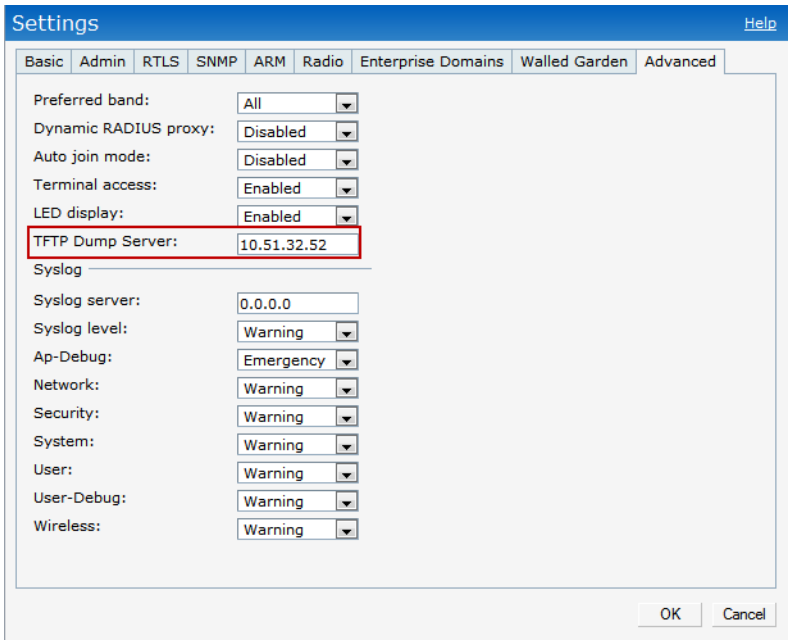
Figure 40 *Terminal Access*



TFTP Dump Server

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

Figure 41 *TFTP Dump Server*

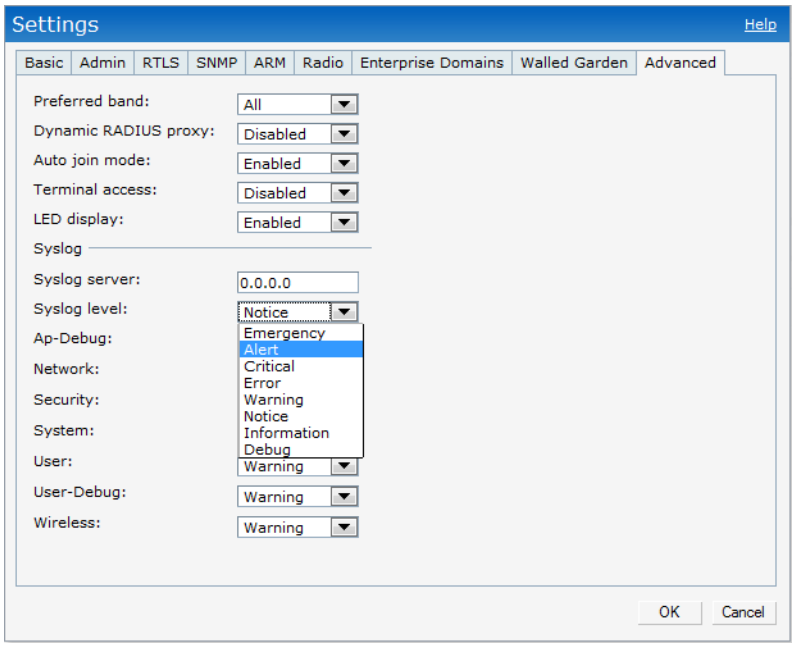


Syslog Server

To specify a Syslog Server for sending syslog messages to the external servers, navigate to **Settings > Advanced > Syslog Server** in the 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 42 *Syslog Server*



Syslog Levels

Dell 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 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 10 describes the logging levels in order of severity, from most to least severe.

Table 10 *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.

Table 10 *Logging Levels (Continued)*

Logging Level	Description
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 an IAP to the Network

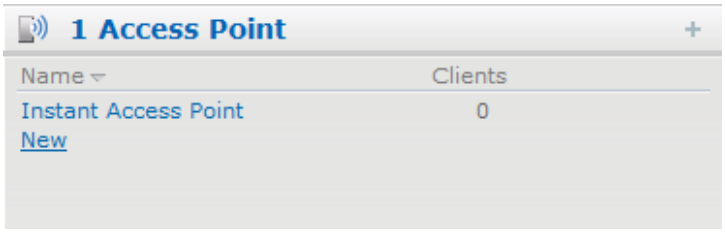
To add an IAP to the Dell Instant network, assign an IP address. For more information, see "Assigning an IP Address to the IAP" on page 18.

After an IAP is connected to the network, if the Auto Join Mode feature is enabled, it is listed in the **Access Points** tab in the Instant UI. The 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 an IAP to the network:

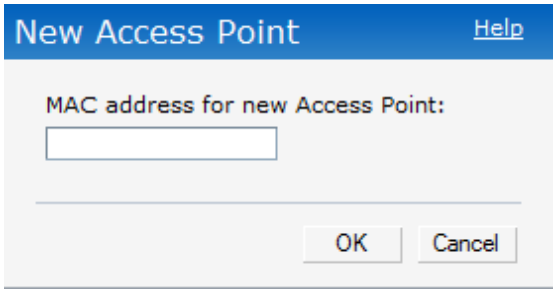
1. In the **Access Points** tab, click the **New** link.

Figure 43 *Adding an IAP to the Instant Network*



2. In the **New Access Point** box, enter the Mac address for the new IAP.

Figure 44 *Entering the Mac Address for the New IAP*



3. Click **OK**.

Removing an IAP from the Network

An IAP can be manually removed from the network only if the Auto Join Mode feature is disabled. To manually remove an IAP from the network, perform the following steps:

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

NOTE: The deleted IAP(s) cannot join the Instant anymore. These IAPs will still appear in the WebUI until the IAPs are rebooted.

Editing IAP Settings

This section explains the steps required to edit the following IAP settings:

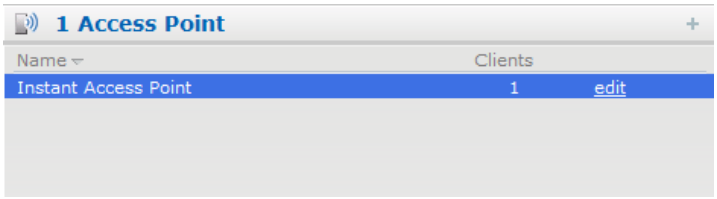
- Name
- IP Address
- Adaptive Radio Management (ARM) Configuration
- External Antenna Configuration
- Migrating from a Virtual Controller Managed Network to Mobility Controller Managed Network

Changing IAP Name

To change the IAP name, perform the following steps:

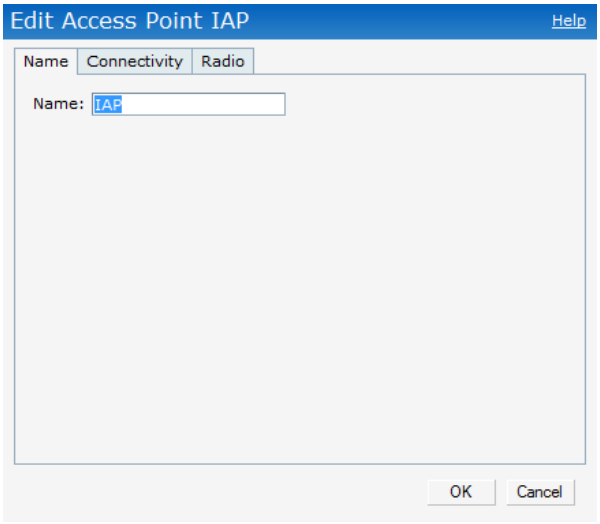
1. In the **Access Points** tab, click the AP of the IAP that you want to rename. The **edit** link appears.

Figure 45 *Editing IAP Settings*



2. Click the **edit** link.

Figure 46 *Changing IAP Name*



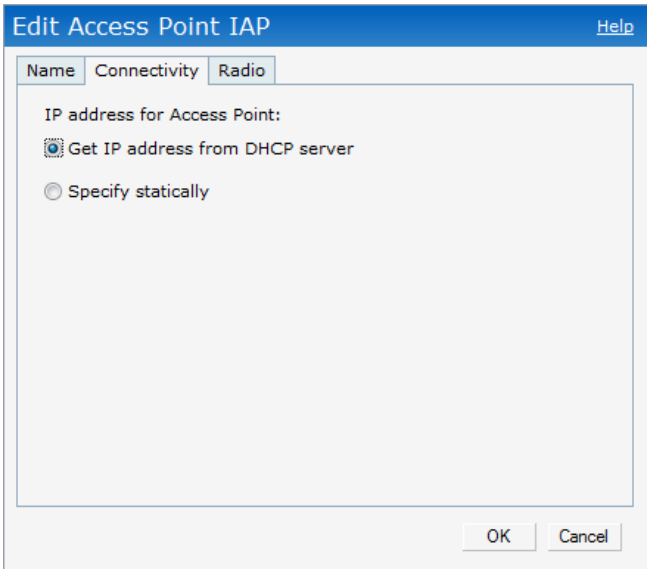
3. Edit the IAP name in the **Name** text box.
4. Click **OK.**

Changing IP Address of the IAP

The Instant UI allows you to change the IP address of the IAP connected to the network. To change the IP address of the IAP, perform the following steps:

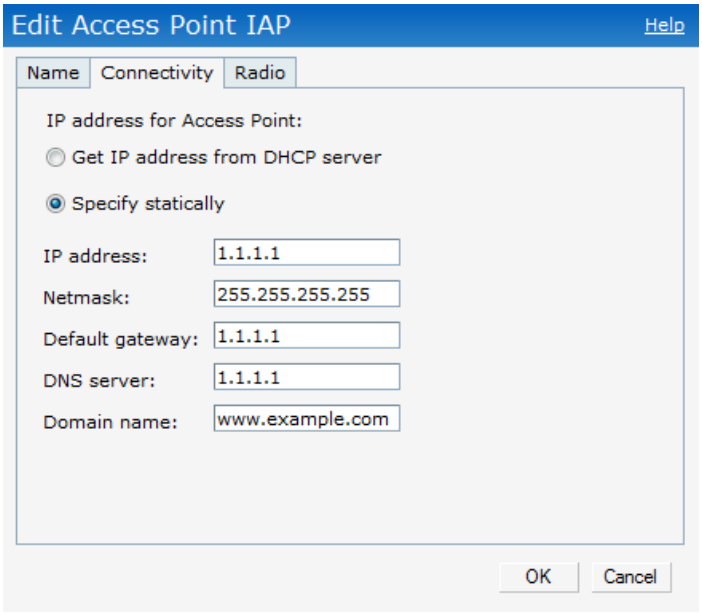
1. In the **Access Points** tab, click the IAP for which you want to change the IP address. The **edit** link appears.
2. Click the **edit** link. The **Edit AP** box appears.
3. Click the **Connectivity** tab.

Figure 47 *Configuring IAP Settings—Connectivity Tab*



4. Select the **Get IP address from DHCP server** or **Specify statically** option. If you selected the **Specify statically** option, perform the following steps:
   1. Enter the new IP address for the IAP in the **IP address** text box.
   2. Enter the netmask of the network in the **Netmask** text box.
   3. Enter the IP address of the default gateway in the **Default gateway** text box.
   4. Enter the IP address of the DNS server in the **DNS server** text box.
   5. Enter the domain name in the **Domain name** text box.

Figure 48 *Configuring IAP Connectivity Settings—Specifying Static Settings*



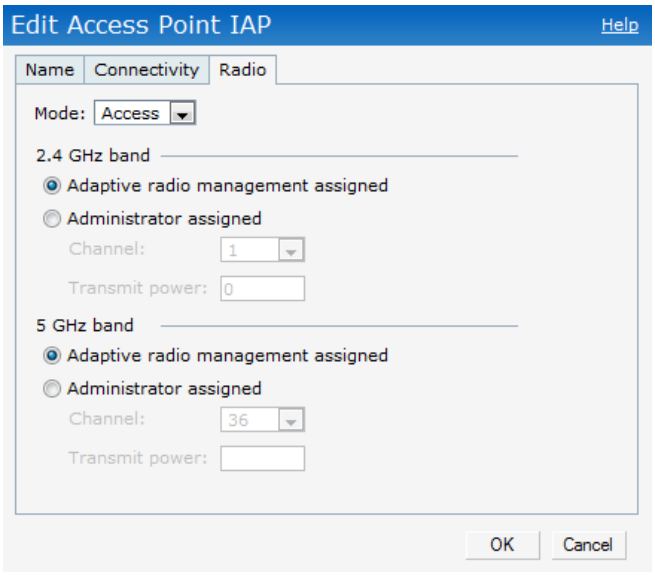
5. Click **OK,** and reboot the IAP.

Configuring Adaptive Radio Management

Adaptive Radio Management (ARM) is enabled in Dell Instant by default. However, if ARM is disabled, perform the following steps to enable it. For more information about ARM, see "Adaptive Radio Management" on page 115.

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

Figure 49 *Configuring IAP Radio Settings Mode—Access*



5. Click **OK.**

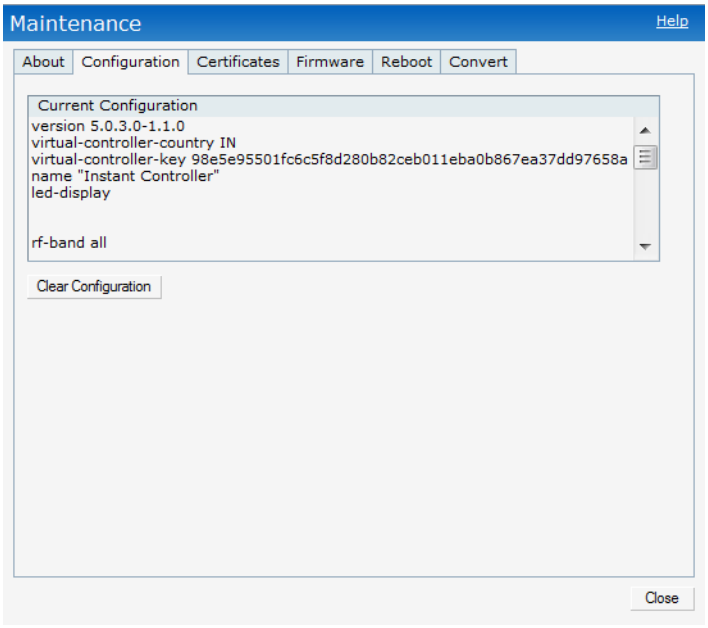
Migrating from a Virtual Controller Managed Network to Mobility Controller Managed Network

An IAP can be provisioned as a Campus AP in a controller-based network, but a Campus AP cannot be provisioned as an IAP. Before converting the IAP, ensure that both the IAP and controller are configured to operate in the same regulatory domain. The reset button located on the rear of an IAP can be used to reset the IAP to factory default settings. If you have converted your IAP to a campus AP, pressing the reset button converts it back to an IAP. The IAP will then boot with the factory default image. Refer to the Dell PowerConnect W-IAP92/93/105 Instant Access Point Installation Guide for details.

To convert an IAP to Campus AP, do the following:

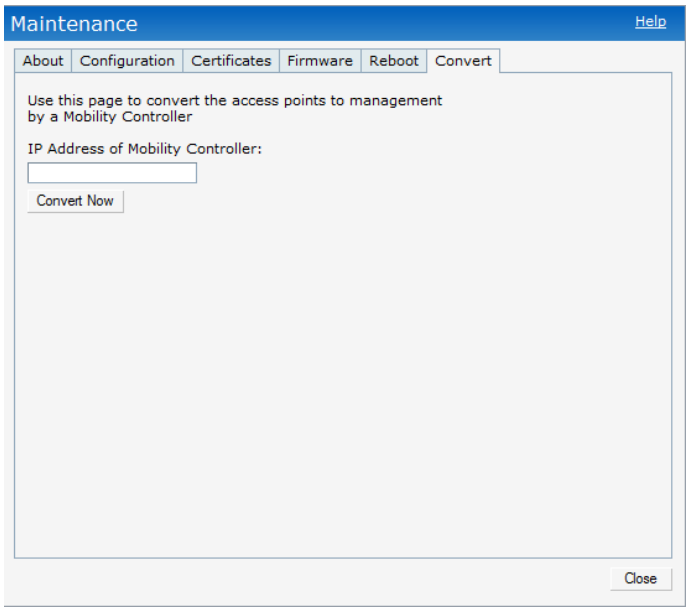
1. At the top right corner of Instant UI, click the **Maintenance** link. The **Maintenance** box appears.

Figure 50 *Maintenance Box*



2. Click the **Convert** tab.

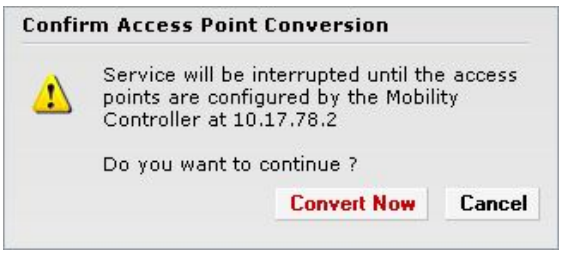
Figure 51 *Maintenance—Convert Tab*



3. Enter the IP address of mobility controller in the **IP Address of Mobility Controller** text box.

4. Click **Convert Now**. Confirm the conversion in the **Confirm Access Point Conversion** box.

Figure 52 *Confirm Access Point Conversion Box*



5. Click **Close**.

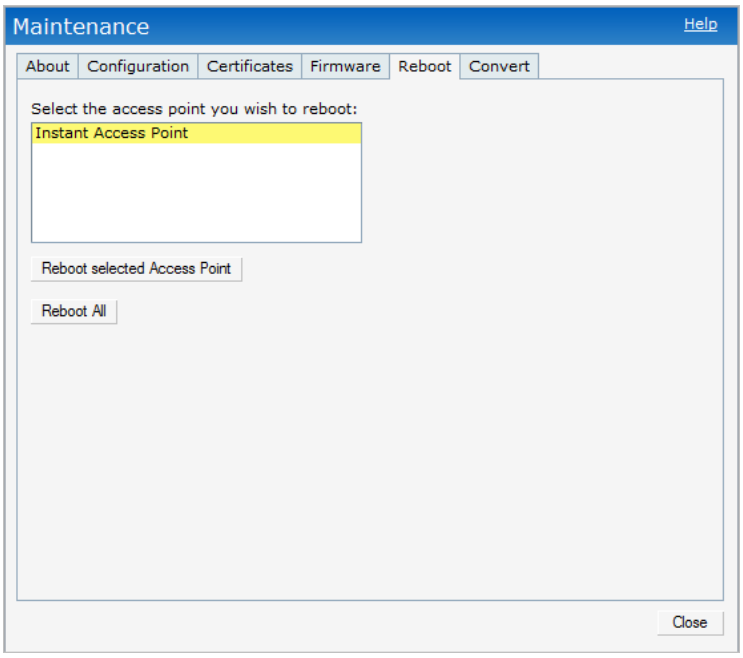
NOTE: An IAP can be converted to an ArubaOS Campus AP only if the controller is running ArubaOS 6.1 or later.

Rebooting the IAP

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

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

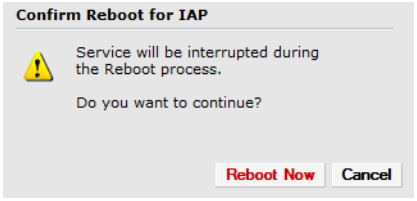
Figure 53 *Rebooting the IAP*



3. In the IAP list, select the IAP that you want to reboot and click **Reboot selected Access Point**. To reboot all the IAPs in the network, click **Reboot All.**

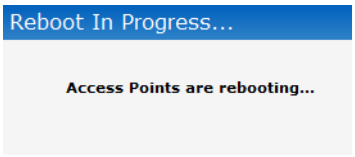
4. The **Confirm Reboot for IAP window** will appear. Click **Reboot Now** to proceed.

Figure 54 *Confirm Reboot message*



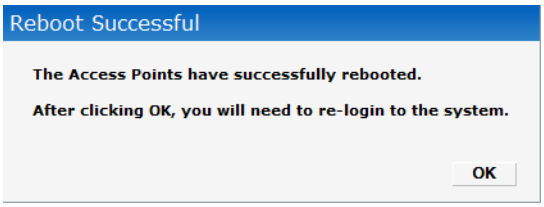
5. The **Reboot in Progress** message will appear indicating that the reboot is in progress.

Figure 55 *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** will appear.

Figure 56 *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 IAP to discover new software image versions on a cloud-based image server hosted by Dell. 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 ArubaOS software for its products.

The Virtual Controller (VC) in Instant AP communicates with the Image server via an Aruba Networks proprietary protocol. The Image server queries the VC. The VC returns the following information:

- Current software version
- Type Code
- Globally Unique ID (GUID)
- OEM-Tag
- Organization (if available)
- Access Point Information (for each AP attached to the VC)
  - AP type
  - AP serial number

The VC expects the available upgrade VC software version and the URL in return. This query normally happens once in a week.

Automatic Firmware Image Check and Upgrade

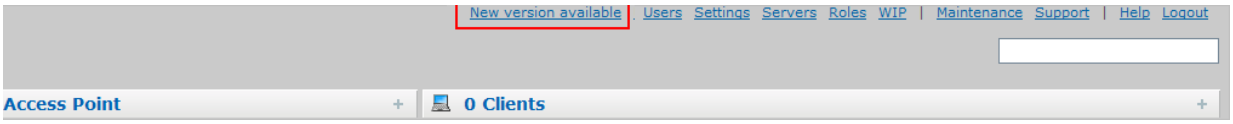
Automatic image check is enabled by default. If AirWave is configured, then the automatic image check is automatically disabled, use the manual image check option to check for the latest image. For more information, see "Manual Firmware Image Check and Upgrade" on page 71.

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

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

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

Figure 57 *Automatic Image Check—New Version Available Link*

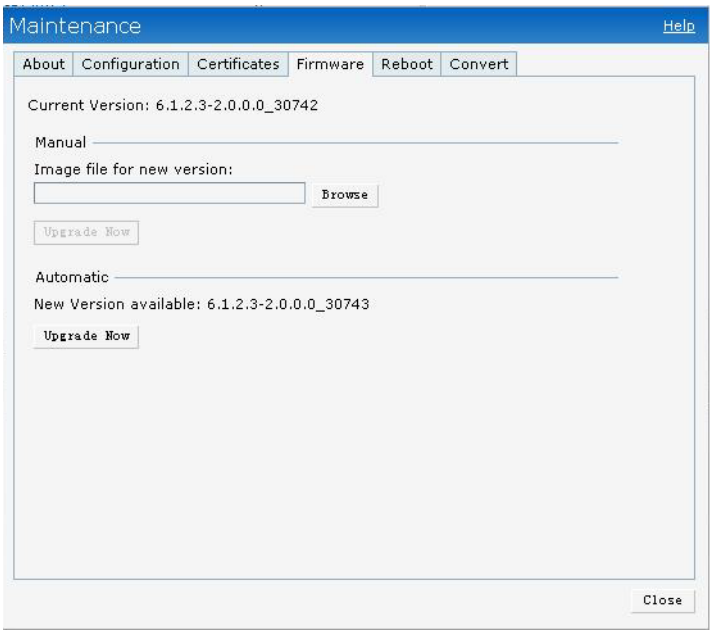


Upgrading to new version

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

1. Click the **New version available** link. The **Maintenance** window appears.
2. Click **Upgrade Now** to upgrade the IAP to the newer version.

Figure 58 *New Version Available Box*



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 will be displayed:

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

Manual Firmware Image Check and Upgrade

To manually check for a new firmware image version, perform the following steps:

1. Navigate to **Maintenance > Firmware** and 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 will appear:

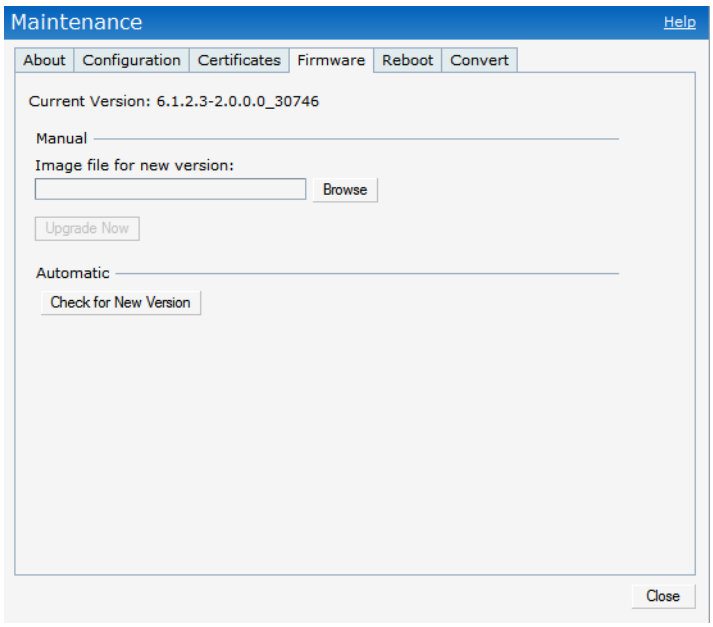
- No new version available—If there is no new version available.
- Image server timed out—Connection or session between the image server and the IAP is timed out.
- Image server failure—If the image server does not respond.
- A new image version found—If a new image version is found.

2. If a new version is found, the **Upgrade Now** button becomes available and displays the version number.
3. Click **Upgrade Now**.

   The 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 will be displayed:

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

Figure 59 *Manual Image Check*



Chapter 6

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.

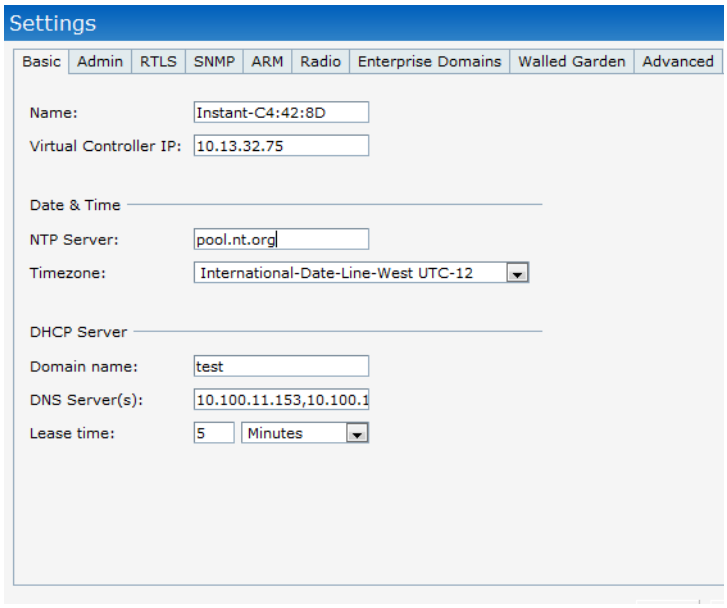
Network Time Protocol (NTP) is required to obtain the precise time from a server and to regulate the local time in each network element. If NTP server is not configured in the Dell Instant network, an IAP reboot may lead to variation in time and data.

Configuring an NTP Server

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

1. At the top right corner of the Instant UI, click the **Settings** link.
2. In the **Settings** box, click the **Basic** tab.
3. Enter the IP address or the URL (domain name) of the NTP server in the **NTP Server** text box and click **OK.**

Figure 60 *Configuring NTP Server*



Dell Instant does not require an external controller to regulate and manage the Wi-Fi network. Any IAP in the Dell Instant network dynamically takes up the role of a Virtual Controller (VC) without impacting the network. 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 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 IAPs.

Master Election Protocol

The Dell Instant network supports 16 IAPs without any external controller. However, there is a need to manage the network. The Master Election Protocol enables the Dell Instant network to dynamically elect an 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 IAP to self-elect as a VC.

Virtual Controller IP Address

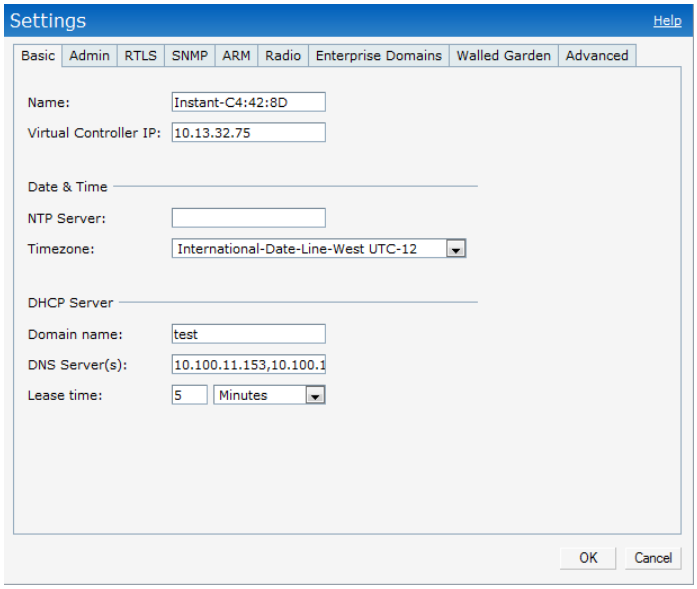
You can specify a single static IP address that can be used to manage a multi-AP Dell Instant network. This IP address is automatically provisioned on a shadow interface on the IAP that takes the role of a Virtual Controller. When an IAP becomes a Virtual Controller, it sends three Address Resolution 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, perform the following steps:

1. At the top right corner of WebUI, click the **Settings** link. The **Settings** box appears.

Figure 61 *Specifying Virtual Controller Name and IP Address*



2. Enter a name for Virtual Controller in the **Name** text box.

3. Enter the appropriate IP address in the **IP address** text box.

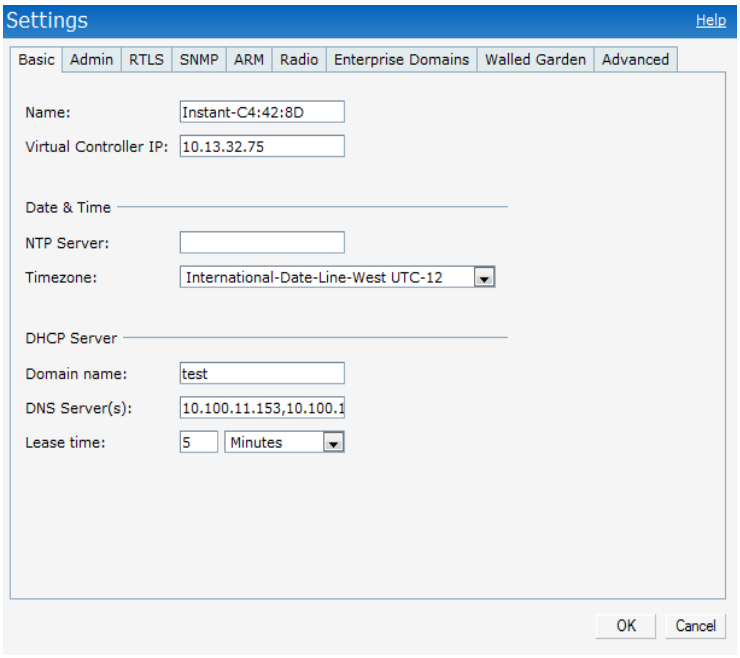
Configuring the DHCP Server

The DHCP Server is the built-in server, used for networks which have **Client IP Assignment** set to **Virtual Controller** Assigned.

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

1. At the top right corner of the Instant UI, click the **Settings** link.
2. In the **Settings** box, click the **Basic** tab.
3. Enter the domain name of the client in the **Domain name** text box.
4. Enter the IP addresses of the DNS servers seperated 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**.

Figure 62 *Configuring the DHCP Server*



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

Chapter 8

Authentication

Authentication Methods in Dell 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 Instant:

- 802.1X Authentication
- Captive Portal
- Mac Authentication

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 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 Instant network supports internal RADIUS server and external RADIUS server for 802.1x authentication.

Internal RADIUS Server

Each IAP has an instance of FreeRADIUS server operating locally. When you enable the Internal RADIUS server option for the network, the authenticator on the 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 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 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 Instant does not ship with any 802.1x server certificate. EAP-TTLS and EAP-PEAP support is not available until the administrator uploads a valid 802.1x server certificate to the Dell Instant network. By default, the 802.1x authentication is limited to LEAP only.

NOTE: It is not recommended the use of LEAP authentication method because it does not provide any resistance to network attacks.

External RADIUS Server

In the external RADIUS server, IP address of the Virtual Controller is configured as the NAS IP address. Instant RADIUS is implemented on the Virtual Controller. This feature eliminates the need to configure multiple NAS clients for every IAP on the RADIUS server for client authentication.

Instant RADIUS dynamically forwards 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. Users are allowed or denied access to the network depending on the response from the RADIUS server.

When you enable the Internal RADIUS server option for the network, the authenticator on the 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 Instant network:

Authentication Terminated on IAP

Dell Instant allows EAP termination for EAP-GTC and will be able to authorize its against an LDAP server. This will allow users to run EAP-GTC termination with their own certificates 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 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 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

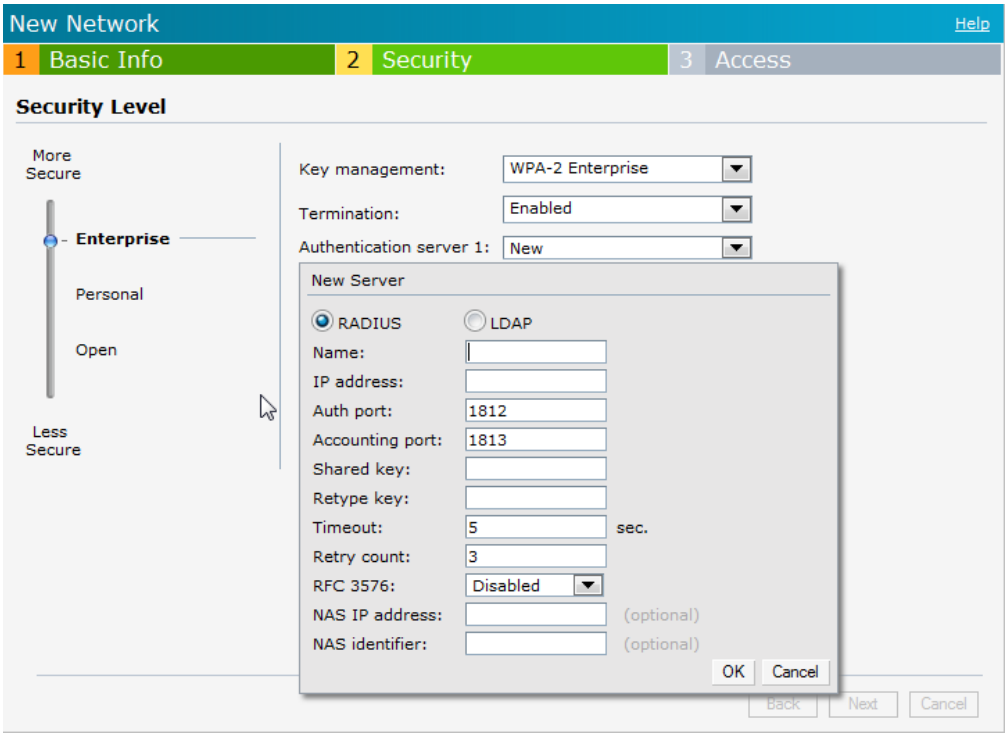
To configure an external RADIUS server for a wireless network, perform the following steps:

1. Click **New** in the **Networks** tab and update the **Basic Information** fields and click **Next** to continue.
2. 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 IAP will retry 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 will be 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 will 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 don't 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 will be 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 63 *Configuring an External RADIUS Server*



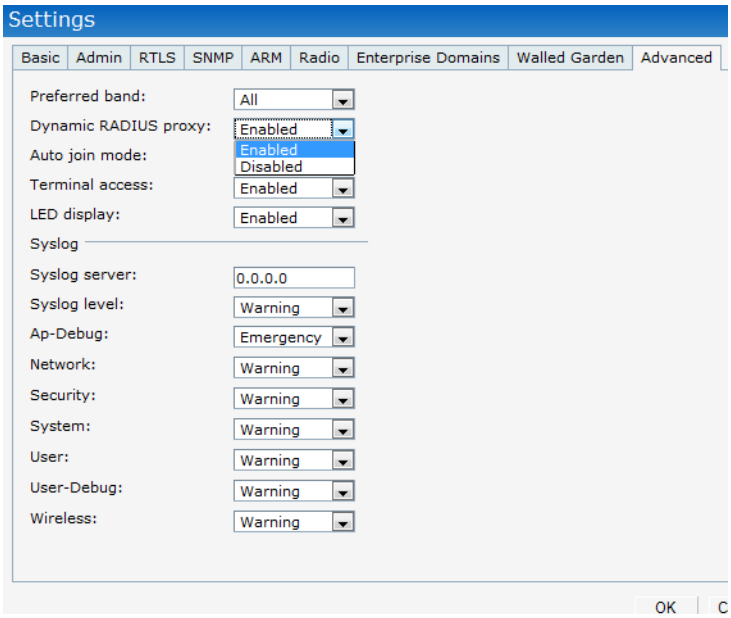
3. Click **OK** after updating the fields.
4. **Reauth interval**—When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients.
5. Click **Next** to continue and then click **Finish.**

Enabling Instant RADIUS

To enable Instant RADIUS, perform the following steps:

1. At the upper right corner of the Instant UI, click the **Settings** link.
2. In the **Settings** box, click the **Advanced** tab.
3. Select **Enabled** from the **Dynamic RADIUS Proxy** drop-down list. When enabled, the Virtual Controller network will use 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 64 *Enabling Instant RADIUS*



4. Click **OK**.

RADIUS Server Authentication with VSA

An external RADIUS server authenticates network users and returns to the 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's

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
- Aruba-AP-Group
- Aruba-Admin-Role
- Aruba-Essid-Name
- Aruba-Location-Id
- Aruba-Named-User-Vlan
- Aruba-Port-Id
- Aruba-Priv-Admin-User
- Aruba-Template-User
- Aruba-User-Role
- Aruba-User-Vlan
- 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

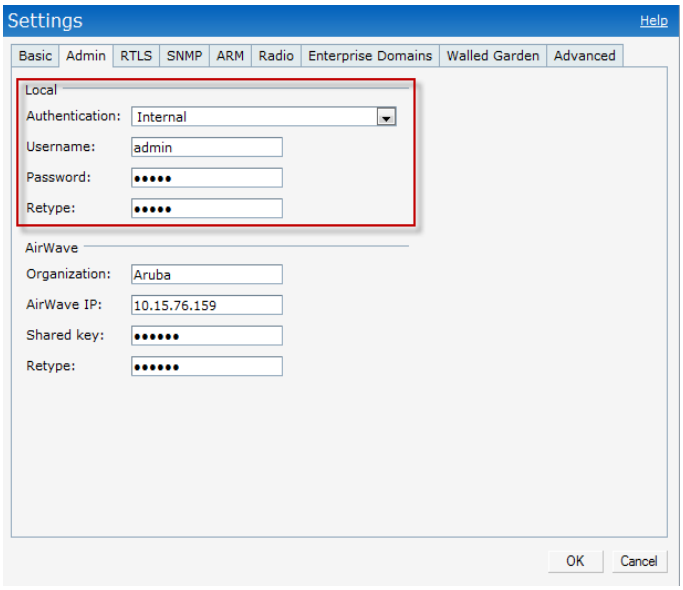
Management Authentication Settings

To authenticate the Virtual Controller Management in the Instant UI, perform the following steps:

1. Click the **Settings** link.
2. Select the **Admins** tab.
3. In the **Authentication** drop-down list, select any one of the following:

- **Internal**—Select the **Username** and **Password** specified in the respective text boxes to access the Virtual "Configuring an External RADIUS Server" on page 79 Management UI.
- **RADIUS Server**—Specify one or two radius servers to authenticate 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 78.
- **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 will switch to "Internal".

Figure 65 *Management Authentication Settings*



4. Click **OK**.

Captive Portal

Dell 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 Instant:

- Internal Captive Portal
- External Captive Portal

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:

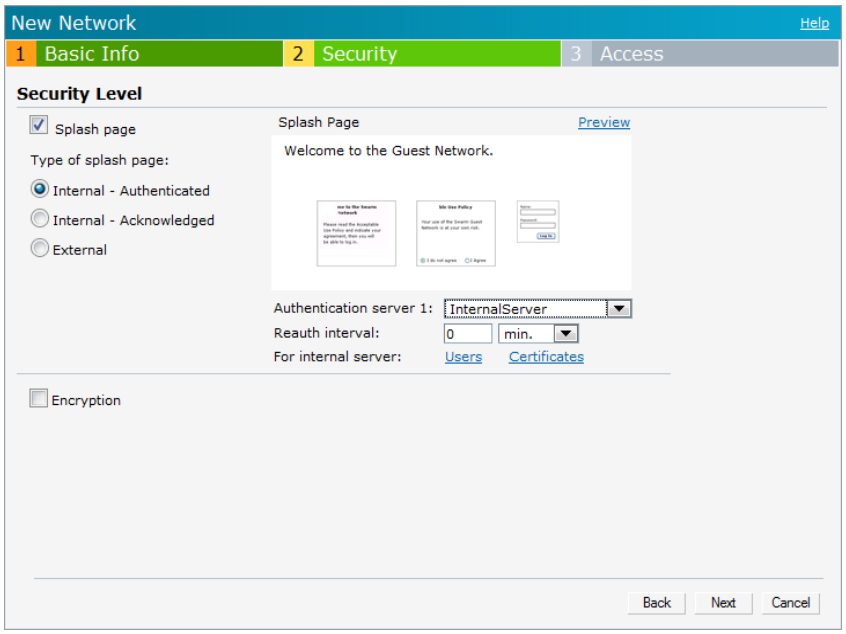
- Internal Authenticated—To gain access to the wireless network, a user must authenticate in the captive portal page. If this option is selected, then users who are required to authenticate have to be added to the user database. Click the **Users** link to add the users. For information about adding users, see "Adding a User" on page 151.
- 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 Network** box opens.
2. In the **Basic Info** tab, perform the following:
   1. Enter a name for the network in the **Name (SSID)** text box.
   2. Click **Guest** and click **Next.**
3. In the **Security** tab, select one of the following options for the splash page type:
   a. **Internal—Authenticated**
   b. **Internal—Acknowledged**

Figure 66 *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 87.

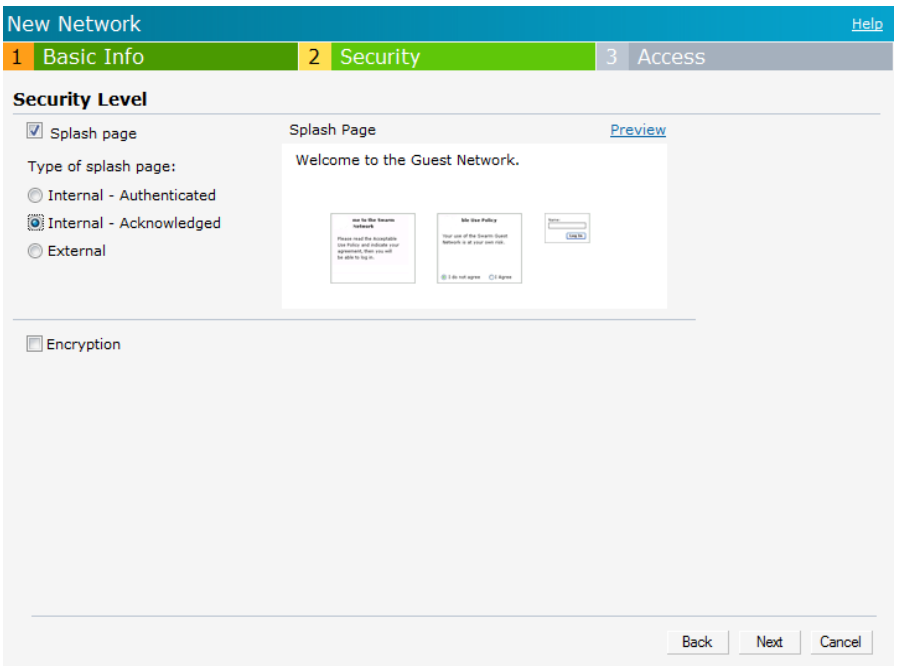
4. Select **InternalServer** from the **Authentication server 1** drop-down list to authenticate user credentials at run time.
5. Click **Next** and click **Finish.**

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** box for the network appears.
3. Click **Next** and select one of the following options for the splash page type in the **Security** tab:
   a. **Internal—Authenticated**
   a. **Internal—Acknowledged**

Figure 67 *Configuring Captive Portal when Editing 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 87.

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

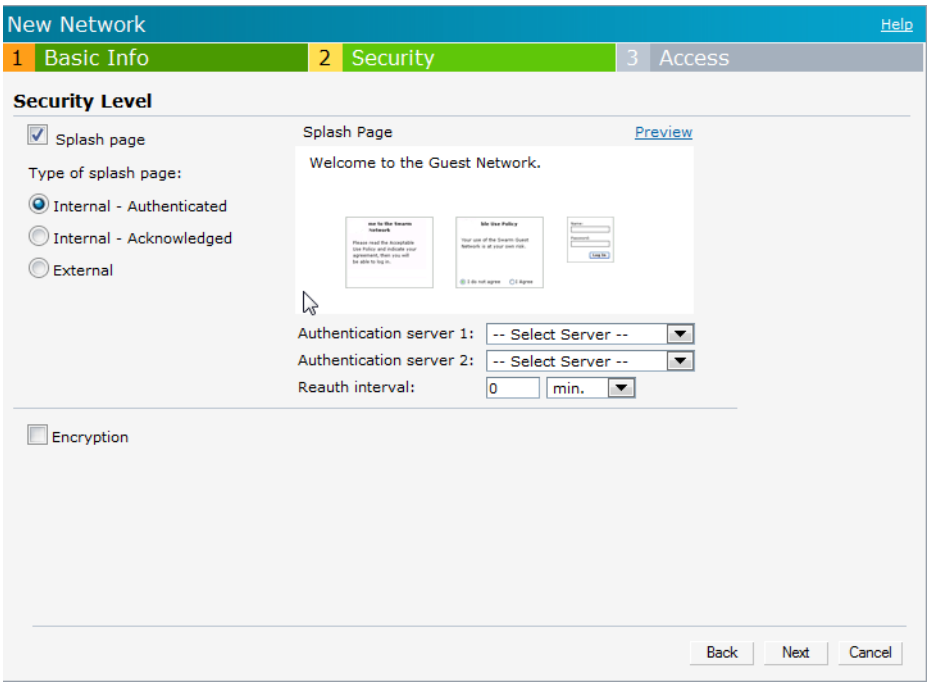
Configuring Internal Captive Portal with External Radius Server Authentication when Adding a Guest Network

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 Network** box opens.
2. In the **Basic Info** tab, perform the following:
   1. Enter a name for the network in the **Name (SSID)** text box.
   2. Select **Guest** and then click **Next.**
3. In the **Security** tab, select **Internal—Authenticated** under the splash page type.

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

Figure 68 *Configuring Internal Captive Portal with External Radius Server Authentication*



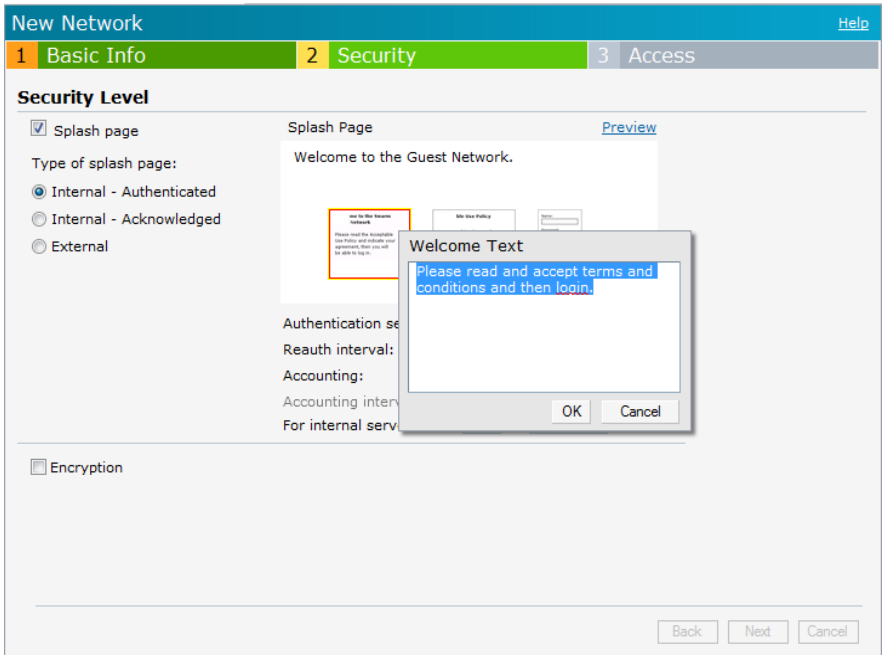
Customizing a Splash Page

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 will be 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** box for the network appears.
3. Click **Next** and perform the following steps in the **Security** tab:
    1. To change the color of the splash page, click the Splash page rectangle and select the required color from the Background Color palette.
    2. 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.
    3. 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 69 *Customizing a Splash Page*



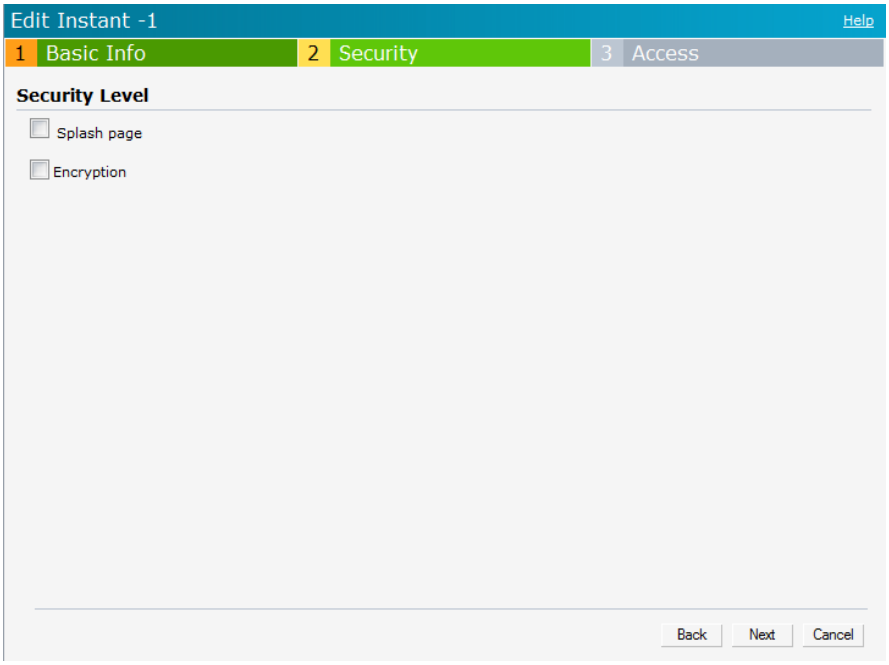
4. Click **Next** and then click **Finish.**

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** box for the network appears.
3. Click **Next** and clear the **Splash page** check box in the **Security** tab.

Figure 70 *Disabling Captive Portal Authentication*



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

External Captive Portal

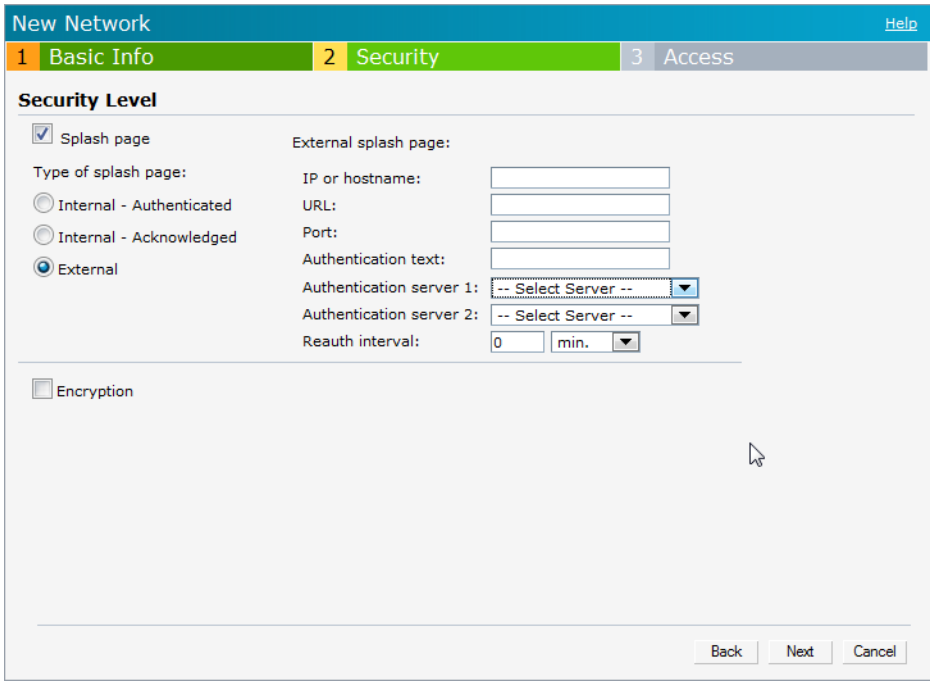
Dell Instant supports external captive portal authentication. The external portal can be in a cloud or on a server outside the enterprise network.

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 Network** box appears.
2. In the **Basic Info** tab, perform the following:
    1. Enter a name for the network in the **Name (SSID)** text box.
    2. Select **Guest** and click **Next.**
3. In the **Security** tab, click **External** and perform the following steps:
    1. Enter the IP address or the hostname in the **IP or hostname** text box.
    2. Enter the URL for the splash page in the **URL** text box.
    3. Enter the number of the port to be used for communicating with the external server in the **Port** text box.
    4. In the **Authentication** text box, enter the unique signature that the external server will return in the response after a successful authentication. The 'authentication text' is not mandatory.

Figure 71 *Configuring External Captive Portal when adding a Guest Network*



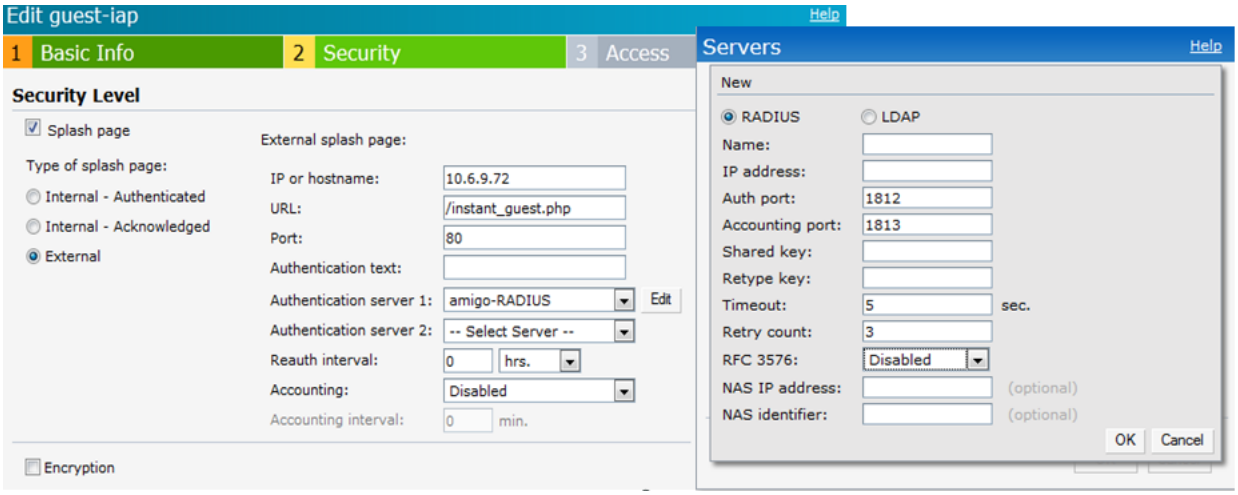
4. **Authentication server 1**: Select New and update the fields for the external RADIUS server to authenticate user credentials at runtime. Refer to "Configuring an External RADIUS Server" on page 79 for more details on server settings.
5. **Reauth interval**—When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients.
6. 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** box for the network appears.
3. Click **Next**, and click **External** and perform the following steps in the **Security** tab:
    1. Enter the IP address or the hostname in the **IP or hostname** text box.
    2. Enter the URL for the splash page in the **URL** text box.
    3. Enter the number of the port to be used for communicating with the external server in the **Port** text box.
    4. In the **Authentication** text box, enter the unique signature that the external server will return in the response after a successful authentication.

Figure 72 *Configuring External Captive Portal Authentication when Editing a Guest Network*



4. **Authentication server 1**: Click **Edit** to modify the external RADIUS servers settings. Refer to "Configuring an External RADIUS Server" on page 79 for more details on server settings.
5. **Reauth interval**—When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients.
6. **Accounting—**When enabled, the Access Points will post accounting information as RADIUS START and RADIUS STOP accounting records to the RADIUS server.
7. Click **Next** and click **Finish.**

External Captive Portal Authentication via Dell PowerConnect W-ClearPass GuestConnect

You can now configure Instant to point to Dell PowerConnect W-ClearPass GuestConnect as an external Captive Portal server. User authentication is performed by:

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

Creating a Web Login page in the Dell PowerConnect W-ClearPass GuestConnect

The Dell PowerConnect W-ClearPass GuestConnect Visitor Management Appliance provides a simple and personalized user interface through which operational staff can quickly and securely manage visitor network access. With Dell PowerConnect W-ClearPass GuestConnect, 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 Dell PowerConnect W-ClearPass GuestConnect Visitor Management Appliance you are able to provide a customized graphical login page for visitors accessing the network.

Refer to the RADIUS Services chapter in the **Dell PowerConnect W-ClearPass GuestConnect Deployment Guide** for information on setting up the Radius Web Login feature.

Configuring the RADIUS Server in Instant

To configure Instant to point to Dell PowerConnect W-ClearPass GuestConnect as an external Captive Portal server, perform the following steps:

1. Navigate to the **Networks** tab in the UI, click the **New** link. The **New Network** box appears.
2. In the **Basic Info** tab, perform the following steps:
   a. Type 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. In the **Security** tab, select **External** and update the following fields.
   a. Enter the IP address of the Dell PowerConnect W-ClearPass GuestConnect 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 Dell PowerConnect W-ClearPass GuestConnect RADIUS Web Login page. For example, if the Page Name is **aruba**, then the URL should be **/aruba.php** in the Instant UI.
   c. Enter the **Port** number (generally should be 80). The Dell PowerConnect W-ClearPass GuestConnect 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 79 to update the RADIUS server fields.
5. The new network appears in the **Networks** tab. Click the wireless network icon and select the new network.
6. Open any browser and type any URL. Instant redirects the URL to Dell PowerConnect W-ClearPass GuestConnect login page.
7. Login to the network with the username and password specified used while configuring the RADIUS server in step d.

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 that will not deter the determined intruder. It is recommended against the use of Mac based authentication.

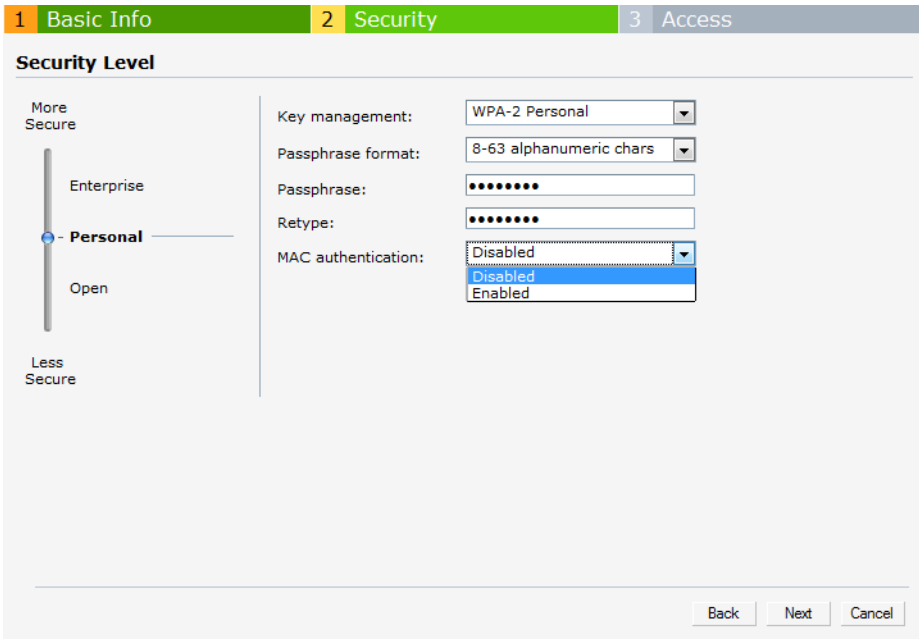
Configuring Mac Authentication

To enable Mac Authentication for a wireless network, perform the following steps:

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. The **Edit** box for the network appears.

3. Click **Next** in the **Basic Info** tab.
4. For a network with **Personal** or **Open** security level, select **Enabled** from the **Mac Authentication** drop-down list.
5. Select **New** from the **Authentication server 1** drop-down list perform the following steps:
   a. **Name:** Enter the name of the new external RADIUS server.
   b. **IP address**: Enter the IP address of the external RADIUS server.
   c. **Auth port:** Enter the authorization port number of the external RADIUS server. The port number is set to 1812 by default.
   d. **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
   e. **Shared key:** Enter a shared key for communicating with the external RADIUS server.
   f. **Timeout:** Specify a number between1 and 30 seconds. User will be disconnected after this time. The default value is 5 seconds.
   g. **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.
   h. **RFC 3576:** When enabled, the Access Points will 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.
   i. **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.
   j. **NAS identifier:** Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
   5. Click **OK** to continue.

Figure 73 *Configuring Mac Authentication*



6. Click **Next** and click **Finish.**

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.

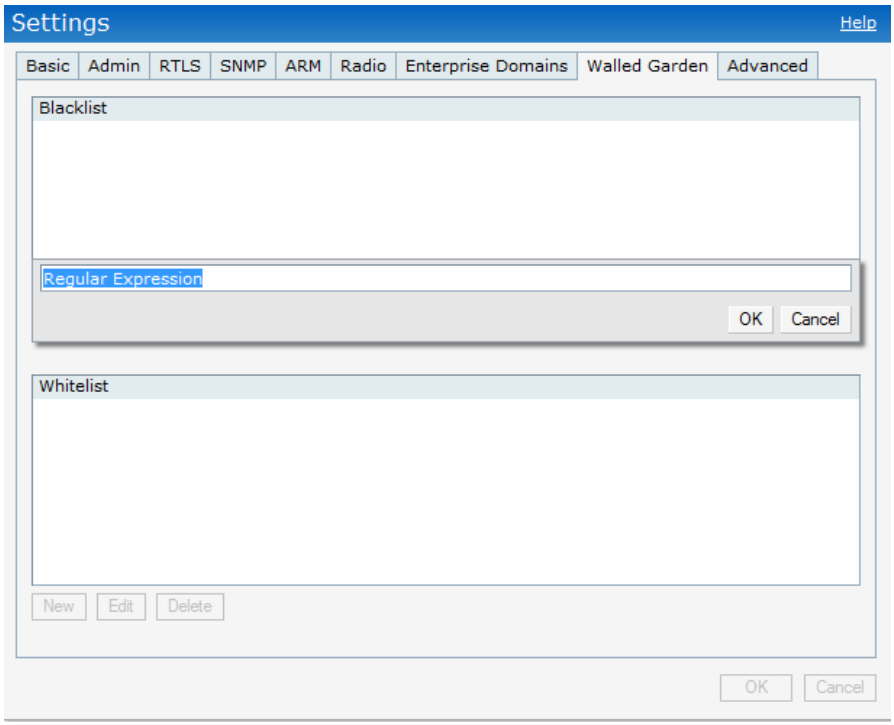
Creating Walled Garden Access

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 74 *Walled Garden*



To create a Walled Garden access:

1. In the **Settings** window, select **Walled Garden**.
2. Click **New** and enter the domain name or URL in the **Whitelist** field. This will allow access 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 will only allow subset of www.apple.com site corresponding to path /library/test/*
   - favicon.ico will allow 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** field. This prevents unauthenticated users from viewing specific websites. When a URL specified in blacklist is accessed by an unauthenticated user, Instant AP will send an HTTP 403 response to the client with a simple error message.
4. Select the domain name/URL and click **Edit** to modify or **Delete** to remove it from the list.
5. Click **OK** to apply the changes.

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 Instant supports the following certificate files:

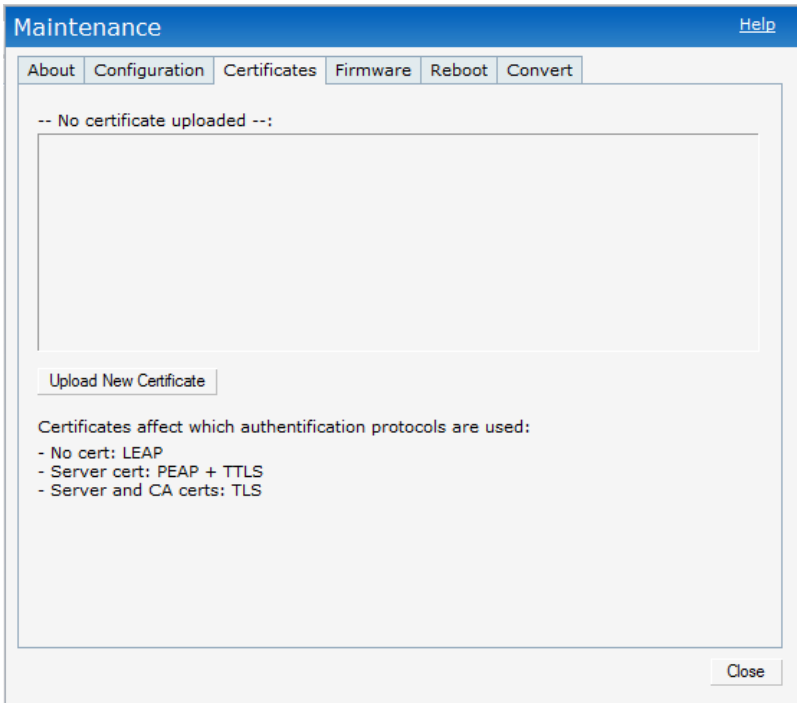
- Server certificate for EAP-PEAP i.e. PKCS12
- PEM support for EAP-PEAP and TLS termination
- DER i.e. CA Certs for TLS termination

Loading Certificates

To load a certificate, perform the following steps:

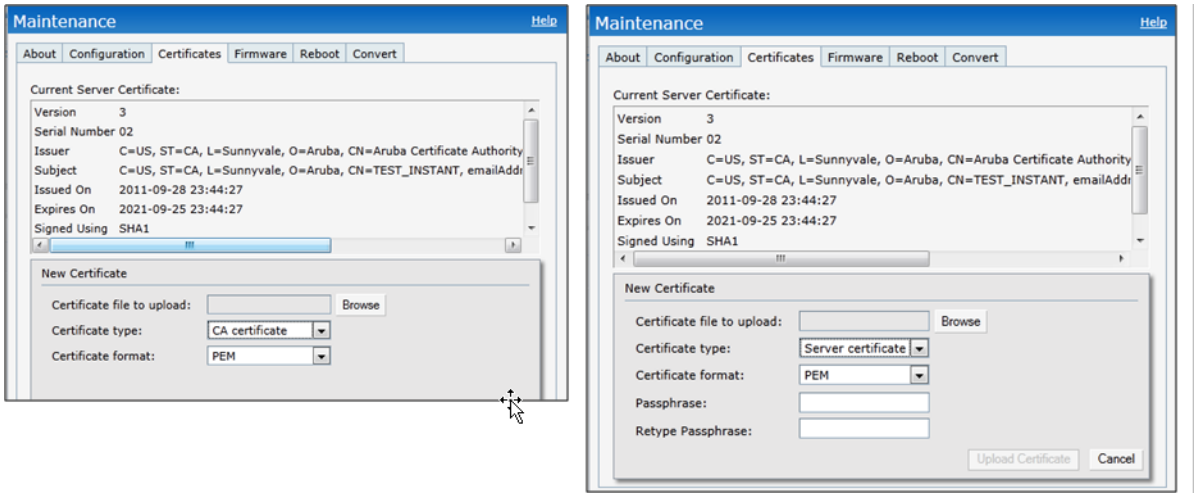
1. Navigate to the **Maintenance > Certificates** page.

Figure 75 *Loading Certificates*



2. Click **Upload New Certificate** and the **New Certificate** window will appear.

Figure 76 *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.
6. Click **Browse** and select the appropriate certificate file, and click **Upload Certificate**.

Chapter 9

Encryption

Encryption Types Supported in Dell 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 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. It is recommended 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. It is recommended 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. It is recommended that all devices 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

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 was taking 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 11 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 as 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 login 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 when compared to 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 11 *WPA and WPA2 Features*

Certification	Authentication	Encryption
WPA	• PSK • IEEE 802.1X with Extensible Authentication Protocol (EAP)	Temporal Key Integrity Protocol (TKIP) with message integrity check (MIC)
WPA2	• PSK • IEEE 802.1X with EAP	Advanced Encryption Standard -- Counter Mode with Cipher Block Chaining Message Authentication Code (AESCCMP)

Recommended Authentication and Encryption Combinations

Table 12 summarizes the recommendations for authentication and encryption combinations that should be used in Wi-Fi networks.

Table 12 *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).

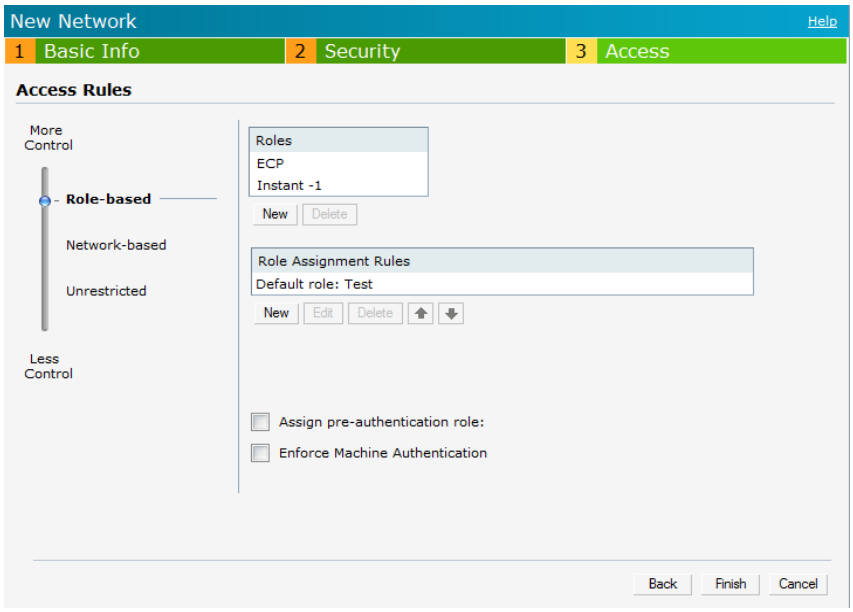
Every client in an Dell Instant network is associated with a user role, which determines the client's network privileges, how often it must re-authenticate, and which bandwidth contracts are applicable.

This chapter describes creating and assigning roles using the Instant UI.

User Roles

This section describes how to create a new user role.

Figure 77 *Access Tab—Instant User Role Settings*



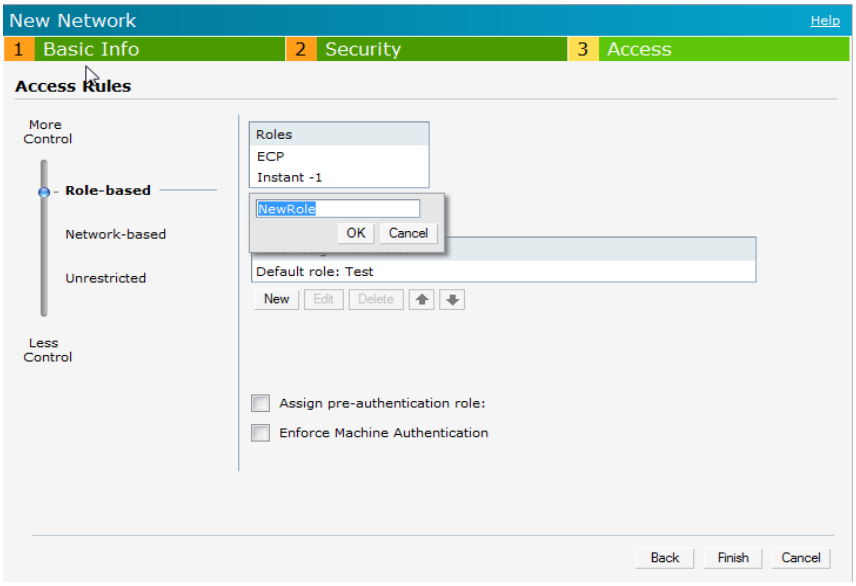
Creating a New User Role

To create a new user role, perform the following steps:

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 **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate values in the **Security** tab.
4. Click **Next**. The **Access** tab appears.
5. Select **Role-based** from the scroll bar in the left.

6. Click the **New** button. The **New Rule** box appears. Enter the name of the new user role in this box.

Figure 78 *Creating a New User Role*



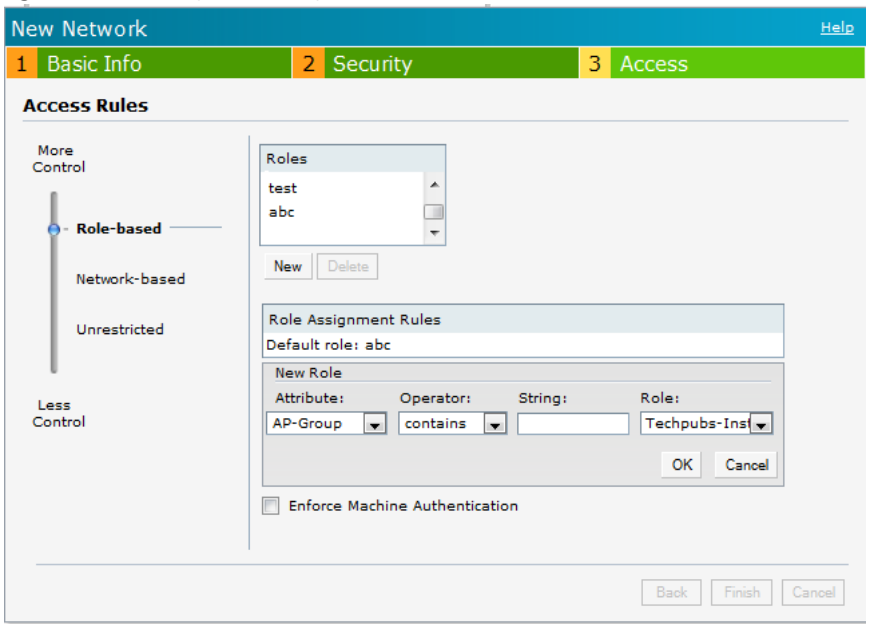
7. Click **OK**. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To create new access rules, see "Example Access Rules" on page 105.
8. To delete a user role, select the user role and click the **Delete** button.

Creating Role Assignment Rules

To create role assignment rules for the user role, perform the following steps:

1. Click **New** button in the Role Assignment Rules table. The default user role is the newly created user role.
2. Select the attribute from the **Attribute** drop-down list. To view the list of supported attributes, see "List of supported VSA's" on page 81.
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**.

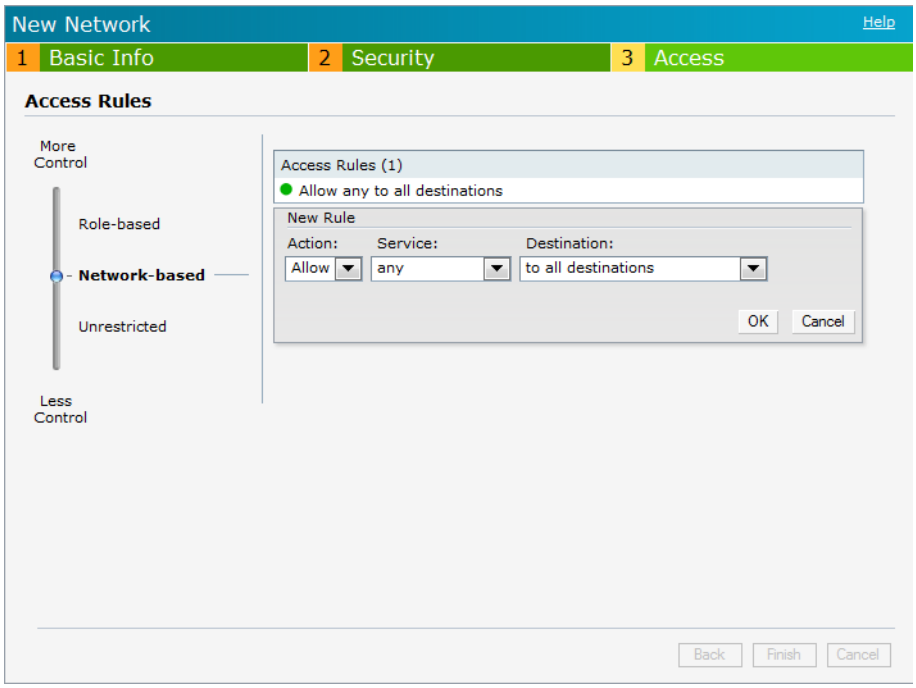
Figure 79 *Creating Role Assignment Rules*



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

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

Figure 80 *Access Tab—Instant Firewall Settings*



Service Options

Table 13 lists a sample set of service options available in the Instant UI. You can allow or deny access to any or all of these services depending on your requirements.

Table 13 *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 other option, enter the appropriate ID.
adp	Application Distribution Protocol
bootp	Bootstrap Protocol

Table 13 *Network Service Options (Continued)*

Service	Description
dhcp	Dynamic Host Configuration Protocol
dns	Domain Name Server
esp	Encapsulating Security Payload
ftp	File Transfer Protocol
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
smb-tcp	Server Message Block-Transmission Control Protocol
smb-udp	Server Message Block-User Datagram Protocol
smtp	Simple mail transfer protocol

Table 13 *Network Service Options (Continued)*

Service	Description
snmp	Simple network management protocol
snmp-trap	Simple network management protocol-trap
svp	Software Validation Protocol
tftp	Trivial file transfer protocol

Destination Options

Table 14 lists the destination options available in the Instant UI. You can allow or deny access to any or all of these destinations depending on your requirements.

Table 14 *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.

Example Access Rules

This section provides procedures to create the following access rules.

- Allow TCP service to a particular network
- Allow PoP3 service to a particular server
- Deny FTP service except to a particular server
- Deny bootp service except to a particular network

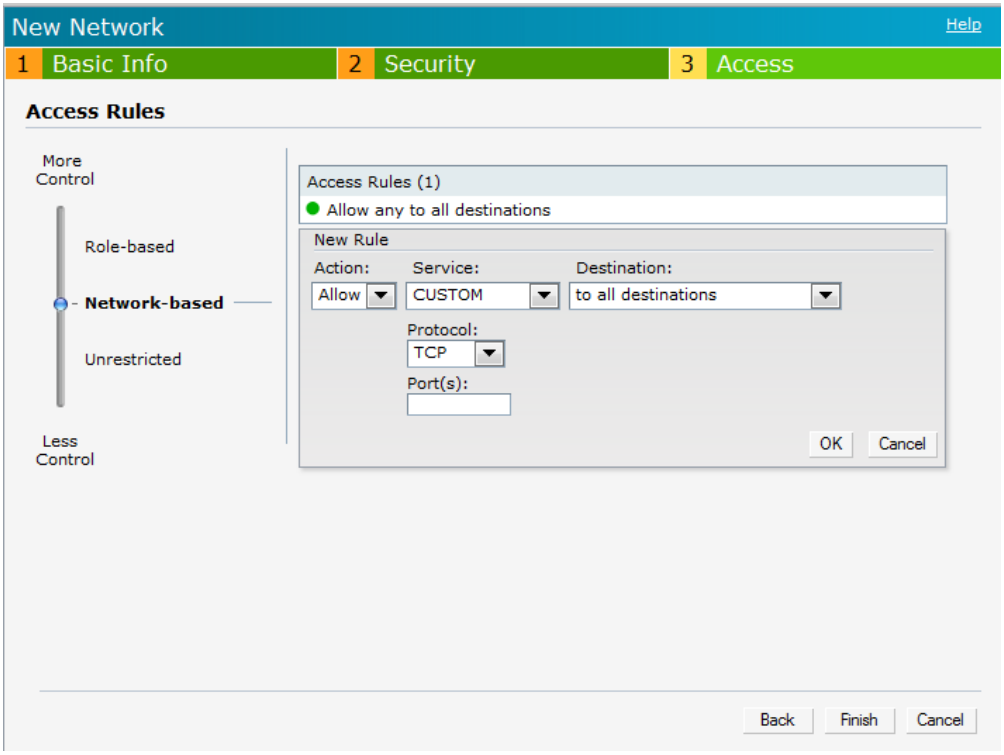
Allow TCP service to a particular network

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 **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate values in the **Security** tab.
4. 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, perform the following steps:
   a. Click **New**, the **New Rule** box 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 81 *Defining Rule—Allow TCP Service to a Particular Network*



e. Click **OK**.

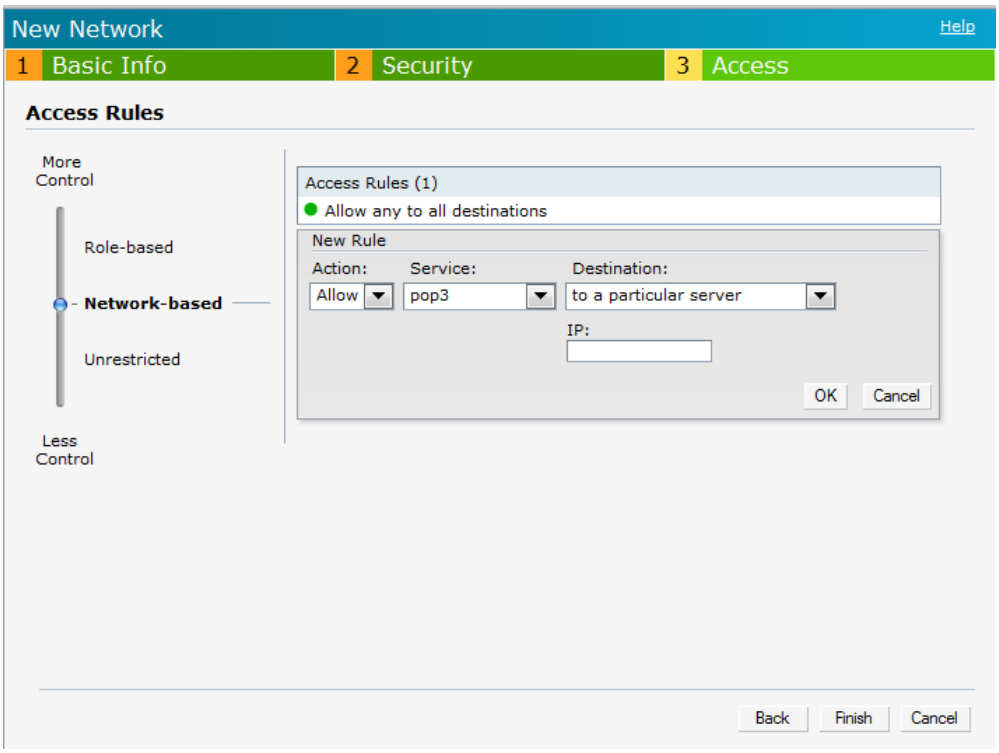
5. Click **Finish**.

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 **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate security levels using the slider button in the **Security** tab.
4. 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, perform the following steps:
   1. Click **New**, the **New Rule** box appears.
   2. Select **Allow** from the **Action** drop-down list.
   3. Select **pop3** from the **Service** drop-down list.
   4. Select **to a particular server** from the **Destination** drop-down list and enter appropriate IP address in the IP text box.
   5. Click **OK**.

5. Click **Finish**.

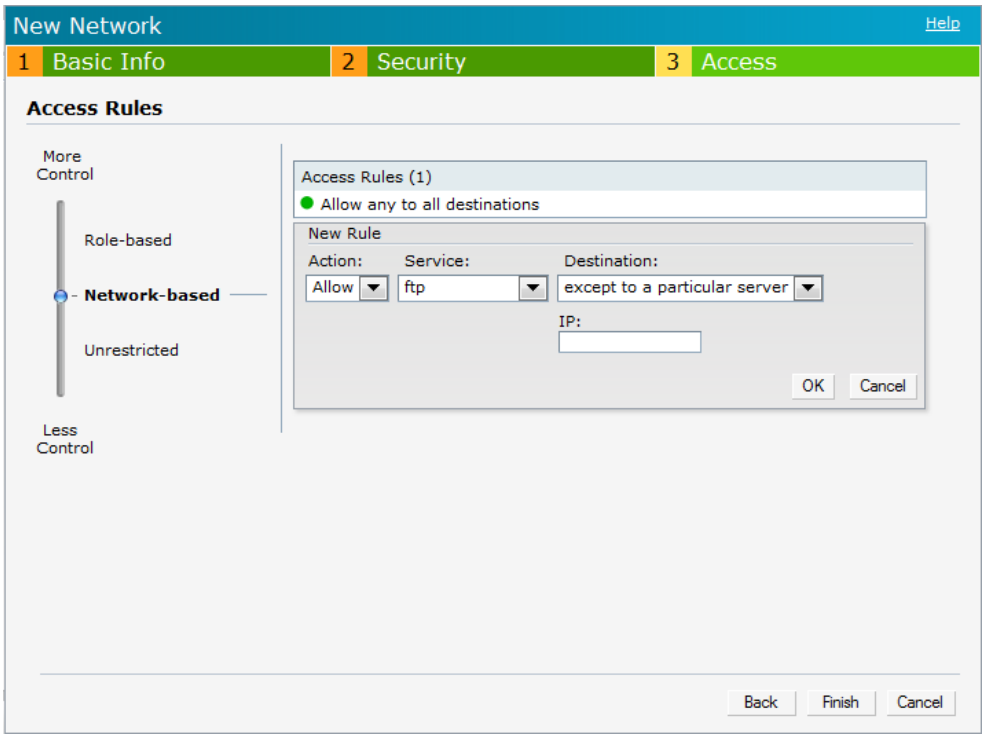
Figure 82 *Defining Rule—Allow POP3 Service to a Particular Server*



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 **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate security levels using the slider button in the **Security** tab.
4. 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, perform the following steps:
   1. Click **New**, the **New Rule** box appears.
   2. Select **Deny** from the **Action** drop-down list.
   3. Select **ftp** from the **Service** drop-down list.
   4. Select **except to a particular server** from the **Destination** drop-down list and enter appropriate IP address in the **IP** text box.
   5. Click **OK**
5. Click **Finish**

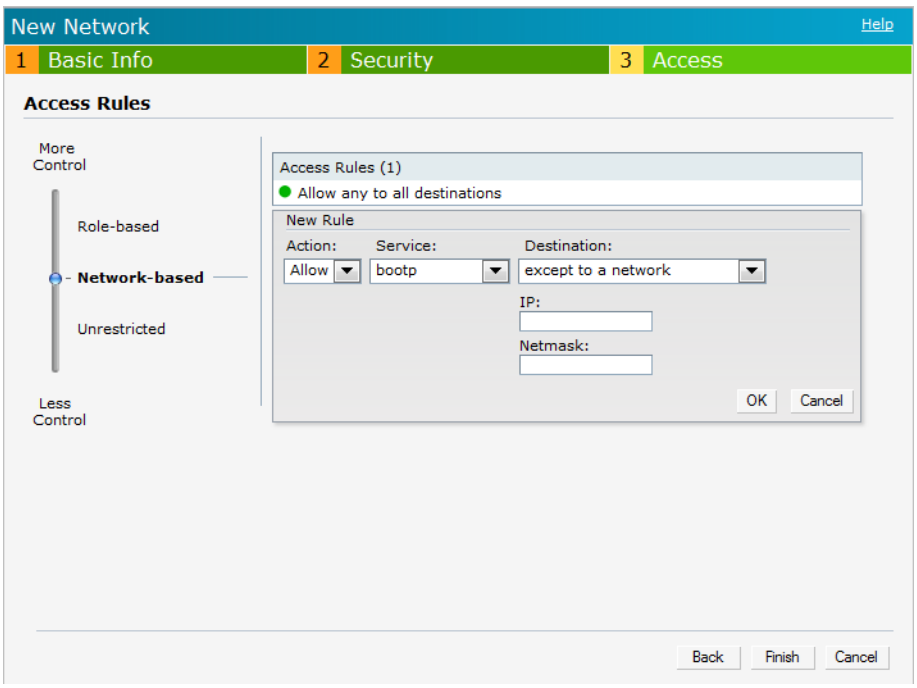
Figure 83 *Defining Rule—Deny FTP Service Except to a Particular Server*



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 **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate security levels using the slider button in the **Security** tab.
4. 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, perform the following steps:
   1. Click **New,** the **New Rule** box appears.
   2. Select **Deny** from the **Action** drop-down list.
   3. Select **bootp** from the **Service** drop-down list.
   4. Select **except 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.
   5. Click **OK**.
5. Click **Finish**.

Figure 84 *Defining Rule—Deny bootp Service Except to a Particular Network*



Chapter 12

Content Filtering

Dell Instant uses OpenDNS to implement the Content Filtering feature. OpenDNS is a Domain Name System (DNS) resolution service provider. It offers features such as misspelling correction, phishing protection, and integrated web content filtering. For more information on OpenDNS, refer to **opendns.com/.**

The Content Filtering feature allows you to create internet access policies that allow or deny user access to websites based on the 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 OpenDNS.

NOTE: Regardless of whether content filtering is disabled or enabled, **instant.dell-pcw.com** is always resolved internally on Instant.

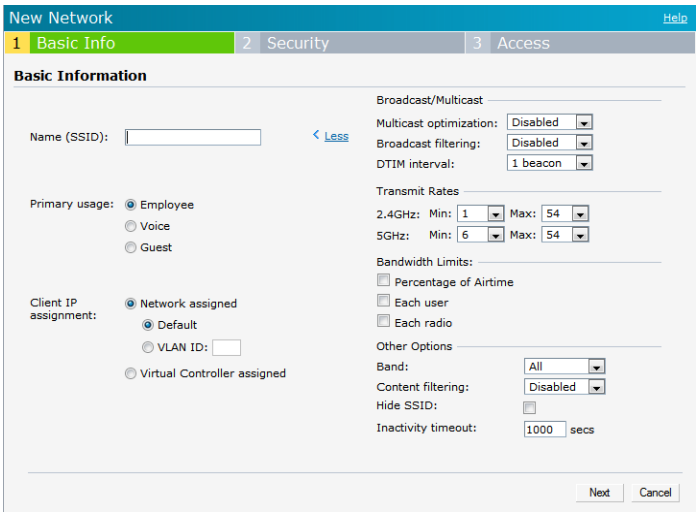
Enabling Content Filtering

To enable content filtering per SSID, perform the following steps:

1. Click **New** in the Networks tab and then click **More** to view the options
2. In the **Other Options** field, select **Enabled** from the **Content Filtering** drop-down list and click **Next** to continue.

NOTE: On startup, the IAP learns the default domain name via DHCP. This domain name also applies for Content Filtering. Go to **Settings > Basic > Domain name** to configure a domain name for a virtual controller assigned network. This domain name applies for Content Filtering. When you select Virtual Controller assigned option, the client gets the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the IAPs for the wireless clients, this VLAN is called "virtual controller assigned networks". The Virtual Controller NATs all traffic that passes out of this interface. See "Employee Network" on page 39 to select Virtual Controller assigned option and Chapter 7, "Virtual Controller" on page 75 for DHCP server configuration.

Figure 85 *Enabling Content Filtering*

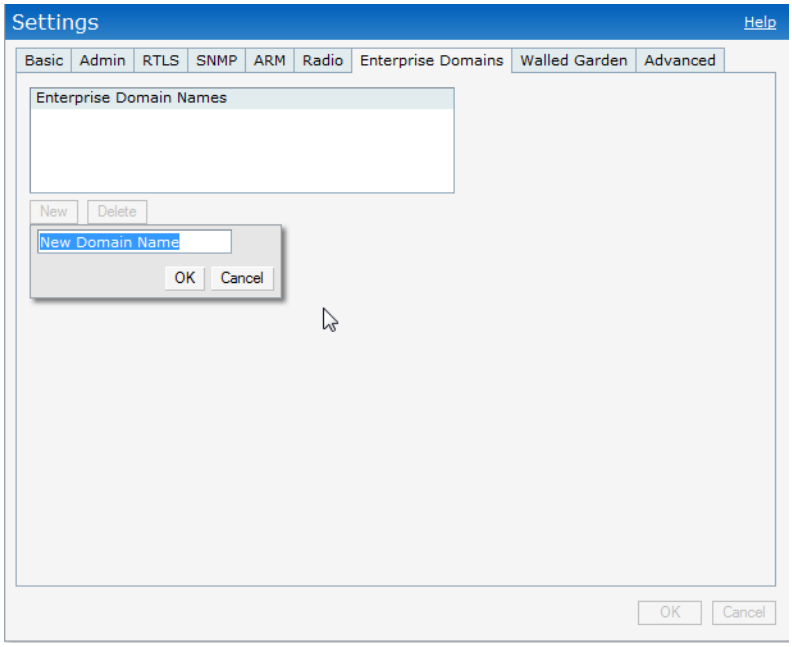


The content filtering configuration applies to all the IAPs in the Dell Instant network and the service is enabled or disabled globally across all the wireless networks that are configured in the Dell Instant.

Enterprise Domains

The Enterprise Domain Names displays all the DNS domain names 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 OpenDNS.

Figure 86 *Enterprise Domains*



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

1. Navigate to **Settings > Enterprise Domains** in the UI.
2. Click **New** and enter a New Domain Name or select the domain and click **Delete** to remove from the list.
3. Click **OK** to apply the changes.

Chapter 13

OS Fingerprinting

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

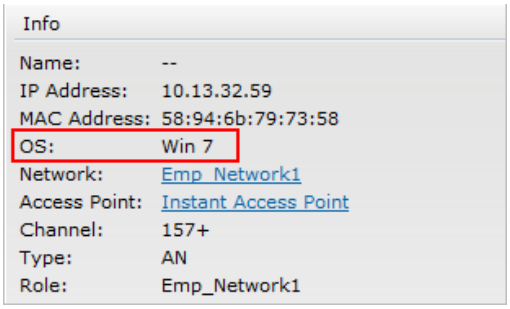
- Identifying rogue clients—Helps to identify clients that are running on forbidden operating systems.
- Identifying outdated operating systems—Helps to locate outdated and unexpected OS in the company network.
- Locating and patching vulnerable operating systems—Assists in locating and patching specific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

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

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

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

Figure 87 *OS Fingerprinting*



Chapter 14

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 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 Instant.

Channel or Power Assignment

This feature automatically assigns channel and power settings for all the 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 the IAP that is supporting an active voice call from scanning for other channels in the RF spectrum. The IAP resumes scanning when no more active voice calls are present on that 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 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 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 5Ghz**—If you configure the IAP to use prefer-5GHz band steering mode, the IAP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts.
- **Force 5Ghz**—When the IAP is configured in force-5GHz band steering mode, the IAP will try to force 5Ghz-capable IAPs to use that radio band.
- **Balance Bands**—In this band steering mode, the IAP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5Ghz band has

more channels than the 2.4Ghz band, and that the 5Ghz channels operate in 40MHz while the 2.5Ghz band operates in 20MHz.

Airtime Fairness Mode

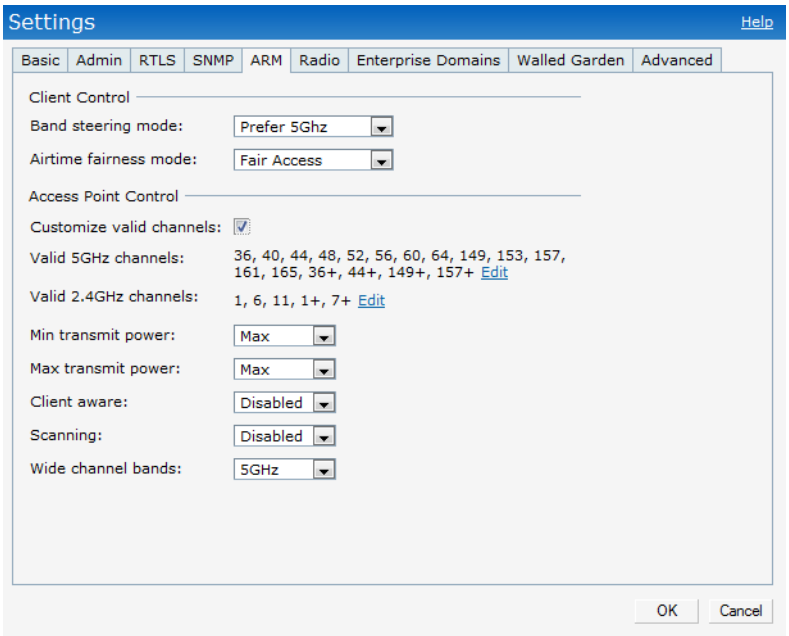
This feature provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system, thus delivering uniform performance to all clients. This feature prevents some clients from monopolizing resources at the expense of other clients.

Airtime Fairness Modes

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 contracts are not enforced
- Fair Access—Allocates Airtime evenly across all the clients
- Preferred Access—Allocates Airtime to all the clients but preference is for higher performing clients

Figure 88 *Airtime fairness mode*



Customize valid channels

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

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 will be reduced to the highest supported power setting.

The default value is18 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 will be reduced to the highest supported power setting.

Default value: 127 dBm

Client Aware

When **Enabled**, Adaptive Radio Management (ARM) will 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 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 IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and will report everything it sees to the 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, an 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 IAP RF environment. Each IAP gathers other metrics on their ARM-assigned channel to provide a snapshot of the current RF health state.

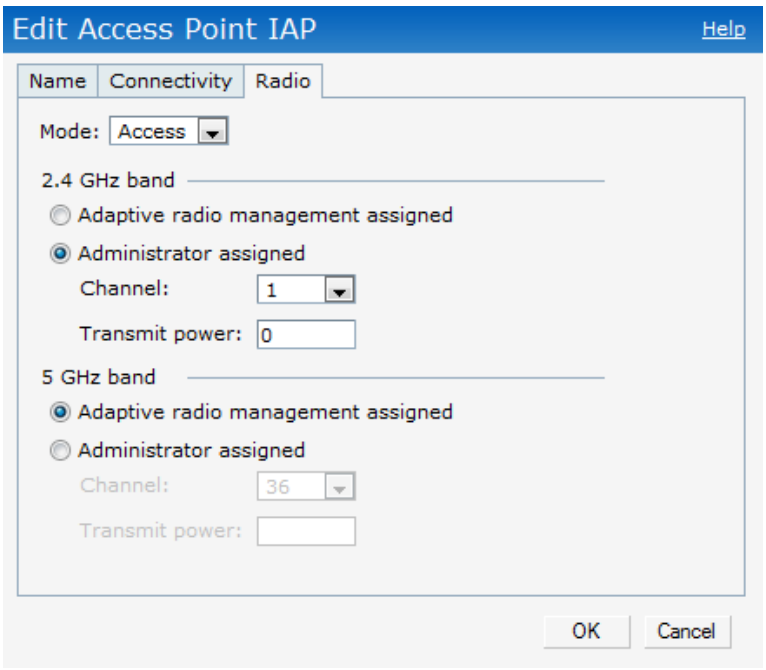
Configuring Administrator Assigned Radio Settings for IAP

ARM is enabled on Dell Instant by default. It automatically assigns appropriate channel and power for the IAPs.

To manually configure radio settings using the Instant UI, perform the following steps:

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** box appears.
3. Click the **Radio** tab.

Figure 89 *Configuring Administrator Assigned Radio Settings for IAP*



4. Select the **Access** Mode from the drop-down list.

NOTE: Select the Monitor Mode to configure the specific IAP in the Instant network in Monitor Mode and click OK.

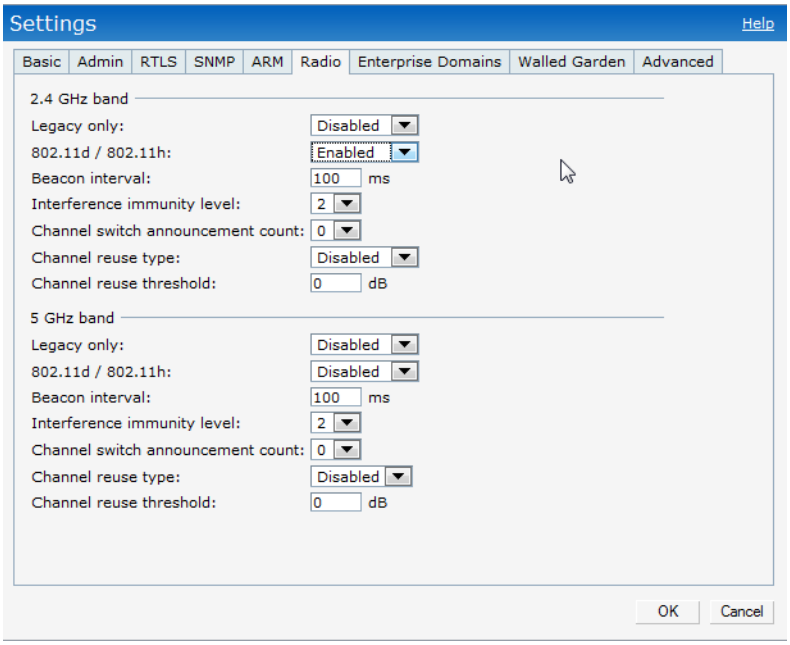
5. Select **Administrator assigned** in **2.4 GHz** and **5 GHz** band sections.
6. Select appropriate channel number from the **Channel** drop-down list for both **2.4 GHz** and **5 GHz** band sections.
7. Enter appropriate transmit power value in the **Transmit power** text box in **2.4 GHz** and **5 GHz** band sections.
8. Click **OK.**

Configuring Radio Profiles in Instant

Dell 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 Instant's radio attributes for the 2.4GHz and 5GHz frequency bands.

Figure 90 *Radio Profile*



1. Navigate to **Settings > Radio** in the UI.
2. Configure the radio settings described in Table 15 for bands—2.4GHz and 5GHz.

Table 15 *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 500mps) for the 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.

Table 15 *Radio Profile Configuration Parameters (Continued)*

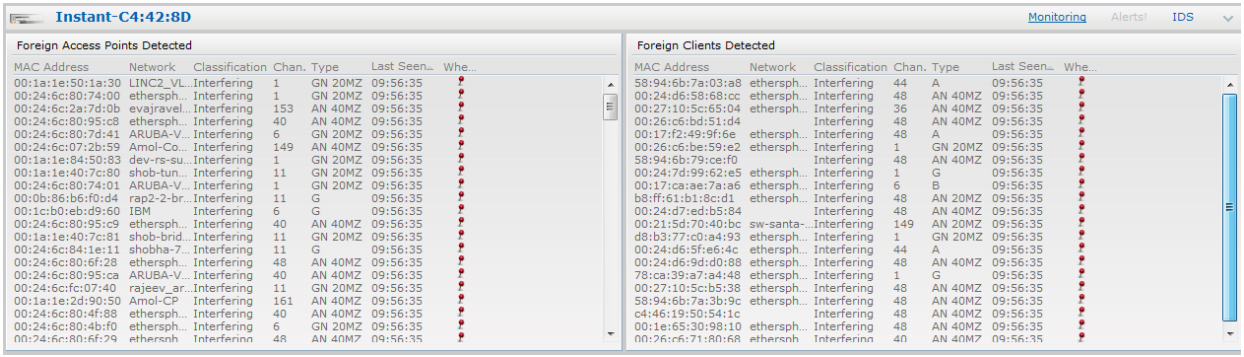
Parameter	Description
Interference immunity level	Select to increase the immunity level to improve performance in high-interference environments. The default immunity level is 2. NOTE: Increasing the immunity level makes the AP slightly "deaf" to its surroundings, causing the AP to lose a small amount of range. • Level 0: no ANI adaptation. • Level 1: Noise immunity only. This level enables power-based packet detection by controlling the • amount of power increase that makes a radio aware that it has received a packet. • Level 2: Noise and spur immunity. This level also controls the detection of OFDM packets, and is the • default setting for the Noise Immunity feature. • Level 3: Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4Ghz appliances such as cordless phones. • Level 4: Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. • Level 5: The AP completely disables PHY error reporting, improving performance by eliminating the time the IAP would spend on PHY processing.
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	When set to Dynamic, the access point, when busy, will automatically adjust its Clear Channel Assessment (CCA) threshold to accommodate transmissions to the most distant associated client. When set to Static, the access point will set its CCA threshold to the value specified in Channel reuse threshold.
Channel reuse threshold	When set to Static, this value specifies the tolerable interference that must be maintained.

Intrusion Detection System (IDS) is a feature that monitors the network for the presence of unauthorized IAPs and clients. It also logs information about the unauthorized 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 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.

Figure 91 *Intrusion Detection*



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 IAP.

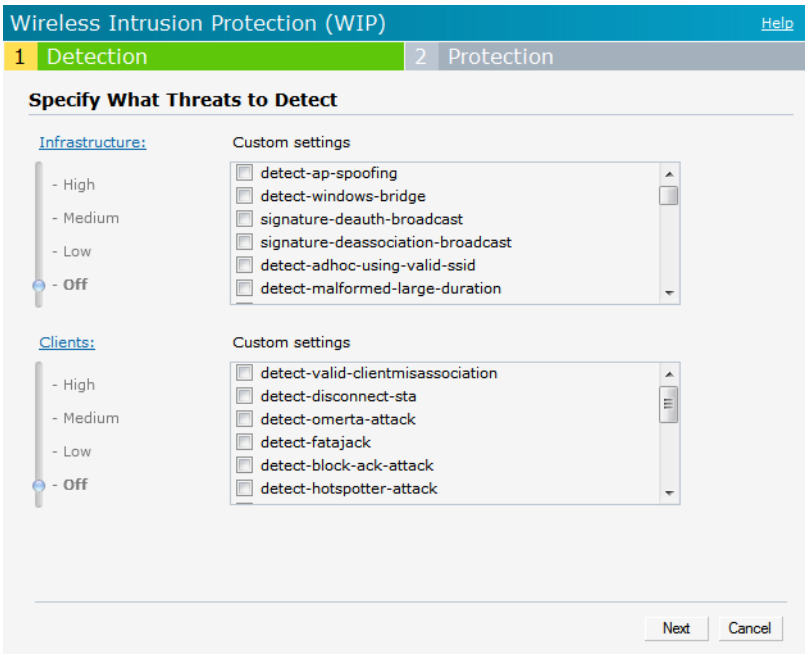
An administrator can configure the following five main options.

- 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: To prevent unauthorized stations from connecting to your 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 92).

Figure 92 *Wireless Intrusion Protection—Detection*



The following table describes the detection policies that are enabled in Infrastructure Detection Custom settings box.

Table 16 *Infrastructure Detection Policies*

Detection Level	Detection Policy
Off	Rogue Classification
Low	• Detect AP Spoofing • Detect Windows Bridge • IDS Signature: Deauthentication Broadcast • IDS Signature: Disassociation Broadcast
Medium	• Detect Adhoc networks using VALID SSID: Valid SSID list will be auto-configured based on Instant AP configuration • Detect Malformed Frame: Large Duration

Table 16 *Infrastructure Detection Policies* (Continued)

Detection Level	Detection Policy
High	• Detect AP Impersonation • Detect Adhoc Networks • Detect Valid SSID Misuse • Detect Wireless Bridge • Detect 802.11 40MHz intolerance settings • Detect Active 802.11n Greenfield Mode • Detect AP Flood Attack • Detect Client Flood Attack • Detect Bad WEP • Detect CTS Rate Anomaly • Detect RTS Rate Anomaly • Detect Invalid Address Combination • Detect Malformed Frame: HT IE • Detect Malformed Frame: Association Request • Detect Malformed Frame: Auth • Detect Overflow IE • Detect Overflow EAPOL Key • Detect Beacon Wrong Channel • Detect devices with invalid Mac OUI

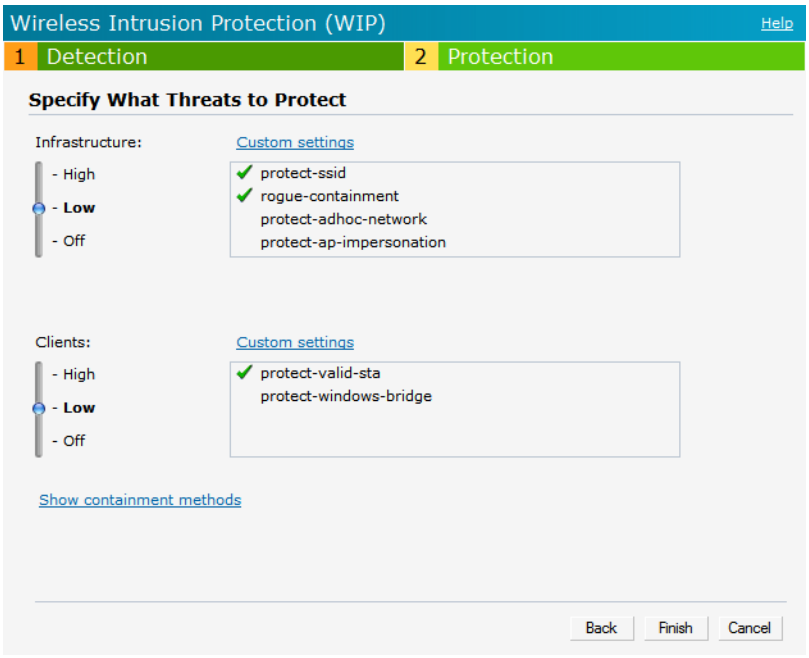
The following table describes the detection policies that are enabled in Client Detection Custom settings box.

Table 17 *Client Detection Policies*

Detection Level	Detection Policy
Off	All detection policies are disabled.
Low	• Detect Valid Station Mis association
Medium	• Detect Disconnect Station Attack • Detect Omerta Attack • Detect FATA-Jack Attack • Detect Block ACK DOS • Detect Hotspotter Attack • Detect unencrypted Valid Client • Detect Power Save DOS Attack
High	• Detect EAP Rate Anomaly • Detect Rate Anomaly • Detect Chop Chop Attack • Detect TKIP Replay Attack • IDS Signature:Air Jack • IDS Signature: ASLEAP

Three levels of detection can be configured in the WIP Protection page—**Off**, **Low**, and **High** (as shown in Figure 93).

Figure 93 *Wireless Intrusion Protection—Protection*



The following table describes the detection policies that are enabled in Infrastructure Protection Custom settings box.

Table 18 *Infrastructure Protection Policies*

Detection Level	Detection Policy
Off	All detection policies are disabled
Low	• Protect SSID – Valid SSID list should be auto derived from Instant configuration • Rogue Containment
High	• Protect from Adhoc Networks • Protect AP Impersonation

The following table describes the detection policies that are enabled in Client Protection Custom settings box.

Table 19 *Client Protection Policies*

Detection Level	Detection Policy
Off	All detection policies are disabled
Low	• Protect Valid Station
High	• Protect Windows Bridge

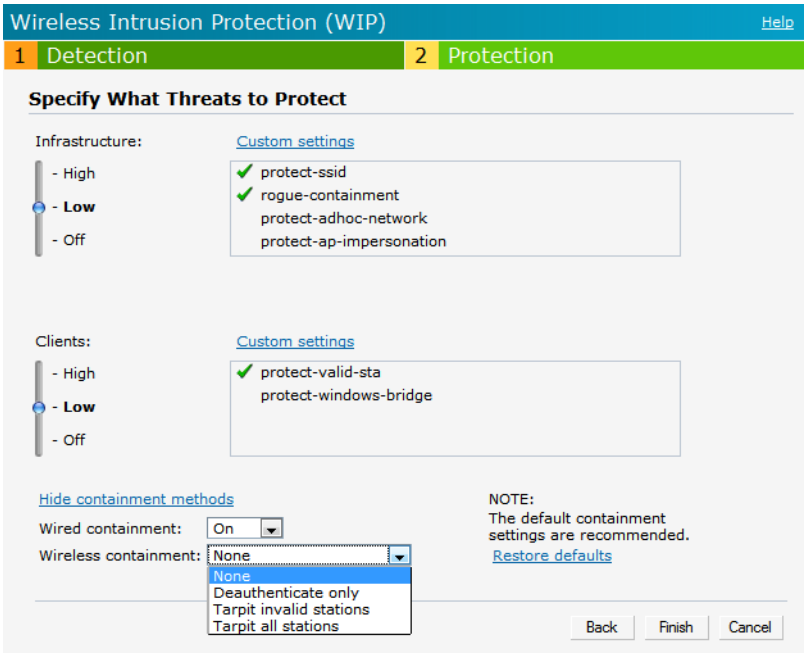
Containment Methods

You can enable wired and wireless containments to prevent unauthorized stations from connecting to your Instant network.

Instant supports the following types of containment mechanisms:

- Wired containment—When enabled, Dell Access Points will generate ARP packets on the wired network to contain wireless attacks.
- Wireless containment- When enabled, the system will attempt 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 94 *Containment Methods*



Chapter 16

SNMP

Dell Instant supports versions 1, 2c, and 3 of Simple Network Management Protocol (SNMP) for reporting purposes only. In other words, SNMP cannot be used for setting values in an Dell system in the current IAP.

SNMP Parameters for IAP

You can configure the following parameters for IAP.

Table 20 *SNMP Parameters for IAP*

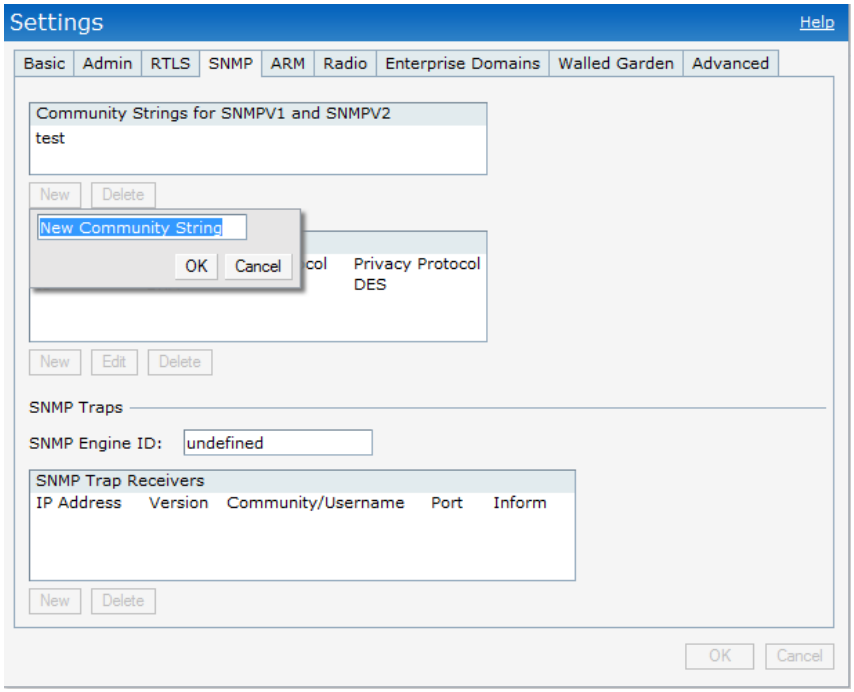
Field	Description
Community Strings for SNMPV1 and SNMPV2	An SNMP Community string is a text string that acts as a password, and is used to authenticate messages sent between the Virtual Controller and the SNMP agent.
If you are using SNMPv3 to obtain values from the Dell Instant, you can configure the 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: • MD5: HMAC-MD5-96 Digest Authentication Protocol • SHA: HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption).
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**.

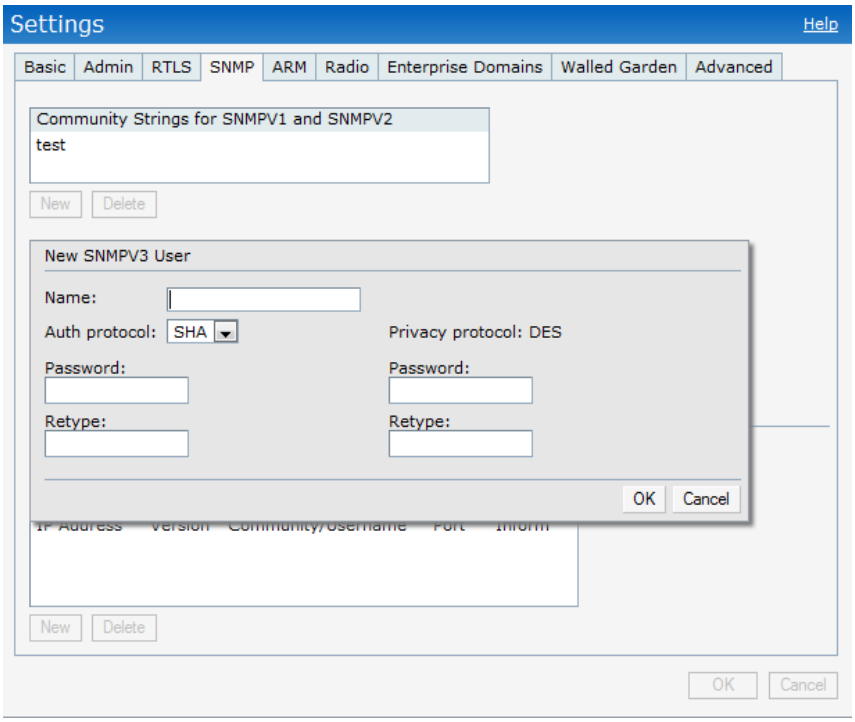
Figure 95 *Creating Community Strings for SNMPV1 and SNMPV2*



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** tex box and retype the password in the **Retype** tex 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.**
9. To edit the details for a particular user, select the user and click **Edit**.
10. To delete a particular user, select the user and click **Delete**.

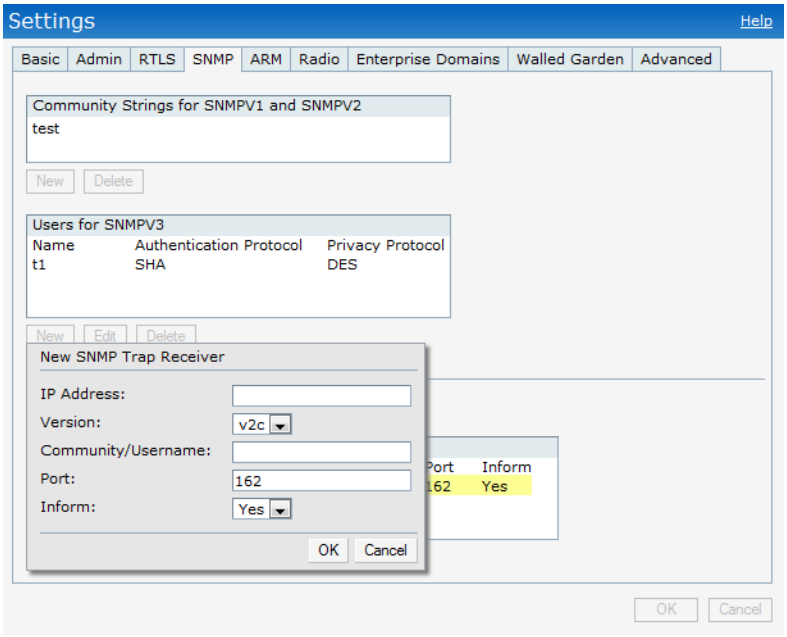
Figure 96 *Creating Users for SNMPV3*



SNMP Traps

Dell Instant supports the configuration of external trap receivers in the Instant UI. Only the IAP acting as the Virtual Controller will generate traps. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

Figure 97 *SNMP Traps*



To configure an SNMP trap receiver, follow this procedure.

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 PowerConnect W-Series-specific management information bases (MIBs) describe the objects that can be managed using SNMP. See the *Dell PowerConnect W-Series Instant Access Point MIB Reference Guide* for information about the Dell PowerConnect W-Series and Aruba MIBs and SNMP traps.

Chapter 17

Airwave Integration and Management

Dell PowerConnect W-AirWave is a solution for managing rapidly changing wireless networks. The easy-to-use interface and user-centric approach lets you to easily solve any connectivity issues. It allows you to efficiently and remotely manage and monitor enterprise wireless LAN. It allows you to monitor and change wireless LAN settings, generate compliance reports, locate users and IAPs, and diagnose problems from any Internet connection. Dell IAPs communicate with AirWave using the HTTPS protocol. This allows an AirWave server to be deployed in the cloud across a NAT device such as a router.

AirWave Features

This section describes the AirWave features that are available in the Dell Instant network.

Image Management

AirWave allows updating the firmware 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 also schedules the firmware updates such that updating is completed without the necessity 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 can set desired firmware preference per group of devices.

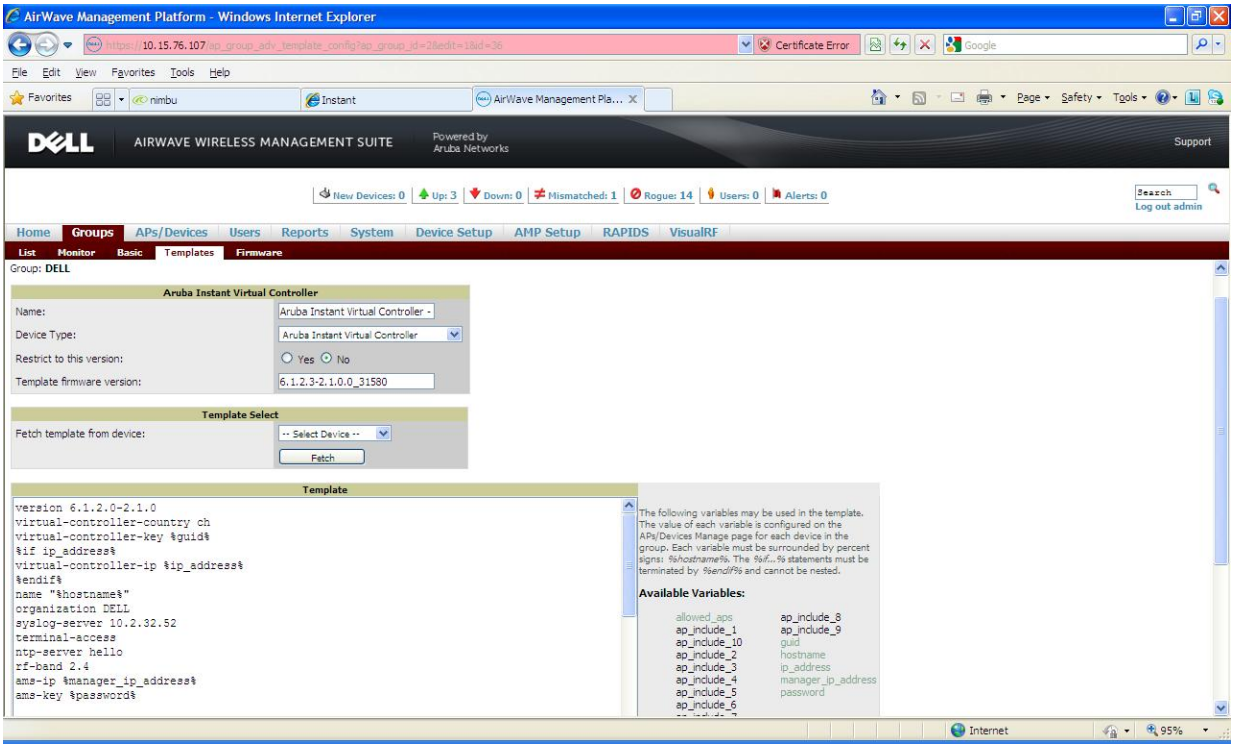
IAP and Client Monitoring

AirWave allows you to find any 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

AirWave automatically creates a configuration template based on any of the existing IAPs, and it applies that template across the network as shown in Figure 98. 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 98 *Template Based Configuration*



Trending Reports

AirWave saves up to two years 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

AirWave provides advanced, rules-based rogue classification. It automatically detects rogue APs irrespective of their location in the network. It prevents authorized IAPs from being detected as rogue IAPs. It tracks and correlates the IDS events to provide a complete picture of network security.

Wireless Intrusion Detection System (WIDS) Event Reporting to Airwave

Airwave supports WIDS Event Reporting which is provided by Dell Instant. This includes WIDS classification integration with RAPIDS (Rogue Access Point Detection Software) module. RAPIDS is a powerful and easy-to-use tool for automatic detection of unauthorized wireless devices, supports multiple methods of rogue detection and uses authorized wireless APs to report other devices within range.

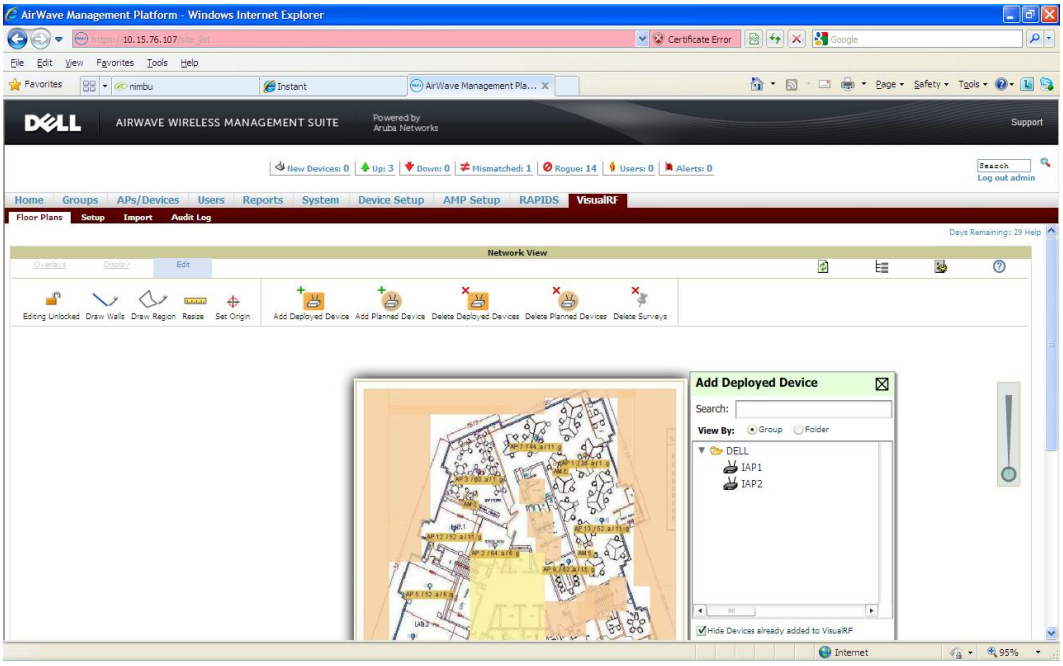
The WIDS report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours, and provides links to support additional analysis or configuration in response.

RF Visualization support for Dell Instant

Airwave supports RF visualization for Dell Instant. The VisualRF module is an add-on to the AirWave Wireless Management Suite that 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 99 *Adding an IAP in VisualRF*



Configuring AirWave

This section describes how to configure AirWave. Before configuring the AirWave, you need the following:

- IP address of the AirWave server.
- Shared key for service authorization—This is assigned by the AirWave administrator.

Creating your Organization String

The Organization String is a set of colon-separated strings created by the AirWave administrator to accurately represent the deployment of each Dell Instant system. This string is entered into the Dell 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

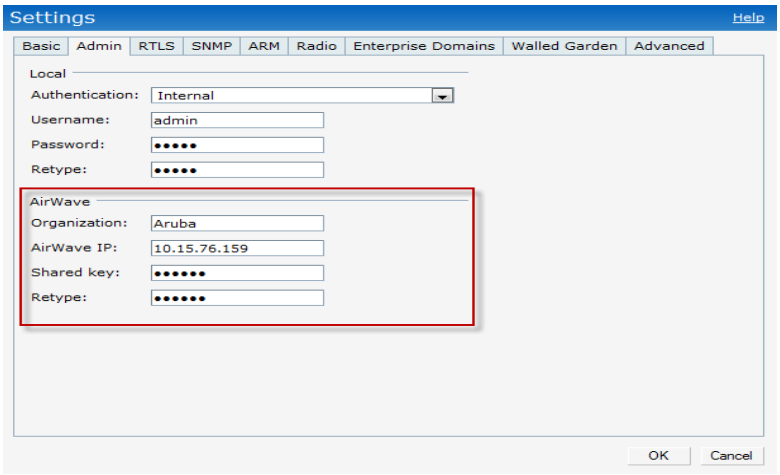
About Shared Key

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 IAP

1. Click the **AirWave Set Up Now link** in the bottom-middle region of the Instant UI. The **Settings** box with the **AirWave** tab selected appears.

Figure 100 *Configuring AirWave*



2. Enter the name of your organization in the **Organization** name text box.
3. Enter the IP address of the AirWave server in the **Airwave IP** text box.
4. 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 Instant network.
5. Click **OK**.

Airwave Discovery through DHCP Option

The AirWave configuration can also be performed on the DHCP option that is configured on the DHCP server. You can configure this only if the Airwave is not configured earlier or have deleted the precedent configuration.

On the DHCP server, the format for option 60 is "ArubaInstantAP", and the format for option 43 is "**ams-ip, ams-key**".

Chapter 18

Monitoring

Monitor the Dell Instant network, IAPs, Wi-Fi networks, and clients in the network for various parameters using one or all of the following views:

- Virtual Controller View
- Network View
- Instant Access Point View
- Client View

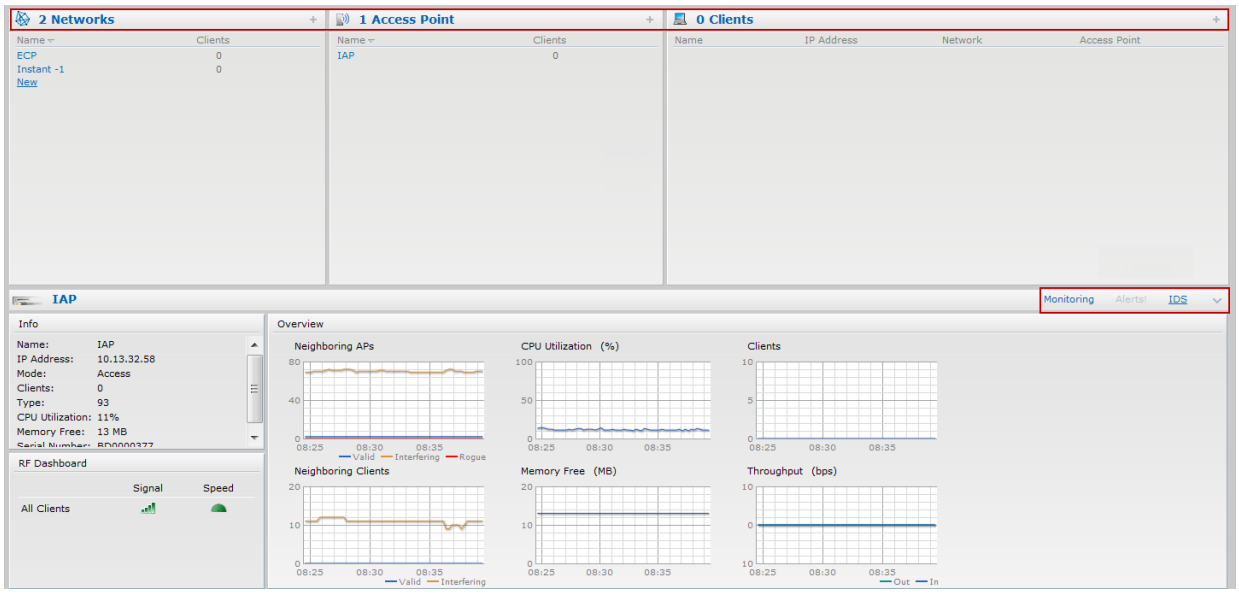
This chapter provides information about the parameters that can be monitored using these views. It also provides procedures to monitor these parameters.

Virtual Controller View

The Virtual Controller view is the default view.This view allows you to monitor the Dell Instant network. The following Instant UI elements are available in this view:

- Tabs—Contains three tabs: Networks, Access Points, and Clients. For detailed information about the tabs, see Chapter 2, “Instant User Interface” .
- Links—Contains three links: Monitoring, Client Alerts, and IDS. These links allow you to monitor the Dell Instant network. For detailed information about the sections in these links and how they can be used to monitor the network, see Monitoring Link , IDS Link , Client Alerts Link sections.

Figure 101 *Virtual Controller View*



Monitoring Link

This link is clicked 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**—Virtual Controller name.
- **Country Code**—Country in which the Virtual Controller is operating.
- **IP address**—IP address of the Virtual Controller.
- **Organization**—Name of the organization.
- **AirWave IP**—IP address of the AirWave server.
- **Band**—Band in which the Virtual Controller is operating: 2.4 GHz band, 5.4 GHz band, or both.

RF Dashboard

The **RF Dashboard** section displays the following information:

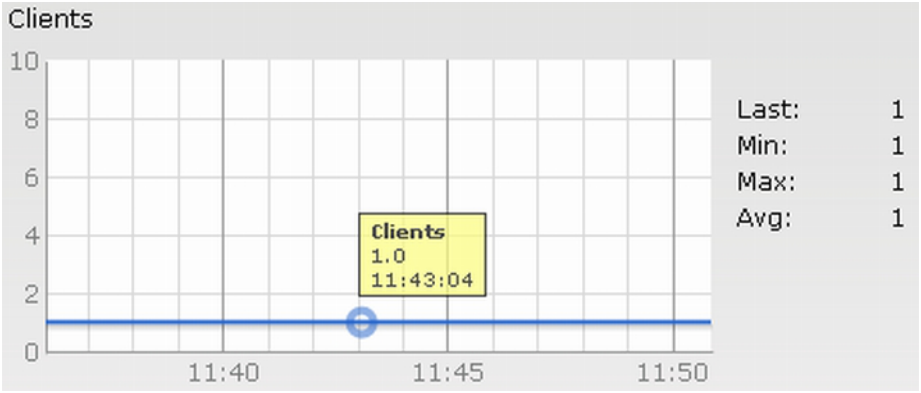
- IP address, Signal, and Speed information about the clients in the Dell Instant network. If the speed or signal strength of a client is low, IP address of the client appears as a link. Click the link to monitor the client. For more information, see "Client View" on page 144.
- Instant Access Points, Utilization, Noise, and Errors information about the IAPs in the Dell Instant network. If utilization, noise or errors of an IAP are not within the specified threshold, the IAP name appears as a link. Click the link to monitor the IAP. For more information, see "Instant Access Point View" on page 140.

Usage Trends

The **Usage Trends** section displays the following graphs for the Virtual Controller:

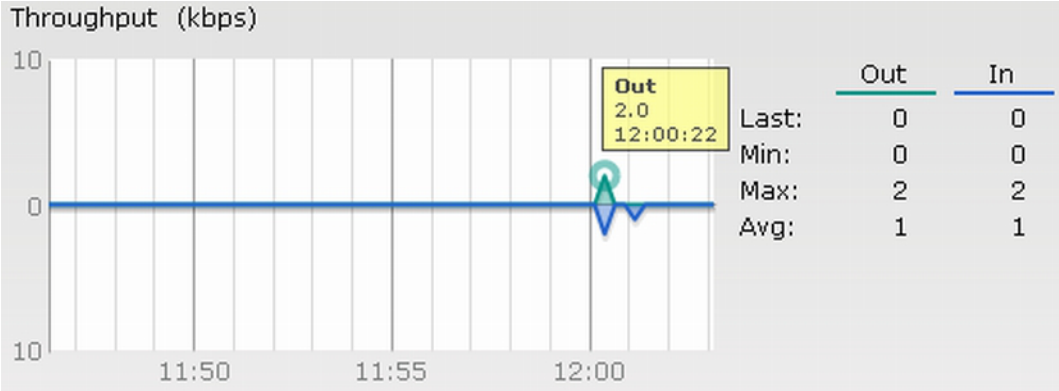
- Clients Graph

Figure 102 *Clients Graph*



- Throughput Graph

Figure 103 *Throughput Graph*



For more information about the graphs in the Virtual Controller view and for monitoring procedures, see Table 21.

Table 21 *Virtual Controller View—Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients	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. • 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. • To see the exact number of clients in the Dell Instant network at a particular time, hover the cursor over the graph line.	To check the number of clients associated with the Virtual Controller for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. Study the Clients graph in the Usage Trends pane. For example, the graph on the left shows that one client is associated with the Virtual Controller at 11:43 hours.
Throughput	The Throughput graph shows the throughput of all networks and IAPs associated with the Virtual Controller for the last 15 minutes. • Outgoing traffic—Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. • Incoming traffic—Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. • 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. To see the exact throughput of the Dell Instant network at a particular time, hover the cursor over the graph line.	To check the throughput of the networks and IAPs associated with the Virtual Controller for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. Study the Throughput graph in the Usage Trends pane. For example, the graph on the left shows 2.0 kbps outgoing traffic throughput at 12:00 hours. It also shows some incoming traffic throughput at the same time.

Client Alerts Link

For information about the Client Alerts link, see Chapter 2, "Instant User Interface" and Chapter 19, "Alert Types and Management" chapters.

IDS Link

For information about the IDS link, see Chapter 2, "Instant User Interface" .

Network View

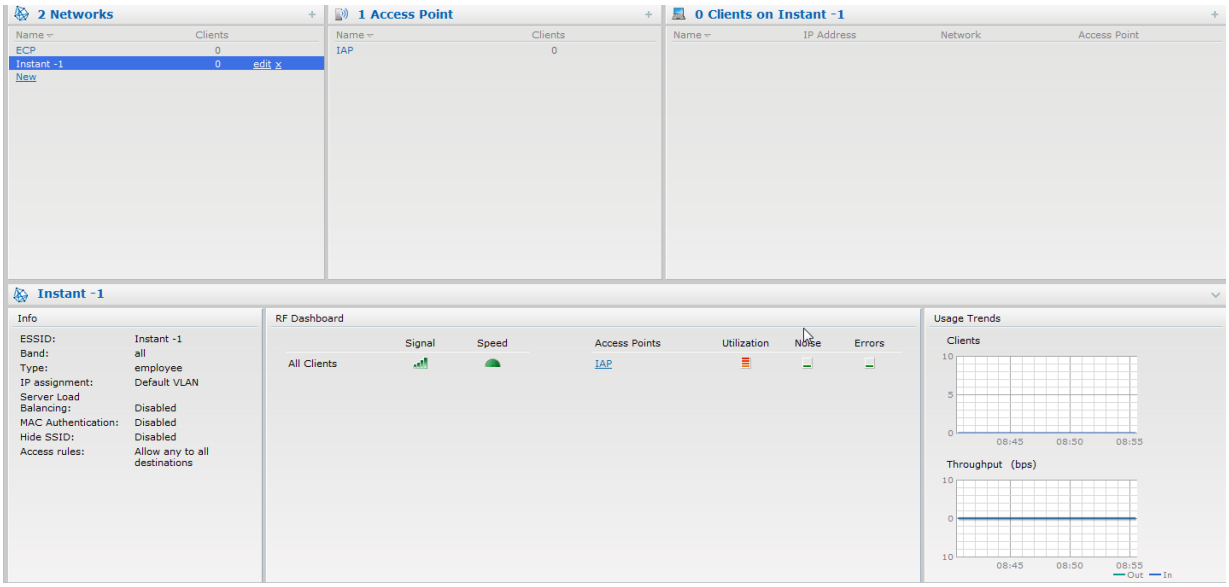
All Wi-Fi networks in the Dell Instant network are listed in the **Networks** tab. Click the network that you want to monitor. Network View for the selected network appears.

Similar to the Virtual Controller view, the Network view also has three tabs: Networks, Access Points, and Clients.

The following sections in the Instant UI, provide information about the selected network:

- Info
- Usage Trends

Figure 104 *Network View*



Info

The **Info** section displays the following information about the selected network:

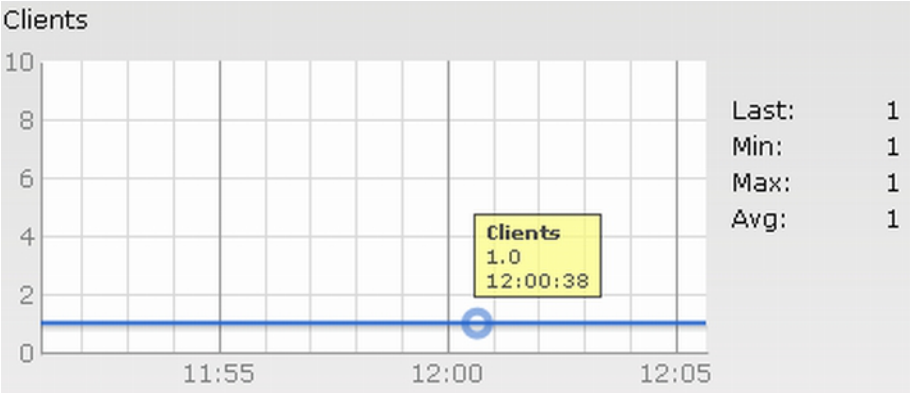
- **Name**—Name of the network.
- **Key Management**—Authentication key type.
- **Band**—Band in which the network is broadcast: 2.4 GHz band, 5.4 GHz band, or both.
- **Type**—Network type: Employee, Guest, or Voice.
- **IP Assignment**—Source of IP address for the client.
- **Authentication Server**—System's internal server or External RADIUS server.
- **Mac Authentication**—Settings for Mac authentication: Enabled or Disabled.
- **Captive Portal**—Status of Captive portal: Enabled or Disabled.
- **HIDE SSID**—Settings for hiding the network: Enabled or Disabled.
- **Access Rules**—Access rules settings.

Usage Trends

The **Usage Trends** section displays the following graphs for the selected network:

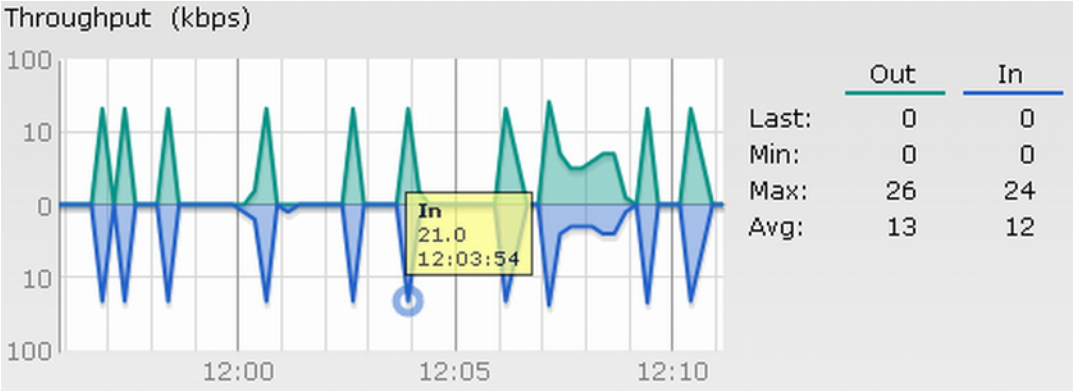
- Clients

Figure 105 *Clients Graph*



- Throughput

Figure 106 *Throughput Graph*



For more information about the graphs in the network view and for monitoring procedures, see Table 22.

Table 22 *Network View—Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients	The Clients graph shows the number of clients associated with the network for the last 15 minutes. 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 Virtual Controller for the last 15 minutes. • To see the exact number of clients in the Dell Instant network at a particular time, hover the cursor over the graph line.	To check the number of clients associated with the network for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the Networks tab, click the network for which you want to check the client association. The Network view appears. 3. Study the Clients graph in the Usage Trends pane. For example, the graph on the left shows that one client is associated with the selected network at 12:00 hours

Table 22 *Network View—Graphs and Monitoring Procedures (Continued)*

Graph Name	Description	Monitoring Procedure
Throughput	The Throughput graph shows the throughput of the selected network for the last 15 minutes. • Outgoing traffic—Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. • Incoming traffic—Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. • 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. To see the exact throughput of the selected network at a particular time, hover the cursor over the graph line.	To check the throughput of the selected network for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the Networks tab, click the network for which you want to check the client association. The Network view appears. 3. Study the Throughput graph in the Usage Trends pane. For example, the graph on the left shows 22.0 kbps incoming traffic throughput for the selected network at 12:03 hours.

Instant Access Point View

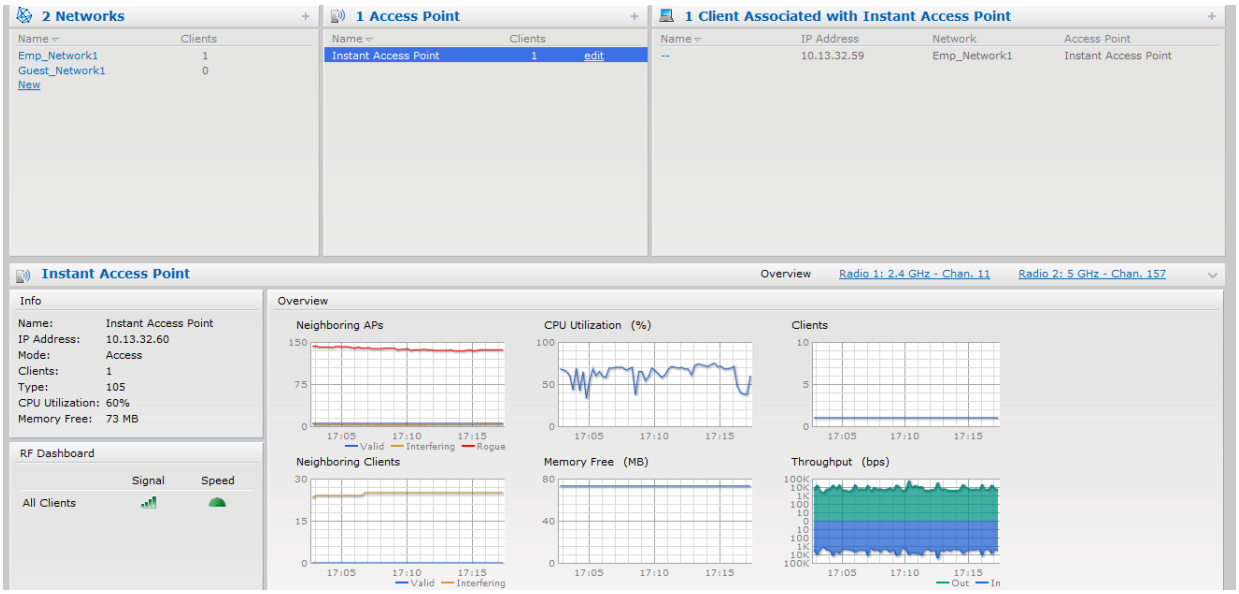
All IAPs in the Dell Instant network are listed in the **Access Points** tab. Click the IAP that you want to monitor. Access Point view for that IAP appears.

Similar to the Virtual Controller view, the Access Point view also has three tabs: Networks, Access Points, and Clients.

The following sections in the Instant UI provide information about the selected IAP:

- Info
- RF Dashboard
- RF Trends
- Usage Trends

Figure 107 *Instant Access Point View*



Info

The **Info** section provides the following information about the selected IAP:

- **Name**—Name of the selected IAP.
- **IP Address**—IP address of the IAP.
- **Clients**—Number of clients associated with the IAP.
- **Type**—Model number of the IAP.
- **CPU Utilization**—CPU utilization in percentage.
- **Memory Free**—Memory availability of the IAP in Mega Bytes.

RF Dashboard

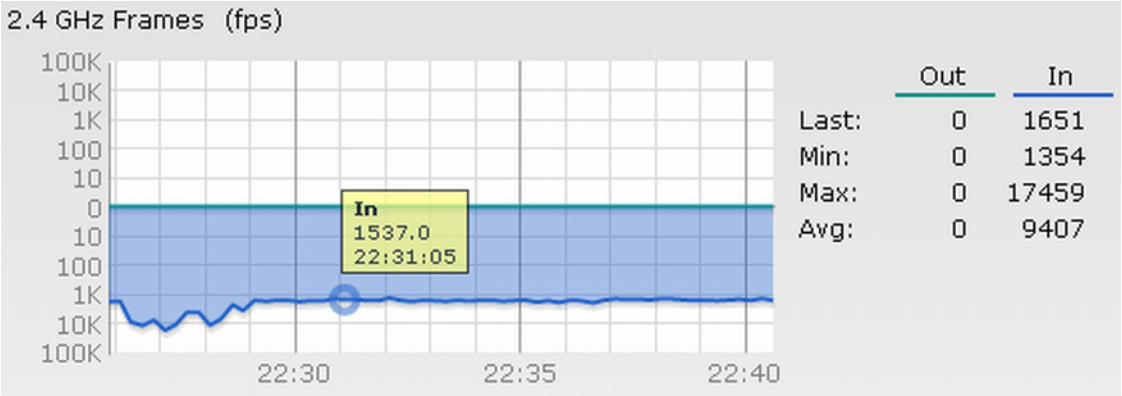
In the Instant Access Point view, the **RF Dashboard** section is moved below the **Info** section. It lists the IP address of the clients that are associated with the selected IAP if the signal strength or the data transfer speed of the client is low.

RF Trends

The **RF Trends** section has two links—**2.4 GHz** and **5 GHz**. The **2.4 GHz** link is clicked by default and the following graphs are displayed for that band:

- Utilization
- 2.4 GHz Frames

Figure 108 *2.4 GHz Frames Graph*



- Noise Floor
- Errors

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 23.

Table 23 *Instant Access Point View—RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Utilization	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 IAP for the last 15 minutes. To see the exact utilization percent at a particular time, hover the cursor over the graph line.	To monitor the utilization of the selected IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the Access Points tab, click the IAP for which you want to monitor the utilization. The IAP view appears. 3. Study the Utilization graph in the RF Trends pane. For example, the graph on the left shows 62% IAP radio utilization for the 2.4 GHz band at 22:28 hours. NOTE: You can also click the rectangle icon under  the Utilization column in the RF Dashboard pane to see the Utilization graph for the selected IAP.
2.4 GHz Frames	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. • Outgoing frames—Outgoing frame traffic is displayed in green. It is shown above the median line. • Incoming frames—Incoming frame traffic is displayed in blue. It is shown below the median line. To see an enlarged view, click the graph. • The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing frames. To see the exact utilization percent at a particular time, hover the cursor over the graph line.	To monitor the In and Out frame rate per second for the radio in 2.4 GHz band, for the last 15 minutes, 1. Log in to the WebUI. The Virtual Controller view appears. This is the default view. 2. In the Access Points tab, click the name link of the IAP for which you want to monitor the frame rate. The IAP view appears. 3. Study the 2.4 GHz Frames graph in the RF Trends pane. For example, the graph on the left shows 1537.0 incoming frames at 22:31 hours.
Noise Floor	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 IAP. Monitor the noise floor regularly for optimal performance of the IAP. 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.	To monitor the noise floor for the IAP for the last 15 minutes, 1. Log in to the WebUI. The Virtual Controller view appears. This is the default view. 2. In the Access Points tab, click the name link of the IAP for which you want to monitor the noise floor. The IAP view appears. 3. Study the Noise Floor graph in the RF Trends pane. For example, the graph on the left shows that the noise floor for the IAP at 22:38 hours is -82.0 dBm. NOTE: You can also click the rectangle icon under  the Noise column in the RF Dashboard pane to see the Noise graph for the selected IAP.

Table 23 *Instant Access Point View—RF Trends Graphs and Monitoring Procedures (Continued)*

Graph Name	Description	Monitoring Procedure
Errors	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.	To monitor the errors for the IAP for the last 15 minutes, 1. Log in to the WebUI. The Virtual Controller view appears. This is the default view. 2. In the Access Points tab, click the name link of the IAP for which you want to monitor the errors. The IAP view appears. 3. Study the Errors graph in the RF Trends pane. For example, the graph on the left shows that the errors for the IAP at 22:48 hours is 9514.0 frames per second. NOTE: You can also click the rectangle icon under  the Errors column in the RF Dashboard pane to see the Errors graph for the selected IAP.

Usage Trends

The **Usage Trends** section displays the following graphs for the selected network:

- Clients Graph
- Throughput Graph

For more information about the usage trends graphs in the instant access point view and or monitoring procedures, see Table 24.

Table 24 *Instant Access Point View—Usage Trends and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients	The Clients graph shows the number of clients associated with the selected IAP for the last 15 minutes. 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 IAP for the last 15 minutes. To see the exact number of clients associated with the selected IAP at a particular time, hover the cursor over the graph line.	To check the number of clients associated with the IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the Access Points tab, click the IAP for which you want to monitor the client association. The IAP view appears. 3. Study the Clients graph in the Usage Trends pane. For example, the graph on the left shows that one client is associated with the IAP at 12:12 hours.
Throughput	The Throughput graph shows the throughput for the selected IAP for the last 15 minutes. • Outgoing traffic—Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown about the median line. • Incoming traffic—Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. • The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the IAP for the last 15 minutes. To see the exact throughput of the selected IAP at a particular time, hover the cursor over the graph line.	To check the throughput of the selected IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the Access Points tab, click the IAP for which you want to monitor the throughput. The IAP view appears. 3. Study the Throughput graph in the Usage Trends pane. For example, the graph on the left shows 4.0 kbps incoming traffic throughput at 12:08 hours.

Client View

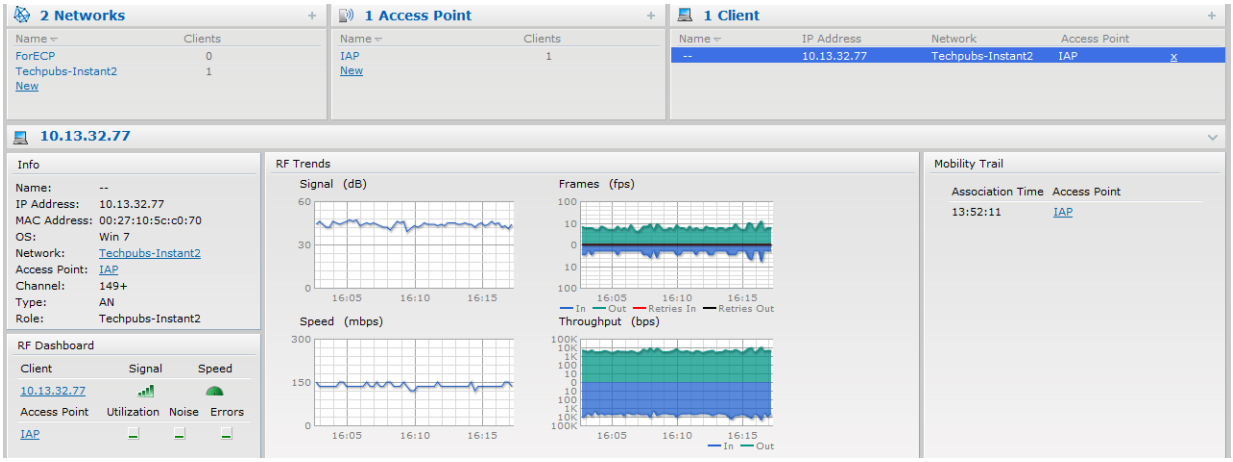
In the Virtual Controller view, all clients in the Dell Instant network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor. Client view for that client appears.

The Client view has three tabs: Networks, Access Points, and Clients.

The following sections in the Instant UI provide information about the selected client:

- Info
- RF Dashboard
- RF Trends
- Usage Trends

Figure 109 *Client View*



Info

The **Info** section provides the following information about the selected 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**—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

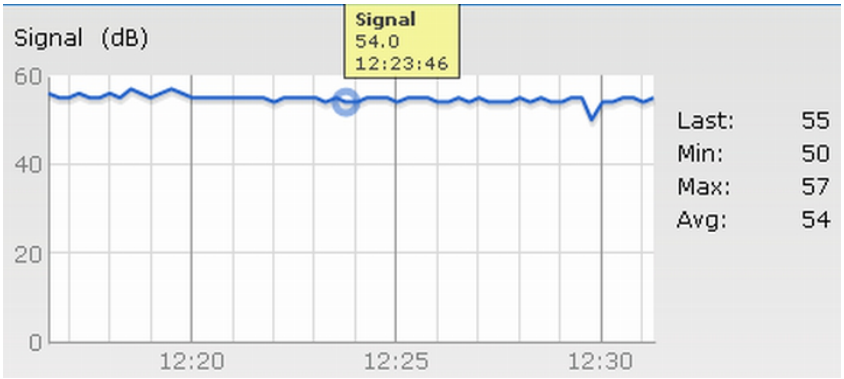
In the Client view, the **RF Dashboard** section is moved below the **Info** section. The **RF Dashboard** section in the client view shows the speed and the signal information for the client and the RF information for the IAP to which the client is connected to.

RF Trends

The **RF Trends** section displays the following graphs for the selected client:

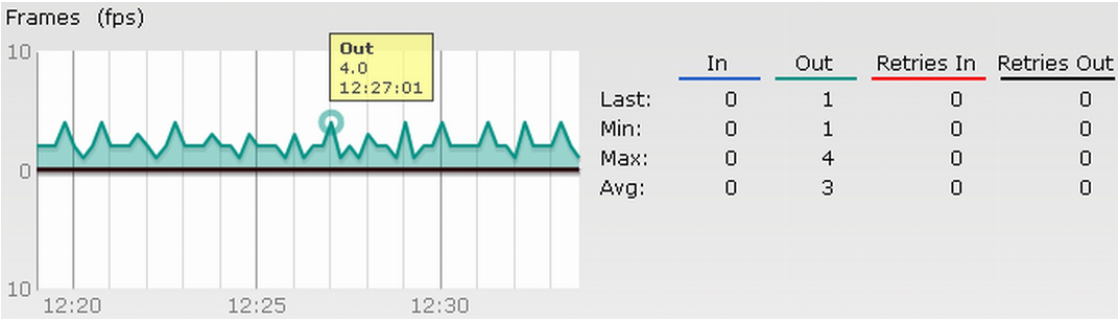
- Signal

Figure 110 *Signal Graph*



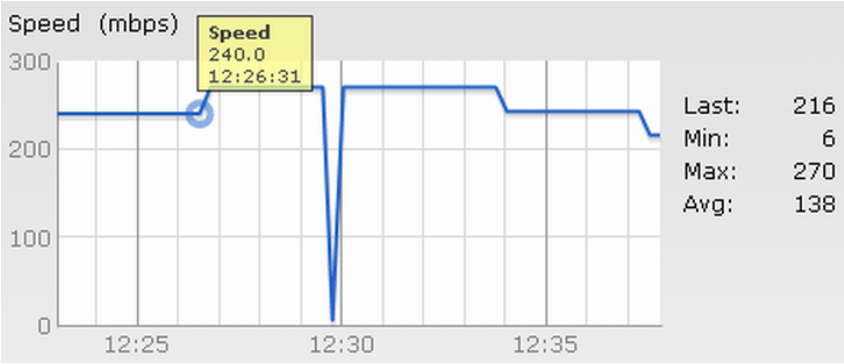
- Frames

Figure 111 *Frames Graph*



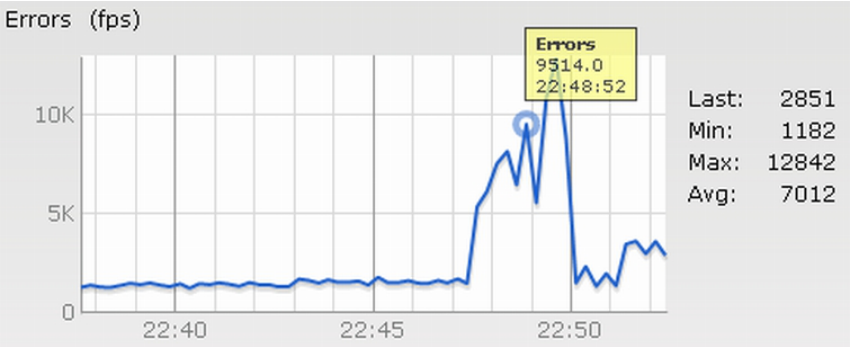
- Speed

Figure 112 *Speed Graph*



- Throughput

Figure 113 *Throughput Graph*



For more information about RF trends graphs in the client view and for monitoring procedures, see Table 25.

Table 25 *Client View—RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Signal	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 fr the last 15 minutes. To see the exact signal strength at a particular time, hover the cursor over the graph line.	To monitor the signal strength of the selected client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the Clients tab, click the IP address of the client for which you want to monitor the signal strength. The client view appears. 3. Study the Signal graph in the RF Trends pane. For example, the graph on the left shows that signal strength for the client is 54.0 dB at 12:23 hours.
Frames	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. • Outgoing frames—Outgoing frame traffic is displayed in green. It is shown above the median line. • Incoming frames—Incoming frame traffic is displayed in blue. It is shown below the median line. • Retry Out—Retries for the outgoing frames is displayed in black and is show above the median line. • Retry In—Retries for the incoming frames is displayed in red and is shown below the median line. 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. To see the exact frames at a particular time, hover the cursor over the graph line.	To monitor the In and Out frame rate per second and retry frames for the In and Out traffic, for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the Clients tab, click the IP address of the client for which you want to monitor the frames. The client view appears. 3. Study the Frames graph in the RF Trends pane. For example, the graph on the left shows 4.0 frames per second for the client at 12:27 hours.

Table 25 *Client View—RF Trends Graphs and Monitoring Procedures (Continued)*

Graph Name	Description	Monitoring Procedure
Speed	The Speed graph shows the data transfer speed for the client. Data transfer is measured in Mega bits per second (mbps). 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. To see the exact speed at a particular time, hover the cursor over the graph line.	To monitor the speed for the client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the Clients tab, click the IP address of the client for which you want to monitor the speed. The client view appears. 3. Study the Speed graph in the RF Trends pane. For example, the graph on the left shows that the data transfer speed at 12:26 hours is 240 mbps.
Throughput	The Throughput Graph shows the throughput for the selected client for the last 15 minutes. • Outgoing traffic—Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. • Incoming traffic—Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. 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.	To monitor the errors for the client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the Clients tab, click the IP address of the client for which you want to monitor the throughput. The client view appears. 3. Study the Throughput graph in the RF Trends pane. For example, the graph on the left shows 1.0 kbps outgoing traffic throughput for the client at 12:30 hours.

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 IAP. It shows the client-IAP association for the last 15 minutes.
- **Access Point**—IAP name with which the client was associated.

NOTE: Mobility information about the client is reset each time it roams from one IAP to another.

Alert Types

Alerts are generated when a user encounters problems while accessing or connecting to the Wi-Fi network. These alerts enable you to troubleshoot the problems. The alerts that are generated on Dell 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 26 displays a list of alerts that are generated on the Dell Instant network.

Table 26 *Alerts List*

Type Code	Description	Details	Corrective Actions
100101	Internal error	The IAP has encountered an internal error for this client.	Contact the Dell customer support team.
100102	Unknown SSID in association request	The 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 IAP cannot allow this client to associate because its authentication or encryption settings do not match IAP's configuration.	Ascertain the correct authentication or encryption settings and try to associate again.
100104	Unsupported 802.11 rate	The 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 IAP to see if the desired rate can be supported; if not, consider replacing the IAP with another model that can support the rate.
100105	Maximum capacity reached on IAP	The IAP has reached maximum capacity and cannot accommodate any more clients.	Consider expanding capacity by installing additional IAPs or balance load by relocating IAPs.
100206	Invalid Mac Address	The IAP cannot authenticate this client because the client's Mac address is not valid.	This condition may be 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 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 IAP cannot authenticate this client using 802.1X because the RADIUS server did not respond to the authentication request.	If the IAP is using the internal RADIUS server, recommend checking the related configuration as well as the installed certificate and passphrase. If the IAP is using an external RADIUS server, check if there are any issues with the RADIUS server and try connecting again.

Table 26 *Alerts List (Continued)*

Type Code	Description	Details	Corrective Actions
100309	RADIUS server authentication failure	The 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 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 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 20

User Database

In Dell 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 Instant system.

A guest user can be a visitor who will be temporarily using the enterprise network to access the internet. However, you would 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 will be 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.

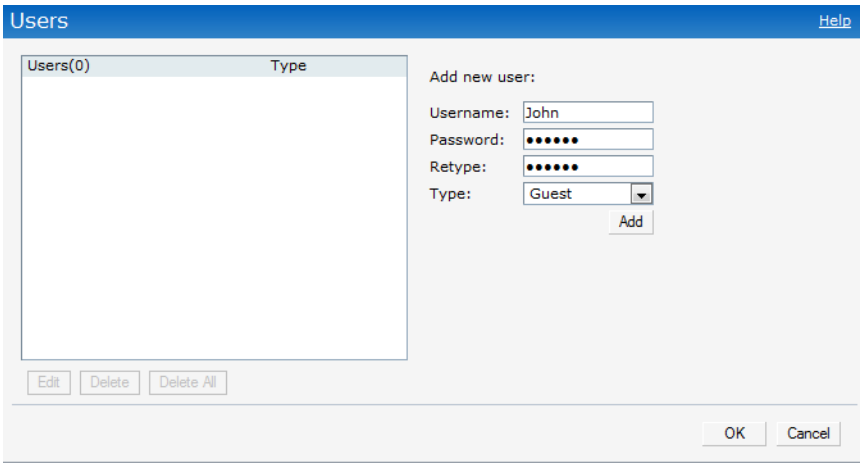
NOTE: User Database is also used when Instant is employed as an internal RADIUS server.

Adding a User

To add a user, perform the following steps:

1. At the top right corner of the Instant UI, click the **Users** link. The **Users** box appears.

Figure 114 *Adding a User*



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, perform the following steps:

1. At the top right corner of the Instant UI, click the **Users** link. The **Users** box 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, perform the following steps:

1. At the top right corner of the Instant UI, click the **Users** link. The **Users** box 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 under this username.

Chapter 21

Regulatory Domain

The IEEE 802.11/b/g/n Wi-Fi networks operate in 2.4 GHz and IEEE 802.11a/n operate in 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 Instant will operate. This configuration sets the regulatory domain for the radio frequencies that the 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 IAPs designated for US, Japan, and Israel. 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. Table 27 shows the list of country codes.

Figure 115 *Specifying a Country Code*

Country Codes List

Table 27 *Country Codes List*

Code	Country Name
US	United States
CA	Canada
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
IL	Israel
SA	Saudi Arabia
LB	Lebanon
AE	United Arab Emirates
ZA	South Africa
AR	Argentina
AU	Australia
AT	Austria
BO	Bolivia
CL	Chile
GR	Greece

Table 27 *Country Codes List (Continued)*

Code	Country Name
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
PR	Puerto Rico
SK	Slovak Republic
SI	Slovenia
TH	Thailand
UY	Uruguay
PA	Panama
RU	Russia
EG	Egypt
TT	Trinidad and Tobago
TR	Turkey

Table 27 *Country Codes List (Continued)*

Code	Country Name
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
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

Abbreviations

The following table lists the abbreviations used in this user guide.

Table 28 *List of abbreviations*

Abbreviation	Expansion
ABR	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
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
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

Table 28 *List of abbreviations (Continued)*

Abbreviation	Expansion
VC	Virtual Controller
VSA	Vendor-Specific Attributes
WLAN	Wireless Local Area Network