Aruba Instant 6.3.1.1-4.0

User Guide

Copyright

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

Chapter 1
About this Guide

This User Guide describes the features supported by Aruba Instant and provides detailed instructions for setting up and configuring Instant network.

Intended Audience

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

Related Documents

In addition to this document, the Instant product documentation includes the following:

- *Aruba Instant 6.3.1.1-4.0 Quick Start Guide*
- *Aruba Instant 6.3.1.1-4.0 CLI Reference Guide*
- *Aruba Instant 6.3.1.1-4.0 MIB Reference Guide*
- *Aruba Instant 6.3.1.1-4.0 Syslog Messages Reference Guide*
- *Aruba Instant 6.3.1.1-4.0 Release Notes*

Conventions

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

Table 1: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: ● Sample screen output ● System prompts ● Filenames, software devices, and specific commands when mentioned in the text
`Commands`	In the command examples, this style depicts the keywords that must be typed exactly as shown.
<*Arguments*>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: # **`send`** <*text message*> In this example, you would type "send" at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
`[Optional]`	Command examples enclosed in brackets are optional. Do not type the brackets.
`{Item A | Item B}`	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

The following informational icons are used throughout this guide:

NOTE

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

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

WARNING Indicates a risk of personal injury or death.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	arubanetworks.com/support/wsirt.php
Support Email Addresses	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

This chapter provides the following information:

- Aruba Instant Overview
- What is New in Aruba Instant 6.3.1.1-4.0

Aruba Instant Overview

Aruba Instant virtualizes Aruba Mobility Controller capabilities on 802.11 access points (APs), creating a feature-rich enterprise-grade wireless LAN (WLAN) that combines affordability and configuration simplicity.

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

Instant consists of an IAP and a Virtual Controller. The Virtual Controller resides within one of the APs. In an Instant deployment scenario, only the first IAP needs to be configured. After the first IAP is configured, the other IAPs inherit all the required configuration information from the Virtual Controller. Instant continually monitors the network to determine the IAP that should function as the Virtual Controller at any time, and the Virtual Controller will move from one IAP to another as necessary without impacting network performance.

Supported Devices

The following devices are supported in the current release of Instant:

- IAP-92
- IAP-93
- IAP-104
- IAP-105
- IAP-114
- IAP-115
- IAP-134
- IAP-135
- IAP-175P/175AC
- RAP-3WN/3WNP
- RAP-108
- RAP-109
- RAP155/155P
- IAP-224
- IAP-225

NOTE

All APs support an unlimited number of IAPs. In a network comprising of IAP-92 and IAP-93, an AP can support up to 16 IAPs only.

All IAPs are available as the following variants:

- IAP-US (United States)

- IAP-JP (Japan)
- IAP-IL (Israel)
- IAP-RoW (Rest of World)

For information on the complete list of the countries supported by the IAP-RoW type, see Country Codes List on page 343.

Instant UI

The Instant User Interface (UI) provides a standard web based interface that allows you to configure and monitor a Wi-Fi network. Instant is accessible through a standard web browser from a remote management console or workstation and can be launched using the following browsers:

- Internet Explorer 10 or lower
- Safari 6.0 or later
- Google Chrome 23.0.1271.95 m or later
- Mozilla Firefox 17.0 or later

To view the Instant UI, ensure that the JavaScript is enabled on the web browser. For more information on Instant UI features, see Instant User Interface on page 39.

NOTE In the current release, Instant UI does not support Internet Explorer 11.

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

Instant CLI

The Instant Command Line Interface (CLI) is a text-based interface accessible through a Secure Shell (SSH) session.

SSH access requires that you configure an IP address and a default gateway on the IAP and connect the IAP to your network. This is typically performed when the Instant network on an IAP is set up.

What is New in Aruba Instant 6.3.1.1-4.0

The following features are added in the Aruba Instant 6.3.1.1-4.0 release:

Table 2: *New Features in 6.3.1.1-4.0*

Feature	Description
Bandwidth contract enhancements	Instant supports assigning bandwidth contracts to the user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the IAP) or downstream (IAP to clients) traffic for a user role. All users in that role will be part of that bandwidth contract. The administrators can also set per user bandwidth to provide a specific bandwidth for each user connecting to the SSID or wired profile.
Support for 802.11r Roaming and Fast BSS Transition	Instant supports 802.11r roaming standard. As part of the 802.11r implementation, Instant supports the Fast BSS Transition protocol. The Fast BSS Transition mechanism minimizes the time required to resume data connectivity when a BSS transition happens.

Table 2: *New Features in 6.3.1.1-4.0*

Feature	Description
Support for Client Roaming Based on Opportunistic Key Caching	Instant also supports opportunistic key caching (OKC) based roaming. In the OKC based roaming, the 802.1X authentication profile enables a cached pairwise master key (PMK), which is used when a client roams to a new IAP. This allows faster roaming of clients between the IAPs in a cluster, without the need for a complete 802.1X authentication.
LACP on IAP-220 Series	IAP-220 Series supports link aggregation using either standard port-channel (configuration based) or Link Aggregation Control Protocol (protocol signaling based).
IAP Guest Management Interface	Instant now supports a guest management interface for managing guest users.
IAP Integration with Analytics and Location Engine (ALE)	Instant supports integration with Application and Location Engine (ALE). The ALE server acts as a primary interface to all third-party applications and the IAP sends client information and other status information to the ALE server.
IAP Integration with Palo Alto Networks Firewall	Instant supports integration with the Palo Alto Networks (PAN) firewall. To integrate an IAP with PAN user ID, a global profile is added. This profile can be configured on an IAP with PAN firewall information such as IP address, port, user name, password, firewall enabled or disabled status. IAP maintains the network (such as mapping IP address) and user information for its clients in the network and can provide the required information for the user ID feature on PAN firewall.
Domain-name based ACL	Instant supports configuration of domain-based Access Control List (ACL) rule. Access to specific domains is allowed or denied based on the ACL rule definition.
Enhancements to Internal Captive Portal Splash Page	Instant now supports customization of logo, policy text, and usage terms for the internal Captive portal splash page.
Support for multiple Captive portal profiles	Instant supports multiple Captive portal profiles and allows the users to customize the Captive portal profiles based on guest logon role and SSID. You can create a set of captive portal profiles and associate them with an SSID or wired profile, or create an external Captive portal profile for a WLAN SSID or a wired profile in the WLAN wizard or Wired Network window.
Client Match	Instant supports the ARM client match feature that continually monitors a client's RF neighborhood to provide the ongoing client bandsteering service and load balancing, and enhanced IAP reassignment for roaming mobile clients.
Support for Spanning Tree Protocol	Instant allows enabling of Spanning Tree Protocol (STP) on a wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. By default, Spanning Tree is disabled on wired profiles.
Customizing Internal Captive Portal Certificate	Instant now supports uploading of customized internal Captive Portal server certificates to the IAP database.
Provisioning an IAP as a master IAP	Instant now allows you to manually provision an IAP as a master IAP, based on network-specific parameters such as the physical location of the Virtual Controller.
Support for Aruba GRE	Instant now allows the automatic configuration of GRE tunnel from an IAP to Aruba Controller. By using an IPsec connection, the IAPs can now set up a GRE tunnel with the Aruba Controller. This feature eliminates the need for the manual configuration of tunnel interface on Aruba Controller.

Table 2: *New Features in 6.3.1.1-4.0*

Feature	Description
DHCP Relay Support	Instant now supports the Centralized DHCP scope to serve the L3 clients. When this feature is enabled, the IAP relays all DHCP request packets to the DHCP server and acts as gateway for the centralized DHCP scope serving L3 clients.
IAP Provisioning Enhancements	For option DHCP 43, besides the old format **<organization>,<ams-ip>,<ams-key>**, Instant now supports a new format **<organization>,<ams-domain>**. Also, the IAP now performs a certificate-based authentication with AirWave Management server, instead of the current PSK-based login process.
Support for HTTP Proxy Configuration	Instant now supports HTTP proxy configuration. The HTTP proxy enables the IAP to download the image from the cloud server.
AirGroup Enhancements	Instant now supports different AirGroup services such as iTunes, Sharing, Chat, and so on. You can either allow all services or customize the required services.
Dynamic RADIUS Proxy (DRP) IP address configuration	Instant allows the configuration of separate IP address and VLAN details, which can be used as source IP address and VLAN for RADIUS packets. When the dynamic RADIUS proxy IP address and VLAN are configured, the clients associated with an IAP can be authenticated with multiple RADIUS servers, across different geographical areas, networks, and VLANs.
Restricted access management	Instant allows you to configure management subnets and restrict access to the corporate network in order to prevent unauthorized users from accessing the corporate network.
Uplink VLAN monitoring and detection on upstream devices	The Instant UI now displays an alert message when a client connects to an SSID or wired interface with a VLAN ID that is not allowed on the upstream device. The alert message notifies the users about the mismatch in the VLAN configuration on the IAP or the upstream device of an IAP.
Telnet access to the Instant CLI	Instant now supports Telnet access to the Instant CLI.

Table 3: *New Hardware Platforms introduced in this release*

IAP Platform	Description
IAP-224/225	The Aruba AP-224 and AP-225 wireless access points support the IEEE 802.11ac standard for high-performance WLAN. These APs use MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11n 2.4 GHz and 802.11ac 5 GHz functionality while simultaneously supporting existing legacy wireless services. The IAP-220 Series support 802.11ac on the 5GHz band using 80 MHz channels. For more information about this product, go to www.arubanetworks.com.
IAP-114/115	The Aruba AP-114 and AP-115 are dual radio, dual-band wireless access points that support the IEEE 802.11n standard for high-performance WLAN. These APs use MIMO (Multiplein, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11n 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services. For more information about this product, go to www.arubanetworks.com

Conventions

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

Table 4: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: ● Sample screen output ● System prompts ● Filenames, software devices, and specific commands when mentioned in the text
`Commands`	In the command examples, this bold font depicts the keywords that must be typed exactly as shown.
<*Arguments*>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: # **`send`** <*text message*> In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
`[Optional]`	Command examples enclosed in brackets are optional. Do not type the brackets.
`{Item A | Item B}`	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

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.

This chapter describes the following procedures:

- Setting up Instant Network on page 33
- Logging in to the Instant UI on page 35
- Accessing the Instant CLI on page 36

Setting up Instant Network

Before installing an IAP:

- Ensure that you have an Ethernet cable of the required length to connect an IAP to the home router.
- Ensure that you have one of the following power sources:
  - IEEE 802.3af/at-compliant Power over Ethernet (PoE) source. The PoE source can be any power source equipment (PSE) switch or a midspan PSE device.
  - IAP power adapter kit.

Perform the following procedures to set up the Instant network:

1. Connecting an IAP on page 33
2. Assigning an IP address to the IAP on page 33
3. Connecting to a Provisioning Wi-Fi Network on page 34

Connecting an IAP

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

- PoE switch– Connect the ENET 0 port of the IAP to the appropriate port on the PoE switch.
- PoE midspan– Connect the ENET 0 port of the 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.

NOTE

RAP-155P supports PSE for 802.3at powered device (class 0-4) on one port (E1 or E2), or 802.3af powered DC IN (Power Socket) on two ports (E1 and E2).

Assigning an IP address to the IAP

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

To obtain an IP address for an IAP:

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

NOTE

If there is no DHCP service on the network, the IAP can be assigned a static IP address. If a static IP is not assigned, the IAP obtains an IP automatically within the 169.254 subnet.

Assigning a Static IP

To assign a static IP to an IAP:

1. Connect a terminal, PC, or workstation running a terminal emulation program to the **Console** port on the IAP.
2. Power on the IAP. An autoboot countdown prompt that allows you to interrupt the normal startup process and access **apboot** is displayed.
3. Click **Enter** before the timer expires. The IAP goes into the **apboot** mode.
4. In the **apboot** mode, use the following commands to assign a static IP to the IAP.

   ```
   Hit <Enter> to stop autoboot:  0
   apboot>
   apboot> setenv ipaddr 192.0.2.0
   apboot> setenv netmask 255.255.255.0
   apboot> setenv gatewayip 192.0.2.2
   apboot> save
   Saving Environment to Flash...
   Un-Protected 1 sectors
   .done
   Erased 1 sectors
   Writing
   ```

5. Use the `printenv` command to view the configuration.

```
apboot> printenv
```

Connecting to a Provisioning Wi-Fi Network

The IAPs boot with factory default configuration and try to provision automatically. If the automatic provisioning is successful, the **instant** SSID will not be available. If AirWave and Activate are not reachable and the automatic provisioning fails, the **instant** SSID becomes available and the users can connect to a provisioning network by using the instant SSID.

To connect to a provisioning Wi-Fi network:

1. Ensure that the client is not connected to any wired network.
2. Connect a wireless enabled client to a provisioning Wi-Fi network: for example, **instant**.
3. If the Windows OS system is used:
   a. Click the wireless network connection icon in the system tray. The **Wireless Network Connection** window appears.
   b. Click on the **instant** network and then click **Connect**.
4. If the Mac OS system is used:
   a. Click the **AirPort** icon. A list of available Wi-Fi networks is displayed.
   b. Click on the **instant** network.

NOTE

The **instant** SSIDs are broadcast in 2.4 GHz only.

IAP Cluster

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

NOTE

Moving an IAP from one cluster to another requires a factory reset of the IAP.

Disabling the Provisioning Wi-Fi Network

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

To disable the provisioning network:

1. Connect a terminal or PC/workstation running a terminal emulation program to the **Console** port on the IAP.
2. Configure the terminal or terminal emulation program to use the following communication settings:

Table 5: *Terminal Communication Settings*

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

3. Power on the IAP. An autoboot countdown prompt that allows you to interrupt the normal startup process and access apboot is displayed.
4. Click **Enter** before the timer expires. The IAP goes into the apboot mode through console.
5. In the apboot mode, use the following commands to disable the provisioning network:
   - `apboot> factory_reset`
   - `apboot> setenv disable_prov_ssid 1`
   - `apboot> saveenv`
   - `apboot> reset`

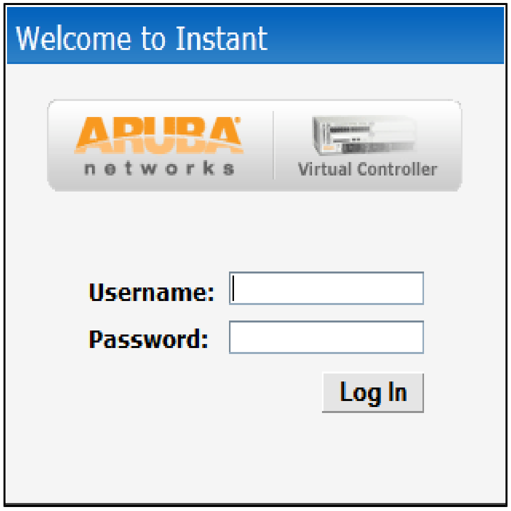
Logging in to the Instant UI

Launch a web browser and enter http://instant.arubanetworks.com. In the login screen, enter the following credentials:

- Username– admin
- Password– admin

The following figure shows the **Login** screen:

Figure 1 *Login Screen*



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

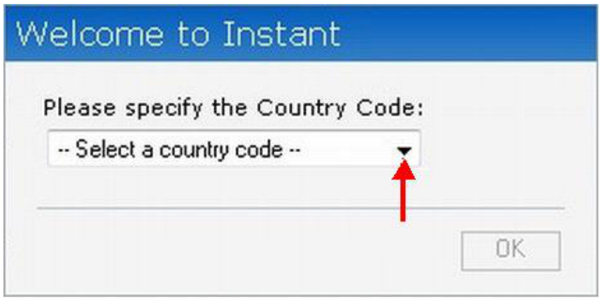
Specifying Country Code

NOTE

This procedure is applicable to the IAP-ROW (Rest of World) variants only. Skip this step if you are installing IAP in the United States, Japan, or Israel.

The **Country Code** window is displayed for the IAP-ROW (Rest of World) variants when you log in to the Instant UI for the first time. You can specify a country code by selecting an appropriate option from the **Please Specify the Country Code** drop-down list.

Figure 2 *Specifying a Country Code*



Welcome to Instant

Please specify the Country Code:

.

For the complete list of the country codes supported by the IAP-ROW variant type, see Regulatory Domain on page 343.

Accessing the Instant CLI

In the current release, Aruba supports the use of Command Line Interface (CLI) for scripting purposes. When you make configuration changes on a master IAP in the CLI, all associated IAPs in the cluster inherit these changes and subsequently update their configurations. By default, you can access the CLI from the serial port or from an SSH session. You must explicitly enable Telnet access on the IAP to access the CLI through a Telnet session.

For information on enabling SSH and Telnet access to the IAP CLI, see Enabling Terminal Access on page 75.

Connecting to a CLI Session

On connecting to a CLI session, the system displays its host name followed by the login prompt. Use the administrator credentials to start a CLI session. For example:

```
(Instant Access Point)
User: admin
```

ode is enabled and a command prompt is displayed. For example:

```
(Instant Access Point)#
```

The privileged mode provides access to **show**, **clear**, **ping**, **traceroute**, and **commit** commands. The configuration commands are available in `config` mode. To move from privileged mode to the configuration mode, enter the following command at the command prompt:

```
(Instant Access Point)# configure terminal
```

The configure terminal command allows you to enter the basic configuration mode and the command prompt is displayed as follows:

```
(Instant Access Point)(config)#
```

The Instant CLI allows CLI scripting in several other sub-command modes to allow the users to configure individual interfaces, SSIDs, access rules, and security settings.

You can use the question mark (?) to view the commands available in a privileged mode, configuration mode, or sub-mode.

NOTE

Although automatic completion is supported for some commands such as **configure terminal**, the complete **exit** and **end** commands must be entered at command prompt.

Applying Configuration Changes

Each command processed by the Virtual Controller is applied on all the slaves in a cluster. The changes configured in a CLI session are saved in the CLI context. The CLI does not support the configuration data exceeding the 4K buffer size in a CLI session. Therefore, Aruba recommends that you configure fewer changes at a time and apply the changes at regular intervals.

To apply and save the configuration changes at regular intervals, use the following command in the privileged mode:

```
(Instant Access Point)# commit apply
```

To apply the configuration changes to the cluster without saving the configuration, use the following command in the privileged mode:

```
(Instant Access Point)# commit apply no-save
```

To view the changes that are yet to be applied, use the following command in the privileged mode:

```
(Instant Access Point)# show uncommitted-config
```

To revert to the earlier configuration, use the following command in the privileged mode.

```
(Instant Access Point)# commit revert
```

Example:

```
(Instant Access Point)(config)# rf dot11a-radio-profile
(Instant Access Point)(RF dot11a Radio Profile)# beacon-interval 200
(Instant Access Point)(RF dot11a Radio Profile)# no legacy-mode
(Instant Access Point)(RF dot11a Radio Profile)# dot11h
(Instant Access Point)(RF dot11a Radio Profile)# interference-immunity 3
(Instant Access Point)(RF dot11a Radio Profile)# csa-count 2
(Instant Access Point)(RF dot11a Radio Profile)# spectrum-monitor
(Instant Access Point)(RF dot11a Radio Profile)# end

(Instant Access Point)# show uncommitted-config
   rf dot11a-radio-profile
   no legacy-mode
   beacon-interval 200
   no dot11h
   interference-immunity 3
   csa-count 1
   no spectrum-monitor

Instant Access Point# commit apply
```

Using Sequence Sensitive Commands

The Instant CLI does not support positioning or precedence of sequence-sensitive commands. Therefore, Aruba recommends that you remove the existing configuration before adding or modifying the configuration details for sequence-sensitive commands. You can either delete an existing profile or remove a specific configuration by using the **no…** commands.

The following table lists the sequence-sensitive commands and the corresponding **no** command to remove the configuration.

Table 6: *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command
`opendns <username <password>`	`no opendns`

Table 6: *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command
`rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit |deny | src-nat | dst-nat {<IP-address> <port>| <port>}}[<option1....option9>]`	`no rule <dest> <:mask> <match> <protocol> <start-port> <end-port> {permit | deny | src-nat | dst-nat}`
`mgmt-auth-server <auth-profile-name>`	`no mgmt-auth-server <auth-profile-name>`

`set-role <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator> <role>| value-of}`	`no set-role <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator>| value-of}`
	`no set-role`

`set-vlan <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator> <VLAN-ID>| value-of}`	`no set-vlan <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator>| value-of}`
	`no set-vlan`

`auth-server <name>`	`no auth-server <name>`

Chapter 2
Instant User Interface

This chapter describes the following Instant UI elements:

- Login Screen
- Main Window

Login Screen

The Instant login page allows you to:

- Log in to the Instant UI.
- View Instant Network Connectivity summary
- View the InstantUI in a specific language

Logging into the Instant UI

To log in to the Instant UI, enter the following credentials:

- Username– admin
- Password– admin

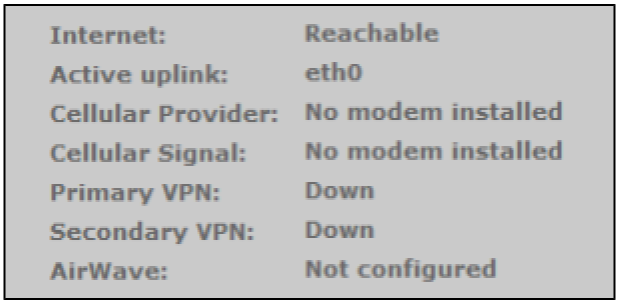
The Instant UI main window is displayed.

Viewing Connectivity Summary

The Login page also displays the connectivity status to the Instant network. The users can view a summary that indicates the status of the Internet availability, uplink, cellular modem and signal strength, VPN, and AirWave configuration details before logging in to the Instant UI.

The following figure shows the information displayed in the connectivity summary:

Figure 3 *Connectivity Summary*



Internet:	Reachable
Active uplink:	eth0
Cellular Provider:	No modem installed
Cellular Signal:	No modem installed
Primary VPN:	Down
Secondary VPN:	Down
AirWave:	Not configured

The Internet status is available only if the Internet failover feature (**System>Show advanced option>uplink>Internet failover**) is enabled.
The cellular provider and cellular strength information is only available when a 3G or 4G modem is in use.

Language

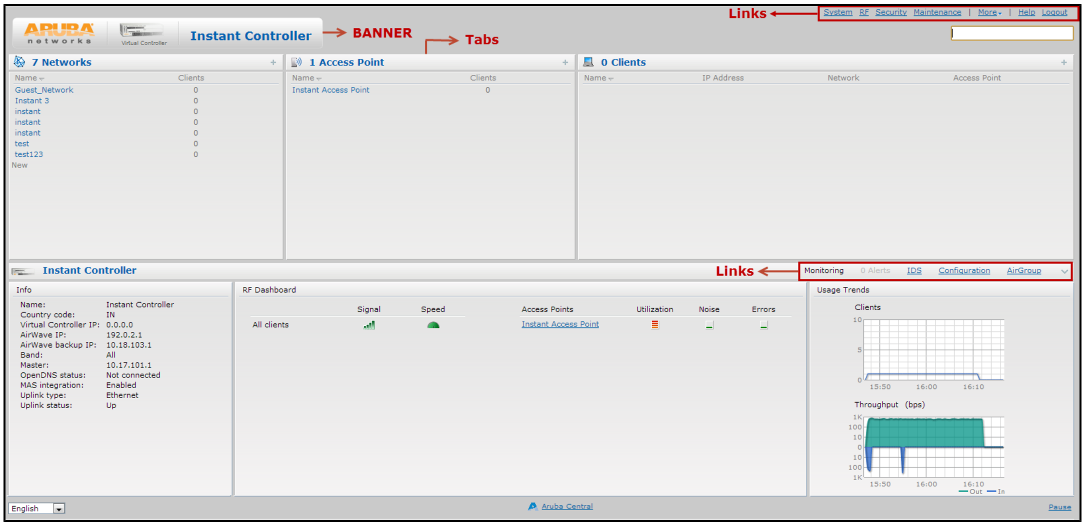
The **Language** drop-down lists the languages and allow users to select their preferred language before logging in to the Instant UI. A default language is selected based on the language preferences in the client desktop operating system or browser. If Instant cannot detect the language, then **English** is used as the default language.

You can also select the required language option from the **Languages** drop-down located at the bottom left corner of the Instant main window.

Main Window

On logging into Instant, the Instant UI Main Window is displayed. The following figure shows the Instant main window:

Figure 4 *Instant Main Window*



7 Networks

Name	Clients
Guest_Network	0
Instant 3	0
instant	0
instant	0
instant	0
test	0
test123	0
New	

1 Access Point

Name	Clients
Instant Access Point	0

0 Clients

Name	IP Address	Network	Access Point

Instant Controller

Info

Name:	Instant Controller
Country code:	IN
Virtual Controller IP:	0.0.0.0
AirWave IP:	192.0.2.1
AirWave backup IP:	10.18.103.1
Band:	All
Master:	10.17.101.1
OpenDNS status:	Not connected
MAS integration:	Enabled
Uplink type:	Ethernet
Uplink status:	Up

RF Dashboard

	Signal	Speed	Access Points	Utilization	Noise	Errors
All clients			Instant Access Point			

The main window consists of the following elements:

- Banner
- Search
- Tabs
- Links
- Views

Banner

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

Search

Administrators can search for an IAP, client, or a network in the **Search** text box. When you type a search text, the search function suggests matching keywords and allows you to automatically complete the search text entry.

Tabs

The Instant main window consists of the following tabs:

- Networks Tab– Provides information about the network profiles configured in the Instant network.
- Access Points Tab– Provides information about the IAPs configured in the Instant network.
- Clients Tab– Provides information about the clients in the Instant network.

Each tab appears in a compressed view by default. The number of networks, IAPs, or clients in the network precedes the tab names. The individual tabs can be expanded or collapsed by clicking on the tabs. The list items in each tab can be sorted by clicking the triangle icon next to the heading labels.

Networks Tab

This tab displays a list of Wi-Fi networks that are configured in the Instant network. The network names appear as links.

The expanded view displays the following information about each Wi-Fi network:

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

To add a Wi-Fi network, click the **New** link in the **Networks** tab. An **edit** link appears on clicking the network name in the **Networks** tab. To delete a network, click on the link **x** next to the **edit** link.

For more information on the procedure to add or modify a wireless network, see Wireless Network Profiles on page 89.

Access Points Tab

If the Auto Join Mode feature is enabled, a list of enabled and active IAPs in the 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 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 of the **Access Points** tab displays the following information about each IAP:

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

An **edit** link appears on clicking the IAP name. For details about editing IAP settings see Initial Configuration Tasks on page 69.

Clients Tab

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

- **Name** – User name of the client or guest users if available.
- **IP Address** – IP address of the client.
- **MAC Address** – MAC address of the client.
- **OS** – Operating system that runs on the client.
- **Network** – The network to which the client is connected.
- **Access Point** – IAP to which the client is connected.
- **Channel** – The client operating channel.
- **Type** – Type of the Wi-Fi client: A, G, AN, or GN.
- **Role** – Role assigned to the client.
- **Signal** – Current signal strength of the client, as detected by the AP.
- **Speed (mbps)** – Current speed at which data is transmitted. When the client is associated with an AP, it constantly negotiates the speed of data transfer. A value of 0 means that the AP has not heard from the client for some time.

Links

The following links allow you to configure various features for the Instant network:

- New Version Available
- System
- RF
- Security
- Maintenance
- More
- Help
- Logout
- Monitoring
- Spectrum
- Alerts
- IDS
- Configuration
- AirGroup
- AirWave Setup
- Pause/Resume

Each of these links is explained in the subsequent sections.

New Version Available

This link appears in the top right corner of Instant main window 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 Upgrading an IAP on page 72.

System

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

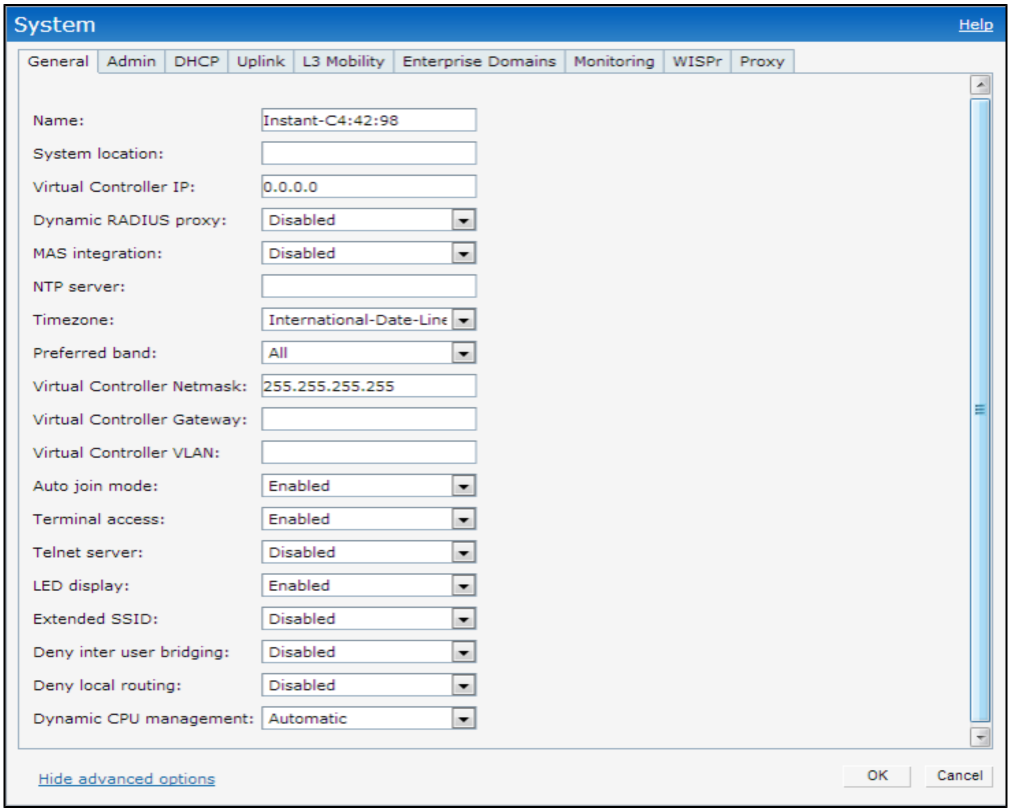
NOTE

Use the **Show/Hide Advanced** option at the bottom of the **System** window to view or hide the advanced options.

- **General**– Allows you to configure, view or edit the Name, IP address, NTP Server, and other IAP settings for the Virtual Controller.
  - For information about Virtual Controller configuration, see Virtual Controller Configuration on page 85.
  - For information about NTP Server configuration, see Configuring an NTP Server on page 78.
  - For information about Auto join mode, Terminal Access, LED display, TFTP Dump Server, and Deny inter user bridging, see IAP Management on page 321.
  - For information on MAS integration, see Mobility Access Switch Overview on page 341.
- **Admin** – Allows you to configure administrator credentials for access to the Virtual Controller Management User Interface. You can also configure AirWave in this tab. For more information on management interface and AirWave configuration, see Configuring Authentication Parameters for Virtual Controller Management Interface on page 154 and Configuring AirWave on page 271 respectively.
- **DHCP** – Allows you to configure DHCP server settings of the Virtual Controller. See DHCP Configuration on page 241for more information.
- **Uplink** – Allows you to view or configure uplink settings. See Uplink Configuration on page 193 for more information.
- **L3 Mobility** – Allows you to view or configure the Layer-3 mobility settings. See Configuring L3-Mobility on page 208 for more information.
- **Enterprise Domains** – Allows you to view or configure the DNS domain names that are valid in the enterprise network. See Configuring Enterprise Domains on page 238 for more information.
- **Monitoring** – Allows you to view or configure the following details:
  - **Syslog** – Allows you to view or configure Syslog Server details for sending syslog messages to the external servers. See Configuring a Syslog Server on page 332 for more information.
  - **TFTP Dump** – Allows you to view or configure a TFTP dump server for core dump files. See Configuring TFTP Dump Server on page 334 for more information.
  - **SNMP** – Allows you to view or configure SNMP agent settings. See Configuring SNMP on page 329 for more information.
- **WISPr** – Allows you to view or configure the WISPr settings. See Configuring WISPr Authentication on page 161 for more information.
- **Proxy** – Allows you to configure the configure HTTP proxy on an IAP. See Configuring HTTP Proxy on an IAP on page 72 for more information.

The following figure shows the default view of the **System** window.

Figure 5 *System Window*



Name:	Instant-C4:42:98
System location:	
Virtual Controller IP:	0.0.0.0
Dynamic RADIUS proxy:	Disabled
MAS integration:	Disabled
NTP server:	
Timezone:	International-Date-Line
Preferred band:	All
Virtual Controller Netmask:	255.255.255.255
Virtual Controller Gateway:	
Virtual Controller VLAN:	
Auto join mode:	Enabled
Terminal access:	Enabled
Telnet server:	Disabled
LED display:	Enabled
Extended SSID:	Disabled
Deny inter user bridging:	Disabled
Deny local routing:	Disabled
Dynamic CPU management:	Automatic

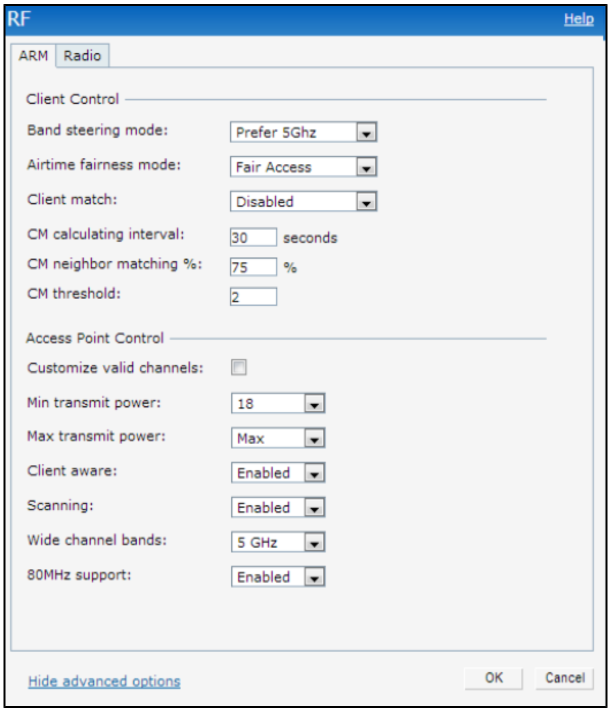
RF

The **RF** link displays a window for configuring Adaptive Radio Management (ARM) and Radio features.

- **ARM** – Allows you to view or configure channel and power settings for all the IAPs in the network. For information about ARM configuration, see ARM Overview on page 219.
- **Radio** – Allows you to view or configure radio settings for 2.4 GHz and the 5 GHz radio profiles. For information about Radio, see Configuring Radio Settings for an IAP on page 226.

The following figure shows the default view of the **RF** window:

Figure 6 *RF Window*



Client Control

Band steering mode: Prefer 5Ghz

Airtime fairness mode: Fair Access

Client match: Disabled

CM calculating interval: 30 seconds

CM neighbor matching %: 75 %

CM threshold: 2

Access Point Control

Customize valid channels: □

Min transmit power: 18

Max transmit power: Max

Client aware: Enabled

Scanning: Enabled

Wide channel bands: 5 GHz

80MHz support: Enabled

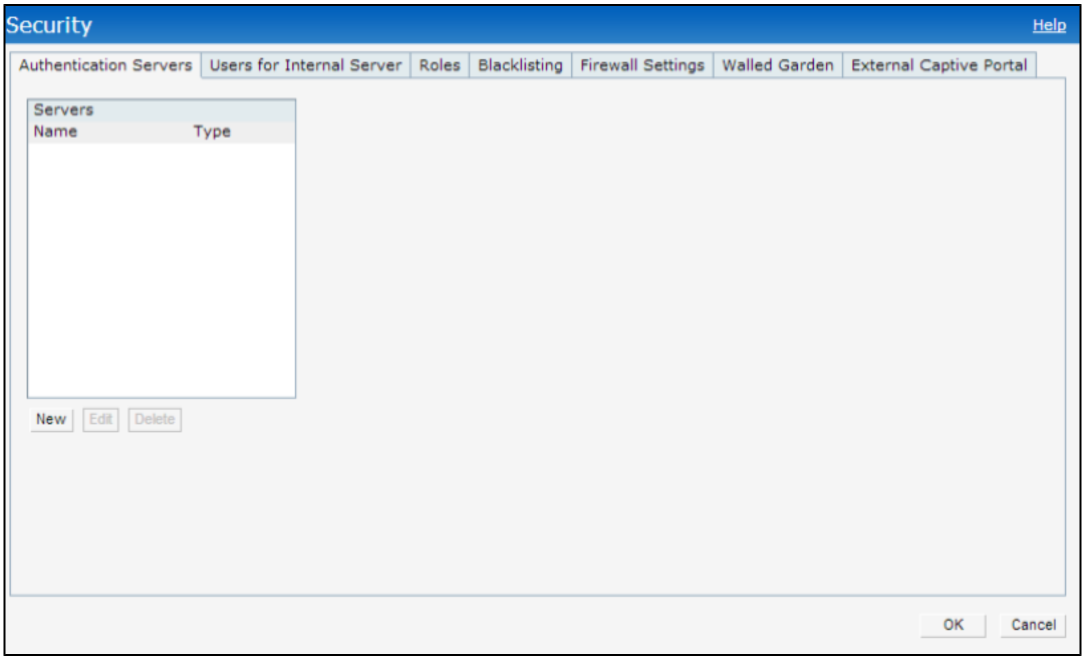
Security

The **Security** link displays a window with the following tabs:

- **Authentication Servers**– Use this window to configure an external RADIUS server for a wireless network. See Configuring an External Server for Authentication on page 149 for more information.
- **Users for Internal Server**– Use this window to populate the system's internal authentication server with users. This list is used by networks for which per-user authorization is specified using the Virtual Controller's internal authentication server. For more information about users, see User Management on page 133.
- **Roles–** Use this window to view the roles defined for all the Networks. The Access Rules part allows you to configure permissions for each role. For more information, see Configuring User Roles on page 180.
- **Blacklisting**– Use this window to blacklist clients. For more information, see Blacklisting Clients on page 162.
- **Firewall Settings**– Use this window to enable or disable Application Layer Gateway (ALG) supporting address and port translation for various protocols. For more information, see Roles and Policies on page 169.
- **Walled Garden**–Use this window to allow or prevent access to a selected list of Websites. For more information, see Configuring Walled Garden Access on page 131.
- **External Captive Portal**– Use this window to configure external Captive portal profiles. For more information, see Configuring External Captive Portal for a Guest Network on page 123.

The following figure shows the default view of the **Security** window:

Figure 7 *Security Window - Default View*



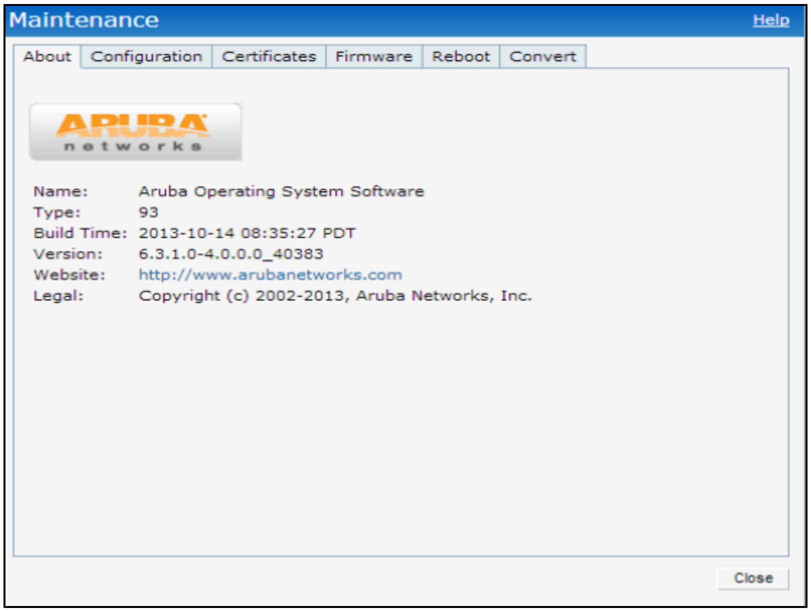
Maintenance

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

- **About**–Displays the name of the product, build time, IAP model name, the Instant version, Website address of Aruba Networks, , , and Copyright information.
- **Configuration**– Displays the following details:
  - **Current Configuration** – Displays the current configuration details.
  - **Clear Configuration** –Allows you to clear the current configuration details of the network.
  - **Factory Reset** –Allows you to reset an IAP to the default factory configuration settings.
  - **Backup Configuration** – Allows you to back up local configuration details. The backed up configuration data is saved in the file named **instant.cfg**.
  - **Restore Configuration** – Allows you to restore the backed up configuration. The IAP must be rebooted after restoring the configuration for the changes to affect.
- **Certificates** – Displays information about the certificates installed in the Instant network. You can also upload new certificates and set a passphrase for the certificates. For more information, see Uploading Certificates on page 164.
- **Firmware** – Displays the current firmware version and provides various options to upgrade to a new firmware version. For more information, see Upgrading an IAP on page 72.
- **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 Upgrading an IAP on page 72.
- **Convert** – Provides an option to convert an IAP to a mobility controller managed Remote AP or Campus AP, or a standalone AP. For more information, see Converting an IAP to a Remote AP and Campus AP on page 322.

The following figure shows the default view of the **Maintenance** window:

Figure 8 *Maintenance Window - Default View*



Name: Aruba Operating System Software
Type: 93
Build Time: 2013-10-14 08:35:27 PDT
Version: 6.3.1.0-4.0.0.0_40383
Website: http://www.arubanetworks.com
Legal: Copyright (c) 2002-2013, Aruba Networks, Inc.

Help

The **Help** link allows you to view a short description or definition of selected terms and fields in the UI windows or dialogs.

To activate the context-sensitive help:

1. Click the **Help** link at the top right corner of Instant main window.
2. Click any text or term displayed in green italics to view its description or definition.
3. To disable the help mode, click **Done**.

More

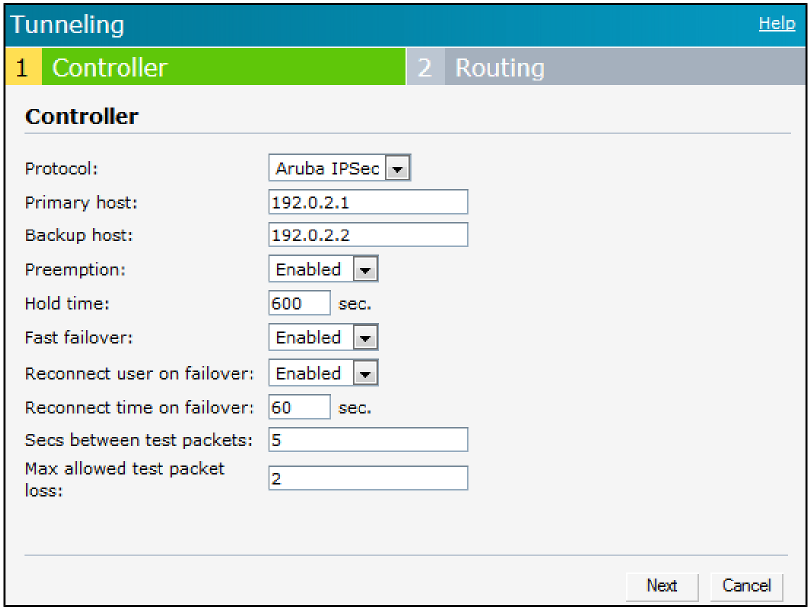
The **More** link allows you to select the following options:

- VPN
- IDS
- Wired
- Services
- DHCP Server
- Support

VPN

The **VPN** window allows you to define communication settings with a remote Controller. See VPN Configuration on page 249 for more information. The following figure shows the an example of the IPSec configuration options available in the **VPN** window:

Figure 9 *VPN window for IPSec Configuration*



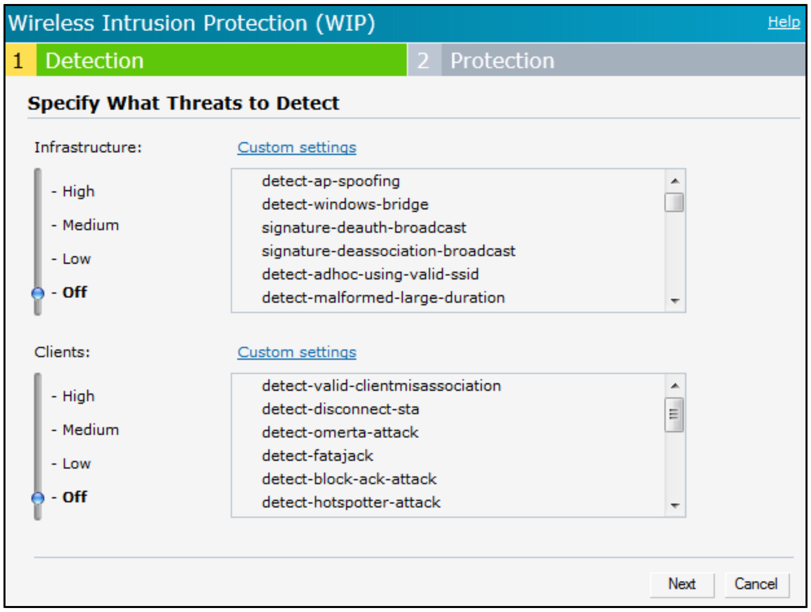
Controller

Protocol: Aruba IPSec
Primary host: 192.0.2.1
Backup host: 192.0.2.2
Preemption: Enabled
Hold time: 600 sec.
Fast failover: Enabled
Reconnect user on failover: Enabled
Reconnect time on failover: 60 sec.
Secs between test packets: 5
Max allowed test packet loss: 2

IDS

The IDS window allows you to configure wireless intrusion detection and protection levels. The following figures show the **IDS** window:

Figure 10 *IDS Window: Intrusion Detection*



Specify What Threats to Detect

Infrastructure: Custom settings

- Off

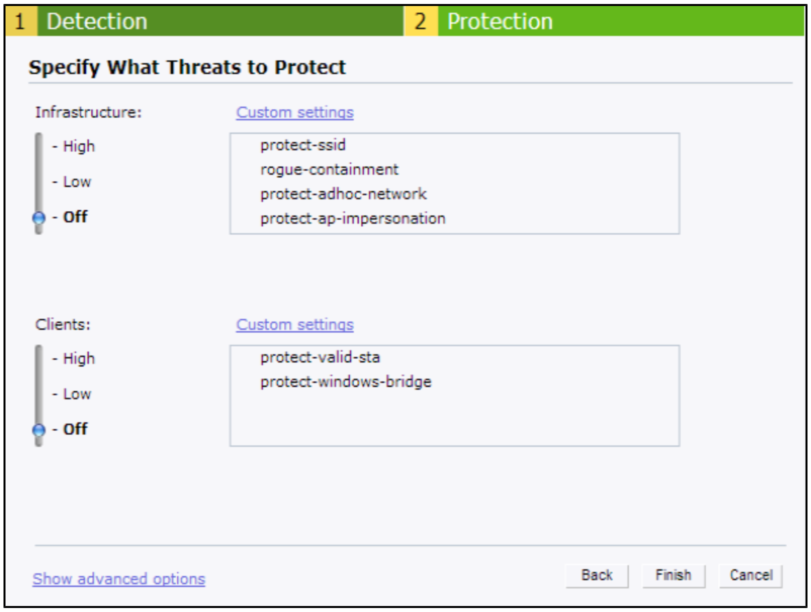
detect-ap-spoofing
detect-windows-bridge
signature-deauth-broadcast
signature-deassociation-broadcast
detect-adhoc-using-valid-ssid
detect-malformed-large-duration

Clients: Custom settings

- Off

detect-valid-clientmisassociation
detect-disconnect-sta
detect-omerta-attack
detect-fatajack
detect-block-ack-attack
detect-hotspotter-attack

Figure 11 *IDS Window: Intrusion Protection*



Infrastructure: Off

protect-ssid
rogue-containment
protect-adhoc-network
protect-ap-impersonation

Clients: Off

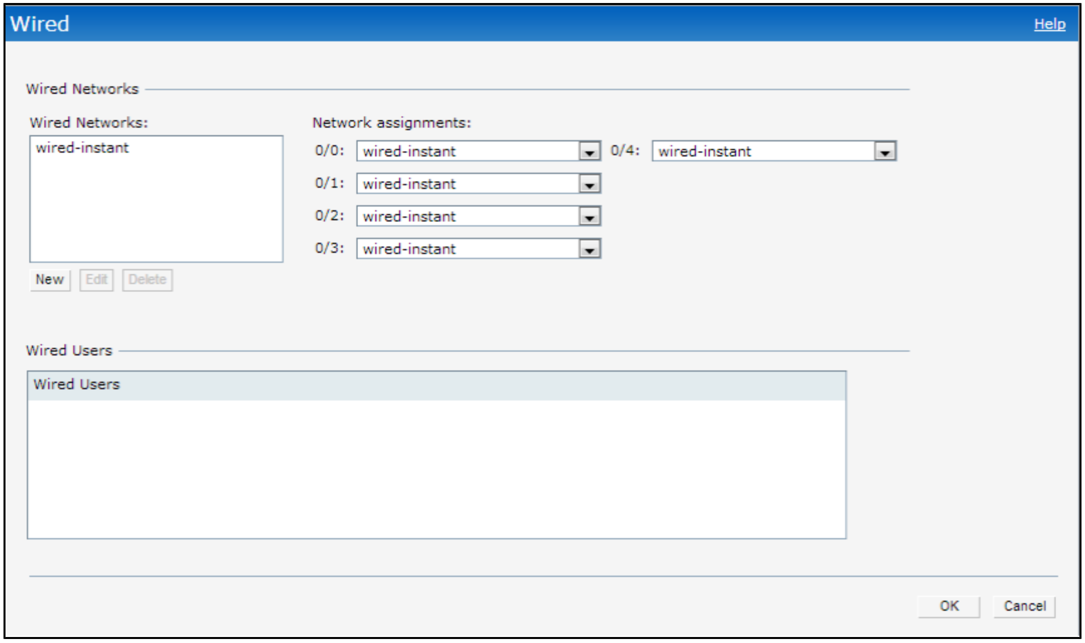
protect-valid-sta
protect-windows-bridge

For more information on wireless intrusion detection and protection, see Detecting and Classifying Rogue APs on page 229.

Wired

The **Wired** window allows you to configure a wired network profile. See Wired Profiles on page 107 for more information. The following figure shows the **Wired** window:

Figure 12 *Wired Window*



Wired Networks: wired-instant

Network assignments:

0/0: wired-instant
0/1: wired-instant
0/2: wired-instant
0/3: wired-instant
0/4: wired-instant

Services

The **Services** window allows you to configure services such as AirGroup, RTLS, and OpenDNS. The Services window consists of the following tabs:

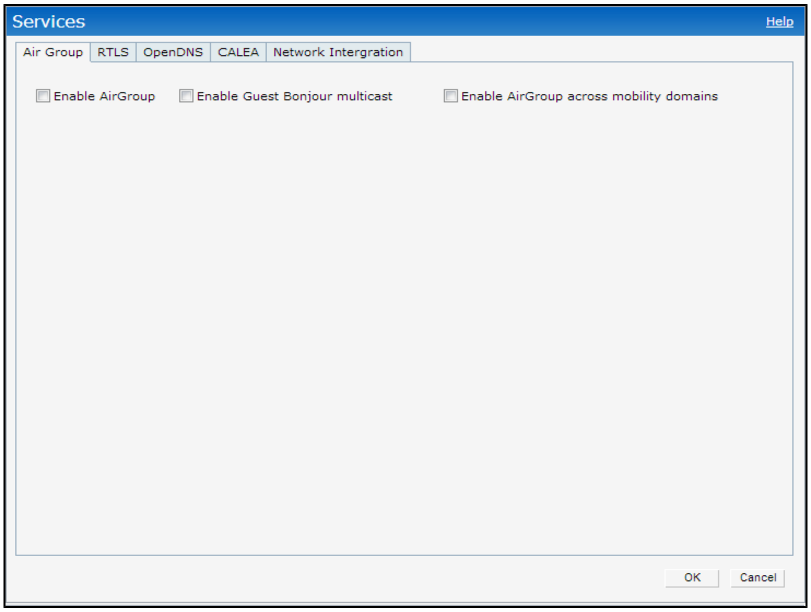
- **AirGroup** – Allows you to configure the AirGroup and AirGroup services. For more information, see AirGroup Configuration on page 281.

- **RTLS** – Allows you to integrate AirWave Management platform or third-party Real Time Location Server such as Aeroscout Real Time Location Server with Instant. For more information, see IAP Integration with Security and Location Services Applications on page 289.

  The RTLS tab also allows you to integrate IAP with the Analytics and Location Engine (ALE). For more information about configuring an IAP for ALE integration, see Configuring an IAP for Analytics and Location Engine Support on page 289.
- **OpenDNS**– Allows you to configure support for OpenDNS business solutions, which require an OpenDNS (www.opendns.com) account. The OpenDNS credentials are used by Instant and AirWave to filter content at the enterprise level. For more information, see Configuring OpenDNS Credentials on page 238.
- **CALEA**–Allows you configure support for Communications Assistance for Law Enforcement Act (CALEA) server integration, thereby ensuring compliance with Lawful Intercept and CALEA specifications. For more information, see Lawful Intercept and CALEA Integration on page 295
- **Network Integration**–Allows you configure an IAP for integration with Palo Alto Networks (PAN) Firewall. For more information about IAP integration with PAN, see Integrating an IAP with Palo Alto Networks Firewall on page 291.

The following figure shows the default view of the **Services** window:

Figure 13 *Services Window: Default View*



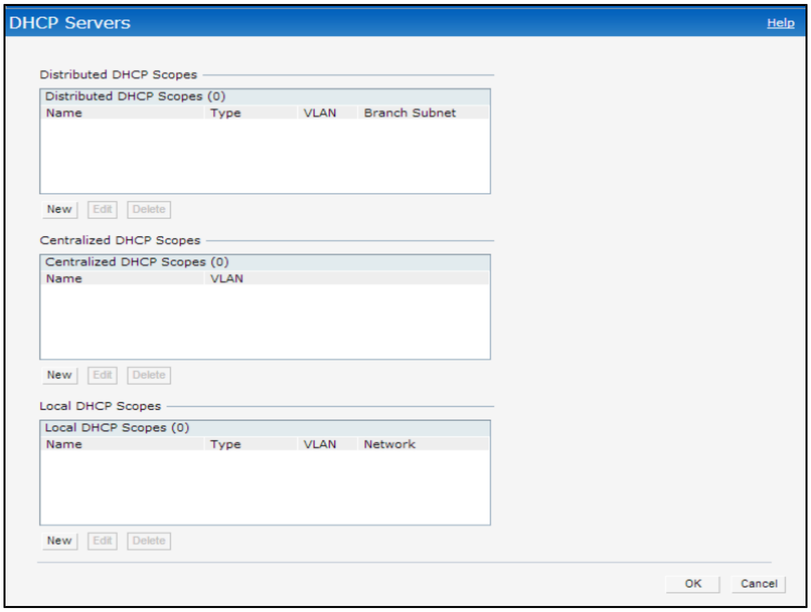
Services

□ Enable AirGroup □ Enable Guest Bonjour multicast □ Enable AirGroup across mobility domains

DHCP Server

The DHCP Servers window allows you to configure various DHCP modes. The following figure shows the contents of the **DHCP Servers** window:

Figure 14 *DHCP Servers Window*



Distributed DHCP Scopes

Distributed DHCP Scopes (0)

Name	Type	VLAN	Branch Subnet

Centralized DHCP Scopes

Centralized DHCP Scopes (0)

Name	VLAN

Local DHCP Scopes

Local DHCP Scopes (0)

Name	Type	VLAN	Network

For more information, see DHCP Configuration on page 241.

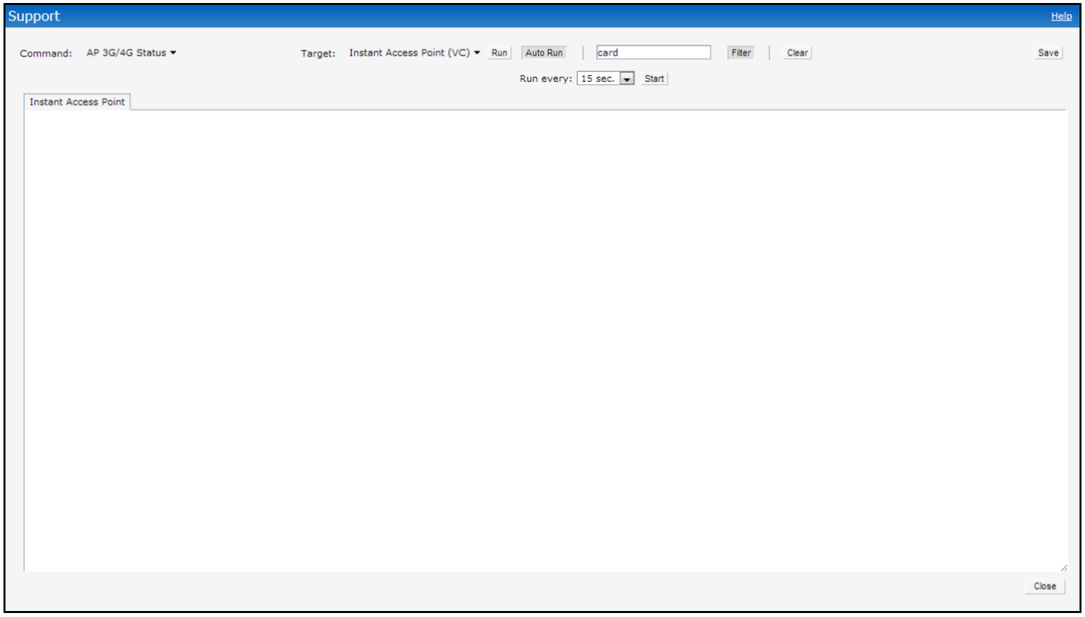
Support

The **Support** consists of the following fields:

- **Command**– Allows you to select a support command for execution.
- **Target**–Displays a list of IAPs in the network.
- **Run**– Allows you to execute the selected command for a specific IAP or all IAPs and view logs.
- **Auto Run**– Allows you to configure a schedule for automatic execution of a support command for a specific IAP or all IAPs.
- **Filter**–Allows you to filter the contents of a command output.
- **Clear**–Clears the command output displayed after a command is executed.
- **Save Results**– Allows you to save the support command logs as an HTML or text file.

For more information on support commands, see Running Debug Commands from the Instant UI on page 335. The following figure shows the **Support** window:

Figure 15 *Support Window*



Command: AP 3G/4G Status
Target: Instant Access Point (VC)
card
Run every: 15 sec.

Logout

The **Logout** link allows you to log out of the Instant UI.

Monitoring

The **Monitoring** link displays the Monitoring pane for the 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
- RF Trends
- Usage Trends
- Mobility Trail

Info

The **Info** section displays the configuration information of the Virtual Controller by default. On selecting the Network View tab, the monitoring pane displays configuration information of the selected network. Similarly in the Access Point or the Client view, this section displays the configuration information of the selected IAP or the client.

Table 7: *Contents of the Info Section in the Instant Main Window*

Name	Description
Info section in Virtual Controller view	The **Info** section in the Virtual Controller view displays the following information: ● **Name**– Displays the Virtual Controller name. ● **System Location**–Displays the system location. ● **Country Code**– Displays the Country in which the Virtual Controller is operating. ● **Virtual Controller IP address**– Displays the IP address of the Virtual Controller. ● **AirWave Server** and **Backup Server** – Displays the names of the AirWave server and the backup servers if AirWave servers are configured. ● **Band**– Displays the band in which the Virtual Controller is operating – 2.4 GHz band, 5 GHz band, or both.

Table 7: *Contents of the Info Section in the Instant Main Window*

Name	Description
	- **Master**– Displays the IP address of the Access Point acting as Virtual Controller. - **OpenDNS Status**– Displays the OpenDNS status. If the OpenDNS status indicates as **Not Connected**, ensure that the network connection is up and appropriate credentials are configured for **OpenDNS**. - **MAS integration**– Displays the status of the MAS integration feature. - **Uplink type** – Displays the type of uplink configured on the IAP: for example, Ethernet or 3G. - **Uplink status** – Indicates the uplink status. - **Blacklisted clients** – Displays the number of blacklisted clients. - **Internal RADIUS Users** – Displays the number of internal RADIUS users. - **Internal Guest Users** – Displays the number of internal guest users. - **Internal User Open Slots**– Displays the available slots for user configuration as supported by the IAP model.
Info section in Client view	The **Info** section in the Client view displays the following information: - **Name**– Displays the name of the client. - **IP Address**– Displays IP address of the client. - **MAC Address**– Displays MAC Address of the client. - **OS**– Displays the Operating System that is running on the client. - **Network**– Indicates the network to which the client is connected. - **Access Point**– Indicates the IAP to which the client is connected. - **Channel**– Indicates the channel that is currently used by the client. - **Type**– Displays the channel type on which client is broadcasting.
Info section in Network view	The **Info** section in the Network view displays the following information: - **Name** – Displays Name of the network. - **Status** – Displays the status of network. - **Band** – Displays the band in which the network is broadcast: For example, 2.4 GHz band, 5 GHz band, or both. - **Type** – Displays the type of network: For example, Employee, Guest, or Voice. - **IP Assignment**– Displays the source of IP address for the client. - **Access**– Indicates the level of access control configured for the network. - **Security level**– Indicates the type of user authentication and data encryption configured for the network The **info** section for WLAN SSIDs also indicates status of Captive Portal and CALEA ACLs.
Info section in Access Point view	The **Info** section in the Access Point view displays the following information : - **Name** – Displays the name of the selected IAP. - **IP Address** – Displays the IP address of the IAP. - **Mode** – Displays the mode in which the AP is configured to operate: - In **Access** mode, the IAP serves clients, while also monitoring for rogue APs in the background. - In **Monitor** mode, the IAP acts as a dedicated monitor, scanning all channels for rogue APs and clients. - **Spectrum** – Displays the status of the spectrum monitor. - **Clients** – Number of clients associated with the IAP. - **Type** – Displays the model number of the IAP. - **CPU Utilization** – Displays the CPU utilization in percentage. - **Memory Free** – Displays the memory availability of the IAP in MB. - **Serial number** – Displays the serial number of the IAP. - **From Port**– Displays the port from where the slave IAP is learned in hierarchy mode.

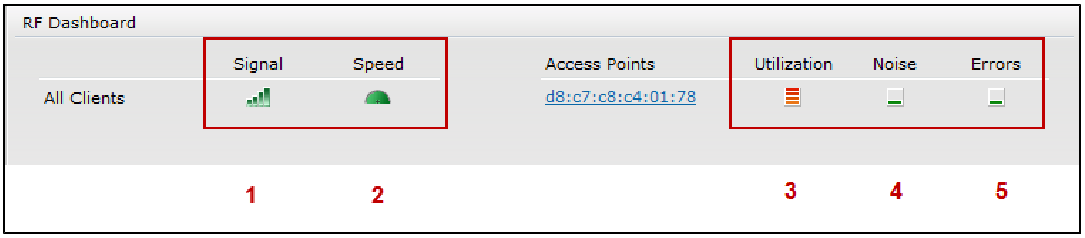
RF Dashboard

The **RF Dashboard** section lists the IAPs that exceed the utilization, noise, or error threshold. It also shows the clients with low speed or signal strength in the network and the RF information for the IAP to which the client is connected.

The IAP names appear as links. When an IAP is clicked, the IAP configuration information is displayed in the Info section and the RF Dashboard section is displayed at the bottom left corner of the Instant main window.

The following figure shows an example of the RF dashboard with Utilization, Band frames, Noise Floor, and Errors details:

Figure 16 *RF Dashboard in the Monitoring Pane*



RF Dashboard

	Signal	Speed	Access Points	Utilization	Noise	Errors
All Clients			d8:c7:c8:c4:01:78			

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

Table 8: *RF Dashboard Icons*

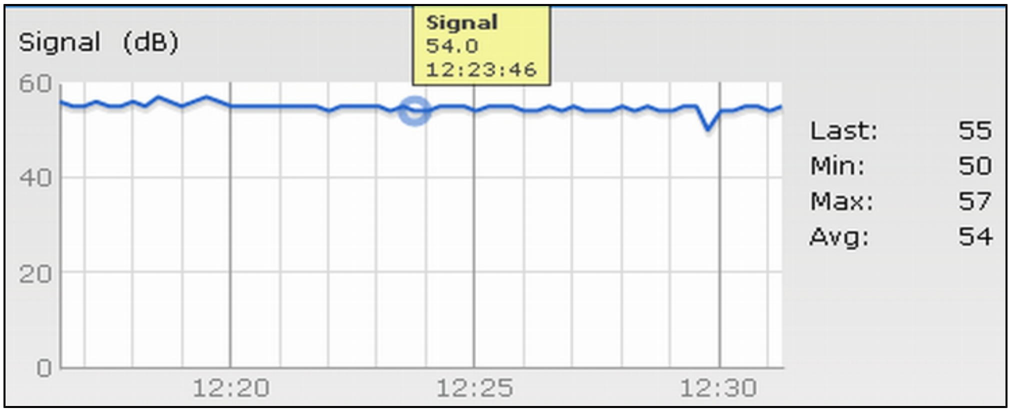
Icon	Name	Description
1	Signal Icon	Displays the signal strength of the client. Depending on the signal strength of the client, the color of the lines on the Signal bar changes from Green > Orange > Red. ● Green– Signal strength is more than 20 decibels. ● Orange– Signal strength is between 15-20 decibels. ● Red– Signal strength is less than 15 decibels. To view the signal graph for a client, click on the signal icon next to the client in the **Signal** column.
2	Speed icon	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.
3	Utilization icon	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 the Utilization icon next to the IAP in the Utilization column.
4	Noise icon	Displays the noise floor details for 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 87 dBm. ● 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 the noise icon next to the IAP in the Noise column.

Icon	Name	Description
5	Errors icon	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 the **Errors** icon next to the IAP in the **Errors** column.

RF Trends

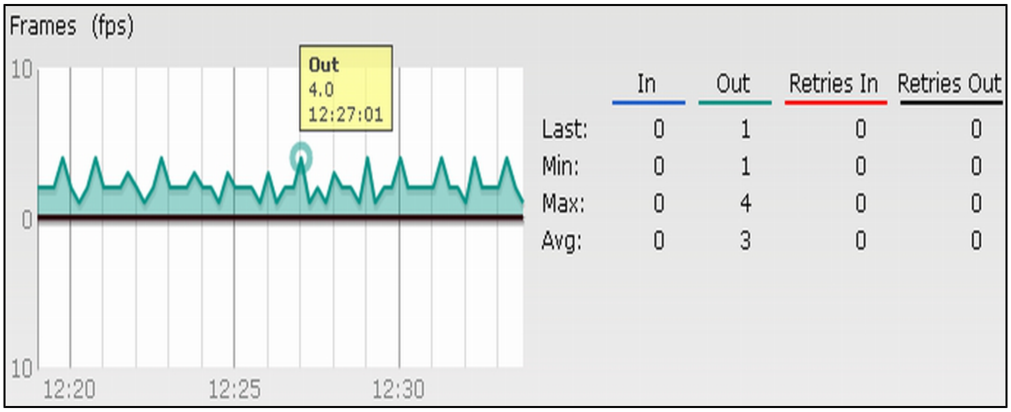
The **RF Trends** section displays the following graphs for the selected client:

Figure 17 *Signal Graph*



Last:	55
Min:	50
Max:	57
Avg:	54

Figure 18 *Frames Graph*



	In	Out	Retries In	Retries Out
Last:	0	1	0	0
Min:	0	1	0	0
Max:	0	4	0	0
Avg:	0	3	0	0

Figure 19 *Speed Graph*

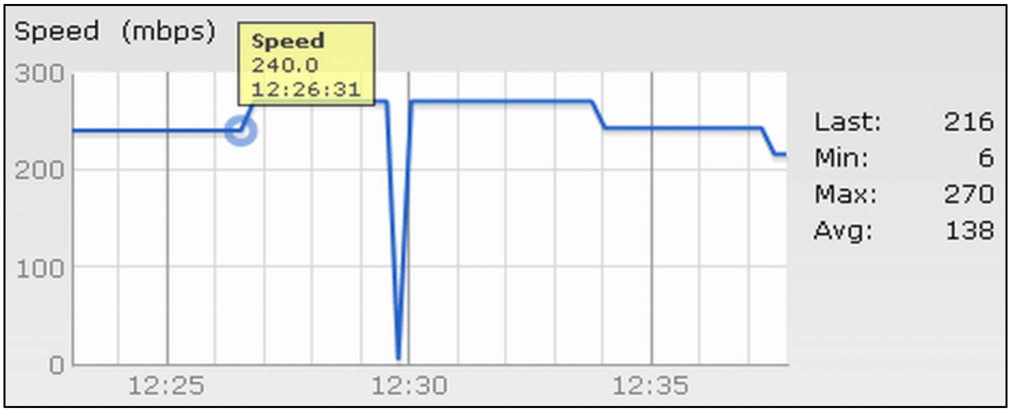
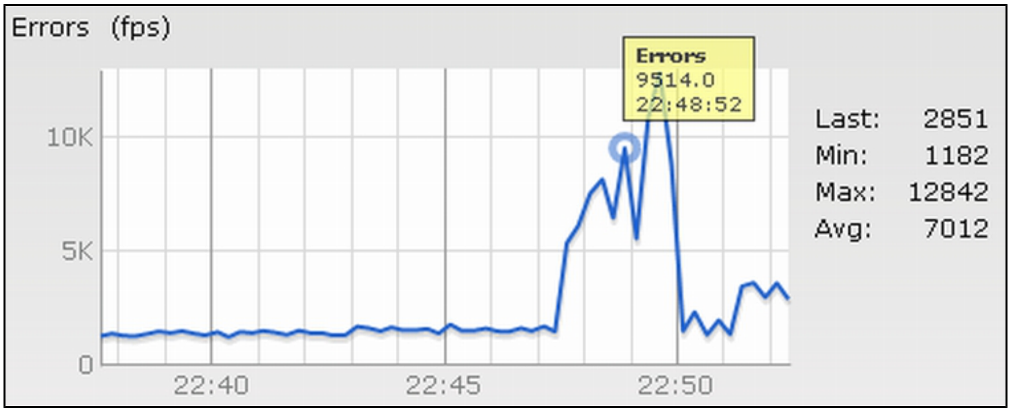


Figure 20 *Throughput Graph*

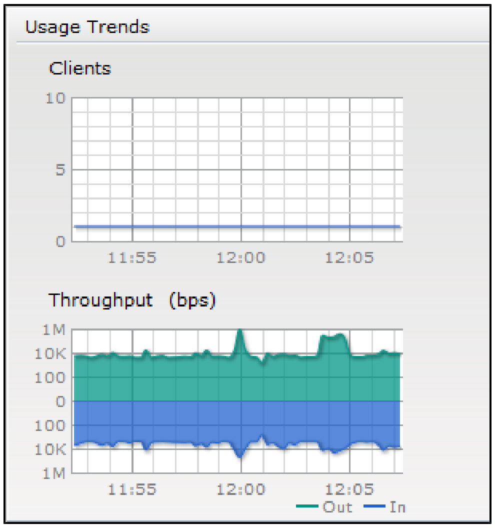


Usage Trends

The **Usage Trends** displays the following graphs:

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

Figure 21 *Usage Trends Section in the Monitoring Pane*



The following table describes the graphs displayed in the Network view:

Table 9: *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 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 shows that one client is associated with the selected network at 12:00 hours.
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 shows 22.0 Kbps incoming traffic throughput for the selected network at 12:03 hours.

The following table describes the graphs displayed in the Access Point view:

Table 10: *Access Point View – Usage Trends and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Neighboring APs	The Neighboring APs graph shows the number of APs heard by the selected IAP: ● Valid APs: An AP that is part of the enterprise providing WLAN service. ● Interfering APs: An AP that is seen in the RF environment but is not connected to the network. ● Rogue APs: An unauthorized AP that is plugged into the wired side of the network. To see the number of different types of neighboring APs for the last 15 minutes, hover the cursor over the respective graph lines.	To check the neighboring APs detected by 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 Neighboring APs graph in the **Overview** section. For example, the graph shows that 148 interfering APs are detected by the IAP at 12:04 hours.
CPU Utilization	The CPU Utilization graph displays the utilization of CPU for the selected IAP. To see the CPU utilization of the IAP, hover the cursor over the graph line.	To check the CPU utilization of 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 CPU Utilization graph in the **Overview** pane. For example, the graph shows that the CPU utilization of the IAP is 30% at 12:09 hours.
Neighboring Clients	The Neighboring Clients graph shows the number of clients not connected to the selected AP, but heard by it. ● Any client that successfully authenticates with a valid AP and passes encrypted traffic is classified as a valid client. ● Interfering: A client associated to any AP and is not valid is classified as an interfering client. To see the number of different types of neighboring clients for the last 15 minutes, hover the cursor over the respective graph lines.	To check the neighboring clients detected by 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 Neighboring Clients graph in the **Overview** pane. For example, the graph shows that 20 interfering clients were detected by the IAP at 12:15 hours.
Memory free (MB)	The memory free graph displays the memory availability of the IAP in MB. To see the free memory of the IAP, hover the cursor over the graph line.	To check the free memory of 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 Memory free graph in the **Overview** pane. For example, the graph shows that the free memory of the IAP is 64 MB at 12:13 hours.
Clients	The Clients graph shows the number of clients associated with the selected IAP for the last 15 minutes.	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.

Table 10: *Access Point View – Usage Trends and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
	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.	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. For example, the graph shows that six clients are associated with the IAP at 12:11 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. For example, the graph shows 44.03 Kbps incoming traffic throughput at 12:08 hours.

The following table describes the RF trends graphs available in the client view:

Table 11: *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 of the client for the last 15 minutes. To see the exact signal strength at a particular time, move 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 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 of the client for the last 15 minutes. It also shows data for the Retry In and Retry Out frames. ● Outgoing frames – Outgoing frame	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.

Table 11: *Client View – RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
	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 are displayed above the median line in black . - Retry In – Retries for the incoming frames are displayed below the median line in red. 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 move the cursor over the graph line.	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 shows 4.0 frames per second for the client at 12:27 hours.
Speed	The Speed graph shows the data transfer speed for the client. Data transfer is measured in Mbps. To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics of the client for the last 15 minutes. To see the exact speed at a particular time, move 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 shows that the data transfer speed at 12:26 hours is 240 Mbps.
Throughput	The Throughput Graph shows the throughput of 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, move 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 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.
  The Instant UI shows the client and IAP association over the last 15 minutes.
- **Access Point**– The 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.

Spectrum

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

The spectrum link displays the following:

- **Device list** - The device list display consists of a device summary table and channel information for active non Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio.
- **Channel Utilization and Monitoring** - This chart provides an overview of channel quality across the spectrum. It shows channel utilization information such as channel quality, availability, and utilization metrics as seen by a spectrum monitor for the 2.4 GHz and 5 GHz radio bands. The first bar for each channel represents the percentage of air time used by non Wi-Fi interferers and Wi-Fi devices. The second bar indicates the channel quality. A higher percentage value indicates better quality.
- **Channel Details** - When you move your mouse over a channel, the channel details or the summary of the 5 GHz and 2.4 GHz channels as detected by a spectrum monitor are displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference and the Signal-to-Noise and Interference Ratio (SNIR). Spectrum monitors display spectrum analysis data seen on all channels in the selected band, and hybrid IAPs display data from the one channel they are monitoring.

For more information on spectrum monitoring, see Spectrum Monitor on page 211.

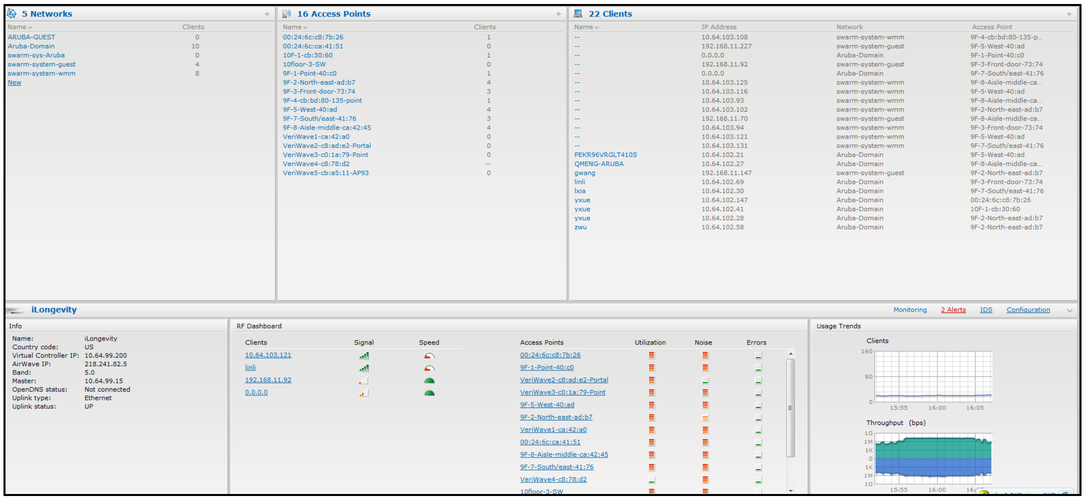
Alerts

Alerts are generated when a user encounters problems while accessing or connecting to a network. The alerts that are generated on 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 failures - Static IP address or DHCP related alerts.

The following figure shows the contents of details displayed on clicking the **Alerts** link:

Figure 22 *Alerts Link*



5 Networks

Name	Clients
ARUBA-GUEST	0
Aruba-Domain	10
swarm-sys-Aruba	0
swarm-system-guest	4
swarm-system-wmm	8
New	

16 Access Points

Name	Clients
00:24:6c:c8:7b:26	1
00:24:6c:ca:41:51	0
10F-1-cb:30:60	1
10floor-3-SW	0
9F-1-Point-40:c0	1
9F-2-North-east-ad:b7	4
9F-3-Front-door-73:74	3
9F-4-cb:bd:80-135-point	1
9F-5-West-40:ad	4
9F-7-South/east-41:76	3
9F-8-Aisle-middle-ca:42:45	4
VeriWave1-ca:42:a0	0
VeriWave2-c8:ad:e2-Portal	0
VeriWave3-c0:1a:79-Point	0
VeriWave4-c8:78:d2	--
VeriWave5-cb:a5:11-AP93	0

22 Clients

Name	IP Address	Network	Access Point
--	10.64.103.108	swarm-system-wmm	9F-4-cb:bd:80-135-p...
--	192.168.11.227	swarm-system-guest	9F-5-West-40:ad
--	0.0.0.0	Aruba-Domain	9F-1-Point-40:c0
--	192.168.11.92	swarm-system-guest	9F-3-Front-door-73:74
--	0.0.0.0	Aruba-Domain	9F-7-South/east-41:76
--	10.64.103.125	swarm-system-wmm	9F-8-Aisle-middle-ca...
--	10.64.103.116	swarm-system-wmm	9F-5-West-40:ad
--	10.64.103.93	swarm-system-wmm	9F-8-Aisle-middle-ca...
--	10.64.103.102	swarm-system-wmm	9F-2-North-east-ad:b7
--	192.168.11.70	swarm-system-guest	9F-8-Aisle-middle-ca...
--	10.64.103.94	swarm-system-wmm	9F-3-Front-door-73:74
--	10.64.103.121	swarm-system-wmm	9F-5-West-40:ad
--	10.64.103.131	swarm-system-wmm	9F-7-South/east-41:76
PEKR96VRGLT410S	10.64.102.21	Aruba-Domain	9F-5-West-40:ad
QMENG-ARUBA	10.64.102.27	Aruba-Domain	9F-8-Aisle-middle-ca...
gwang	192.168.11.147	swarm-system-guest	9F-2-North-east-ad:b7
linli	10.64.102.69	Aruba-Domain	9F-3-Front-door-73:74
lxia	10.64.102.30	Aruba-Domain	9F-7-South/east-41:76
yxue	10.64.102.147	Aruba-Domain	00:24:6c:c8:7b:26
yxue	10.64.102.41	Aruba-Domain	10F-1-cb:30:60
yxue	10.64.102.28	Aruba-Domain	9F-2-North-east-ad:b7
zwu	10.64.102.58	Aruba-Domain	9F-2-North-east-ad:b7

iLongevity

Info

Name:	iLongevity
Country code:	US
Virtual Controller IP:	10.64.99.200
AirWave IP:	218.241.82.5
Band:	5.0
Master:	10.64.99.15
OpenDNS status:	Not connected
Uplink type:	Ethernet
Uplink status:	UP

RF Dashboard

Clients	Signal	Speed
10.64.103.121	▂▄▆█	◔
linli	▂▄▆█	◔
192.168.11.92	▂	●
0.0.0.0	▂▄	●

Access Points	Utilization	Noise	Errors
00:24:6c:c8:7b:26	≡	≡	▁
9F-1-Point-40:c0	≡	≡	▁
VeriWave2-c8:ad:e2-Portal	≡	▁	▁
VeriWave3-c0:1a:79-Point	≡	≡	▁
9F-5-West-40:ad	≡	≡	▁
9F-2-North-east-ad:b7	≡	≡	▁
VeriWave1-ca:42:a0	≡	≡	▁
00:24:6c:ca:41:51	≡	≡	▁
9F-8-Aisle-middle-ca:42:45	≡	≡	▁
9F-7-South/east-41:76	≡	≡	▁
VeriWave4-c8:78:d2	▁	≡	▁
10floor-3-SW	≡	≡	▁

Usage Trends

The **Alerts** link displays the following types of alerts:

- Client Alerts
- Active Faults

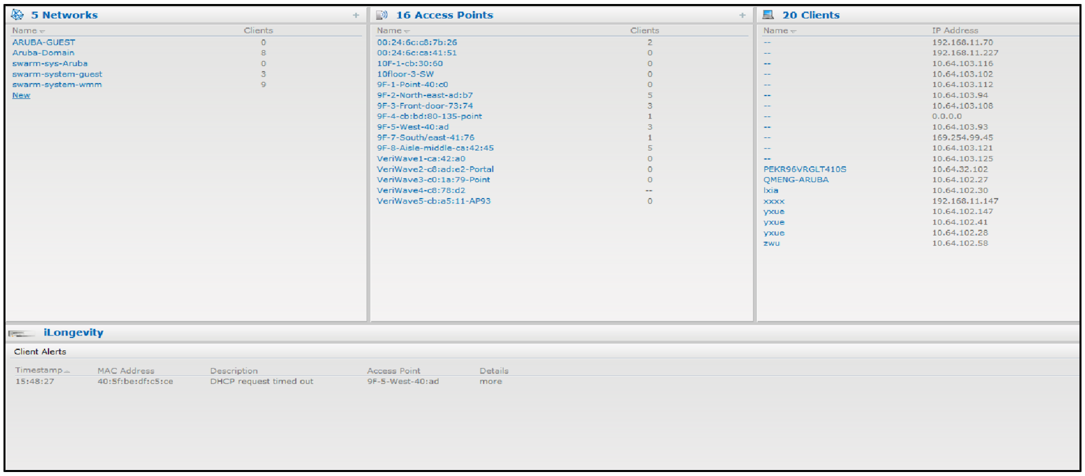
- Fault History

Table 12: *Types of Alerts*

Type of Alert	Description	Information Displayed
Client Alerts	The **Client alerts** occur when clients are connected to the Instant network.	A client alert displays 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.
Active Faults	The **Active Faults** occur in the event of a system fault.	An **Active Faults** 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.
Fault History	The Fault History alerts occur in the event of a system fault.	The **Fault History** displays the following information: ● **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.

The following figures show the client alerts, fault history, and active faults:

Figure 23 *Client Alerts*



5 Networks

Name	Clients
ARUBA-GUEST	0
Aruba-Domain	8
swarm-sys-Aruba	0
swarm-system-guest	3
swarm-system-wmm	9
New	

16 Access Points

Name	Clients
00:24:6c:c8:7b:26	2
00:24:6c:ca:41:51	0
10F-1-cb:30:60	0
10floor-3-SW	0
9F-1-Point-40:c0	0
9F-2-North-east-ad:b7	5
9F-3-Front-door-73:74	3
9F-4-cb:bd:80-135-point	1
9F-5-West-40:ad	3
9F-7-South/east-41:76	1
9F-8-Aisle-middle-ca:42:45	5
VeriWave1-ca:42:a0	0
VeriWave2-c8:ad:e2-Portal	0
VeriWave3-c0:1a:79-Point	0
VeriWave4-c8:78:d2	--
VeriWave5-cb:a5:11-AP93	0

20 Clients

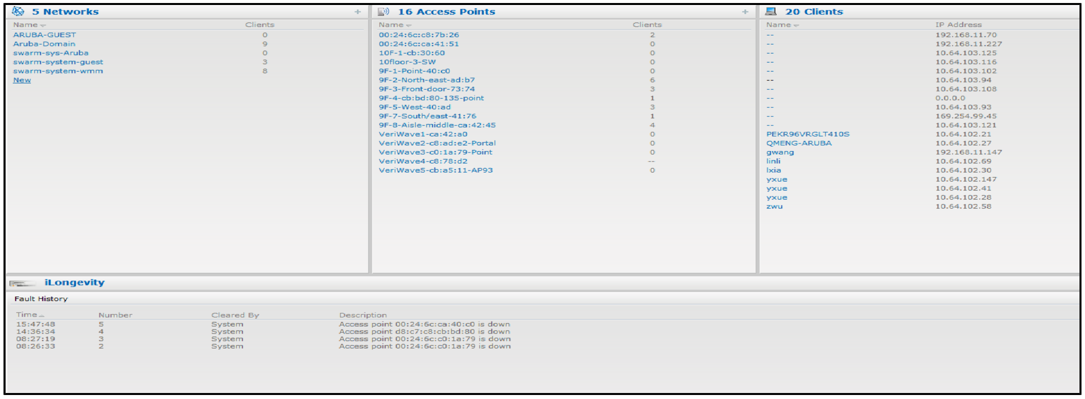
Name	IP Address
--	192.168.11.70
--	192.168.11.227
--	10.64.103.116
--	10.64.103.102
--	10.64.103.112
--	10.64.103.94
--	10.64.103.108
--	0.0.0.0
--	10.64.103.93
--	169.254.99.45
--	10.64.103.121
--	10.64.103.125
PEKR96VRGLT410S	10.64.32.102
QMENG-ARUBA	10.64.102.27
lxia	10.64.102.30
xxxx	192.168.11.147
yxue	10.64.102.147
yxue	10.64.102.41
yxue	10.64.102.28
zwu	10.64.102.58

iLongevity

Client Alerts

Timestamp	MAC Address	Description	Access Point	Details
15:48:27	40:5f:be:df:c5:ce	DHCP request timed out	9F-5-West-40:ad	more

Figure 24 *Fault History*



5 Networks

Name	Clients
ARUBA-GUEST	0
Aruba-Domain	9
swarm-sys-Aruba	0
swarm-system-guest	3
swarm-system-wmm	8
New	

16 Access Points

Name	Clients
00:24:6c:c8:7b:26	2
00:24:6c:ca:41:51	0
10F-1-cb:30:60	0
10floor-3-SW	0
9F-1-Point-40:c0	0
9F-2-North-east-ad:b7	6
9F-3-Front-door-73:74	3
9F-4-cb:bd:80-135-point	1
9F-5-West-40:ad	3
9F-7-South/east-41:76	1
9F-8-Aisle-middle-ca:42:45	4
VeriWave1-ca:42:a0	0
VeriWave2-c8:ad:e2-Portal	0
VeriWave3-c0:1a:79-Point	0
VeriWave4-c8:78:d2	--
VeriWave5-cb:a5:11-AP93	0

20 Clients

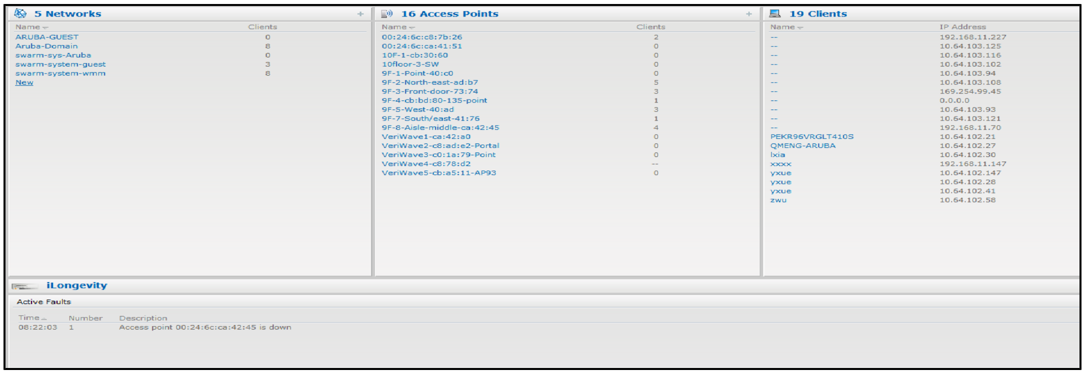
Name	IP Address
--	192.168.11.70
--	192.168.11.227
--	10.64.103.125
--	10.64.103.116
--	10.64.103.102
--	10.64.103.94
--	10.64.103.108
--	0.0.0.0
--	10.64.103.93
--	169.254.99.45
--	10.64.103.121
PEKR96VRGLT410S	10.64.102.21
QMENG-ARUBA	10.64.102.27
gwang	192.168.11.147
linli	10.64.102.69
lxia	10.64.102.30
yxue	10.64.102.147
yxue	10.64.102.41
yxue	10.64.102.28
zwu	10.64.102.58

iLongevity

Fault History

Time	Number	Cleared By	Description
15:47:48	5	System	Access point 00:24:6c:ca:40:c0 is down
14:36:34	4	System	Access point d8:c7:c8:cb:bd:80 is down
08:27:19	3	System	Access point 00:24:6c:c0:1a:79 is down
08:26:33	2	System	Access point 00:24:6c:c0:1a:79 is down

Figure 25 *Active Faults*



5 Networks

Name	Clients
ARUBA-GUEST	0
Aruba-Domain	8
swarm-sys-Aruba	0
swarm-system-guest	3
swarm-system-wmm	8
New	

16 Access Points

Name	Clients
00:24:6c:c8:7b:26	2
00:24:6c:ca:41:51	0
10F-1-cb:30:60	0
10floor-3-SW	0
9F-1-Point-40:c0	0
9F-2-North-east-ad:b7	5
9F-3-Front-door-73:74	3
9F-4-cb:bd:80-135-point	1
9F-5-West-40:ad	3
9F-7-South/east-41:76	1
9F-8-Aisle-middle-ca:42:45	4
VeriWave1-ca:42:a0	0
VeriWave2-c8:ad:e2-Portal	0
VeriWave3-c0:1a:79-Point	0
VeriWave4-c8:78:d2	--
VeriWave5-cb:a5:11-AP93	0

19 Clients

Name	IP Address
--	192.168.11.227
--	10.64.103.125
--	10.64.103.116
--	10.64.103.102
--	10.64.103.94
--	10.64.103.108
--	169.254.99.45
--	0.0.0.0
--	10.64.103.93
--	10.64.103.121
--	192.168.11.70
PEKR96VRGLT410S	10.64.102.21
QMENG-ARUBA	10.64.102.27
lxia	10.64.102.30
xxxx	192.168.11.147
yxue	10.64.102.147
yxue	10.64.102.28
yxue	10.64.102.41
zwu	10.64.102.58

iLongevity

Active Faults

Time	Number	Description
08:22:03	1	Access point 00:24:6c:ca:42:45 is down

The following table displays a list of alerts that are generated on the Instant network:

Table 13: *Alerts list*

Type Code	Description	Details	Corrective Actions
100101	Internal error	The IAP has encountered an internal error for this client.	Contact the Aruba 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.

Table 13: *Alerts list*

Type Code	Description	Details	Corrective Actions
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 are 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.
100309	RADIUS server authentication failure	The IAP cannot authenticate this client using 802.1X , because the RADIUS server rejected the authentication credentials (password and so on) 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.

IDS

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

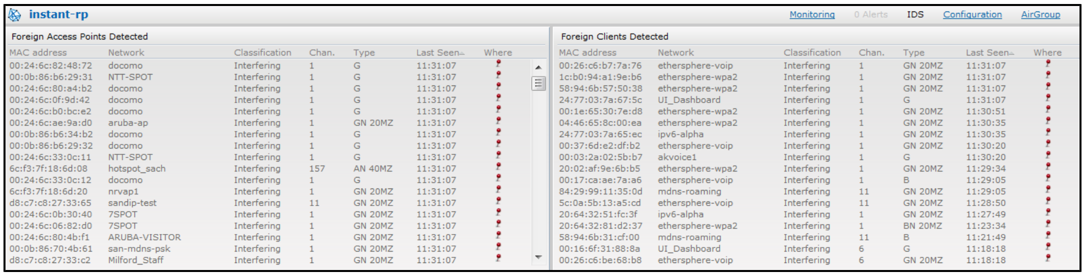
- Foreign Access Points Detected– Lists the APs that are not controlled by the Virtual Controller. The following information is displayed for each foreign AP:
  - MAC address– Displays the MAC address of the foreign AP.
  - Network– Displays the name of the network to which the foreign AP is connected.
  - Classification– Displays the classification of the foreign AP, for example, 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.

The following figure shows an example for the intrusion detection log.

Figure 26 *Intrusion Detection*



Foreign Access Points Detected

MAC address	Network	Classification	Chan.	Type	Last Seen	Where
00:24:6c:82:48:72	docomo	Interfering	1	G	11:31:07	📍
00:0b:86:b6:29:31	NTT-SPOT	Interfering	1	G	11:31:07	📍
00:24:6c:80:a4:b2	docomo	Interfering	1	G	11:31:07	📍
00:24:6c:0f:9d:42	docomo	Interfering	1	G	11:31:07	📍
00:24:6c:b0:bc:e2	docomo	Interfering	1	G	11:31:07	📍
00:24:6c:ae:9a:d0	aruba-ap	Interfering	1	GN 20MZ	11:31:07	📍
00:0b:86:b6:34:b2	docomo	Interfering	1	G	11:31:07	📍
00:0b:86:b6:29:32	docomo	Interfering	1	G	11:31:07	📍
00:24:6c:33:0c:11	NTT-SPOT	Interfering	1	G	11:31:07	📍
6c:f3:7f:18:6d:08	hotspot_sach	Interfering	157	AN 40MZ	11:31:07	📍
00:24:6c:33:0c:12	docomo	Interfering	1	G	11:31:07	📍
6c:f3:7f:18:6d:20	nrvap1	Interfering	1	GN 20MZ	11:31:07	📍
d8:c7:c8:27:33:65	sandip-test	Interfering	11	GN 20MZ	11:31:07	📍
00:24:6c:0b:30:40	7SPOT	Interfering	1	GN 20MZ	11:31:07	📍
00:24:6c:06:82:d0	7SPOT	Interfering	1	GN 20MZ	11:31:07	📍
00:24:6c:80:4b:f1	ARUBA-VISITOR	Interfering	1	GN 20MZ	11:31:07	📍
00:0b:86:70:4b:61	san-mdns-psk	Interfering	1	GN 20MZ	11:31:07	📍
d8:c7:c8:27:33:c2	Milford_Staff	Interfering	1	GN 20MZ	11:31:07	📍

Foreign Clients Detected

MAC address	Network	Classification	Chan.	Type	Last Seen	Where
00:26:c6:b7:7a:76	ethersphere-voip	Interfering	1	GN 20MZ	11:31:07	📍
1c:b0:94:a1:9e:b6	ethersphere-wpa2	Interfering	1	GN 20MZ	11:31:07	📍
58:94:6b:57:50:38	ethersphere-wpa2	Interfering	1	GN 20MZ	11:31:07	📍
24:77:03:7a:67:5c	UI_Dashboard	Interfering	1	G	11:31:07	📍
00:1e:65:30:7e:d8	ethersphere-wpa2	Interfering	1	GN 20MZ	11:30:51	📍
04:46:65:8c:00:ea	ethersphere-wpa2	Interfering	1	GN 20MZ	11:30:35	📍
24:77:03:7a:65:ec	ipv6-alpha	Interfering	1	GN 20MZ	11:30:35	📍
00:37:6d:e2:df:b2	ethersphere-voip	Interfering	1	GN 20MZ	11:30:20	📍
00:03:2a:02:5b:b7	akvoice1	Interfering	1	G	11:30:20	📍
20:02:af:9e:6b:b5	ethersphere-wpa2	Interfering	1	GN 20MZ	11:29:34	📍
00:17:ca:ae:7a:a6	ethersphere-voip	Interfering	1	B	11:29:05	📍
84:29:99:11:35:0d	mdns-roaming	Interfering	11	GN 20MZ	11:29:05	📍
5c:0a:5b:13:a5:cd	ethersphere-voip	Interfering	11	GN 20MZ	11:28:50	📍
20:64:32:51:fc:3f	ipv6-alpha	Interfering	1	GN 20MZ	11:27:49	📍
20:64:32:81:d2:37	ethersphere-wpa2	Interfering	1	BN 20MZ	11:23:34	📍
58:94:6b:31:cf:00	mdns-roaming	Interfering	11	B	11:21:49	📍
00:16:6f:31:88:8a	UI_Dashboard	Interfering	6	G	11:18:18	📍
00:26:c6:be:68:b8	ethersphere-voip	Interfering	6	GN 20MZ	11:18:18	📍

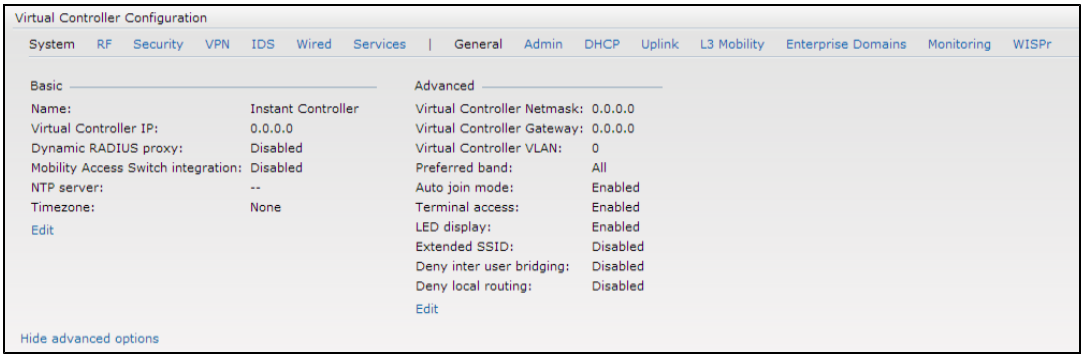
For more information on the intrusion detection feature, see Intrusion Detection on page 229.

Configuration

The **Configuration** link provides an overall view of your Virtual Controller configuration.

The following figure shows the Virtual Controller configuration details displayed on clicking the **Configuration** link.

Figure 27 *Configuration Link*



Basic

Name: Instant Controller
Virtual Controller IP: 0.0.0.0
Dynamic RADIUS proxy: Disabled
Mobility Access Switch integration: Disabled
NTP server: --
Timezone: None

Advanced

Virtual Controller Netmask: 0.0.0.0
Virtual Controller Gateway: 0.0.0.0
Virtual Controller VLAN: 0
Preferred band: All
Auto join mode: Enabled
Terminal access: Enabled
LED display: Enabled
Extended SSID: Disabled
Deny inter user bridging: Disabled
Deny local routing: Disabled

AirGroup

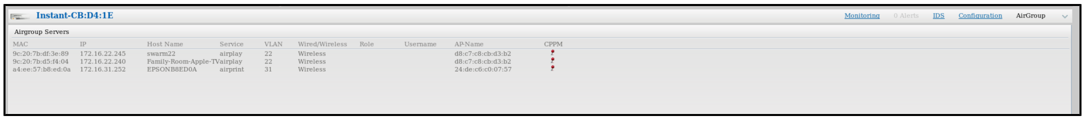
This **AirGroup** link provides an overall view of your AirGroup configuration. Click each field to view or edit the settings.

- **MAC** – Displays the MAC address of the AirGroup servers.

- **IP** – Displays the IP address of the AirGroup servers.
- **Host Name** – Displays the machine name or hostname of the AirGroup servers.
- **Service**– Displays the type of the services such as AirPlay or AirPrint.
- **VLAN**– Displays VLAN details of the AirGroup servers.
- **Wired/Wireless** – Displays if the AirGroup server is connected via wired or wireless interface.
- **Role** –Displays the user role if the server is connected through 802.1X authentication. If the server is connected through PSK or open authentication, this field is blank.
- **AP-MAC**– Displays the MAC address of the IAP to which the server is connected.
- **Update no/hash**– This is used for debugging issues. Use this to identify the internal database of AirGroup.
- **CPPM**– By clicking on this, you get details of the registered rules in ClearPass Policy Manager (CPPM) for this server.
- **MDNS Cache**– By clicking on this, you receive MDNS record details of a particular server.

The following figure shows the AirGroup server details available on clicking the **AirGroup** link:

Figure 28 *AirGroup Link*



Airgroup Servers

MAC	IP	Host Name	Service	VLAN	Wired/Wireless	Role	Username	AP-Name	CPPM
9c:20:7b:df:3e:89	172.16.22.245	swarm22	airplay	22	Wireless			d8:c7:c8:cb:d3:b2	📍
9c:20:7b:d5:f4:04	172.16.22.240	Family-Room-Apple-TV	airplay	22	Wireless			d8:c7:c8:cb:d3:b2	📍
a4:ee:57:b8:ed:0a	172.16.31.252	EPSONB8ED0A	airprint	31	Wireless			24:de:c6:c0:07:57	📍

AirGroup 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 AirWave Integration and Management on page 269. The AirWave status is displayed at the bottom of the Instant main window. If the AirWave status is **Not Set Up**, click the **Set Up Now** link to configure AirWave. The **System** window appears with **Admin** tab selected. For information to configure AirWave, see Configuring AirWave on page 271.

Aruba Central

The Instant UI provides a link to launch a support portal for Aruba Central. You can use Central's evaluation accounts through this website and get registered for a free account. You must fill in the registration form available on this page. After you complete this process, an activation link will be sent to your registered ID to get started.

Pause/Resume

The **Pause/Resume** link is located at the bottom right corner of the Instant main window.

Click the **Pause** link to pause the automatic refreshing of the Instant UI is automatically refreshed after every 15 seconds by default. The Instant UI is automatically refreshed after every 15 seconds by default. When the automatic refreshing is paused, the **Pause** link changes to **Resume**. Click the **Resume** link to resume automatic refreshing.

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

Views

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

- Virtual Controller view– The Virtual Controller view is the default view. This view allows you to monitor the Instant network. This view allows you to monitor the Instant network.
- The following Instant UI elements are available in this view:
  - Tabs– Networks, Access Points, and Clients. For detailed information about the tabs, see Tabs on page 40.

  - Links– Monitoring, Client Alerts, and IDS. The Spectrum link is visible if you have configured the IAP as a spectrum monitor. These links allow you to monitor the Instant network. For more information about these links, see Monitoring on page 52, IDS on page 64, Alerts on page 61, and Spectrum Monitor on page 211.
- Network view– The Network view provides information that is necessary to monitor a selected wireless network. All Wi-Fi networks in the 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 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 is displayed.
- Client view– The Client view provides information that is necessary to monitor a selected client. In the Client view, all the clients in the Instant network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor. Client view for that client appears.

For more information on the graphs and the views, see Monitoring on page 52.

Chapter 3
Initial Configuration Tasks

This chapter describes the following basic IAP deployment methods and configuration tasks:

- Updating IP Address of an IAP on page 69
- Modifying the IAP Name on page 70
- Updating Location Details of an IAP on page 70
- Configuring External Antenna on page 71
- Upgrading an IAP on page 72
- Adding an IAP to the Network on page 75
- Removing an IAP from the Network on page 76
- Enabling Terminal Access on page 75
- Enabling Auto Join Mode on page 75
- Configuring a Preferred Band on page 76
- Configuring Radio Profiles for an IAP on page 76
- Configuring Inter-user Bridging and Local Routing on page 77
- Configuring Uplink VLAN for an IAP on page 78
- Configuring an NTP Server on page 78

Updating IP Address of an IAP

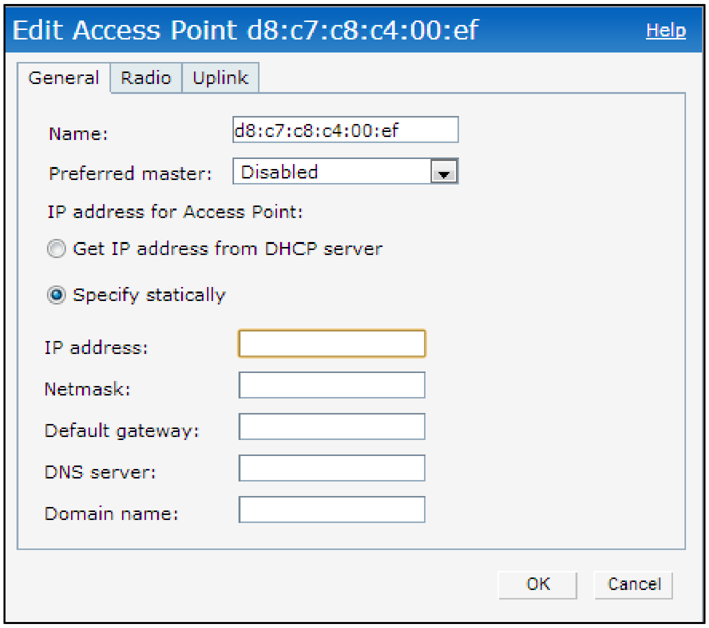
You can configure IP address of an IAP by using Instant UI or CLI.

In the Instant UI

To change the IP address of IAP:

1. In the **Access Points** tab, click the IAP to modify. The **edit** link is displayed.
2. Click the **edit** link. The edit window for modifying IAP details is displayed.

Figure 29 *Configuring IAP Settings*



Edit Access Point d8:c7:c8:c4:00:ef

Name: d8:c7:c8:c4:00:ef

Preferred master: Disabled

IP address for Access Point:

○ Get IP address from DHCP server

● Specify statically

IP address:

Netmask:

Default gateway:

DNS server:

Domain name:

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

In the CLI

To configure IP address:

```
(Instant Access Point)# ip-address <IP-address> <subnet-mask> <NextHop-IP> <DNS-IP-address>
<domain-name>
```

Modifying the IAP Name

You can change the name of an IAP by using the Instant UI or CLI.

In the Instant UI

1. In the **Access Points** tab, click the IAP you want to rename. The **edit** link is displayed.
2. Click the **edit** link. The edit window for modifying IAP details is displayed.
3. Edit the IAP name in the **Name** text box.
4. Click **OK**.

In the CLI

To change the name:

```
(Instant Access Point)# hostname <system-name>
```

Updating Location Details of an IAP

You can update the physical location details of an IAP by using the Instant UI or CLI. The system location details are used for retrieving information through the SNMP *sysLocation* MIB object.

In the Instant UI

To update location details:

1. In the Instant main window, click the **System** link. The **System** window appears.
2. In the **General** tab of **System** window, specify the location of the an IAP in the **System location** text box.
3. Click **OK**.

In the CLI

To update location details of an IAP:

```
(Instant Access Point)(config)# syslocation <location-name>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Configuring External Antenna

If your IAP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system’s Equivalent Isotropically Radiated Power (EIRP) is in compliance with the limit specified by the regulatory authority of the country in which the IAP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know if your AP device supports external antenna connectors, see the *Install Guide* that is shipped along with the AP device.

EIRP and Antenna Gain

The following formula can be used to calculate the EIRP limit related RF power based on selected antennas (antenna gain) and feeder (Coaxial Cable loss):

EIRP = Tx RF Power (dBm)+GA (dB) - FL (dB)

The following table describes this formula:

Table 14: *Formula Variable Definitions*

Formula Element	Description
EIRP	Limit specific for each country of deployment
Tx RF Power	RF power measured at RF connector of the unit
GA	Antenna gain
FL	Feeder loss

The following table lists gain values supported by each type of antenna:

Table 15: *Antenna Types and Maximum Antenna Gains*

Frequency Band	Type	Gain (dBi)
2.4 GHz	Dipole/Omni	6
	Panel	12
	Sector	12
5 GHz	Dipole/Omni	6
	Panel	14
	Sector	14

For information on antenna gain recommended by the manufacturer, see www.arubanetworks.com.

Configuring Antenna Gain

You can configure antenna gain for APs with external connectors using Instant UI or CLI.

In the Instant UI

1. Navigate to the **Access Point** tab, select the access point to configure and then click **edit**.

2. In the **Edit Access Point** window, select **External Antenna** to configure the antenna gain value. This option is available only for access points that support external antennas, for example, IAP-134 or IAP-92.
3. Enter the antenna gain values in dBm for the 2.4GHz and 5GHz bands.
4. Click **OK**.

In the CLI

To configure external antenna for 5 GHz frequency:

```
(Instant Access Point)# a-external-antenna <dBi>
```

To configure external antenna for 2,4 GHz frequency:

```
(Instant Access Point)# g-external-antenna <dBi>
```

Upgrading an IAP

While upgrading an IAP, you can use the image check feature to allow the IAP to find new software image versions available on a cloud-based image server hosted and maintained by Aruba Networks. The location of the image server is fixed and cannot be changed by the user. The image server is loaded with latest versions of Instant software.

Upgrading an IAP and Image Server

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

Image Management Using AirWave

If the multi-class IAP network is managed by AirWave, image upgrades can only be done through the AirWave UI. The IAP images for different classes must be uploaded on the AMP server. When new IAPs joining the network need to synchronize their software with the version running on the Virtual Controller, and if the new IAP belongs to a different class, the image file for the new IAP is provided by AirWave. If AirWave does not have the appropriate image file, the new AP will not be able to join the network.

The Virtual Controller communicates with the AirWave server if AirWave is configured. If AirWave is not configured on the IAP, the image is requested from the Image server.

Image Management Using Cloud Server

If the multi-class IAP network is not managed by AirWave, image upgrades can be done through the cloud-based image check feature. When a new IAP joining the network needs to synchronize its software version with the version on the Virtual Controller and if the new IAP belongs to a different class, the image file for the new IAP is provided by the cloud server.

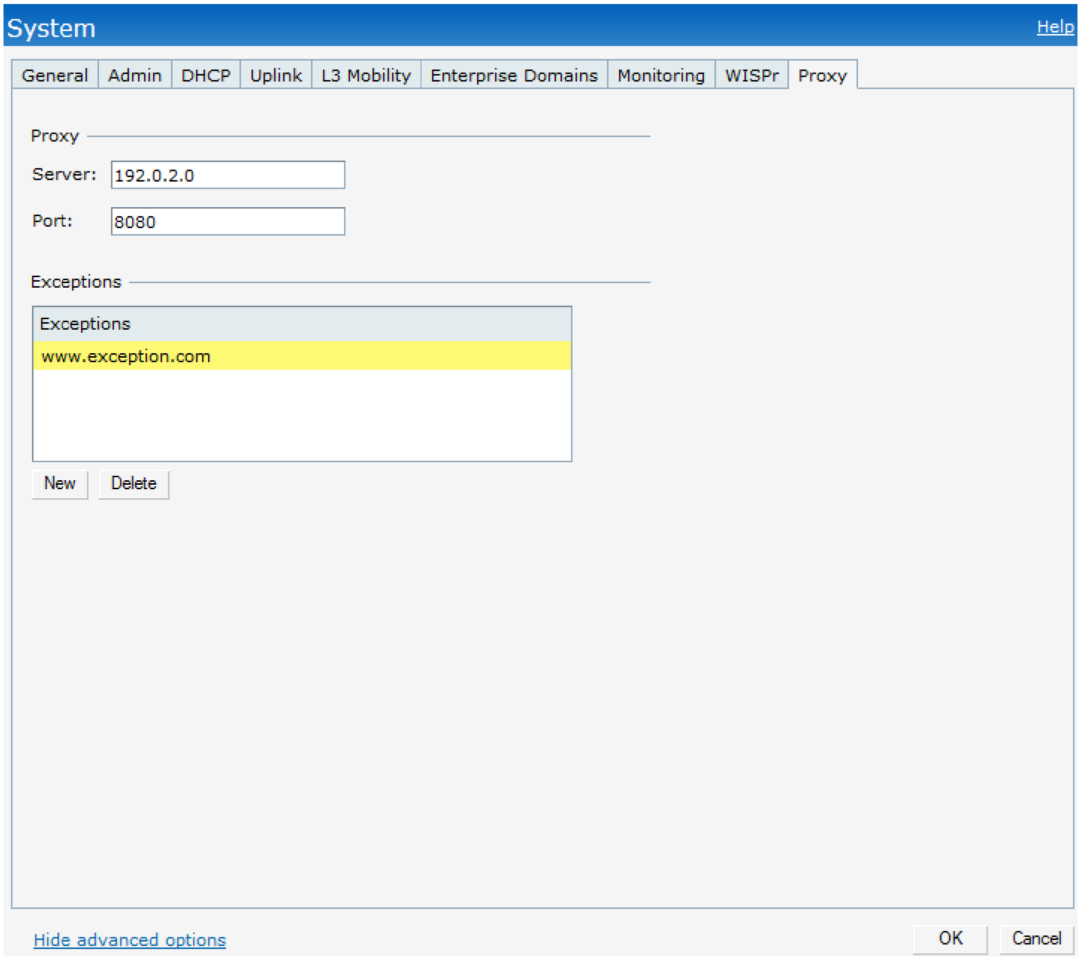
Configuring HTTP Proxy on an IAP

If your network requires a proxy server for internet access, you must first configure the HTTP proxy on the IAP to download the image from the cloud server. After you setup the HTTP proxy settings, the IAP connects to the Activate server, AirWave Management platform, Central, or OpenDNS server through a secure HTTP connection. You can also exempt certain applications from using the HTTP proxy (configured on an IAP) by providing their hostname or IP address under exceptions.

In the Instant UI

Perform these steps to configure the HTTP proxy settings:

1. Navigate to **System > Proxy**.



Proxy

Server: 192.0.2.0

Port: 8080

Exceptions

Exceptions
www.exception.com

2. Enter the HTTP proxy server's IP address and the port number.
3. If you do not want the HTTP proxy to be applied for a particular host, click **New** to enter that IP address or domain name of that host under exceptions list.

In the CLI

```
(Instant Access Point)(config)# proxy server 192.0.2.1 8080
(Instant Access Point)(config)# proxy exception 192.0.2.2
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Upgrading an IAP Using Automatic Image Check

You can upgrade an IAP by using the automatic image check feature. The Automatic image checks are performed once after the AP boots up and every week thereafter.

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

NOTE

If AirWave is configured, the automatic image check is disabled.

To check for a new version on the image server in the cloud:

1. Go to **Maintenance**>**Automatic**>**Check for New Version**. After the image check is completed, one of the following messages appears:
   - No new version available – If there is no new version available.

- Image server timed out – Connection or session between the image server and the 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 the version number is displayed.
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 is displayed:

   - Upgrading – While image upgrading is in progress.
   - Upgrade successful – When the upgrading is successful.
   - Upgrade failed – When the upgrading fails.

If the upgrade fails and an error message is displayed, retry upgrading the IAP.

Upgrading to a New Version Manually

If the automatic image check feature is disabled, you can use obtain an image file from a local file system or from a TFTP or HTTP URL. To manually check for a new firmware image version and obtain an image file:

1. Navigate to **Maintenance**>**Firmware**. The Firmware window is displayed.
2. Under **Manual** section, perform the following steps:

- Select the **Image file** option. This method is only available for single-class IAPs.

  The following examples describe the image file format for different IAP models:

  - For IAP-134/135 – ArubaInstant_Cassiopeia_6.3.1.1-4.0.0.0_xxxx
  - For RAP-108/109 – ArubaInstant_Pegasus_6.3.1.1-4.0.0.0_xxxx
  - For RAP-155/155P – ArubaInstant_Aries_6.3.1.1-4.0.0.0_xxxx
  - For IAP-220 Series– ArubaInstant_Centaurus_6.3.1.1-4.0.0.0_xxxx
  - For all other IAPs –ArubaInstant_Orion_6.3.1.1-4.0.0.0_xxxx
- Select the **Image URL** option. Select this option to obtain an image file from a TFTP, FTP, or HTTP URL.
  - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/ArubaInstant_Orion_6.3.1.1-4.0.0.0_xxxx
  - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/ArubaInstant_Orion_6.3.1.1-4.0.0.0_xxxx
  - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/ArubaInstant_Orion_6.3.1.1-4.0.0.0_xxxx

3. Clear the **Reboot all APs after upgrade** check box if required. The **Reboot all APs after upgrade** check box is selected by default to allow the IAPs to reboot automatically after a successful upgrade. To reboot the IAP at a later time, clear the **Reboot all APs after upgrade** check box.
4. Click **Upgrade Now** to upgrade the IAP to the newer version.

Upgrading an Image Using CLI

To upgrade an image using a HTTP, TFTP, or FTP URL:

```
(Instant Access Point)# upgrade-image <ftp/tftp/http-URL>
```

To upgrade an image without rebooting the IAP:

```
(Instant Access Point)# upgrade-image2-no-reboot <ftp/tftp/http-URL>
```

To view the upgrade information:

```
(Instant Access Point)# show upgrade info
```

```
Image Upgrade Progress
----------------------
Mac                IP Address   AP Class  Status    Image Info  Error Detail
---                ---------    --------  ------    ----------  ------------
d8:c7:c8:c4:42:98  10.17.101.1  Orion     image-ok  image file  none
Auto reboot        :enable
Use external URL   :disable
```

Enabling Terminal Access

When terminal access is enabled, you can access the Instant CLI through SSH or Telnet server. You can enable terminal access to an IAP by using the Instant UI or CLI.

In the Instant UI

1. In the Instant main window, click the **System** link. The **System** window appears.
2. In the **General** tab of **System** window, click **Show advanced options** to display the advanced options.
3. Select **Enabled** from the **Terminal access** drop-down list.
4. To enable Telnet server based access, select **Enabled** from the **Telnet server** drop-down list.
5. Click **OK**.

In the CLI

To enable terminal access:

```
(Instant Access Point)(config)# terminal-access
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To enable access to the Instant CLI through Telnet:

```
(Instant Access Point)(config) # telnet-server
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Enabling Auto Join Mode

The Auto Join Mode feature allows IAPs to automatically discover the Virtual Controller and join the network.

The **Auto Join Mode** feature is enabled by default. If 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. If this feature is disabled, the inactive IAPs appear in red.

Disabling Auto Join Mode

To disable Auto Join Mode:

1. In the Instant main window, click the **System** link. The **System** window appears.
2. In the **General** tab of **System** window, click **Show advanced options**.
3. Select **Disabled** from the **Auto join mode** drop-down list.
4. Click **OK**.

Adding an IAP to the Network

To add an IAP to the Instant network, assign an IP address. For more information, see Assigning an IP address to the IAP on page 33.

After an IAP is connected to the network, if the Auto Join Mode feature is enabled, the IAP inherits the configuration from the Virtual Controller and is listed in the **Access Points** tab.

If the Auto Join Mode is disabled, perform the following steps to add an IAP to the network:

1. In the **Access Points** tab, click the **New** link. The **New Access Point** window is displayed.
2. In the **New Access Point** window, enter the MAC address for the new IAP.
3. Click **OK.**

Removing an IAP from the Network

You can remove an IAP from the network only if the Auto Join Mode feature is disabled. To remove an IAP from the network:

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

NOTE

The deleted IAPs cannot join the Instant network anymore and no longer appear in the Instant UI. However, the master IAP details cannot be deleted from the Virtual Controller database.

Configuring a Preferred Band

You can configure a preferred band for an IAP by using the Instant UI or the CLI.

In the Instant UI

1. In the Instant main window, click the **System** link. The **System** window appears.
2. In the **General** tab of **System** window, select 2.4 GHz, 5 GHz or All from the **Preferred band** drop-down list for single-radio access points.
3. Click **OK**.

NOTE

Reboot the IAP after configuring the radio profile for the changes to affect.

In the CLI

To configure a preferred band:

```
(Instant Access Point)(config)# rf-band <band>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Configuring Radio Profiles for an IAP

You can configure a radio profile on an IAP either manually or by using the Adaptive Radio Management (ARM) feature.

Adaptive Radio Management (ARM) is enabled on Instant by default. It automatically assigns appropriate channel and power settings for the IAPs. For more information on ARM, see Adaptive Radio Management on page 219.

Configuring ARM Assigned Radio Profiles for an IAP

To enable ARM assigned radio profiles:

1. In the **Access Points** tab, click the IAP to modify. The **edit** link is displayed.
2. Click the **edit** link. The edit window for modifying IAP details is displayed.

3. Click the **Radio** tab. The **Radio** tab details are displayed.
4. Ensure that an appropriate mode is selected.
5. Select the **Adaptive radio management assigned** option under the bands that are applicable to the IAP configuration.
6. Click **OK**.

Configuring Radio Profiles Manually for IAP

To manually configure radio settings:

1. In the **Access Points** tab, click the AP for which you want to enable ARM. The **edit** link appears.
2. Click the **edit** link. The **Edit Access Point** window appears.
3. Click the **Radio** tab.
4. Ensure that an appropriate mode is selected.

   By default the channel and power for an AP are optimized dynamically using Adaptive Radio Management (ARM). You can override ARM on the 2.4 GHz and 5 GHz bands and set the channel and power manually if desired. The following table describes various configuration modes for an AP:

Table 16: *IAP Radio Modes*

Mode	Description
Access	In Access mode the AP serves clients, while also monitoring for rogue APs in the background.
Monitor	In Monitor mode, the AP acts as a dedicated monitor, scanning all channels for rogue APs and clients.
Spectrum Monitor	In Spectrum Monitor mode, the AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring APs or from non-WiFi devices such as microwaves and cordless phones.

NOTE

In the Monitor and Spectrum Monitor modes, the APs do not provide access services to clients.

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

In the CLI

To configure a radio profile:

```
(Instant Access Point)# wifi0-mode {<access>|<monitor>|<spectrum-monitor>}
(Instant Access Point)# wifi1-mode {<access>|<monitor>|<spectrum-monitor>}
(Instant Access Point)# a-channel <channel> <tx-power>
(Instant Access Point)# g-channel <channel> <tx-power>
```

Configuring Inter-user Bridging and Local Routing

You can configure inter-user bridging and local routing by using the Instant UI or CLI.

In the Instant UI

To prevent inter-user bridging and local routing:

1. In the Instant main window, click the **System** link. The **System** window appears.
2. In the **General** tab of **System** window, click **Show advanced options** to display the advanced options.
   - From the **Deny inter user bridging** drop-down menu, select **Enabled** to prevent traffic between two clients connected to the same IAP.
   - From the **Deny local routing** drop-down menu, select **Enabled** to prevent local routing traffic between two clients connected to the same IAP.

In the CLI

To configure inter-user bridging and local routing:

```
(Instant Access Point)(config)# deny-inter-user-bridging
(Instant Access Point)(config)# deny-local-routing
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Configuring Uplink VLAN for an IAP

Instant supports a management VLAN for the uplink traffic on an IAP. After an IAP is provisioned with the uplink management VLAN, all management traffic sent from the IAP is tagged with the management VLAN.

You can configure the uplink management VLAN on an IAP by using the Instant UI or CLI.

In the Instant UI

To configure uplink management VLAN:

1. In the **Access Points** tab, click the IAP to modify. The **edit** link is displayed.
2. Click the **edit** link. The **edit** window for modifying IAP details is displayed.
3. Click the **Uplink** tab.
4. Specify the VLAN in the **Uplink Management VLAN** field.
5. Click **OK**.

In the CLI

To configure uplink VLAN:

```
(Instant Access Point)# uplink-vlan <VLAN-ID>
```

To view the uplink VLAN status:

```
(Instant Access Point)# show uplink-vlan

Uplink Vlan Current      :0
Uplink Vlan Provisioned  :1
```

Configuring an NTP Server

To facilitate communication between various elements in a network, time synchronization between the elements and across the network is critical. Time synchronization allows you to:

- 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.

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

The NTP server is set to **pool.ntp.org** by default.

You can configure an NTP server by using the Instant UI or the CLI.

In the Instant UI

To configure an NTP server:

1. Click **System** link at the top right corner of the Instant UI. The **System** window appears.
2. In the **General** tab of **System** window, enter the IP address or the URL (domain name) of the NTP server in the **NTP Server** text box.
3. Select a time zone from the **Timezone** drop-down list. The time zone indicates the time returned by the NTP server.

You can enable daylight saving time (DST) on IAPs if the time zone you selected supports the daylight saving time. If the Time Zone selected does not support DST, the **Daylight Saving Time** option does not appear. When enabled, the Daylight saving time ensures that the IAPs reflect the seasonal time changes in the region they serve.

4. To enable daylight saving time, select the **Daylight Saving Time** check box.
5. Click **OK**.

In the CLI

To configure an NTP server:

```
(Instant Access Point)(config)# ntp-server <name>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To configure timezone:

```
(Instant Access Point)(config)# clock timezone <name> <hour-offset> <minute-offset>
(Instant Access Point)(config)# clock summer-time <timezone> recurring <start-week> <start-da
y> <start-month> <start-hour> <end-week> <end-day> <end-month> <end-hour>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Chapter 4
Mesh IAP Configuration

This chapter provides the following information:

Mesh Network Overview

The Aruba 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 and allows the network to continue operation even when an IAP stops functioning or if a connection fails.

Mesh IAPs

Mesh network requires at least one valid uplink (wired or 3G) connection. Any provisioned IAP that has a valid uplink (wired or 3G) functions as a mesh portal, and the IAP without an Ethernet link functions as a mesh point. The mesh portal can also act as a Virtual Controller. A Mesh portal (MPP) uses its uplink connection to reach the controller, a mesh point, or establishes an all wireless 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.

If two IAPs have valid uplink connections, there is redundancy in the mesh network, and most mesh points try to mesh directly with one of the two portals. However, depending on the actual deployment and RF environment, some mesh points may mesh through other intermediate mesh points.

In an Instant mesh network, the maximum hop count is two nodes (point >point >portal) and the maximum number of mesh points per mesh portal is eight.

Mesh IAPs detect the environment when they boot up, locate and associate with their nearest neighbor, to determine the best path to the mesh portal.

Instant mesh functionality is supported only on dual radio IAPs only. On dual-radio IAPs, the 5 GHz radio is always used for both mesh-backhaul and client traffic, while the 2.4 GHz radio is always used for client traffic.

NOTE

Mesh service is automatically enabled on 802.11a band for dual-radio IAP only, and this is not configurable.

The mesh network must be provisioned for the first time by plugging into the wired network. After that, mesh works on IAP-ROWs like any other regulatory domain.

Mesh Portals

A mesh portal (MPP) is a gateway between the wireless mesh network and the enterprise wired LAN. The mesh roles are automatically assigned based on the IAP configuration. A mesh network could have 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 a mesh services set identifier (MSSID/ mesh cluster name) to advertise the mesh network service to other mesh points in that Instant network. This is not configurable and is transparent to the user. The mesh points authenticate to the mesh portal and establish a link that is secured using Advanced Encryption Standard (AES) encryption.

The mesh portal reboots after 5 minutes when it loses its uplink connectivity to a wired network.

Mesh Points

The mesh point establishes an all-wireless path to the mesh portal. 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.

Mesh point also supports LAN bridging. You can connect any wired device to the downlink port of the mesh point. In the case of single Ethernet port platforms such as AP-93 and AP-105, you can convert the Eth0 uplink port to a downlink port by enabling **Eth0 Bridging**. For additional information, see Configuring Wired Bridging on Ethernet 0 on page 112.

Setting up Instant Mesh Network

Instant mesh can be provisioned in two ways:

- Over-the-air provisioning
- Over-the-wire provisioning

Over-the-air provisioning is available when only one IAP mesh network is being advertised. The IAP-ROW must have a the country code set to transmit or receive; therefore, over-the-air provisioning is not supported by the IAP-ROW variants.

To set up a mesh network:

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. 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.

The IAP mesh point gets an IP address from the same DHCP pool as the portal, and the DHCP request goes through the portal.

3. Ensure that an open SSID, **instant** is listed. Connect a laptop to the default (**instant**) SSID.
4. Type http://instant.arubanetworks.com in a browser.
5. Click **I understand the risks** and **Add exception** to ignore the certificate warnings.
6. In the login window, enter the following credentials:
   - Username– **admin**
   - Password– **admin**
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. All the IAPs show up on the Virtual Controller.

Disconnect the IAPs that you want to deploy as Mesh Points from the switch and place the IAPs at the desired location. The IAPs with valid uplink connections function as the mesh portal.

The IAPs in US, JP, or IL regulatory domain which are in factory default state scan for several minutes after booting. An IAP mesh point in factory default state automatically joins the portal only if a single Instant mesh network is found. You can also enable the auto-join feature in the existing network to allow mesh points to automatically join the network.

VLAN Configuration

VLAN configuration is required for networks with more devices and broadcast traffic on a WLAN SSID or wired profile. Based on the network type and its requirements, you can configure the VLANs for a WLAN SSID or wired port profile.

For more information on VLAN configuration for a WLAN SSID and wired port profile, see Configuring VLAN Settings for a WLAN SSID Profile on page 93 and Configuring VLAN for a Wired Profile on page 108.

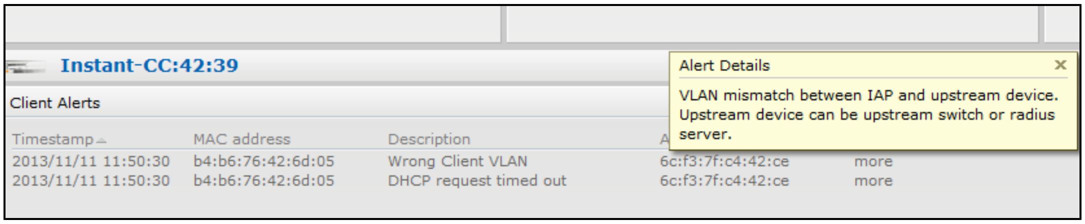
VLAN Pooling

In a single IAP cluster, a large number of clients can be assigned to the same VLAN. Using the same VLAN for multiple clients can lead to a high level of broadcasts in the same subnet. To manage the broadcast traffic, you can partition the network into different subnets and use L3-mobility between those subnets when clients roam. However, if a large number of clients need to be in the same subnet, you can configure VLAN pooling, in which each client is randomly assigned a VLAN from a pool of VLANs on the same SSID. Thus, VLAN pooling allows automatic partitioning of a single broadcast domain of clients into multiple VLANs.

Uplink VLAN Monitoring and Detection on Upstream Devices

If a client connects to an SSID or wired interface with a VLAN that is not allowed on the upstream device, the client will not be assigned an IP address and thus cannot connect to the Internet. When a client connects to an SSID or a wired interface with VLAN that is not allowed on the upstream device, the Instant UI now displays the following alert message:

Figure 30 *Uplink VLAN Detection*



Instant-CC:42:39

Client Alerts

Timestamp	MAC address	Description	A	
2013/11/11 11:50:30	b4:b6:76:42:6d:05	Wrong Client VLAN	6c:f3:7f:c4:42:ce	more
2013/11/11 11:50:30	b4:b6:76:42:6d:05	DHCP request timed out	6c:f3:7f:c4:42:ce	more

Alert Details ×

VLAN mismatch between IAP and upstream device. Upstream device can be upstream switch or radius server.

To resolve this issue, ensure that there is no mismatch in the VLAN configuration.

This chapter provides the following information:

- Virtual Controller Overview
- Virtual Controller IP Address Configuration

Virtual Controller Overview

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

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 Master Election Protocol enables the Instant network to dynamically elect an IAP to take on a Virtual Controller role and allow graceful failover to a new Virtual Controller when the existing Virtual Controller is not available. This protocol ensures stability of the network during initial startup or when the Virtual Controller goes down by allowing only one IAP to self-elect as a Virtual Controller.

Preference to an IAP with 3G/4G Card

The Master Election Protocol prefers the IAP with a 3G/4G card, when electing a Virtual Controller for the Instant network during the initial setup. The Virtual Controller is selected based on the following criteria:

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

NOTE

IAP-135 is preferred over IAP-105 when a Virtual Controller is elected.

Preference to an IAP with Non-Default IP

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

Manual Provisioning of Master IAP

In most cases, the master election process automatically determines the best IAP that can perform the role of Virtual Controller, which will apply its image and configuration to all other IAPs in the same AP management VLAN. When the Virtual Controller goes down, a new Virtual Controller is elected.

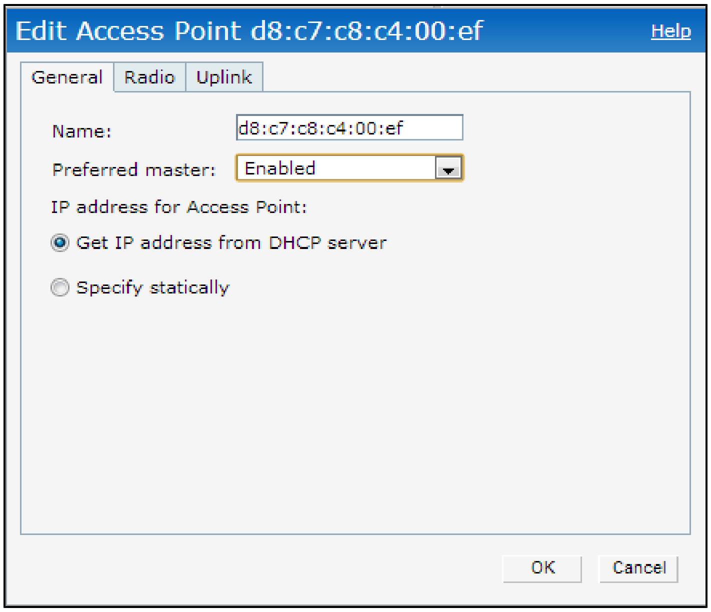
Provisioning an IAP as a Master IAP

You can provision an IAP as a master IAP by using the Instant UI or CLI.

In the Instant UI

1. In the **Access Points** tab, click the IAP to modify. The **edit** link is displayed.
2. Click the **edit** link. The edit window for modifying IAP details is displayed.
3. Select **Enabled** from **Preferred master** drop-down. This option is disabled by default.

Figure 31 *IAP Settings—Provisioning Master IAP*



Edit Access Point d8:c7:c8:c4:00:ef

Name: d8:c7:c8:c4:00:ef

Preferred master: Enabled

IP address for Access Point:

● Get IP address from DHCP server

○ Specify statically

4. Click **OK**.

In the CLI

To provision an IAP as a master IAP:

```
(Instant Access Point)# iap-master
```

To verify if the IAP is provisioned as master IAP:

```
(Instant Access Point)# show ap-env
Antenna Type:Internal
Iap_master:1
```

Virtual Controller IP Address Configuration

You can specify a single static IP address that can be used to manage a multi-AP 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 MAC address to update the network ARP cache.

Configuring IP Address for Virtual Controller

You can configure the Virtual Controller name and IP address using Instant UI or CLI.

In the Instant UI

1. Click the **System** link at top right corner of the Instant main window. The **System** window appears.
2. Click the **Show advanced options** link. The advanced options are displayed.

3. In the **General** tab, enter the appropriate IP address in the **Virtual Controller IP** text box. The IP configured for the Virtual Controller can be in the same subnet as IAP or can be in a different subnet. If the Virtual Controller IP is in a different subnet, configure the Virtual Controller mask, gateway, and VLAN as described in the following steps:
   a. Enter subnet mask details in the **Virtual Controller Netmask** text box.
   b. Enter a gateway address in the **Virtual Controller Gateway** text box.
   c. Enter Virtual Controller VLAN n the **Virtual Controller VLAN** text box.

NOTE

Ensure that Virtual Controller VLAN is not the same as native VLAN of the IAP.

4. Click **OK**.

In the CLI

To configure the Virtual Controller Name and IP address:

```
(Instant Access Point)(config)# virtual-controller-ip <IP-address>
(Instant Access Point)(config)# virtual-controller-vlan <vcvlan> <vcmask> <vcgw>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

This chapter provides the following information:

Understanding Wireless Network Profiles

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

Instant wireless networks are categorized as:

- **Employee network** – An Employee network is a classic Wi-Fi network. This network type is used by the employees in an organization and it supports passphrase-based or 802.1X based authentication methods. Employees can access the protected data of an enterprise through the employee network after successful authentication. The employee network is selected by default during a network profile configuration.
- **Voice network** –This Voice network type allows you to configure a network profile for devices that provide only voice services such as handsets or applications that require voice traffic prioritization.
- **Guest network** –The Guest wireless network is created for guests, visitors, contractors, and any non-employee users who use the enterprise Wi-Fi network. The Virtual Controller assigns the IP address for the guest clients. Captive portal or passphrase based authentication methods can be set for this wireless network. Typically, a guest network is an un-encrypted network. However, you can specify the encryption settings when configuring a guest network.

NOTE

When a client is associated to the Voice network, all data traffic is marked and placed into the high priority queue in QoS (Quality of Service).

To configure a new wireless network profile, complete the following procedures:

1. Configuring WLAN Settings
2. Configuring VLAN Settings
3. Configuring Security Settings
4. Configuring Access Rules for a Network

Configuring WLAN Settings for an SSID Profile

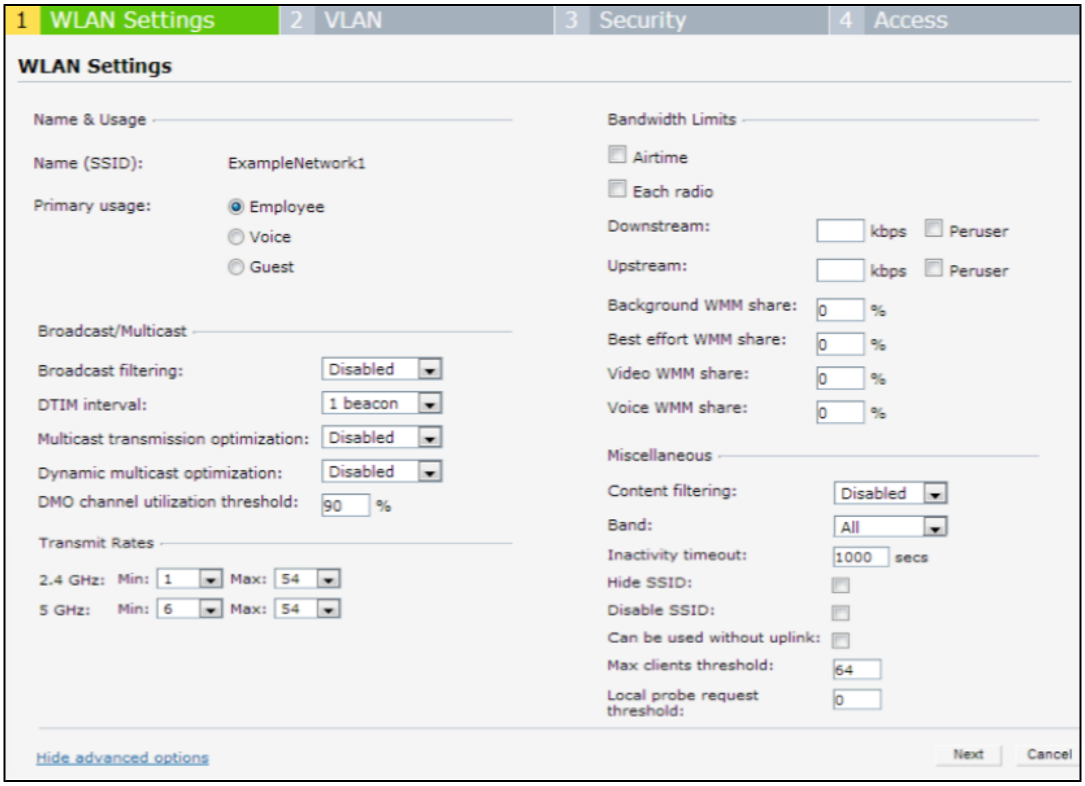
You can configure WLAN settings using Instant UI or CLI.

In the Instant UI

To configure WLAN settings:

1. In the **Networks** tab of the Instant main window, click the **New** link. The **New WLAN** window appears. The following figure shows the contents of **WLAN Settings** tab:

Figure 32 *WLAN Settings Tab*



WLAN Settings

Name & Usage

Name (SSID): ExampleNetwork1

Primary usage: ● Employee ○ Voice ○ Guest

Broadcast/Multicast

Broadcast filtering: Disabled

DTIM interval: 1 beacon

Multicast transmission optimization: Disabled

Dynamic multicast optimization: Disabled

DMO channel utilization threshold: 90 %

Transmit Rates

2.4 GHz: Min: 1 Max: 54

5 GHz: Min: 6 Max: 54

Bandwidth Limits

□ Airtime

□ Each radio

Downstream: kbps □ Peruser

Upstream: kbps □ Peruser

Background WMM share: 0 %

Best effort WMM share: 0 %

Video WMM share: 0 %

Voice WMM share: 0 %

Miscellaneous

Content filtering: Disabled

Band: All

Inactivity timeout: 1000 secs

Hide SSID: □

Disable SSID: □

Can be used without uplink: □

Max clients threshold: 64

Local probe request threshold: 0

2. Enter a name that uniquely identifies a wireless network in the **Name (SSID)** text box.
3. Based on the type of network profile, select any of the following options under **Primary usage**:
   - **Employee**
   - **Voice**
   - **Guest**
4. Click the **Show advanced options** link. The advanced options for configuration are displayed. Specify the following parameters as required.

Table 17: *WLAN Configuration Parameters*

Parameter	Description
Broadcast filtering	Select any of the following values: - **All**–When set to **All**, the IAP drops all broadcast and multicast frames except DHCP and ARP. - **ARP**–When set to **ARP**, the IAP converts ARP requests to unicast and send frames

Table 17: *WLAN Configuration Parameters*

Parameter	Description
	directly to the associated client. - **Disabled**– When set to **Disabled**, all broadcast and multicast traffic is forwarded.
DTIM interval	The **DTIM interval** indicates the delivery traffic indication message (DTIM) period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the IAP should deliver the buffered broadcast and multicast frames to associated clients in the powersave mode. The default value is 1, which means the client checks for buffered data on the IAP at every beacon. You can also configure a higher DTIM value for power saving.
Multicast transmission optimization	Select **Enabled** if you want the IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5.0 GHz is 6 Mbps. This option is disabled by default.
Dynamic multicast optimization	Select **Enabled** to allow IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
DMO channel utilization threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the IAP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the IAP sends multicast traffic over the wireless link.
Transmit Rates	specify the following parameters: - **2.4 GHz**–If the 2.4 GHz band is configured on the IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. - **5 GHz**–If the 5 GHz band is configured on the IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
Bandwidth Limits	Under **Bandwidth Limits**: - **Airtime**–Select this check box to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. - **Each radio**– Select this check box to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. - **Downstream** and **Upstream**–Specify the downstream and upstream rates within a range of 1 to 65535 Kbps for the SSID users. If the assignment is specific for each user, select the **Peruser** checkbox.
Wi-Fi Multimedia (WMM) traffic management	Configure the following options for WMM traffic management. WMM supports voice, video, best effort, and background access categories. You can allocate a higher bandwidth for voice and video traffic than other types of traffic based on the network profile. Specify a percentage value for the following parameters: - **Background WMM share** – Allocates bandwidth for background traffic such as file downloads or print jobs. - **Best effort WMM share** –Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. - **Video WMM share** – Allocates bandwidth for video traffic generated from video streaming. - **Voice WMM share** – Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication.

Table 17: *WLAN Configuration Parameters*

Parameter	Description
	In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can allocate higher values for **Best effort WMM** share and **Voice WMM share** to allocate a higher bandwidth to clients transmitting best effort and voice traffic.
Content filtering	Select **Enabled** to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to **2.4 GHz**, **5 GHz**, or **All**. The **All** option is selected by default.
Inactivity timeout	Specify an interval for session timeout. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. The minimum value is set to 60 seconds and the default value is 1000 seconds.
Hide SSID	Select this checkbox if you do not want the SSID (network name) to be visible to users.
Disable SSID	Select this checkbox if you want to disable the SSID. On selecting this, the SSID will be disabled, but will not be removed from the network. By default, all SSIDs are enabled.
Can be used without Uplink	Select the checkbox if you do not want to SSID profile to use uplink.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0 to 255. The default value is 64.
Local probe request threshold	Specify a threshold value to limit the number of incoming probe requests. When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls system response for this network profile and ignores probe requests if required. You can specify a Received signal strength indication (RSSI) value within range of 0 to 100 dB.

5. Click **Next** to configure VLAN settings. For more information, see Configuring VLAN Settings for a WLAN SSID Profile on page 93.

In the CLI

To configure WLAN settings for an SSID profile:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# essid <ESSID-name>
(Instant Access Point)(SSID Profile <name>)# type {<Employee> | <Voice>| <Guest>}
(Instant Access Point)(SSID Profile <name>)# broadcast-filter <type>
(Instant Access Point)(SSID Profile <name>)# dtim-period <number-of-beacons>
(Instant Access Point)(SSID Profile <name>)# multicast-rate-optimization
(Instant Access Point)(SSID Profile <name>)# dynamic-multicast-optimization
(Instant Access Point)(SSID Profile <name>)# dmo-channel-utilization-threshold
(Instant Access Point)(SSID Profile <name>)# a-max-tx-rate <rate>
(Instant Access Point)(SSID Profile <name>)# a-min-tx-rate <rate>
(Instant Access Point)(SSID Profile <name>)# g-max-tx-rate <rate>
(Instant Access Point)(SSID Profile <name>)# g-min-tx-rate <rate>
(Instant Access Point)(SSID Profile <name>)# bandwidth-limit <limit>
(Instant Access Point)(SSID Profile <name>)# per-user-bandwidth-limit <limit>
(Instant Access Point)(SSID Profile <name>)# air-time-limit <limit>
(Instant Access Point)(SSID Profile <name>)# wmm-background-share <percentage-of-traffic_shar
e>
(Instant Access Point)(SSID Profile <name>)# wmm-best-effort-share<percentage-of-traffic-shar
e>
(Instant Access Point)(SSID Profile <name>)# wmm-video-share <percentage-of-traffic_share>
(Instant Access Point)(SSID Profile <name>)# wmm-voice-share <percentage-of-traffic_share>
(Instant Access Point)(SSID Profile <name>)# rf-band {<2.4>|<5.0>|<all>}
```

```
(Instant Access Point)(SSID Profile <name>)# content-filtering
(Instant Access Point)(SSID Profile <name>)# hide-ssid
(Instant Access Point)(SSID Profile <name>)# inactivity-timeout <interval>
(Instant Access Point)(SSID Profile <name>)# work-without-uplink
(Instant Access Point)(SSID Profile <name>)# local-probe-req-thresh <threshold>
(Instant Access Point)(SSID Profile <name>)# max-clients-threshold <number-of-clients>
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring VLAN Settings for a WLAN SSID Profile

If you are creating a new SSID profile, complete the WLAN Settings procedure before configuring VLAN. For more information, see Configuring WLAN Settings for an SSID Profile on page 90.

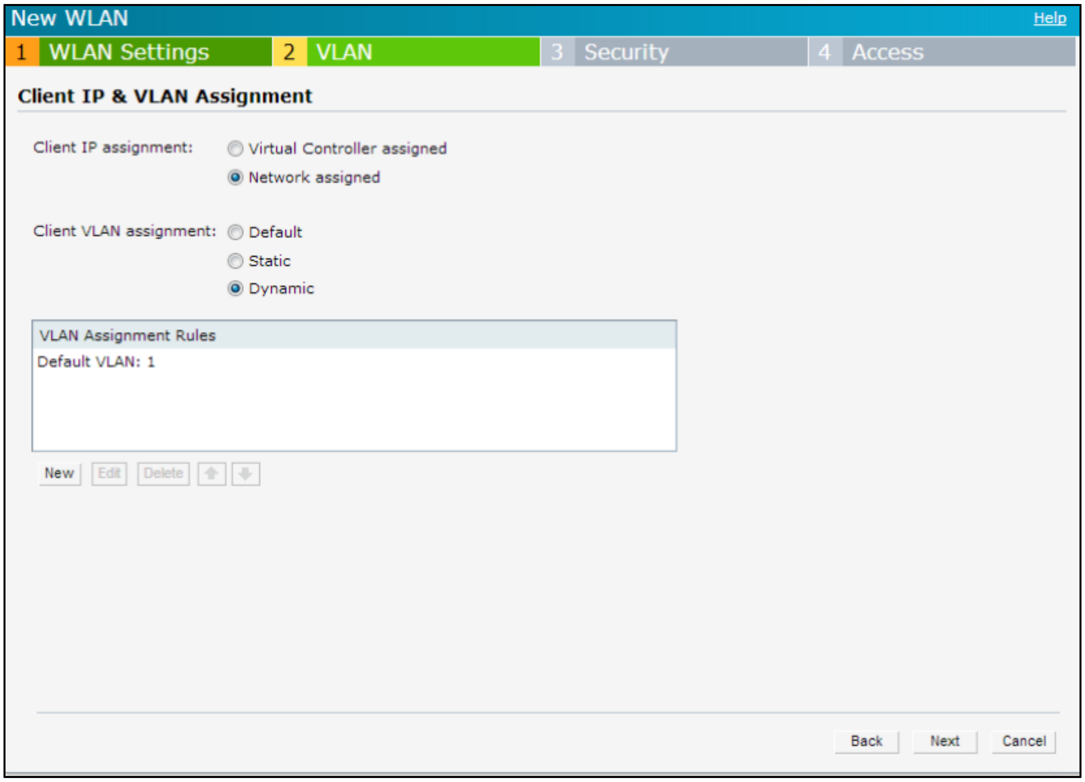
You can configure VLAN settings for an SSID profile using the Instant UI or CLI.

In the Instant UI

To configure VLAN settings for an SSID:

1. In the **VLAN** tab of **New WLAN** window. The VLAN tab contents are displayed.

Figure 33 *VLAN Tab*



Client IP & VLAN Assignment

Client IP assignment: ○ Virtual Controller assigned ● Network assigned

Client VLAN assignment: ○ Default ○ Static ● Dynamic

VLAN Assignment Rules

Default VLAN: 1

2. Select any for the following options for **Client IP assignment**:
   - **Virtual Controller assigned**–On selecting this option, the client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the IAP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see DHCP Configuration on page 241.
   - **Network assigned**–Select this option to obtain the IP address from the network.
3. If the **Network assigned** is selected, specify any of the following options for the **Client VLAN assignment**.

- **Default**– On selecting this option, the client obtains the IP address in the same subnet as the IAPs. By default, the client VLAN is assigned to the native VLAN on the wired network.
- **Static**– On selecting this option, you need to specify a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling.
- **Dynamic**– On selecting this option, you can assign the VLANs dynamically from a Dynamic Host Configuration Protocol (DHCP) server. To create VLAN assignment rules:

  a. Click **New** to assign the user to a VLAN. The **New VLAN Assignment Rule** window appears.

  b. Enter the following information:

     - **Attribute**– Select an attribute returned by the RADIUS server during authentication.
     - **Operator**– Select an operator for matching the string.
     - **String**– Enter the string to match.
     - **VLAN**– Enter the VLAN to be assigned.

4. Click **Next** to configure security settings for the employee network. For more information, see Configuring Security Settings for a WLAN SSID Profile on page 94.

In the CLI

To manually assign VLANs for WLAN SSID users:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# vlan <vlan-ID>
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To enforce DHCP-based VLAN assignment:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# enforce-dhcp
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To create a new VLAN assignment rule:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals| starts-wi
th| ends-with| contains|matches-regular-expression} <operator> <VLAN-ID>| value-of}
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring Security Settings for a WLAN SSID Profile

This section describes the procedure for configuring security settings for employee and voice network only. For information on guest network configuration, see Captive Portal for Guest Access.

NOTE

If you are creating a new SSID profile, configure the WLAN and VLAN settings before defining security settings. For more information, see Configuring WLAN Settings for an SSID Profile on page 90 and Configuring VLAN Settings for a WLAN SSID Profile on page 93.

Configuring Security Settings for an Employee or Voice Network

You can configure security settings for an employee or voice network by using the Instant UI or CLI.

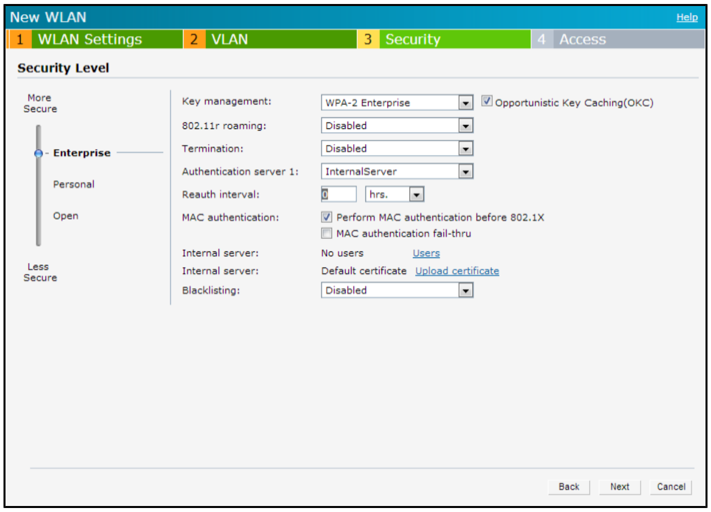
In the Instant UI

To configure security settings for an employee or voice network:

1. In the **Security** tab, specify any of the following types of security levels by moving the slider to a desired level:
   - **Enterprise**–On selecting enterprise security level, the authentication options applicable to the enterprise network are displayed.
   - **Personal** – On selecting personal security level, the authentication options applicable to the personalized network are displayed.
   - **Open**–On selecting Open security level, the authentication options applicable to an open network are displayed:

   The default security setting for a network profile is **Personal**. The following figures show the configuration options for **Enterprise**, **Personal**, and **Open** security settings:

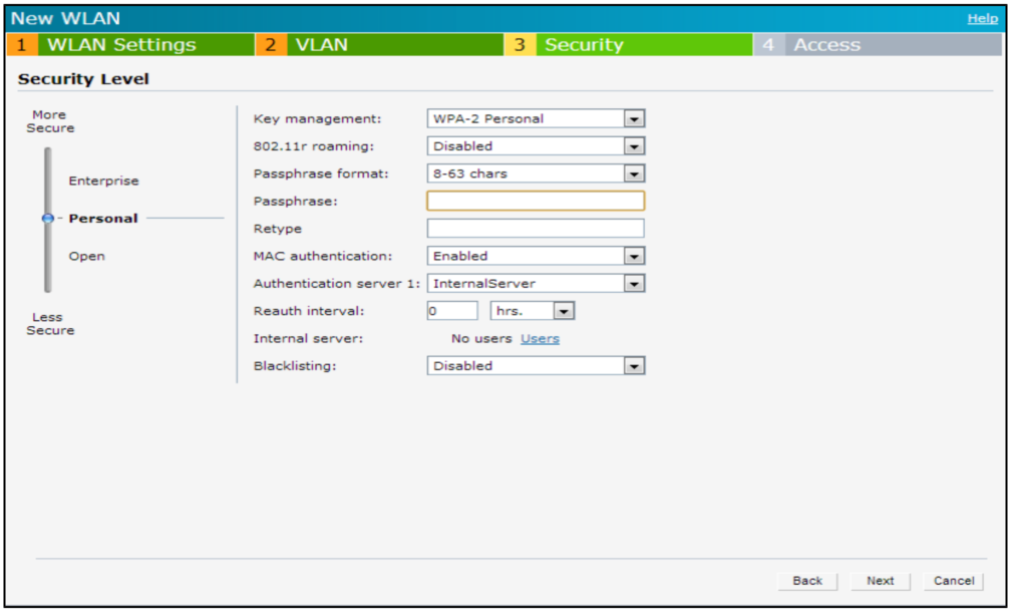
Figure 34 *Security Tab: Enterprise*



Security Level

Key management: WPA-2 Enterprise ☑ Opportunistic Key Caching(OKC)
802.11r roaming: Disabled
Termination: Disabled
Authentication server 1: InternalServer
Reauth interval: 0 hrs.
MAC authentication: ☑ Perform MAC authentication before 802.1X
☐ MAC authentication fail-thru
Internal server: No users Users
Internal server: Default certificate Upload certificate
Blacklisting: Disabled

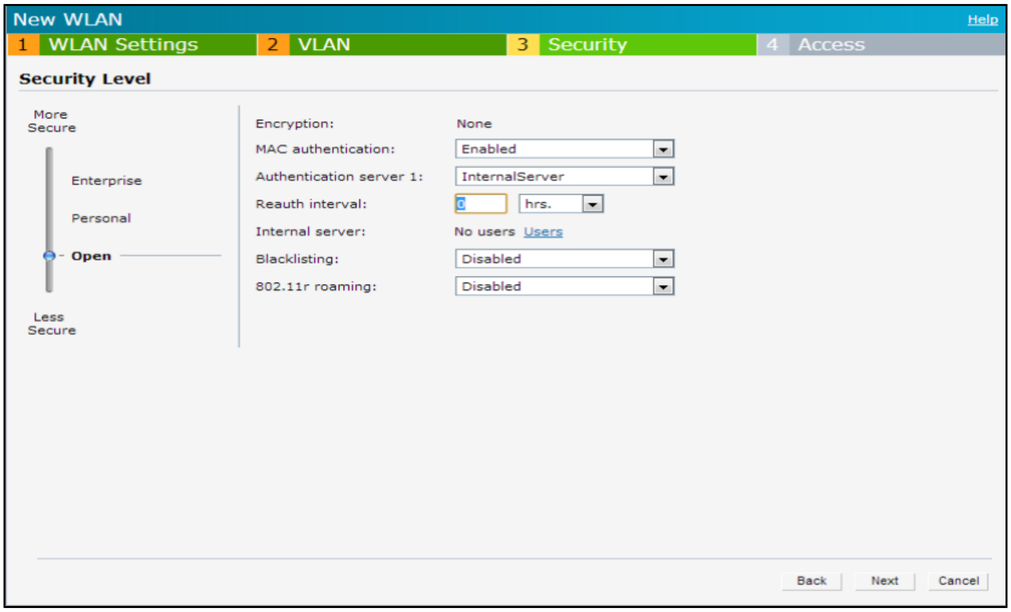
Figure 35 *Security Tab: Personal*



Security Level

Key management: WPA-2 Personal
802.11r roaming: Disabled
Passphrase format: 8-63 chars
Passphrase:
Retype
MAC authentication: Enabled
Authentication server 1: InternalServer
Reauth interval: 0 hrs.
Internal server: No users Users
Blacklisting: Disabled

Figure 36 *Security Tab: Open*



Security Level

Encryption: None

MAC authentication: Enabled

Authentication server 1: InternalServer

Reauth interval: 0 hrs.

Internal server: No users Users

Blacklisting: Disabled

802.11r roaming: Disabled

2. Based on the security level specified, specify the following parameters:

Table 18: *Configuration Parameters for WLAN Security Settings*

Parameter	Description	Security Level Type
Key Management	For **Enterprise** security level, select any of the following options from the **Key management** drop-down list: ● WPA-2 Enterprise ● Both (WPA-2 & WPA) ● WPA Enterprise ● Dynamic WEP with 802.1X – If you do not want to use a session key from the RADIUS Server to derive pair wise unicast keys, set **Session Key for LEAP** to **Enabled**. This is required for old printers that use dynamic WEP through Lightweight Extensible Authentication Protocol (LEAP) authentication. The **Session Key for LEAP** feature is **Disabled** by default. **NOTE:** When **WPA-2 Enterprise** and **Both (WPA2-WPA)** encryption types are selected and if 802.1x authentication method is configured, the **Opportunistic Key Caching** (OKC) is enabled by default. If OKC is enabled, a cached pairwise master key (PMK) is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication. OKC roaming can be configured only for the **Enterprise** security level.	Applicable to **Enterprise** and **Personal** security levels only. For the **Open** security level, no encryption settings are required.
	For **Personal** security level, select an encryption key from the **Key management** drop-down list. ● For WPA-2 Personal, WPA Personal, and Both (WPA-2&WPA) keys, specify the following parameters: 1. **Passphrase format**: Select a passphrase format from the **Passphrase format** drop-down list. The options are available are 8-63 alphanumeric characters and 64 hexadecimal characters. 2. Enter a passphrase in the **Passphrase** text box and reconfirm. ● For **Static WEP**, specify the following parameters:	

Table 18: *Configuration Parameters for WLAN Security Settings*

Parameter	Description	Security Level Type
	1. Select an appropriate value for **WEP key size** from the WEP key size drop-down list. You can specify 64-bit or 128-bit . 2. Select an appropriate value for Tx key from the **Tx Key** drop-down list. You can specify **1**, **2**, **3**, or **4**. 3. Enter an appropriate **WEP key** and reconfirm.	
802.11r roaming	To enable 802.11r roaming, select **Enabled** from the **802.11r roaming** drop-down. Selecting this checkbox enables fast BSS transition. The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster.	**Enterprise**, **Personal**, and **Open** security levels.
Termination	To terminate the EAP portion of 802.1X authentication on the IAP instead of the RADIUS server, set **Termination** to **Enabled**. Enabling **Termination** can reduce network traffic to the external RADIUS server by terminating the authorization protocol on the IAP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the IAP acts as a relay for this exchange. When **Termination** is enabled, the IAP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. **NOTE:** If you are using LDAP for authentication, ensure that AP termination is configured to support EAP.	**Enterprise** security level
Authentication server 1 and **Authentication server 2**	Select any of the following options from the **Authentication server 1** drop-down list: - Select an authentication server from the list if an external servers are already configured. - Select **New** to configure any of the following servers as an external server: - RADIUS Server - LDAP Server - CPPM Server for AirGroup **CoA** For information on configuring external servers, see Configuring an External Server for Authentication on page 149. - To use an internal server, select **Internal server** and add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add the users. For information on adding a user, see User Management on page 133. If an external server is selected, you can also configure another authentication server.	**Enterprise**, **Personal**, and **Open** security levels.
Load balancing	Set this to **Enabled** if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced.	**Enterprise**, **Personal**, and **Open** security levels.
Reauth interval	Specify a value for **Reauth interval**. When set to a value greater than zero, APs periodically reauthenticate all associated and authenticated clients.	**Enterprise**, **Personal**, and **Open** security levels.
Blacklisting	To enable blacklisting of the clients with a specific number of authentication failures, select **Enabled** from the **Blacklisting** drop-down list and specify a value for **Max authentication failures**. The users who fail to authenticate the number of times specified in **Max authentication failures** field are dynamically blacklisted.	**Enterprise**, **Personal**, and **Open** security levels.

Table 18: *Configuration Parameters for WLAN Security Settings*

Parameter	Description	Security Level Type
Accounting	To enable accounting, select **Enabled** from the **Accounting** drop-down list. On setting this option to **Enabled**, APs post accounting information to the RADIUS server at the specified **Accounting interval**.	**Enterprise**, **Personal**, and **Open** security levels.
Authentication survivability	To enable authentication survivability, set **Authentication survivability** to **Enabled**. Specify a value in hours for **Cache timeout (global)** to set the duration after which the authenticated credentials in the cache must expire. When the cache expires, the clients are required to authenticate again. You can specify a value within range of 1 to 99 hours and the default value is 24 hours. **NOTE:** The authentication survivability feature requires ClearPass Policy Manager 6.0.2 or later, and is available only when the **New** server option is selected authentication. On setting this parameter to **Enabled**, Instant authenticates the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily lost. The Authentication survivability feature is not applicable when a RADIUS server is configured as an internal server.	**Enterprise** security level
MAC authentication	To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC authentication** to **Enabled**. For **Enterprise** security level, the following options are available: ● **Perform MAC authentication before 802.1X** – Select this check box to use 802.1X authentication only when the MAC authentication is successful. ● **MAC authentication fail-thru** – On selecting this check box, the 802.1X authentication is attempted when the MAC authentication fails.	**Enterprise**, **Personal**, and **Open** security levels.
Delimiter character	Specify if a character, for example colon (:), as a delimiter for MAC address string. This option is available only when MAC authentication is enabled. You can specify colon or dash for delimiter. If the delimiter is not specified, the MAC address must be in the xxxxxxxxxxxx format. If you specify colon for the delimiter, you can enter MAC addresses in the xx:xx:xx:xx:xx:xx format.	**Enterprise**, **Personal**, and **Open** security levels.
Uppercase support	Set to **Enabled** to allow uppercase letters in MAC address string. This option is available only if MAC authentication is enabled.	**Enterprise**, **Personal**, and **Open** security levels.
Upload Certificate	Click **Upload Certificate** and browse to upload a certificate file for the internal server. For more information on certificates, see Uploading Certificates on page 164.	**Enterprise**, **Personal**, and **Open** security levels.

4. Click **Next** to configure access rules. For more information, see Configuring Access Rules for a WLAN SSID Profile on page 99.

In the CLI

To configure enterprise security settings for the employee and voice users of a WLAN SSID profile:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip,wpa2-aes|wpa-psk-tkip,w
pa2-psk-aes|dynamic-wep}
(Instant Access Point)(SSID Profile <name>)# leap-use-session-key
(Instant Access Point)(SSID Profile <name>)# termination
(Instant Access Point)(SSID Profile <name>)# auth-server <server-name>
(Instant Access Point)(SSID Profile <name>)# external-server
(Instant Access Point)(SSID Profile <name>)# server-load-balancing
```

```
(Instant Access Point)(SSID Profile <name>)# blacklist
(Instant Access Point)(SSID Profile <name>)# mac-authentication
(Instant Access Point)(SSID Profile <name>)# l2-auth-failthrough
(Instant Access Point)(SSID Profile <name>)# auth-survivability
(Instant Access Point)(SSID Profile <name>)# radius-accounting
(Instant Access Point)(SSID Profile <name>)# radius-accounting-mode {user-authentication| user
association}
(Instant Access Point)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>
(Instant Access Point)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant Access Point)(SSID Profile <name>)# max-authentication-failures <number>
(Instant Access Point)(SSID Profile <name>)# exit
(Instant Access Point)(config)# auth-survivability cache-time-out
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To configure personal security settings for the employee and voice users of a WLAN SSID profile:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# opmode {wpa2-psk-aes|wpa-tkip| wpa-psk-tkip|wpa-p
sk-tkip,wpa2-psk-aes| static-wep}
(Instant Access Point)(SSID Profile <name>)# mac-authentication
(Instant Access Point)(SSID Profile <name>)# auth-server <server-name>
(Instant Access Point)(SSID Profile <name>)# external-server
(Instant Access Point)(SSID Profile <name>)# server-load-balancing
(Instant Access Point)(SSID Profile <name>)# blacklist
(Instant Access Point)(SSID Profile <name>)# max-authentication-failures <number>
(Instant Access Point)(SSID Profile <name>)# radius-accounting
(Instant Access Point)(SSID Profile <name>)# radius-accounting-mode {user-authentication| user
association}
(Instant Access Point)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>
(Instant Access Point)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure open security settings for employee and voice users of a WLAN SSID profile:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# opmode {opensystem}
(Instant Access Point)(SSID Profile <name>)# mac-authentication
(Instant Access Point)(SSID Profile <name># auth-server <server-name>
(Instant Access Point)(SSID Profile <name># external-server
(Instant Access Point)(SSID Profile <name># server-load-balancing
(Instant Access Point)(SSID Profile <name># blacklist
(Instant Access Point)(SSID Profile <name># max-authentication-failures <number>
(Instant Access Point)(SSID Profile <name># radius-accounting
(Instant Access Point)(SSID Profile <name># radius-accounting-mode {user-authentication| usera
ssociation}
(Instant Access Point)(SSID Profile <name># radius-interim-accounting-interval <minutes>
(Instant Access Point)(SSID Profile <name># radius-reauth-interval <minutes>
(Instant Access Point)(SSID Profile <name># end
(Instant Access Point)# commit apply
```

Configuring Access Rules for a WLAN SSID Profile

This section describes the procedure for configuring security settings for employee and voice network only. For information on guest network configuration, see Captive Portal for Guest Access.

NOTE

If you are creating a new SSID profile, complete the WLAN Settings and configure VLAN and security parameters, before defining access rules. For more information, see Configuring WLAN Settings for an SSID Profile on page 90, Configuring VLAN Settings for a WLAN SSID Profile on page 93, and Configuring Security Settings for a WLAN SSID Profile on page 94.

You can configure up to 64 access rules for an employee, voice , or guest network using the Instant UI or CLI.

In the Instant UI

To configure access rules for an employee or voice network:

1. In the **Access Rules** tab, set slider to any of the following types of access control:
   - **Unrestricted**– Select this to set unrestricted access to the network.
   - **Network-based**– Set the slider to **Network-based** to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule:
     a. Click **New**.
     b. Select appropriate options in the **New Rule** window.
     c. Click **OK**.
   - **Role-based**– Select **Role-based** to enable access based on user roles. For role-based access control:
     - Create a user role if required. For more information, see Configuring User Roles.
     - Create access rules for a specific user role. For more information, see Configuring Access Rules on page 173. You can also configure an access rule to enforce Captive portal authentication for an SSID that is configured to use 802.1X authentication method. For more information, see Configuring Captive Portal Roles for an SSID on page 128.
     - Create a role assignment rule. For more information, see Configuring Derivation Rules on page 182.
2. Click **Finish**.

In the CLI

To configure access control rules for a WLAN SSID:

```
(Instant Access Point)(config)# wlan access-rule <name>
(Instant Access Point)(Access Rule <name>)# rule <dest> <mask> <match> <protocol> <start-port>
<end-port> {permit |deny | src-nat | dst-nat {<IP-address> <port> | <port>}}[<option1....optio
n9>]
(Instant Access Point)(Access Rule <name>)# end
(Instant Access Point)# commit apply
```

To configure access control based on the SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role-by-ssid
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure role assignment rules:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-wi
th|ends-with|contains|matches-regular-expression}<operator><role>|value-of}
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure a pre-authentication role:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role-pre-auth <pre-authentication-role>
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure machine and user authentication roles

```
(Instant Access Point)(config)# wlan ssid-profile <name>
```

```
(Instant Access Point)(SSID Profile <name>)# set-role-machine-auth <machine-authentication-onl
y> <user-authentication-only>
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure unrestricted access:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role-unrestricted
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring Support for Fast Roaming of Clients

Instant supports the following features that enable fast roaming of clients:

- 802.11r Roaming
- Opportunistic Key Caching

802.11r Roaming

802.11r is a roaming standard defined by IEEE. When enabled, 802.11r reduces roaming delay by pre-authenticating clients with multiple target APs before a client roams to an AP. With 802.11r implementation, clients pre-authenticate with multiple APs in a cluster.

As part of the 802.11r implementation, Instant supports the Fast BSS Transition protocol. The Fast BSS Transition mechanism reduces client roaming delay when a client transitions from one BSS to another within the same cluster. This minimizes the time required to resume data connectivity when a BSS transition happens.

NOTE

Fast BSS Transition is operational only if the wireless client supports 802.11r standard. If the client does not support 802.11r standard, it falls back to the normal WPA2 authentication method.

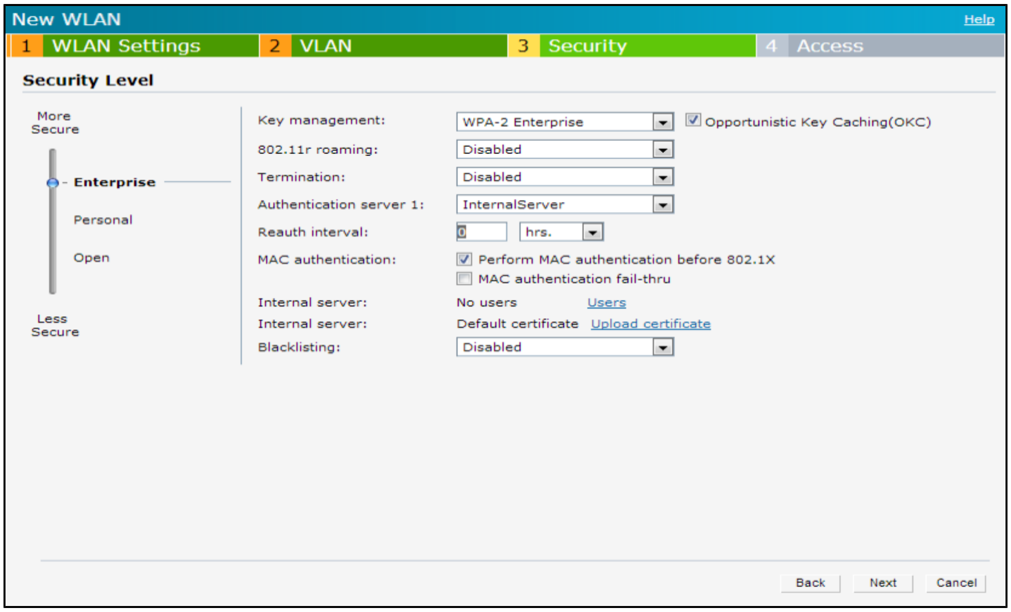
Configuring an IAP for 802.11r support

You can configure 802.11r support for a WLAN SSID by using Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard (click **Network**>**New** or **Network**> Select the WLAN SSID>**edit**).
2. Click the **Security** tab.
3. Slide to **Enterprise**, **Personal** or **Open** security level. On selecting a security level, the authentication options applicable to the corresponding network are displayed. The following figure shows the **Enterprise** security level details.

Figure 37 *WLAN Security Settings—Enterprise Tab*



Security Level

Key management: WPA-2 Enterprise ☑ Opportunistic Key Caching(OKC)
802.11r roaming: Disabled
Termination: Disabled
Authentication server 1: InternalServer
Reauth interval: 0 hrs.
MAC authentication: ☑ Perform MAC authentication before 802.1X
□ MAC authentication fail-thru
Internal server: No users Users
Internal server: Default certificate Upload certificate
Blacklisting: Disabled

4. Set **802.11r roaming** to **Enabled**. 802.11r roaming can also be enabled for **Personal** and **Open** security levels.
5. Click **Next** and then click **Finish**.

In the CLI

To enable 802.11r roaming on an enterprise WLAN SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# opmode {wpa2-aes}
(Instant Access Point)(SSID Profile <name>)# dot11r
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To enable 802.11r roaming for personal security settings:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# opmode {wpa2-psk-aes| wpa-tkip| wpa-psk-tkip|wpa-
tkip,wpa2-aes| wpa-psk-tkip,wpa2-psk-aes}
(Instant Access Point)(SSID Profile <name>)# dot11r
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To enable 802.11r roaming for open security settings:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# opmode {opensystem}
(Instant Access Point)(SSID Profile <name>)# dot11r
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Opportunistic Key Caching

Instant now supports opportunistic key caching (OKC) based roaming. In the OKC based roaming, the AP stores one pairwise master key (PMK) per client, which is derived from last 802.1x authentication completed by the client in the network. The cached PMK is used when a client roams to a new AP. This allows faster roaming of clients between the IAPs in a cluster, without requiring a complete 802.1X authentication.

NOTE

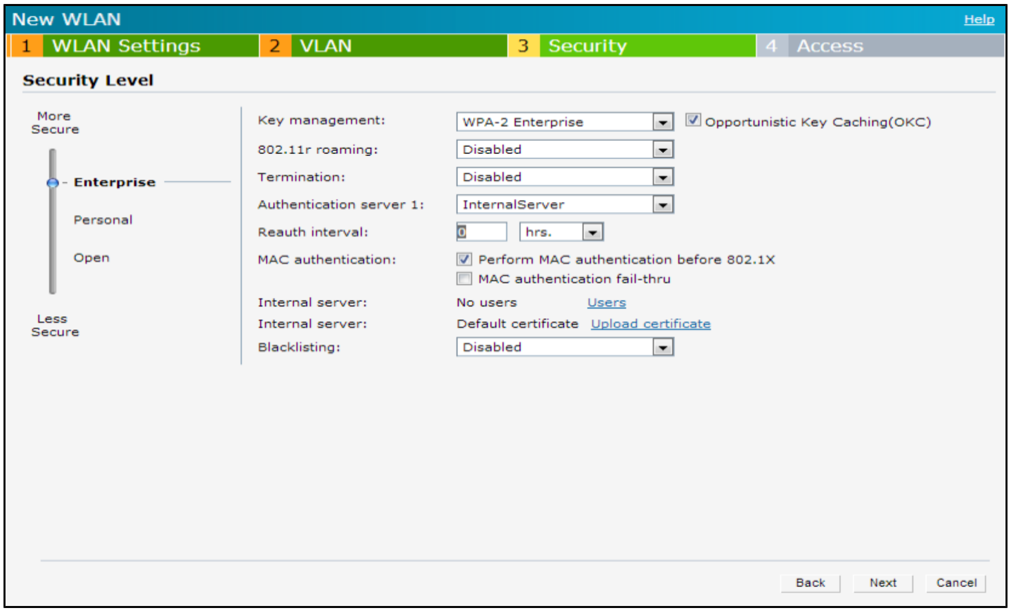
OKC roaming (when configured in the 802.1x Authentication profile) is supported on WPA2 clients. If the wireless client (the 802.1X supplicant) does not support this feature, a complete 802.1X authentication is required whenever a client roams to a new AP.

Configuring an IAP for OKC Roaming

You can enable OKC roaming for WLAN SSID by using Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard (click **Network**>**New** or **Network**> Select the WLAN SSID>**edit**).
2. Click the **Security** tab.
3. Slide to **Enterprise** security level. On selecting a security level, the authentication options applicable to Enterprise network are displayed.



Key management: WPA-2 Enterprise ☑ Opportunistic Key Caching(OKC)
802.11r roaming: Disabled
Termination: Disabled
Authentication server 1: InternalServer
Reauth interval: 0 hrs.
MAC authentication: ☑ Perform MAC authentication before 802.1X
☐ MAC authentication fail-thru
Internal server: No users Users
Internal server: Default certificate Upload certificate
Blacklisting: Disabled

4. Select the **WPA-2 Enterprise** or **Both (WPA-2 & WPA)** option from the **Key management** drop-down list. When any of these encryption types is selected, **Opportunistic Key Caching** (OKC) is enabled by default.
5. Click **Next** and then click **Finish**.

In the CLI

To disable OKC roaming on a WLAN SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip,wpa-aes,wpa2-tkip,wpa2-aes}
(Instant Access Point)(SSID Profile <name>)# okc-disable
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To enable OKC roaming on a WLAN SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# opmode {wpa2-aes| wpa-tkip,wpa-aes,wpa2-tkip,wpa2-aes|}
(Instant Access Point)(SSID Profile <name>)# no okc-disable
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Editing Status of a WLAN SSID Profile

You can enable or disable an SSID profile in the Instant UI or CLI.

In the Instant UI

To modify the status of a WLAN SSID profile:

1. In the **Networks** tab, select the network that you want to edit. The **edit** link appears.
2. Click the **edit** link. The **Edit network** window appears.
3. Select or clear the **Disable SSID** check box to disable or enable the SSID. The SSID is enabled by default.
4. Click **Next** or the tab name to move to the next tab.
5. Click **Finish** to save the modifications.

In the CLI

To disable an SSID

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# disable
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To enable an SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# enable
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring Additional WLAN SSIDs

By default, you can create up to six WLAN SSIDs. With the Extended SSID option enabled, you can create up to 16 WLANs. The IAPs that support 16 WLANs are as follows:

- RAP-3WN
- IAP-92
- IAP-93
- IAP-134
- IAP-135

The number of SSIDs that become active on each IAP depends on the IAP platform.

Enabling the Extended SSID

NOTE

Enabling the Extended SSID option disables mesh.

You can configure additional SSIDs by using the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at top right corner of the Instant main window.
2. Click the **Show advanced options** link.
3. In the **General** tab, select **Enabled** from the **Extended SSID** drop-down list.
4. Click **OK**.
5. Reboot the IAP for the changes to take effect. After you enable the option and reboot the IAP, the Wi-Fi and mesh links are disabled automatically.

In the CLI

To enable the extended SSIDs:

```
(Instant Access Point)(config)# extended-ssid
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Editing a WLAN SSID Profile

To edit a WLAN SSID profile:

1. In the **Networks** tab, select the network that you want to edit. The **edit** link appears.
2. Click the **edit** link. The **Edit network** window appears.
3. Modify the required settings. Click **Next** to move to the next tab.
4. Click **Finish** to save the modifications.

Deleting a WLAN SSID Profile

To delete a WLAN SSID profile:

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

Chapter 8
Wired Profiles

This chapter describes the following procedures:

- Configuring a Wired Profile on page 107
- Assigning a Profile to Ethernet Ports on page 113
- Understanding Hierarchical Deployment on page 112
- Configuring Wired Bridging on Ethernet 0 on page 112
- Editing a Wired Profile on page 113
- Deleting a Wired Profile on page 114

Configuring a Wired Profile

The wired profile configuration for employee network involves the following procedures:

1. Configuring Wired Settings on page 107
2. Configuring VLAN for a Wired Profile on page 108
3. Configuring Security Settings for a Wired Profile on page 109
4. Configuring Access Rules for a Wired Profile on page 110

For information on creating a wired profile for guest network, see Captive Portal for Guest Access

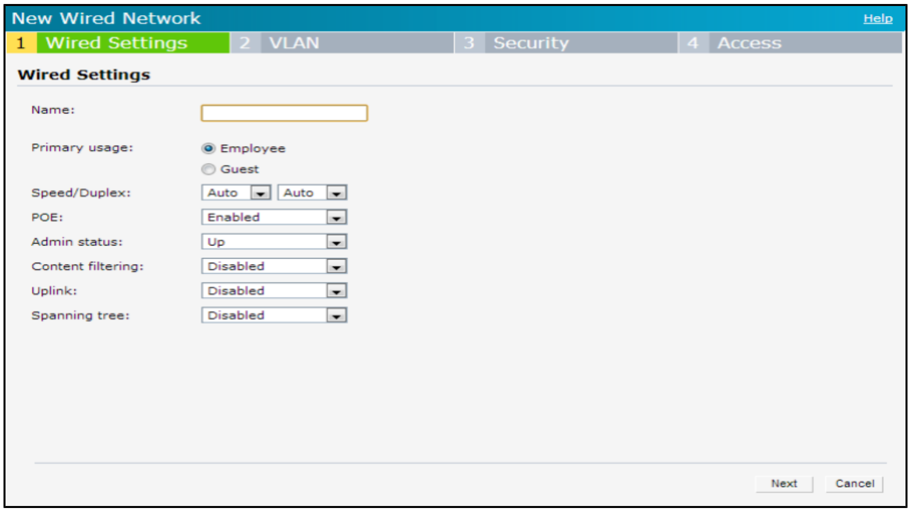
Configuring Wired Settings

You can configure wired settings for a wired profile by using the Instant UI or CLI.

In the Instant UI

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks**. The **New Wired Network** window appears. The following figure shows the contents of **Wired Settings** tab:

Figure 38 *New Wired Network Window: Wired Settings Window*



Wired Settings

Name:

Primary usage: ● Employee ○ Guest

Speed/Duplex: Auto Auto

POE: Enabled

Admin status: Up

Content filtering: Disabled

Uplink: Disabled

Spanning tree: Disabled

3. Click the **Wired Settings** tab and enter the following information:

a. **Name**– Specify a name for the profile.

b. **Primary Usage** – Select **Employee** or **Guest**.

c. **Speed/Duplex** – Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.

d. **POE** – Set **POE** to **Enabled** to enable Power over Ethernet.

> NOTE
>
> The E2 port on RAP-3WNP supports Power Sourcing Equipment (PSE) to supply power to any compliant 802.3af powered (class 0-4) device. RAP-155Psupports PSE for 802.3af powered device (class 0-4) on one port (E1 or E2), or 802.3at powered DC IN (Power Socket) on two ports (E1 and E2).

e. **Admin Status** – Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down.

f. **Content Filtering**– To ensure that all DNS requests to non-corporate domains on this wired network are sent to OpenDNS, select **Enabled** for **Content Filtering**.

g. **Uplink** – Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see Assigning a Profile to Ethernet Ports on page 113.

h. **Spanning Tree**–Select the **Spanning Tree** checkbox to enable Spanning Tree Protocol (STP) on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on IAPs with three or more ports. By default Spanning Tree is disabled on wired profiles.

4. Click **Next**. The VLAN tab details are displayed.
5. Configure VLAN for the wired profile. For more information, see Configuring VLAN for a Wired Profile on page 108.

In the CLI

To configure wired settings for:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# type {<employee> |<guest>}
(Instant Access Point)(wired ap profile <name>)# speed {10 |100 |1000 |auto}
(Instant Access Point)(wired ap profile <name>)# duplex {<half>|<full>|<auto>}
(Instant Access Point)(wired ap profile <name>)# no shutdown
(Instant Access Point)(wired ap profile <name>)# poe
(Instant Access Point)(wired ap profile <name>)# uplink-enable
(Instant Access Point)(wired ap profile <name>)# content-filtering
(Instant Access Point)(wired ap profile <name>)# spanning-tree
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring VLAN for a Wired Profile

> NOTE
>
> If you are creating a new wired profile, complete the Wired Settings procedure before configuring VLAN. For more information, see Configuring Wired Settings on page 107.

You can configure VLAN using Instant UI or CLI.

In the Instant UI

To configure VLAN:

1. In the **VLAN** tab, enter the following information.

a. **Mode** – You can specify any of the following modes:

    - **Access** – Select this mode to allow the port to carry a single VLAN specified as the native VLAN.
    - **Trunk** – Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.

   b. Specify any of the following values for **Client IP Assignment**:

    - **Virtual Controller Assigned**: Select this option to allow the Virtual Controller to assign IP addresses to the wired clients. When the Virtual Controller assignment is used, the source IP address is translated for all client traffic that goes through this interface. The Virtual Controller can also assign a guest VLAN to a wired client.
    - **Network Assigned**: Select this option to allow the clients to receive an IP address from the network to which the Virtual Controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.

   c. If the **Trunk** mode is selected:

    - Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges 1,2,5 or 1-4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
    - If **Client IP Assignment** is set the **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1-4093.

   d. If the **Access** mode is selected:

    - If the **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 2.
    - If the **Client IP Assignment** is set the **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.

2. Click **Next**. The **Security** tab details are displayed.
3. Configure security settings for the wired profile. For more information, see Configuring Security Settings for a Wired Profile on page 109.

In the CLI

To configure VLAN settings for a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# switchport-mode {<trunk> | <access>}
(Instant Access Point)(wired ap profile <name>)# allowed-vlan <vlan>
(Instant Access Point)(wired ap profile <name>)# native-vlan {<guest|1…4095>}
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

To configure a new VLAN assignment rule:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# set-vlan <attribute>{equals| not-equals| star
ts-with| ends-with| contains| matches-regular-expression} <operator> <VLAN-ID>| value-of}
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring Security Settings for a Wired Profile

NOTE

If you are creating a new wired profile, complete the Wired Settings and VLAN procedures before specifying security settings. For more information, see Configuring Wired Settings on page 107 and Configuring VLAN Settings for a WLAN SSID Profile on page 93.

Configuring Security Settings for a Wired Employee Network

You can configure security parameters for an employee network by using the Instant UI or CLI.

In the Instant UI

To configure security parameters for an employee network:

1. Configure the following parameters in the **Security** tab.
   - **MAC authentication** – To enable MAC authentication, select **Enabled**. The MAC authentication is disabled by default.
   - **802.1X authentication** – To enable 802.1X authentication, select **Enabled**.
   - **MAC authentication fail-thru** – To enable authentication fail-thru, select **Enabled**. When this feature is enabled, 802.1X authentication is attempted when MAC authentication fails. The **MAC authentication fail-thru** check box is displayed only when both **MAC authentication** and **802.1X authentication** are **Enabled**.
   - Select any of the following options for **Authentication server 1**:
     - **New** – On selecting this option, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see Configuring an External Server for Authentication on page 149.Authentication on page 139
     - **Internal server**– If an internal server is selected, add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add the users. For information on adding a user, see User Management on page 133.
   - **Reauth interval** – Specify the interval at which all associated and authenticated clients must be reauthenticated.
   - **Load balancing**– Set this to **Enabled** if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced.
2. Click **Next**. The **Access** tab details are displayed.

In the CLI

To configure security settings for an employee network:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# mac-authentication
(Instant Access Point)(wired ap profile <name>)# l2-auth-failthrough
(Instant Access Point)(wired ap profile <name>)# auth-server <name>
(Instant Access Point)(wired ap profile <name>)# server-load-balancing
(Instant Access Point)(wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring Access Rules for a Wired Profile

The Ethernet ports allow third-party devices such as VoIP phones or printers (which support only wired connections) to connect to the wireless network. You can also configure an Access Control List (ACL) for additional security on the Ethernet downlink.

NOTE

If you are creating a new wired profile, complete the Wired Settings and configure VLAN and security parameters, before defining access rules. For more information, see Configuring Wired Settings on page 107, Configuring VLAN for a Wired Profile on page 108, and Configuring Security Settings for a Wired Profile on page 109.

You can configure access rules by using the Instant UI or CLI.

In the Instant UI

To configure access rules:

1. In the **Access** tab, configure the following access rule parameters.
   a. Select any of the following types of access control:

- **Role-based**– Allows the users to obtain access based on the roles assigned to them.
- **Unrestricted**– Allows the users to obtain unrestricted access on the port.
- **Network-based**– Allows the users to be authenticated based on access rules specified for a network.

b. If the **Role-based** access control is selected, perform the following steps:

- Under **Roles**, select an existing role for which you want apply the access rules, or click **New** and add the required role. The list of roles defined for all networks is displayed under **Roles**.

NOTE

The default role with the same name as the network, is automatically defined for each network. The default roles cannot be modified or deleted.

- Select the access rule associated with a specific role and modify if required. To add a new access rule, click **New** in the **Access Rules** window. You can configure up to 64 access rules. For more information on configuring access rules, see Configuring Access Rules on page 173.
- Configure rules to assign roles for an authenticated client. You can also configure rules to derive VLANs for the wired network profile. For more information on role assignment rules and VLAN derivation rules, see Configuring Derivation Rules on page 182 and Configuring VLAN Derivation Rules on page 186.
- Select the **Assign pre-authentication role** check box to add a pre-authentication role that allows some access to the users before the client authentication.
- Select the **Enforce Machine Authentication** check box, to configure access rights to clients based on whether the client device supports machine authentication. Select the **Machine auth only** and **User auth** only rules. Machine Authentication is only supported on Windows devices and devices such as iPads.

NOTE

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

2. Click **Finish**.

In the CLI

To configure access rules for a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# access-rule-name <name>
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

To configure role assignment rules:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# set-role <attribute>{{equals| not-equal| star
ts-with| ends-with| contains| matches-regular-expression}<operator> <role>| value-of}
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

To configure a pre-authentication role:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# set-role-pre-auth <pre-authentication-role>
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

To configure machine and user authentication roles:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# set-role-machine-auth <machine-auth-only>
<user-auth-only>
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

To configure unrestricted access:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# set-role-unrestricted
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Understanding Hierarchical Deployment

An IAP-130 Series or RAP-3WN (with more than one wired port) can be connected to the downlink wired port of another IAP (ethX). An IAP with a single Ethernet port (like IAP-90 or IAP-100 series devices) can be provisioned to use Ethernet bridging, so that Ethernet 0 port is converted to a downlink wired port.

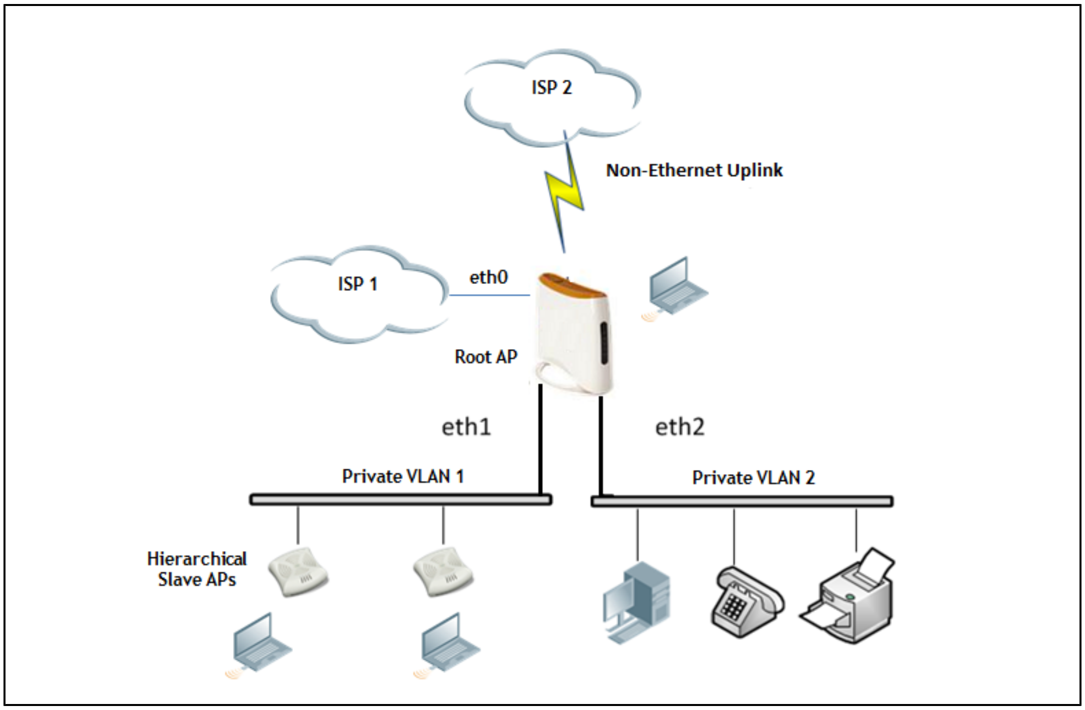
You can also form an IAP network by connecting the downlink port of an AP to other APs. Only one AP in the network uses its downlink port to connect to the other APs. This AP (called the root AP) acts as the wired device for the network, provides DHCP service and an L3 connection to the ISP uplink with NAT. The root AP is always the master of the Instant network. In a single Ethernet port platform deployment, the root AP must be configured to use the 3G uplink.

A typical hierarchical deployment consists of the following:

- A direct wired ISP connection or a wireless uplink.
- One or more DHCP pools for private VLANs.
- One downlink port configured on a private VLAN without authentication for connecting to slave APs. Ensure that the downlink port configured in a private VLAN is not used for any wired client connection. Other downlink ports can be used for connecting to the wired clients.

The following figure illustrates a hierarchical deployment scenario:

Figure 39 *Hierarchical Deployment*



Configuring Wired Bridging on Ethernet 0

Instant supports wired bridging on the Ethernet 0 port of an IAP.

NOTE

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

You can configure support for wired bridging on the Ethernet 0 port of an IAP using Instant UI or CLI.

In the Instant UI

To configure Ethernet bridging:

1. In the **Access Points** tab, click the IAP to modify. The **edit** link is displayed.
2. Click the **edit** link. The **edit** window for modifying IAP details is displayed.
3. Click the **Uplink** tab.
4. Select **Enable** from the **Eth0 Bridging** drop-down menu.
5. Click **OK**.
6. Reboot the IAP.

In the CLI

To configure Ethernet bridging:

```
Instant Access Point# enet0-bridging
```

Assigning a Profile to Ethernet Ports

You can assign profiles to Ethernet ports using Instant UI or CLI.

In the Instant UI

To assign profiles to Ethernet ports:

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. To assign an Ethernet downlink profile to Ethernet 0 port:
   a. Ensure that the wired bridging on the port is enabled. For more information, see Configuring Wired Bridging on Ethernet 0 on page 112.
   b. Select and assign a profile from the **0/0** drop down list.
   c. To assign a wired profile to Ethernet 0/1 port, select the profile from the **0/1** drop down list.
   d. If the IAP supports E2, E3 and E4 ports, assign profiles to other Ethernet ports by selecting a profile from the **0/2**, **0/3**, and **0/4** drop-down list.

In the CLI

To assign profiles to Ethernet ports:

```
(Instant Access Point)(config)# enet0-port-profile <name>
(Instant Access Point)(config)# enet1-port-profile <name>
(Instant Access Point)(config)# enet2-port-profile <name>
(Instant Access Point)(config)# enet3-port-profile <name>
(Instant Access Point)(config)# enet4-port-profile <name>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Editing a Wired Profile

To edit a wired profile:

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window appears.
2. In the **Wired** window, select the wired profile to modify.
3. Click **Edit**. The **Edit Wired Network** window is displayed.
4. Modify the required settings.
5. Click **Finish** to save the modifications.

Deleting a Wired Profile

To delete a wired profile:

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. In the **Wired** window, select the wired profile to delete.
3. Click **Delete**. The wired profile is deleted.

Chapter 9
Captive Portal for Guest Access

This chapter provides the following information:

Understanding Captive Portal

The Aruba Instant supports the Captive portal authentication method, where a web page is presented to the guest users when they try to access the Internet whether in hotels, conference centers or Wi-Fi hotspots. The web page also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at many Wi-Fi hotspots and can be used to control wired access as well.

Aruba Instant Captive portal solution consists of the following:

- The captive portal web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against IAP's internal database.
- The SSID broadcast by the IAP.

With Instant, the administrators can create a wired or WLAN guest network based on Captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. The administrators can also create guest accounts and customize the Captive portal page with organization-specific logo, terms, and usage policy. With Captive portal authentication and guest profiles, the devices associating with the guest SSID are assigned an initial role and are assigned IP addresses. When a guest user tries to access a URL through HTTP or HTTPS, the Captive portal web page prompting the user to authenticate with a user name and password is displayed.

Types of Captive Portal

Instant supports the following types of Captive portal authentication:

- **Internal Captive portal** – For Internal Captive portal authentication, an internal server is used for hosting the captive portal service. It supports the following types of authentication:
  - **Internal Authenticated**– When **Internal Authenticated** is enabled, a guest user must authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database.
  - **Internal Acknowledged**– When **Internal Acknowledged** is enabled, a guest user must accept the terms and conditions to access the Internet.
- **External Captive portal**– For external Captive portal authentication, an external portal on the cloud or on a server outside the enterprise network is used.

Walled Garden

The administrators can also control the resources that the guest users can access and the amount of bandwidth or air time they can use at any given time. When an external Captive portal is used, the administrators can configure a walled garden, which determines access to the URLs requested by the guest users. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents. The users who do not sign up for the Internet service can view only the “allowed” Websites (typically hotel property Websites).

The administrators can allow or block access to specific URLs by creating a whitelist and blacklist. When the users attempt to navigate to other Websites, which are not in the whitelist of the walled garden profile, the users are redirected to the login page. If the requested URL is on the blacklist, it is blocked. If it appears on neither list the request is redirected to the external Captive portal.

Configuring a WLAN SSID for Guest Access

You create an SSID for guest access by using the Instant UI or CLI:

In the Instant UI

1. In the **Networks** tab of the Instant main window, click the **New** link. The **New WLAN** window appears.
2. Enter a name that uniquely identifies a wireless network in the **Name (SSID)** text box.
3. Based on the type of network profile, specify the **Primary usage** as **Guest**.
4. Click the **Show advanced options** link. The advanced options for configuration are displayed.
5. Enter the required values for the following configuration parameters:

Table 19: *WLAS SSID Configuration Parameters for Guest Network*

Parameters	Description
Broadcast/Multicast	Select any of the following values under **Broadcast filtering**: ● **All**–When set to **All**, the IAP drops all broadcast and multicast frames except DHCP and ARP. ● **ARP**–When set to **ARP**, the IAP converts ARP requests to unicast and send frames directly to the associated client. ● **Disabled**– When set to **Disabled**, all broadcast and multicast traffic is forwarded.
DTIM interval	The **DTIM interval** indicates the delivery traffic indication message (DTIM) period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the IAP should deliver the buffered broadcast and multicast frames to associated clients in the powersave mode. The default value is 1, which means the client checks for buffered data on the IAP at every beacon. You can also configure a higher DTIM value for power saving.
Multicast transmission optimization	Select **Enabled** if you want the IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5.0 GHz is 6 Mbps. This option is disabled by default.
Dynamic multicast optimization	Select **Enabled** to allow IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients.

Parameters	Description
DMO channel utilization threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the IAP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the IAP sends multicast traffic over the wireless link. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
Transmit Rates	Specify the following parameters: ● **2.4 GHz**–If the 2.4 GHz band is configured on the IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. ● **5 GHz**–If the 5 GHz band is configured on the IAP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
Bandwidth Limits	Select any of the following check boxes to specify the bandwidth limit: ● **Airtime**–Select this check box to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. ● **Each user**– Select this check box to specify a throughput for any single user in this network. Specify the throughput value in Kbps. ● **Each radio**– Select this check box to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients.
Wi-Fi Multimedia (WMM) traffic management	Configure the following options for Wi-Fi Multimedia (WMM) traffic management. WMM supports voice, video, best effort, and background access categories. You can allocate a higher bandwidth for voice and video traffic than other types of traffic based on the network profile. Specify a percentage value for the following parameters: ● **Background WMM share** – Allocates bandwidth for background traffic such as file downloads or print jobs. ● **Best effort WMM share** –Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. ● **Video WMM share** – Allocates bandwidth for video traffic generated from video streaming. ● **Voice WMM share** – Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication. **NOTE:** In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can allocate higher values for **Best effort WMM** share and **Voice WMM share** to allocate a higher bandwidth to clients transmitting best effort and voice traffic.
Content filtering	Set to **Enabled** to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to **2.4 GHz**, **5 GHz**, or **All**. The **All** option is selected by default.
Inactivity timeout	Specify a timeout interval. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. The minimum value is set to 60 seconds and the default value is 1000 seconds.
Hide SSID	Select the check box if you do not want the SSID (network name) to be visible to users

Parameters	Description
Disable SSID	Select to the checkbox to disable the SSID. On selecting this check box, the SSID is disabled, but not removed from the network. By default, all SSIDs are enabled.
Can be used without Uplink	Select the checkbox if you do not want the SSID users to use uplink.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN in the text box. You can specify a value within the range of 0 to 255. The default value is 64.
Local probe request threshold	Specify a threshold value in the **Local probe request threshold** text box to limit the number of incoming probe requests. When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls system response for this network profile and ignores probe requests if required. You can specify a Received signal strength indication (RSSI) value within range of 0 to 100 dB.

6. Click **Next** to configure VLAN settings. The VLAN tab contents are displayed.
7. Select any for the following options for **Client IP assignment**:
   - **Virtual Controller assigned**–On selecting this option, the client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the IAP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see DHCP Configuration on page 241.
   - **Network assigned**–Select this option to obtain the IP address from the network.
8. If the **Network assigned** is selected, specify any of the following options for the **Client VLAN assignment**.
   - **Default**– On selecting this option, the client obtains the IP address in the same subnet as the IAPs. By default, the client VLAN is assigned to the native VLAN on the wired network.
   - **Static**– On selecting this option, you need to specify a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling.
   - **Dynamic**– On selecting this option, you can assign the VLANs dynamically from a Dynamic Host Configuration Protocol (DHCP) server. To create VLAN assignment rules:

     a. Click **New** to assign the user to a VLAN. The **New VLAN Assignment Rule** window appears.

     b. Enter the following information:

        - **Attribute**– Select an attribute returned by the RADIUS server during authentication.
        - **Operator**– Select an operator for matching the string.
        - **String**– Enter the string to match.
        - **VLAN**– Enter the VLAN to be assigned.
9. Click **Next** to configure internal or external Captive portal authentication, roles and access rules for the guest users.

In the CLI

To configure WLAN settings for an SSID profile:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# essid <ESSID-name>
(Instant Access Point)(SSID Profile <name>)# type <Guest>
(Instant Access Point)(SSID Profile <name>)# broadcast-filter <type>
(Instant Access Point)(SSID Profile <name>)# dtim-period <number-of-beacons>
```

```
(Instant Access Point)(SSID Profile <name># multicast-rate-optimization
(Instant Access Point)(SSID Profile <name># dynamic-multicast-optimization
(Instant Access Point)(SSID Profile <name># dmo-channel-utilization-threshold
(Instant Access Point)(SSID Profile <name># a-max-tx-rate <rate>
(Instant Access Point)(SSID Profile <name># a-min-tx-rate <rate>
(Instant Access Point)(SSID Profile <name># g-max-tx-rate <rate>
(Instant Access Point)(SSID Profile <name># g-min-tx-rate <rate>
(Instant Access Point)(SSID Profile <name># bandwidth-limit <limit>
(Instant Access Point)(SSID Profile <name># per-user-bandwidth-limit <limit>
(Instant Access Point)(SSID Profile <name># air-time-limit <limit>
(Instant Access Point)(SSID Profile <name># wmm-background-share <percentage-of-traffic_share>
(Instant Access Point)(SSID Profile <name># wmm-best-effort-share<percentage-of-traffic-share>
(Instant Access Point)(SSID Profile <name># wmm-video-share <percentage-of-traffic_share>
(Instant Access Point)(SSID Profile <name># wmm-voice-share <percentage-of-traffic_share>
(Instant Access Point)(SSID Profile <name># rf-band {<2.4>|<5.0>|<all>}
(Instant Access Point)(SSID Profile <name># content-filtering
(Instant Access Point)(SSID Profile <name># hide-ssid
(Instant Access Point)(SSID Profile <name># inactivity-timeout <interval>
(Instant Access Point)(SSID Profile <name># work-without-uplink
(Instant Access Point)(SSID Profile <name># local-probe-req-thresh <threshold>
(Instant Access Point)(SSID Profile <name># max-clients-threshold <number-of-clients>
```

To manually assign VLANs for WLAN SSID users:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name># vlan <vlan-ID>
```

To enforce DHCP-based VLAN assignment:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name># enforce-dhcp
```

To create a new VLAN assignment rule:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals| starts-wi
th| ends-with| contains|matches-regular-expression} <operator> <VLAN-ID>| value-of}
```

Configuring Wired Profile for Guest Access

You can configure wired settings for a wired profile by using the Instant UI or CLI.

In the Instant UI

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks**. The **New Wired Network** window appears.
3. Click the **Wired Settings** tab and enter the following information:
   a. **Name**– Specify a name for the profile.
   b. **Primary Usage** – Select **Employee** or **Guest**.
   c. **Speed/Duplex** – Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.
   d. **POE** – Set **POE** to **Enabled** to enable Power over Ethernet.
   e. **Admin Status** – Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down.
   f. **Content Filtering**– To ensure that all DNS requests to non-corporate domains on this wired network are sent to OpenDNS, select **Enabled** for **Content Filtering**.

   g. **Uplink** – Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see Assigning a Profile to Ethernet Ports on page 113.

4. Click **Next**. The VLAN tab details are displayed.
5. Enter the following information.
   a. **Mode** – You can specify any of the following modes:
      - **Access** – Select this mode to allow the port to carry a single VLAN specified as the native VLAN.
      - **Trunk** – Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.

   b. Specify any of the following values for **Client IP Assignment**:
      - **Virtual Controller Assigned**: Select this option to allow the Virtual Controller to assign IP addresses to the wired clients. When the Virtual Controller assignment is used, the source IP address is translated for all client traffic that goes through this interface. The Virtual Controller can also assign a guest VLAN to a wired client.
      - **Network Assigned**: Select this option to allow the clients to receive an IP address from the network to which the Virtual Controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.

   c. If the **Trunk** mode is selected:
      - Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges 1,2,5 or 1-4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
      - If **Client IP Assignment** is set the **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1-4093.

   d. If the **Access** mode is selected:
      - If the **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 2.
      - If the **Client IP Assignment** is set the **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.

6. Click **Next** to configure internal or external Captive portal authentication, roles and access rules for the guest users.

In the CLI

To configure wired settings for:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# type <guest>
(Instant Access Point)(wired ap profile <name>)# speed {10 |100 |1000 |auto}
(Instant Access Point)(wired ap profile <name>)# duplex {<half>|<full>|<auto>}
(Instant Access Point)(wired ap profile <name>)# no shutdown
(Instant Access Point)(wired ap profile <name>)# poe
(Instant Access Point)(wired ap profile <name>)# uplink-enable
(Instant Access Point)(wired ap profile <name>)# content-filtering
```

To configure VLAN settings for a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# switchport-mode {<trunk> | <access>}
(Instant Access Point)(wired ap profile <name>)# allowed-vlan <vlan>
(Instant Access Point)(wired ap profile <name>)# native-vlan {<guest|1…4095>}
```

To configure a new VLAN assignment rule:

```
(Instant Access Point)(config)# wired-port-profile <name>
```

```
(Instant Access Point)(wired ap profile <name>)# set-vlan <attribute>{equals| not-equals| star
ts-with| ends-with| contains| matches-regular-expression} <operator> <VLAN-ID>| value-of}
```

Configuring Internal Captive Portal for Guest Network

In the Internal Captive Portal type, an internal server is used for hosting the Captive portal service. You can configure internal Captive portal authentication when adding or editing a guest network created for wireless or wired profile through the Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard or Wired window.
   - To configure internal captive portal authentication for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure internal captive portal authentication for a wired profile, **More**>**Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Security** tab and assign values for the configuration parameters:

Table 20: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Splash page type	Select any of the following from the drop-down list. ● **Internal - Authenticated**–When **Internal Authenticated** is enabled, the guest users are required to authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database. ● **Internal - Acknowledged**– When **Internal Acknowledged** is enabled, the guest users are required to accept the terms and conditions to access the Internet.
MAC authentication	Select **Enabled** from the drop-down list to enable the MAC authentication.
WISPr (Applicable for WLAN SSIDs only.)	Select **Enabled** if you want to enable WISPr authentication. For more information on WISPr authentication, see Configuring WISPr Authentication on page 161. **NOTE:** The WISPr authentication is applicable only for Internal-Authenticated splash pages and is not applicable for wired profiles.
Auth server 1 **Auth server 2**	Select any one of the following: ● A server from the list of servers if the server is already configured. ● **Internal Server** to authenticate user credentials at run time. ● Select **New** for configuring an new external RADIUS server for authentication.
Load balancing	Select **Enabled** to enable load balancing if two authentication servers are used.
Reauth interval	Select a value to allow the APs to periodically reauthenticate all associated and authenticated clients.
Blacklisting (Applicable for WLAN SSIDs only.)	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.

Parameter	Description
Accounting mode (Applicable for WLAN SSIDs only.)	Select an accounting mode from **Accounting mode** for posting accounting information at the specified **Accounting interval**. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.
Disable if uplink type is	To exclude uplink, select an uplink type.
Encryption (Applicable for WLAN SSIDs only.)	Select **Enabled** to configure encryption parameters.
Splash Page Design	Under **Splash Page Visuals**, use the editor to specify text and colors for the initial page that will be displayed to the users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal -Acknowledged) for which you are customizing the splash page design. Perform the following steps to customize splash page design. ● To change the color of the splash page, click the Splash page rectangle and select the required color from the **Background Color** palette. ● To change the welcome text, click the first square box in the splash page, type the required text in the **Welcome** text box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. ● 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**. Ensure that the policy text does not exceed 255 characters. ● To upload a custom logo, click **Upload your own custom logo Image**, browse the image file, and click **upload image**. ● To redirect users to another URL, specify a URL in **Redirect URL**. ● Click **Preview** to preview the Captive Portal page. **NOTE:** You can customize the captive portal page using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters. Click on the banner, term, or policy in the **Splash Page Visuals** to modify the text in the red box. These fields accept double-byte characters or a combination of English and double-byte characters.

3. Click **Next** to configure access rules.

In the CLI

To configure internal captive portal authentication:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# essid <ESSID-name>
(Instant Access Point)(SSID Profile <name>)# type <Guest>
(Instant Access Point)(SSID Profile <name>)# captive-portal <internal-authenticated> exclude-u
plink {3G|4G|Wifi|Ethernet}
(Instant Access Point)(SSID Profile <name>)# mac-authentication
(Instant Access Point)(SSID Profile <name>)# auth-server <server1>
(Instant Access Point)(SSID Profile <name>)# radius-reauth-interval <Minutes>
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure internal captive portal for a wired profile:

```
(Instant Access Point) (config)# wired-port-profile <name>
(Instant Access Point) (wired ap profile "<name>")# type <guest>
(Instant Access Point) (wired ap profile "<name>")# captive-portal {<internal-authenticated>|
<internal-acknowledged>} exclude-uplink {3G|4G|Wifi|Ethernet}
(Instant Access Point) (wired ap profile "<name>")# mac-authentication
```

```
(Instant Access Point) (wired ap profile "<name>")# auth-server <server1>
(Instant Access Point) (wired ap profile "<name>")# radius-reauth-interval <Minutes>
(Instant Access Point) (wired ap profile "<name>")# end
(Instant Access Point)# commit apply
```

To customize internal captive portal splash page:

```
(Instant Access Point)(config)# wlan captive-portal
(Instant Access Point)(Captive Portal)# authenticated
(Instant Access Point)(Captive Portal)# background-color <color-indicator>
(Instant Access Point)(Captive Portal)# banner-color <color-indicator>
(Instant Access Point)(Captive Portal)# banner-text <text>
(Instant Access Point)(Captive Portal)# decoded-texts <text>
(Instant Access Point)(Captive Portal)# redirect-url <url>
(Instant Access Point)(Captive Portal)# terms-of-use <text>
(Instant Access Point)(Captive Portal)# use-policy <text>
(Instant Access Point)(Captive Portal)# end
(Instant Access Point)# commit apply
```

To upload a customized logo to the internal Captive portal server:

```
(Instant Access Point)# copy config tftp <ip-address> <filename> portal logo
```

Configuring External Captive Portal for a Guest Network

This section provides the following information:

- External Captive Portal Profiles on page 123
- Creating a Captive Portal Profile on page 123
- Configuring an SSID or Wired Profile to Use External Captive Portal Authentication on page 125

External Captive Portal Profiles

You can now configure external Captive portal profiles and associate these profiles to a user role or SSID. You can create a set of Captive portal profiles in the **Security>External Captive Portal** window and associate these profiles with an SSID or a wired profile. You can also create a new Captive portal profile under the **Security** tab of the WLAN wizard or a Wired Network window. In the current release, you can configure up to eight external Captive portal profiles.

When the Captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a Captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the Captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the Captive portal unless explicitly permitted.

Creating a Captive Portal Profile

You can create a Captive portal profile using the Instant UI or CLI.

In the Instant UI

1. Click **Security**>**External Captive Portal**.
2. Click **New**. The **New** pop-up window is displayed.
3. Specify values for the following parameters:

Table 21: *Captive Portal Profile Configuration Parameters*

Parameter	Description
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: ● **Radius Authentication** - Select this option to enable user authentication against a RADIUS server. ● **Authentication Text** - Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or hostname	Enter the IP address or the hostname of the external splash page server.
URL	Enter the URL for the external Captive portal server.
Port	Enter the number of the port to use for communicating with the external Captive portal server.
Use https (Available only if RADIUS Authentication is selected)	Select **Enabled** to enforce clients to use HTTPS to communicate with the Captive portal server.
Captive Portal failure	This field allows you to configure Internet access for the guest clients when the external captive portal server is not available. Select **Deny Internet** to prevent clients from using the network, or **Allow Internet** to allow the guest clients to access Internet when the external Captive portal server is not available.
Automatic URL Whitelisting	Select **Enabled** or **Disabled** to enable or disable automatic whitelisting of URLs. On selecting the check box for the external Captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted. In the current release, the automatic URL whitelisting is disabled by default.
Auth Text (Available only if Authentication Text is selected)	If the External Authentication splash page is selected, specify the authentication text that must be returned by the external server after successful authentication.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

In the CLI

To configure an external Captive Portal profile:

```
(Instant Access Point)(config)# wlan external-captive-portal [profile_name]
(Instant Access Point)(External Captive Portal)# server <server>
(Instant Access Point)(External Captive Portal)# port <port>
(Instant Access Point)(External Captive Portal)# url <url>
(Instant Access Point)(External Captive Portal)# https
(Instant Access Point)(External Captive Portal)# redirect-url <url>
(Instant Access Point)(External Captive Portal)# server-fail-through
(Instant Access Point)(External Captive Portal)# no auto-whitelist-disable
(Instant Access Point)(External Captive Portal)# end
(Instant Access Point)# commit apply
```

Configuring an SSID or Wired Profile to Use External Captive Portal Authentication

You can configure external captive portal authentication for a network profile when adding or editing a guest network using Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard or Wired window.

- To configure external Captive portal authentication for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
- To configure external Captive portal authentication for a wired profile, **More**>**Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.

2. In the **Security** tab, select **External** from the **Splash page type** drop-down.
3. From the Captive portal profile drop-down, select a profile. You can select a default profile, or an already existing profile, or click **New** and create a new profile.
4. Configure the following parameters based on the type of splash page you selected.

Table 22: *External Captive Portal Configuration Parameters*

Parameter	Description
WISPr	Select **Enabled** if you want to enable WISPr authentication. For more information on WISPr authentication, see Configuring WISPr Authentication on page 161. **NOTE:** The WISPr authentication is applicable only for the External - RADIUS Server and Internal-Authenticated splash pages and is not applicable for wired profiles.
MAC authentication	Select **Enabled** if you want to enable MAC authentication. For information on MAC authentication, see Configuring MAC Authentication for a Network Profile on page 157.
Authentication server	To configure Authentication server, select any of the following options: ● If the server is already configured, select the server from the list. ● To create new external RADIUS server, select **New**. For more information, see Configuring an External Server for Authentication on page 149.
Reauth interval	Specify a value for reauthentication interval at which the APs periodically reauthenticate all associated and authenticated clients.
Accounting mode	Select an accounting mode from **Accounting mode** for posting accounting information at the specified **Accounting interval**. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.
Blacklisting	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
Max authentication failures	If you are configuring a wireless network profile and the **Blacklisting** is enabled, specify a maximum number of authentication failures after which users who fail to authenticate must be dynamically blacklisted.
Walled garden	Click the link to open the **Walled Garden** window. The walled garden configuration determines access to the Websites. For more information, see Configuring Walled Garden Access on page 131.
Disable if uplink type	Select the type of the uplink to exclude.

Table 22: *External Captive Portal Configuration Parameters*

Parameter	Description
is	
Encryption	Select Enabled to configure encryption settings and specify the encryption parameters.

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

In the CLI

To configure security settings for guest users of the WLAN SSID profile:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# essid <ESSID-name>
(Instant Access Point)(SSID Profile <name>)# type <Guest>
(Instant Access Point)(SSID Profile <name>)# captive-portal <type> external [profile]
[exclude-uplink <uplink-type>]
(Instant Access Point)(SSID Profile <name>)# blacklist
(Instant Access Point)(SSID Profile <name>)# mac-authentication
(Instant Access Point)(SSID Profile <name>)# max-authentication-failures <number>
(Instant Access Point)(SSID Profile <name>)# auth-server <server-name>
(Instant Access Point (SSID Profile <name>)# radius-accounting
(Instant Access Point (SSID Profile <name>)# radius-interim-accounting-interval
(Instant Access Point (SSID Profile <name>)# radius-accounting-mode {user-association|user-
authentication}
(Instant Access Point)(SSID Profile <name>)# wpa-passphrase <WPA_key>
(Instant Access Point)(SSID Profile <name>)# wep-key <WEP-key> <WEP-index>
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring External Captive Portal Authentication Using ClearPass Guest

You can configure Instant to point to ClearPass Guest as an external Captive Portal server. With this configuration, the user authentication is performed by matching a string in the server response and RADIUS server (either ClearPass Guest or a different RADIUS server).

Creating a Web Login page in the ClearPass Guest

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

For information on setting up the RADIUS Web Login feature, see the *RADIUS Services* section in the **ClearPass Guest Deployment Guide**.

Configuring the RADIUS Server in Instant

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

1. Select the WLAN SSID for which you want to enable external Captive portal authentication with CPPM. You can also configure RADIUS server when configuring a new SSID profile.
2. In the **Security** tab, select **External** from the Splash page type.
3. Select **New** the **Captive portal profile** drop-down and update the following fields:

   a. Enter the IP address of the ClearPass Guest server in the **IP or hostname** field. Obtain the ClearPass Guest IP address from your system administrator.
   b. Enter **/page_name.php** in the **URL** field. This URL must correspond to the **Page Name** configured in the ClearPass Guest RADIUS Web Login page. For example, if the Page Name is **Aruba**, the URL should be **/Aruba.php** in the Instant UI.
   c. Enter the **Port** number (generally should be **80**). The ClearPass Guest server uses this port for HTTP services.
   d. Click **OK**.
4. To create an external RADIUS server, select **New** from the **Authentication server 1** drop-down list. For information on RADIUS server configuration parameters, see Configuring an External Server for Authentication on page 149.
5. Click **Next** and then click **Finish**.
6. Click the updated SSID in Network tab.
7. Open any browser and type any URL. Instant redirects the URL to ClearPass Guest login page.
8. Log in to the network with the username and password specified used while configuring the RADIUS server.

Configuring Guest Logon Role and Access Rules for Guest Users

You can configure up to 64 access rules for guest network using the Instant UI or CLI.

In the Instant UI

To configure access rules for guest network:

1. In the **Access Rules** tab, set slider to any of the following types of access control:
   - **Unrestricted**– Select this to set unrestricted access to the network.
   - **Network-based**– Set the slider to **Network-based** to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule:

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

   - **Role-based**– Select **Role-based** to enable access based on user roles. For role-based access control:
     - Create a user role if required. For more information, see Configuring User Roles.
     - Create access rules for a specific user role. For more information, see Configuring Access Rules on page 173. You can also configure an access rule to enforce Captive portal authentication for an SSID that is configured to use 802.1X authentication method. For more information, see Configuring Captive Portal Roles for an SSID on page 128.
     - Create a role assignment rule. For more information, see Configuring Derivation Rules on page 182. Instant supports role derivation based on DHCP option for Captive Portal authentication. When the Captive Portal authentication is successful, a new user role is assigned to the guest users based on DHCP option configured for the SSID profile, instead of the pre-authenticated role.
2. Click **Finish**.

In the CLI

To configure access control rules for a WLAN SSID:

```
(Instant Access Point)(config)# wlan access-rule <name>
```

```
(Instant Access Point)(Access Rule <name>)# rule <dest> <mask> <match> <protocol> <start-port>
<end-port> {permit |deny | src-nat | dst-nat {<IP-address> <port> | <port>}}[<option1…option
9>]
(Instant Access Point)(Access Rule <name>)# end
(Instant Access Point)# commit apply
```

To configure access control based on the SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role-by-ssid
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure role assignment rules:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-wit
h|ends-with|contains|matches-regular-expression}<operator><role>|value-of}
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure a pre-authentication role:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role-pre-auth <pre-authentication-role>
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure machine and user authentication roles

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role-machine-auth <machine-authentication-onl
y> <user-authentication-only>
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure unrestricted access:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role-unrestricted
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring Captive Portal Roles for an SSID

You can configure an access rule to enforce Captive portal authentication for SSIDs with 802.1X authentication enabled. You can configure rules to provide access to external Captive portal, internal Captive portal, or none, so that some of the clients using this SSID can derive the Captive portal role.

The following conditions apply to the 802.1X and Captive portal authentication configuration:

- If a user role does not have Captive Portal settings configured, the Captive portal settings configured for an SSID are applied to the client's profile.
- If the SSID does not have Captive Portal settings configured, the Captive portal settings configured for a user role are applied to the client's profile.
- If Captive portal settings are configured for both SSID and user role, the Captive portal settings configured for a user role are applied to the client's profile.

You can create a Captive portal role for both **Internal-acknowledged** and **External Authentication Text** splash page types.

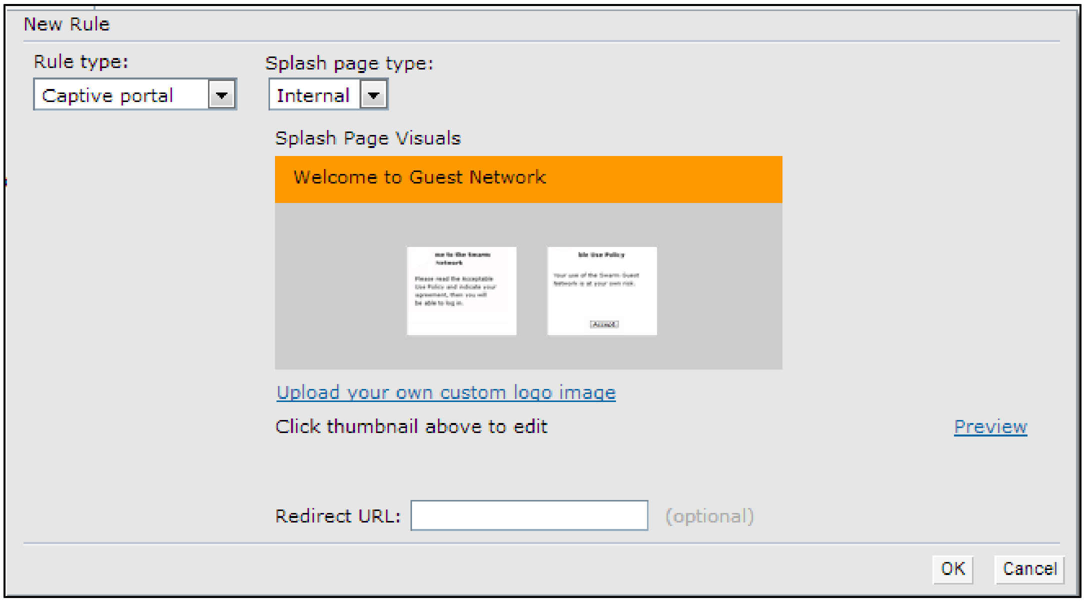
To enforce Captive Portal role, use the Instant UI or CLI.

In the Instant UI

To create a Captive portal role:

1. Select an SSID profile from the **Networks** tab. The **Edit <WLAN-Profile>** window is displayed.
2. In the **Access** tab, slide to **Role-based** access control by using the scroll bar.
3. Select a role or create a new if required.
4. Click **New** to add a new rule. The **New Rule** window is displayed.
5. In the **New Rule** window, specify the following parameters. The following figures show the parameters for Captive Portal role configuration:

Figure 40 *Captive Portal Rule for Internal Acknowledged Splash Page*



New Rule

Rule type: Captive portal

Splash page type: Internal

Splash Page Visuals

Welcome to Guest Network

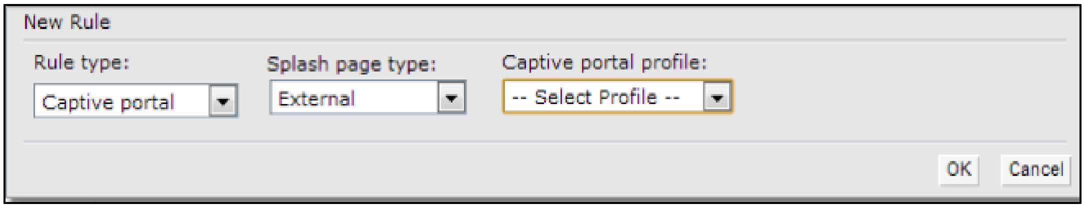
Upload your own custom logo image

Click thumbnail above to edit

Preview

Redirect URL: (optional)

Figure 41 *Captive Portal Rule for External Captive portal profile*



New Rule

Rule type: Captive portal

Splash page type: External

Captive portal profile: -- Select Profile --

Table 23: *New Access Rule Configuration Parameters*

Field	Description
Rule type	Select **Captive Portal** from the drop-down list.
Splash Page Type	Select any of following attributes: ● Select **Internal** to configure a rule for internal captive portal authentication. ● Select **External** to configure a rule for external captive portal authentication.
Internal	If **Internal** is selected as splash page type, perform the following steps: ● Under **Splash Page Visuals**, use the editor to specify text and colors for the initial

Field	Description
	page that would be displayed to users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type configured - To change the color of the splash page, click the Splash page rectangle and select the required color from the **Background Color** palette. - To change the welcome text, click the first square box in the splash page, type the required text in the **Welcome** text box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. - 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**. Ensure that the policy text does not exceed 255 characters. - Specify the URL, to which you want redirect the guest users. - To upload a custom logo, click **Upload your own custom logo Image**, browse the image file, and click **upload image**. - Click **Preview** to preview the Captive Portal page.
External	If **External** is selected, perform the following steps: - Select a profile from the **Captive portal profile** drop-down. - If you want to edit the profile, click **Edit** and update the following parameters: - **Type**–Select either **Radius Authentication** (to enable user authentication against a RADIUS server) or **Authentication Text** (to specify the authentication text to returned by the external server after a successful user authentication). - **IP or hostname**– Enter the IP address or the hostname of the external splash page server. - **URL**– Enter the URL for the external splash page server. - **Port**–Enter the number of the port to use for communicating with the external splash page server - **Redirect URL**–Specify a redirect URL if you want to redirect the users to another URL. - **Captive Portal failure**–This field allows you to configure Internet access for the guest clients when the external captive portal server is not available. Select **Deny Internet** to prevent clients from using the network, or **Allow Internet** to allow the guest clients to access Internet when the external Captive portal server is not available. - **Automatic URL Whitelisting**– Select **Enabled** or **Disabled** to enable or disable automatic whitelisting of URLs. selecting the check box for the external Captive portal authentication, the URLs allowed for the unauthenticated users to access are automatically whitelisted. The automatic URL whitelisting is disabled by default. - **Auth Text**–Indicates the authentication text returned by the external server after a successful user authentication.

6. Click **OK**. The enforce captive portal rule is created and listed as an access rule.
7. Create a role assignment rule based on the user role, to which the Captive portal access rule is assigned.
8. Click **Finish**.

The client can connect to this SSID after authenticating with username and password. After a successful user login, the Captive portal role is assigned to the client.

In the CLI

To create a Captive portal role:

```
(Instant Access Point)(config)# wlan access-rule <Name>
(Instant Access Point)(Access Rule <Name>)# captive-portal {external [profile <name>]|interna
l}
```

```
(Instant Access Point)(Access Rule <Name>)# end
(Instant Access Point)# commit apply
```

Configuring Walled Garden Access

On the Internet, a walled garden typically controls access to web content and services. The Walled garden access is required when an external Captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

The users who do not sign up for the Internet service can view the “allowed” Websites (typically hotel property Websites). The Website names must be DNS-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, which are not in the whitelist of the walled garden profile, the user is redirected to the login page. In addition, a blacklisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some Websites.

You can create a walled garden access in Instant UI or CLI.

In the Instant UI

To create a Walled Garden access:

1. Click the **Security** link at the top right corner of the Instant main window and click **Walled Garden**. The Walled Garden tab contents are displayed.
2. To allow users to access a specific domain, click **New** and enter the domain name or URL in the **Whitelist** section of the window. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)). For example:
   - yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
   - www.apple.com/library/test is a subset of www.apple.com site corresponding to path /library/test/*
   - favicon.ico allows access to /favicon.ico from all domains.
3. To deny users access to a domain, click **New** and enter the domain name or URL in the **Blacklist** section of the window. This prevents the unauthenticated users from viewing specific Websites. When a URL specified in the blacklist is accessed by an unauthenticated user, IAP sends an HTTP 403 response to the client with a simple error message.

   If the requested URL neither appears on the blacklist or whitelist list, the request is redirected to the external Captive portal.
4. Select the domain name/URL and click **Edit** to modify or **Delete** to remove the entry from the list.
5. Click **OK** to apply the changes.

In the CLI

To create a Walled Garden access:

```
(Instant Access Point)(config)# wlan walled-garden
(Instant Access Point)(Walled Garden)# white-list <domain>
(Instant Access Point)(Walled Garden)# black-list <domain>
(Instant Access Point)(Walled Garden)# end
(Instant Access Point)# commit apply
```

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

1. Select an existing wireless or wired profile. Depending on the network profile selected, the **Edit <WLAN-Profile>** or **Edit Wired Network** window is displayed.

NOTE

You can also customize splash page design in the **Security** tab of **New WLAN** and **New Wired Network** windows when configuring a new profile.

2. Navigate to the **Security** tab.
3. Select **None** from the **Splash page type** drop-down list.
4. Click **Next** and then click **Finish** to apply the changes.

This chapter provides the following information:

IAP Users

The IAP users can classified as follows:

- Administrator– An admin user who creates SSIDs, wired profiles, DHCP server configuration parameters, and manages local user database. The admin users can access to the Virtual Controller Management User Interface.
- Guest administrator– A guest interface management user who manages guest users added in the local user database.
- Administrator with read-only access– The read-only admin user does not have access to the Instant CLI. The Instant UI will be displayed in the read-only mode for these users.
- Employee users – Employees who use the enterprise network for official tasks.
- Guest users–Visiting users who temporarily use the enterprise network to access the Internet.

The user access privileges are determined by IAP management settings in the AirWave Management client and Aruba Central, and the type of the user. The following table outlines the access privileges defined for the admin user, guest management interface admin, and read-only users.

Table 24: *User Privileges*

User Category	Aruba Central or AirWave Management Platform in Management Mode	IAP in monitor mode or without AirWave Management Platform or Aruba Central
administrator	Access to local user database only	Complete access to the IAP
read-only administrator	No write privileges	No write privileges
guest administrator	Access to local user database only	Access to local user database only

Configuring Administrator Credentials for the Virtual Controller Interface

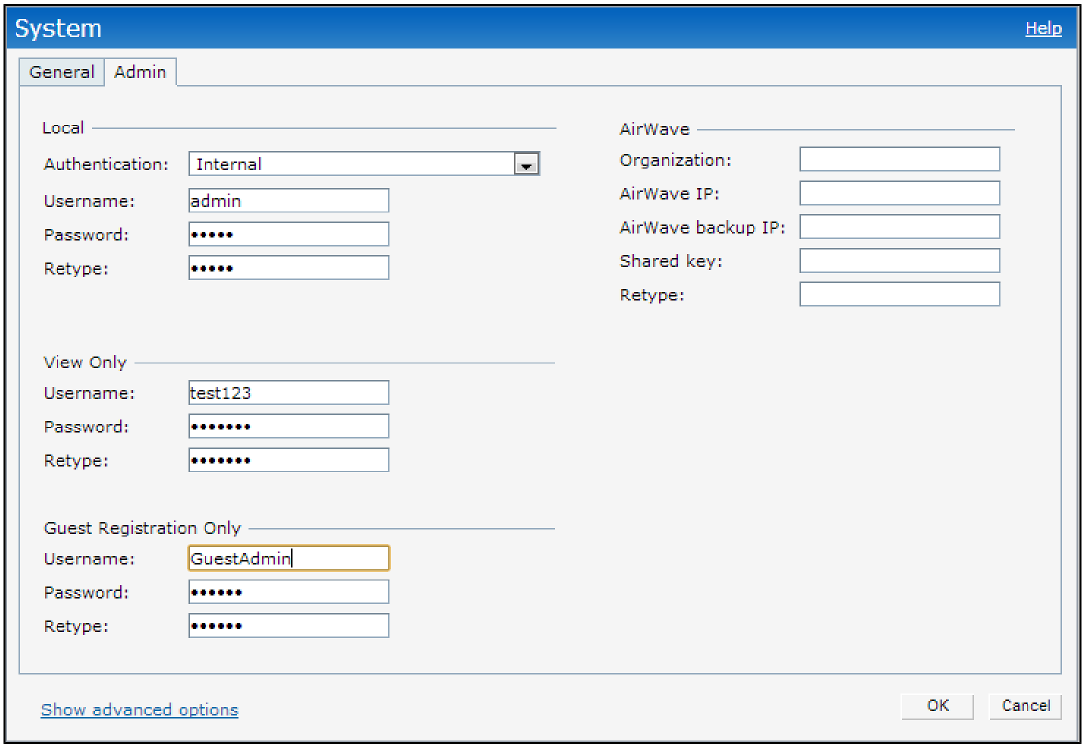
You can configure authentication parameters for admin users to enable access to the Virtual Controller management user interface in the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at top right corner of the Instant main window. The **System** window appears.

2. Click the **Admin** tab. The **Admin** tab details are displayed. The following figure shows the contents of the **Admin** tab:

Figure 42 *Admin Tab: Management Authentication Parameters*



Local

Authentication: Internal

Username: admin

Password: •••••

Retype: •••••

View Only

Username: test123

Password: •••••••

Retype: •••••••

Guest Registration Only

Username: GuestAdmin

Password: ••••••

Retype: ••••••

AirWave

Organization:

AirWave IP:

AirWave backup IP:

Shared key:

Retype:

3. Under Local, select any of the following options from the **Authentication** drop-down list:

- **Internal**– Select this option to specify a single set of user credentials. Enter the **Username** and **Password** for accessing the Virtual Controller Management User Interface.
  a. Specify a **Username** and **Password**.
  b. Retype the password to confirm.
- **RADIUS Server**– Specify one or two RADIUS servers to authenticate clients. If two servers are configured, users can use them in primary or backup mode or load balancing mode. To enable load balancing, select **Enabled** from the **Load balancing** drop-down list.
- **RADIUS server w/ fallback to internal**– Select this option to use both internal and external servers. When enabled, the authentication switches to **Internal** if there is no response from the RADIUS server (RADIUS server timeout). To complete this configuration, perform the following steps:
  a. To enable load balancing, select **Enabled** from the **Load balancing** drop-down list.

4. Click **OK**.

In the CLI

To configure an admin user:

```
(Instant Access Point)(config)# mgmt-user <username> <password>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To configure RADIUS authentication parameters:

```
(Instant Access Point)(config)# mgmt-auth-server <authentication_server1>
(Instant Access Point)(config)# mgmt-auth-server <authentication_server2>
(Instant Access Point)(config)# mgmt-auth-server-load-balancing
(Instant Access Point)(config)# mgmt-auth-server-local-backup
(Instant Access Point)(config)# end
```

```
(Instant Access Point)# commit apply
```

Configuring Guest Management Interface Administrator Credentials

You can configure guest administrator credentials in the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at top right corner of the Instant main window. The **System** window appears.
2. Click the **Admin** tab. The **Admin** tab details are displayed.
3. Under **Guest Registration Only**:
   a. Specify a **Username** and **Password**.
   b. Retype the password to confirm.
4. Click **OK**. When the guest management administrator logs in with these credentials, the guest management interface is displayed.

In the CLI

To configure guest management administrator credentials:

```
(Instant Access Point)(config)# mgmt-user <username> [password] guest-mgmt
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Configuring Users for Internal Database of an IAP

The Instant user database consists of a list of guest and employee users. Addition of a user involves specifying a login credentials for a user. The login credentials for these users are provided outside the Instant system.

A guest user can be a visitor who is temporarily using the enterprise network to access the Internet. However, if you do not want to allow access to the internal network and the Intranet, you can segregate the guest traffic from the enterprise traffic by creating a guest WLAN and specifying the required authentication, encryption, and access rules.

An employee user is the employee who is using the enterprise network for official tasks. You can create Employee WLANs, specify the required authentication, encryption and access rules and allow the employees to use the enterprise network.

NOTE

The user database is also used when an IAP is configured as an internal RADIUS server.

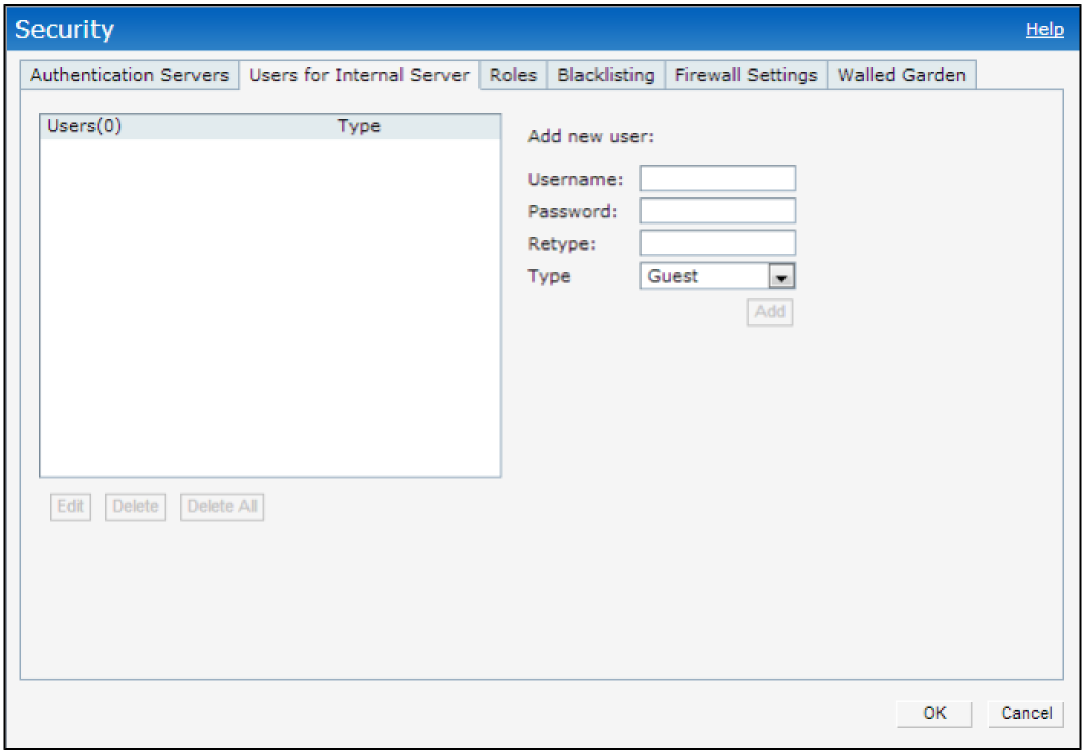
The local user database of APs can support up to 512 user entries except IAP-9x. IAP-9x supports only 256 user entries. If there are already 512 users, IAP-9x will not be able to join the cluster.

In the Instant UI

To configure users:

1. Click the **Security** at the top right corner of Instant main window.
2. Click **Users for Internal Server**. The following figure shows the contents of the **Users for Internal Server** tab.

Figure 43 *Adding a User*



3. Enter the username in the **Username** text box.
4. Enter the password in the **Password** text box and reconfirm.
5. Select a type of network from the **Type** drop-down list.
6. Click **Add** and click **OK.** The users are listed in the **Users** list.
7. To edit user settings:
   a. Select the user to modify under **Users**
   b. Click **Edit** to modify user settings.
   c. Click **OK.**
8. To delete a user:
   a. In the **Users** section, select the username to delete
   b. Click **Delete**.
   c. Click **OK.**
9. To delete all or multiple users at a time:
   a. Select the usernames that you want to delete
   b. Click **Delete All**.
   c. Click **OK.**

NOTE

Deleting a user only removes the user record from the user database, and will not disconnect the online user associated with the username.

In the CLI

To configure an employee user:

```
(Instant Access Point)(config)# user <username> <password> radius
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To configure a guest user:

```
(Instant Access Point)(config)# user  <username> <password> portal
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Configuring the Read-Only Administrator Credentials

You can assign the read-only privilege to an admin user by using the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at top right corner of the Instant main window. The **System** window appears.
2. Click the **Admin** tab. The **Admin** tab details are displayed.
3. Under **View Only**:
   a. Specify a **Username** and **Password**.
   b. Retype the password to confirm.
4. Click **OK**. When the users log in with these credentials, the Instant UI is displayed in the read-only mode.

In the CLI

To configure a user with read-only privilege:

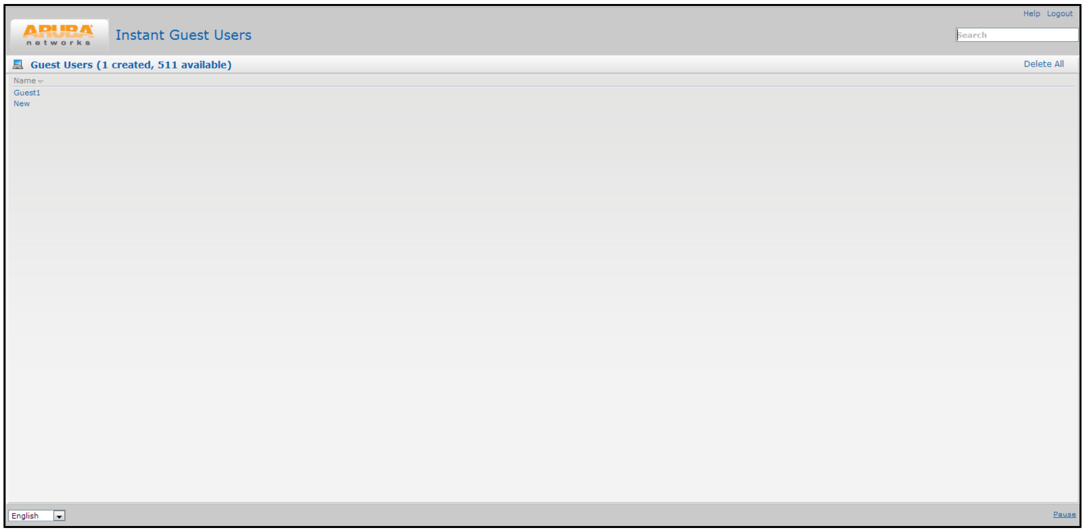
```
(Instant Access Point)(config)# mgmt-user <username> [password] read-only
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Adding Guest Users through the Guest Management Interface

To add guest users through the Guest Management interface:

1. Log in to Instant UI with the guest management interface administrator credentials. The guest management interface is displayed.

Figure 44 *Guest Management Interface*



Guest Users (1 created, 511 available)

Name

Guest1

New

2. To add a user, click **New**. The **New Guest User** pop-up window is displayed.
3. Specify a **Username** and **Password**.
4. Retype the password to confirm.
5. Click **OK**.

Chapter 11
Authentication

This chapter provides the following information:

Understanding Authentication Methods

Authentication is a process of identifying a user by through a valid username and password. Clients can also be authenticated based on their MAC addresses.

The following authentication methods are supported in Instant:

- **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. For more information on configuring an IAP to use 802.1X authentication, see Configuring 802.1X Authentication for a Network Profile on page 156.
- **MAC authentication** – Media Access Control (MAC) authentication is used for authenticating devices based on their physical MAC addresses. MAC authentication requires that the MAC address of a machine matches a manually defined list of addresses. This authentication method is not recommended for scalable networks and the networks that require stringent security settings. For more information on configuring an IAP to use MAC authentication, see Configuring MAC Authentication for a Network Profile on page 157.
- **MAC authentication with 802.1X authentication** –This authentication method has the following features:
  - MAC authentication precedes 802.1X authentication - The administrators can enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. If MAC authentication fails, 802.1X authentication does not trigger. If MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.
  - MAC authentication only role - Allows you to create a **mac-auth-only** role to allow role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client when the MAC authentication is successful and 802.1X authentication fails. If 802.1X authentication is

successful, the **mac-auth-only** role is overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.

  - L2 authentication fall-through - Allows you to enable the **l2-authentication-fallthrough** mode. When this option is enabled, the 802.1X authentication is allowed even if the MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-fallthrough** mode is disabled by default.

  For more information on configuring an IAP to use MAC + 802.1X Authentication, see Configuring MAC Authentication with 802.1X Authentication on page 159.

- **Captive Portal** – Captive portal authentication is used for authenticating guest users. For more information on Captive Portal authentication, see Captive Portal for Guest Access on page 115.
- **MAC authentication with Captive Portal authentication**–This authentication method has the following features:
  - If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
  - If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
  - If the captive portal splash page type is **none**, MAC authentication is disabled.
  - You can configure the **mac-auth-only** role when MAC authentication is enabled with captive portal authentication.

  For more information configuring an IAP to use MAC and Captive Portal authentication, see Configuring MAC Authentication with Captive Portal Authentication on page 160.

- **802.1X authentication with Captive Portal authentication** – This authentication mechanism allows you to configure different Captive portal settings for clients on the same SSID. For example, you can configure an 802.1x SSID and create a role with for captive portal access, so that some of the clients using the SSID derive the Captive portal role. You can configure rules to indicate access to external or internal Captive portal, or none. For more information on configuring Captive portal roles for an SSID with 802.1x authentication, see Configuring Captive Portal Roles for an SSID on page 128.
- **WISPr authentication**–Wireless Internet Service Provider roaming (WISPr) authentication allows a smart client to authenticate on the network when they roam between wireless Internet service providers, even if the wireless hotspot uses an Internet Service Provider (ISP) with whom the client may not have an account.

  If a hotspot is configured to use WISPr authentication in a specific ISP and a client attempts to access the Internet at that hotspot, the WISPr AAA server configured for the ISP authenticates the client directly and allows the client to access the network. If the client only has an account with a *partner* ISP, the WISPr AAA server forwards the client's credentials to the partner ISP's WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on your hotspot's own ISP as per their service agreements. The IAP assigns the default WISPr user role to the client when your ISP sends an authentication message to the IAP. For more information on WISPr authentication, see Configuring WISPr Authentication on page 161.

Supported Authentication Servers

Based on the security requirements, you can configure internal or external RADIUS servers. This section describes the following types of authentication servers and authentication termination, which can be configured for a network profile:

- External RADIUS Server on page 141
- Internal RADIUS Server on page 141
- Authentication Termination on IAP on page 142
- Supported VSAs on page 142

External RADIUS Server

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

When you enable an external RADIUS server for the network, the client on the IAP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

Instant supports the following external authentication servers:

- RADIUS (Remote Authentication Dial-In User Service)
- LDAP (Lightweight Directory Access Protocol)
- CPPM Server for AirGroup CoA

To use an LDAP server for user authentication, configure the LDAP server on the Virtual Controller, and configure user IDs and passwords.

To use a RADIUS server for user authentication, configure the RADIUS server on the Virtual Controller.

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.

For a complete list of VSAs supported by Instant, see Understanding VLAN Assignment on page 184.

Internal RADIUS Server

Each IAP has an instance of free RADIUS server operating locally. When you enable the Internal RADIUS server option for the network, the client 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 Instant network:

- EAP-TLS– The Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) 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 on the IAP. The client certificate is verified on the Virtual Controller (the client certificate must be signed by a known CA), before the username is verified 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)– EAP-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.

To use IAP’s internal database for user authentication, add the names and passwords of the users to be authenticated.

NOTE

Aruba does not recommend the use of LEAP authentication method, because it does not provide any resistance to network attacks.

Authentication Termination on IAP

Instant allows Extensible Authentication Protocol (EAP) termination for Protected Extensible Authentication Protocol (PEAP)-Generic Token Card (PEAP-GTC) and Protected Extensible Authentication Protocol-Microsoft Challenge Authentication Protocol version 2 (PEAP-MSCHAV2). PEAP-GTC termination allows authorization against an Lightweight Directory Access Protocol (LDAP) server and external RADIUS server while PEAP-MSCHAV2 allows authorization against an external RADIUS server.

This allows the users to run PEAP-GTC termination with their username and password to a local Microsoft Active Directory server with LDAP authentication.

- 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 to an external authentication server for user data backup.
- 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 back-end authentication server.

Supported VSAs

Instant supports the following VSAs for user role and VLAN derivation rules:

- 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-Interim-Interval
- 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-AP-Name
- Aruba-AS-Credential-Hash
- Aruba-AS-User-Name
- Aruba-Admin-Role
- Aruba-AirGroup-Device-Type
- Aruba-AirGroup-Shared-Role
- Aruba-AirGroup-Shared-User
- Aruba-AirGroup-User-Name
- Aruba-Auth-Survivability
- Aruba-CPPM-Role
- Aruba-Device-Type
- Aruba-Essid-Name
- Aruba-Framed-IPv6-Address
- Aruba-Location-Id
- Aruba-Mdps-Device-Iccid
- Aruba-Mdps-Device-Imei
- Aruba-Mdps-Device-Name
- Aruba-Mdps-Device-Product
- Aruba-Mdps-Device-Serial
- Aruba-Mdps-Device-Udid
- Aruba-Mdps-Device-Version
- Aruba-Mdps-Max-Devices
- Aruba-Mdps-Provisioning-Settings
- Aruba-Named-User-Vlan
- Aruba-No-DHCP-Fingerprint
- Aruba-Port-Id
- Aruba-Priv-Admin-User
- Aruba-Template-User
- Aruba-User-Role
- Aruba-User-Vlan
- Aruba-WorkSpace-App-Name
- Authentication-Sub-Type
- Authentication-Type
- CHAP-Challenge
- Callback-Id
- Callback-Number
- Chargeable-User-Identity
- 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-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- Framed-Interface-Id
- Framed-MTU
- Framed-Protocol
- Framed-Route
- Framed-Routing
- Full-Name
- Group
- Group-Name
- Hint
- Huntgroup-Name
- Idle-Timeout
- Location-Capable
- Location-Data
- Location-Information
- Login-IP-Host
- Login-IPv6-Host
- Login-LAT-Node
- Login-LAT-Port
- Login-LAT-Service
- Login-Service
- Login-TCP-Port
- Menu

- Message-Auth
- NAS-IPv6-Address
- NAS-Port-Type
- Operator-Name
- Password
- Password-Retry
- Port-Limit
- Prefix
- Prompt
- Rad-Authenticator
- Rad-Code
- Rad-Id
- Rad-Length
- Reply-Message
- Requested-Location-Info
- 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

Understanding Encryption Types

Encryption is the process of converting data into a cryptic format or code when it is transmitted on a network. Encryption prevents unauthorized use of the data.

Instant supports the following types of encryption:

- **WEP** –Wired Equivalent Privacy (WEP) is an authentication method where all users share the same key. WEP is not secure as other encryption types such as TKIP.
- **TKIP** –Temporal Key Integrity Protocol (TKIP) uses the same encryption algorithm as WEP. However, TKIP is more secure and has an additional message integrity check (MIC).
- **AES** – The Advanced Encryption Standard (AES) encryption algorithm a widely supported 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 like IP Security (IPsec) clients.

NOTE

WEP and TKIP are limited to WLAN connection speed of 54 Mbps. The 802.11n connection supports only AES encryption. Aruba recommends AES encryption. Ensure that all devices that do not support AES are upgraded or replaced with the devices that support AES encryption.

WPA and WPA2

WPA is created based on a draft of 802.11i, which allowed users to create more secure WLANs. WPA2 encompasses the full implementation of the 802.11i standard. WPA2 is a superset that encompasses the full WPA feature set.

The following table summarizes the differences between the two certifications:

Table 25: *WPA and WPA2 Features*

Certification	Authentication	Encryption
WPA	● PSK ● IEEE 802.1X with Extensible Authentication Protocol (EAP)	TKIP with message integrity check (MIC)
WPA2	● PSK ● IEEE 802.1X with EAP	AES -- Counter Mode with Cipher Block Chaining Message Authentication Code (AESCCMP)

WPA and WPA2 can be further classified as follows:

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

Recommended Authentication and Encryption Combinations

The following table summarizes the recommendations for authentication and encryption combinations for the Wi-Fi networks.

Table 26: *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 security settings assigned for a user role).

Understanding Authentication Survivability

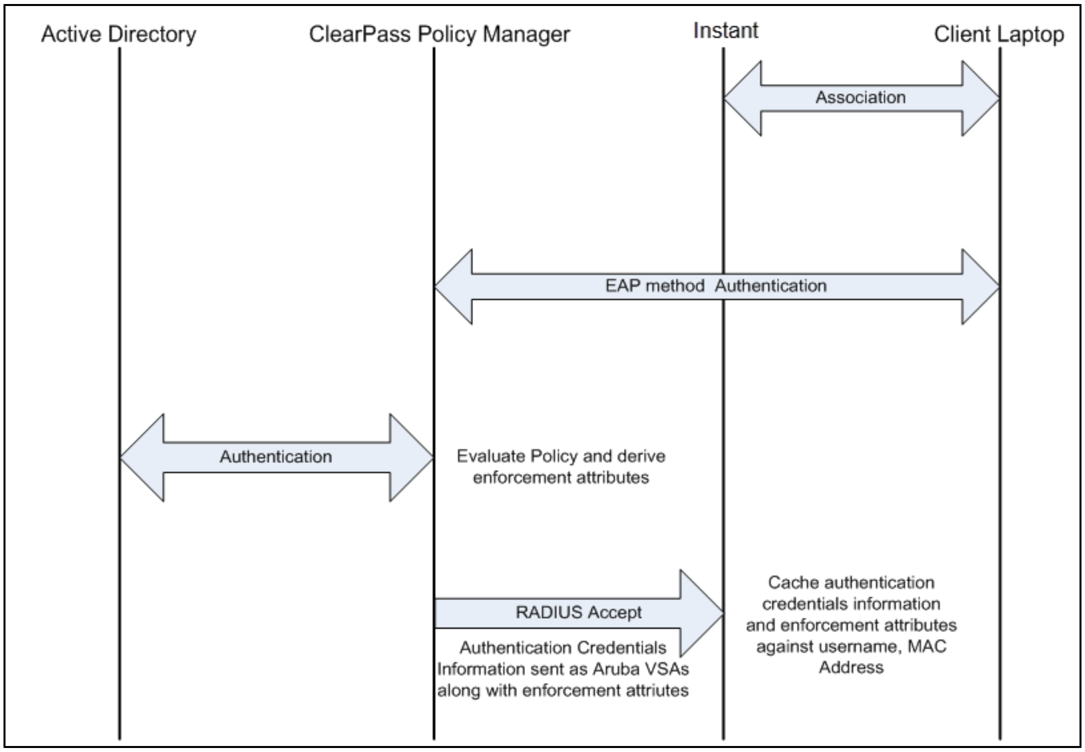
The authentication survivability feature supports authorization survivability against remote link failure for Mobility Controllers when working with ClearPass Policy Manager (CPPM).

When enabled, this feature allows Instant to authenticate the previously connected clients using EAP-PEAP authentication even when connectivity to CPPM is temporarily lost.

The following figure illustrates the scenario where the IAP offloads EAP method authentication to ClearPass over a remote link connection. After authenticating the user against Active Directory and deriving enforcement attributes for the user, the CPPM returns additional information in the RADIUS *Access-Accept* message, which the IAP caches to support authentication survivability.

As shown in the following figure, the information sent by the CPPM varies depending on the authentication method used.

Figure 45 *802.1X Authentication when CPPM is reachable*

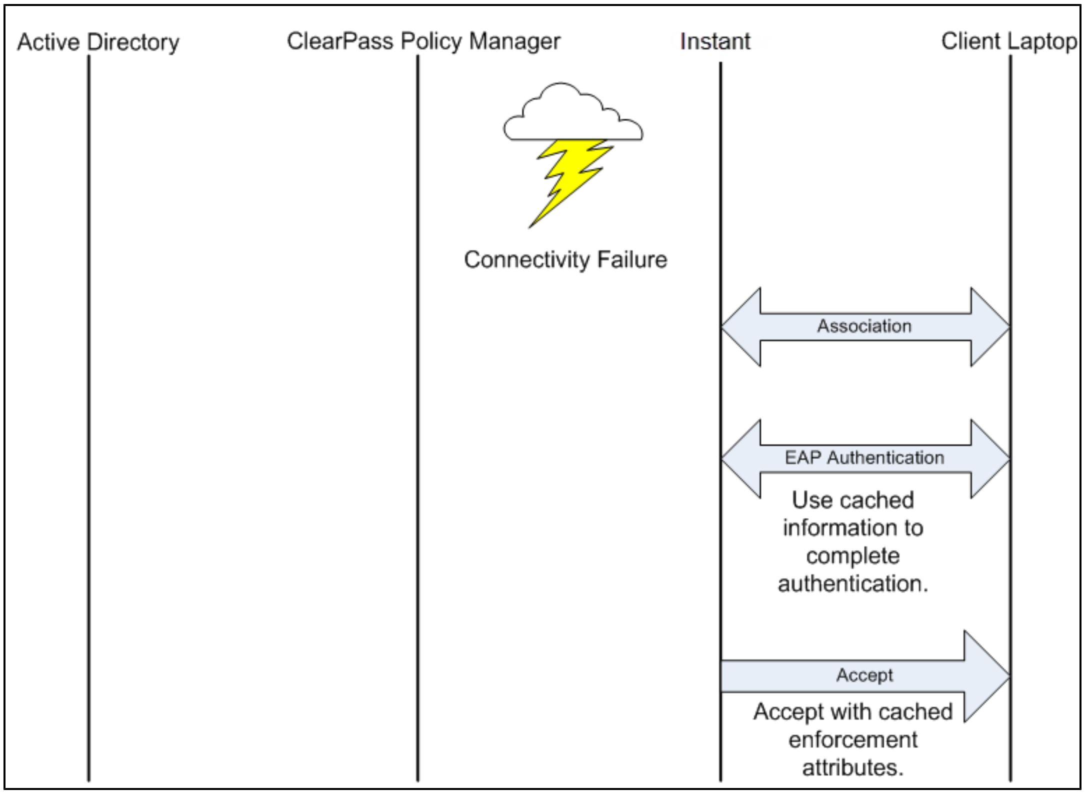

Active Directory
ClearPass Policy Manager
Instant
Client Laptop
Association
EAP method Authentication
Authentication
Evaluate Policy and derive enforcement attributes
RADIUS Accept
Authentication Credentials Information sent as Aruba VSAs along with enforcement attriutes
Cache authentication credentials information and enforcement attributes against username, MAC Address

The following figure illustrates a scenario where when the remote link is not available and the IAP is no longer able to reach the CPPM. Here, the IAP terminates and completes the EAP authentication using the cached credentials.

NOTE

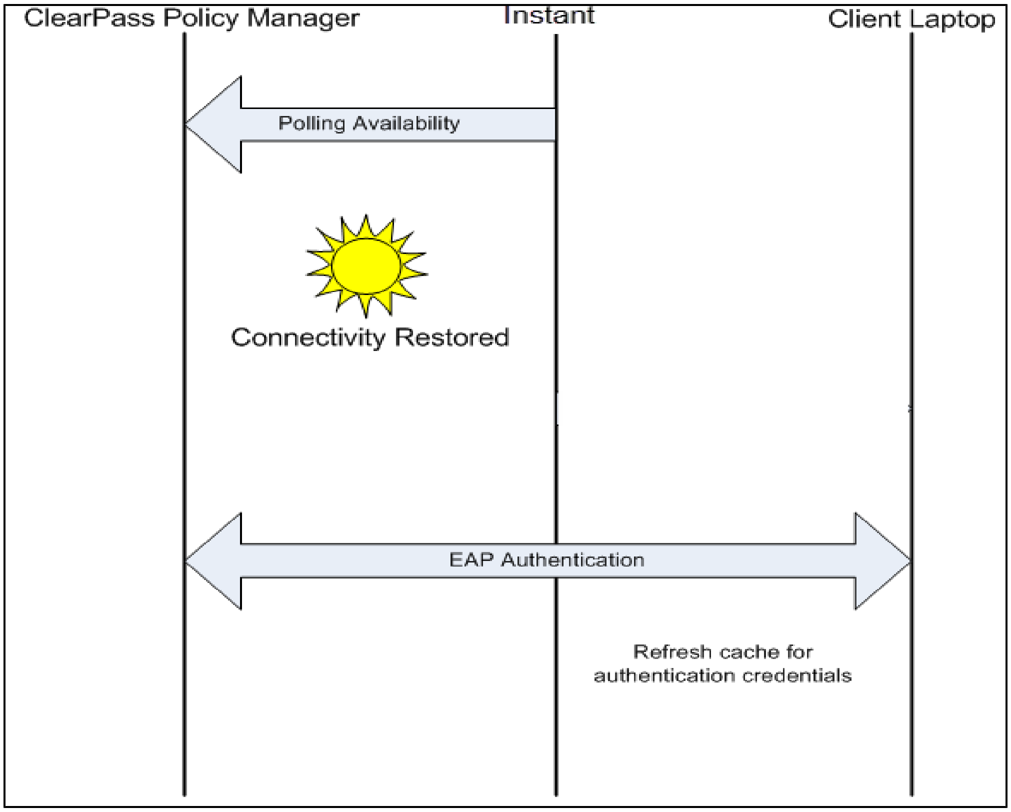
If both the IAP to which the client was associated and the CPPM are not available, the client will be not be able to reauthenticate until the CPPM server is available again.

Figure 46 *802.1X Authentication using cached credentials*



The following figure illustrates a scenario where the CPPM link is available again. The IAP sends the RADIUS-Request message to the CPPM server directly for client authentication.

Figure 47 *802.1X Authentication when CPPM is reachable again*



You can enable authentication survivability for a wireless network profile when configuring enterprise security parameters. For more information, see Configuring Security Settings for a WLAN SSID Profile on page 94.

Configuring Authentication Servers

This section describes the following procedures:

- Configuring an External Server for Authentication on page 149
- Configuring Dynamic RADIUS Proxy Parameters on page 152

Configuring an External Server for Authentication

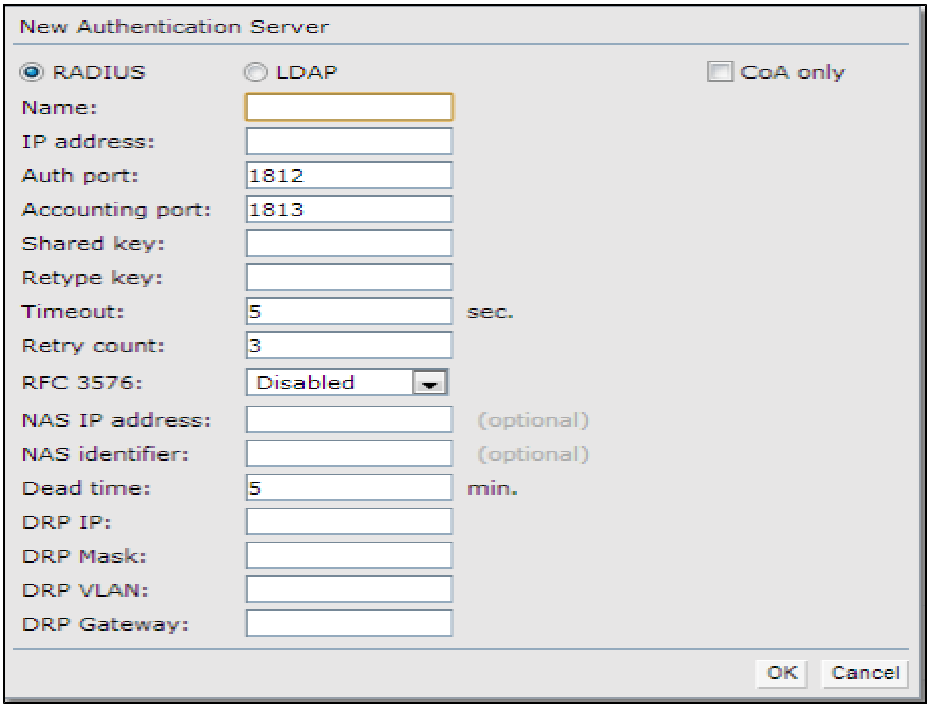
You can add an external RADIUS server, LDAP server, or CPPM server for AirGroup CoA by using the Instant UI or CLI.

In the Instant UI

To configure an authentication server:

1. Navigate to **Security**>**Authentication Servers**. The **Security** window is displayed.
2. To create a new server, click **New**. A window for specifying details for the new server is displayed. The following figure shows the parameters to configure for a new authentication server configuration:

Figure 48 *New Authentication Server Window*



New Authentication Server

● RADIUS ○ LDAP □ CoA only

Name:

IP address:

Auth port: 1812

Accounting port: 1813

Shared key:

Retype key:

Timeout: 5 sec.

Retry count: 3

RFC 3576: Disabled

NAS IP address: (optional)

NAS identifier: (optional)

Dead time: 5 min.

DRP IP:

DRP Mask:

DRP VLAN:

DRP Gateway:

3. Configure any of the following types of server:

- **RADIUS Server** – To configure a RADIUS server, specify the attributes described in the following table:

Table 27: *RADIUS Server Configuration Parameters*

Parameter	Description
Name	Enter the name of the new external RADIUS server.

Parameter	Description
IP address	Enter the IP address of the external RADIUS server.
Auth port	Enter the authorization port number of the external RADIUS server. The default port number is 1812.
Accounting port	Enter the accounting port number. This port is used for sending accounting records to the RADIUS server. The default port number is 1813.
Shared key	Enter a shared key for communicating with the external RADIUS server.
Retype key	Re-enter the shared key.
Timeout	Specify a timeout value in seconds. The value determines the timeout for one RADIUS request. The IAP retries to send the request several times (as configured in the **Retry count**), before the user gets disconnected. For example, if the **Timeout** is 5 seconds, **Retry counter** is 3, user is disconnected after 20 seconds. 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 the server group, and the default value is 3 requests.
RFC 3576	Select **Enabled** to allow the APs to 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 the CoA messages modify session authorization attributes such as data filters.
NAS IP address	Enter the Virtual Controller IP address. The NAS IP address is the Virtual Controller IP address that is sent in data packets. **NOTE:** If you do not enter the IP address, the Virtual Controller IP address is used by default when **Dynamic RADIUS Proxy** is enabled.
NAS identifier	Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
Dead Time	Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the IAP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.
Dynamic RADIUS proxy parameters	Specify the following dynamic RADIUS proxy parameters: ● **DRP IP**– IP address to be used as source IP for RADIUS packets ● **DRP Mask**–Subnet mask of the DRP IP address. ● **DRP VLAN**–VLAN in which the RADIUS packets are sent. ● **DRP Gateway**–Gateway IP address of the DRP VLAN. For more information on dynamic RADIUS proxy parameters and configuration procedure, see Configuring Dynamic RADIUS Proxy Parameters on page 152.

- **LDAP Server** –To configure an LDAP server, specify the attributes described in the following table:

Table 28: *LDAP Server Configuration Parameters*

Parameter	Description
Name	Enter the name of the LDAP server.
IP address	Enter the IP address of the LDAP server.
Auth port	Enter the authorization port number of the LDAP server. The default port number is 389.
Admin-DN	Enter a distinguished name for the admin user with read/search privileges across all the entries in the LDAP database (the user need not have write privileges, but the user must be able to search the database, and read attributes of other users in the database).
Admin password	Enter a password for administrator.
Base-DN	Enter a distinguished name for the node which contains the entire user database.
Filter	Specify the filter to apply when searching for a user in the LDAP database. The default filter string is **(objectclass=*)**.
Key Attribute	Specify the attribute to use as a key while searching 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.

- **CPPM Server** for AirGroup CoA – To configure a CPPM server used for AirGroup CoA (Change of Authorization), select the **CoA only** check box. The RADIUS server is automatically selected.

Table 29: *CPPM Server Configuration Parameters for AirGroupCoA*

Parameter	Description
Name	Enter the name of the server.
IP address	Enter the IP address of the server.
Air Group CoA port	Enter a port number for sending AirGroup CoA on a different port than on the standard CoA port. The default value is 5999.
Shared key	Enter a shared key for communicating with the external RADIUS server.
Retype key	Re-enter the shared key.

4. Click **OK**.

NOTE

The CPPM server acts as a RADIUS server and asynchronously provides the AirGroup parameters for the client device including shared user, role, and location.

To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.

You can also add an external RADIUS server by selecting New for Authentication Server when configuring a WLAN or wired profile. For more information, see Configuring Security Settings for a WLAN SSID Profile on page 94 and Configuring Security Settings for a Wired Profile on page 109.

In the CLI

To configure a RADIUS server:

```
(Instant Access Point)(config)# wlan auth-server <profile-name>
(Instant Access Point)(Auth Server <profile-name>)# ip <IP-address>
(Instant Access Point)(Auth Server <profile-name>)# key <key>
(Instant Access Point)(Auth Server <profile-name>)# port <port>
(Instant Access Point)(Auth Server <profile-name>)# acctport <port>
(Instant Access Point)(Auth Server <profile-name>)# nas-id <NAS-ID>
(Instant Access Point)(Auth Server <profile-name>)# nas-ip <NAS-IP-address>
(Instant Access Point)(Auth Server <profile-name>)# timeout <seconds>
(Instant Access Point)(Auth Server <profile-name>)# retry-count <number>
(Instant Access Point)(Auth Server <profile-name>)# rfc3576
(Instant Access Point)(Auth Server <profile-name>)# deadtime <minutes>
(Instant Access Point)(Auth Server <profile-name>)# drp-ip <IP-address>  <mask> vlan  <vlan>
 gateway <gateway-IP-address)
(Instant Access Point)(Auth Server <profile-name>)# end
(Instant Access Point)# commit apply
```

To configure an LDAP server:

```
(Instant Access Point)(config)# wlan ldap-server <profile-name>
(Instant Access Point)(LDAP Server <profile-name>)# ip <IP-address>
(Instant Access Point)(LDAP Server <profile-name>)# port <port>
(Instant Access Point)(LDAP Server <profile-name>)# admin-dn <name>
(Instant Access Point)(LDAP Server <profile-name>)# admin-password <password>
(Instant Access Point)(LDAP Server <profile-name>)# base-dn <name>
(Instant Access Point)(LDAP Server <profile-name>)# filter <filter>
(Instant Access Point)(LDAP Server <profile-name>)# key-attribute <key>
(Instant Access Point)(LDAP Server <profile-name>)# timeout <seconds>
(Instant Access Point)(LDAP Server <profile-name>)# retry-count <number>
(Instant Access Point)(LDAP Server <profile-name>)# end
(Instant Access Point)# commit apply
```

To configure a CPPM server used for AirGroup CoA (Change of Authorization):

```
(Instant Access Point)(config)# wlan auth-server <profile-name>
(Instant Access Point)(Auth Server <profile-name>)# ip <IP-address>
(Instant Access Point)(Auth Server <profile-name>)# key <key>
(Instant Access Point)(Auth Server <profile-name> # cppm-rfc3576-port <port>
(Instant Access Point)(Auth Server <profile-name>)# cppm-rfc3576-only
(Instant Access Point)(Auth Server <profile-name>)# end
(Instant Access Point)# commit apply
```

Configuring Dynamic RADIUS Proxy Parameters

The RADIUS server can be deployed at different locations and VLANs. In most cases, a centralized RADIUS or local server is used to authenticate users. However, some user networks can use a local RADIUS server for employee authentication and a centralized RADIUS based Captive portal server for guest authentication. To ensure that the RADIUS traffic is routed to the required RADIUS server, the dynamic RADIUS proxy feature must be enabled.

If the IAP clients need to authenticate to the RADIUS servers through a different IP address and VLAN, ensure that the following steps are completed:

1. Enable dynamic RADIUS proxy.
2. Configure dynamic RADIUS proxy IP, VLAN. netmask, gateway for each authentication server.

3. Associate the authentication servers to SSID or a wired profile to which the clients connect.

After completing the above-mentioned configuration steps, you can authenticate the SSID users against the configured dynamic RADIUS proxy parameters.

Enabling Dynamic RADIUS Proxy

You can enable RADIUS Server Support using Instant UI or CLI.

In the Instant UI

To enable RADIUS server support:

1. In the Instant main window, click the **System** link. The **System** window appears.
2. In the **General** tab of **System** window, select **Enabled** from the **Dynamic RADIUS Proxy** drop-down list.
3. Click **OK**.

NOTE

When dynamic RADIUS proxy is enabled, ensure that a static Virtual Controller IP is configured. For more information on configuring Virtual Controller IP address, see Virtual Controller IP Address Configuration on page 86.

When dynamic RADIUS proxy is enabled, the Virtual Controller network uses the IP Address of the Virtual Controller for communication with external RADIUS servers. Ensure that the Virtual Controller IP Address is set as a NAS IP when configuring RADIUS server attributes with dynamic RADIUS proxy enabled. For more information on configuring RADIUS server attributes, see Configuring an External Server for Authentication on page 149.

In the CLI

To enable the dynamic RADIUS proxy feature:

```
(Instant Access Point)(config)# dynamic-radius-proxy
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Configuring Dynamic RADIUS Proxy Parameters for Authentication Servers

You can configure DRP parameters for the authentication server by using the Instant UI or CLI.

In the Instant UI

1. Click the **Security**>**Authentication Servers**.
2. To create a new server, click **New** and configure the required RADIUS server parameters as described in Table 27.
3. Ensure that the following dynamic RADIUS proxy parameters are configured:
   - **DRP IP**– IP address to be used as source IP for RADIUS packets
   - **DRP Mask**–Subnet mask of the DRP IP address.
   - **DRP VLAN**–VLAN in which the RADIUS packets are sent.
   - **DRP Gateway**–Gateway IP address of the DRP VLAN.
4. Click **OK**.

In the CLI

To configure dynamic RADIUS proxy parameters:

```
(Instant Access Point)(config)# wlan auth-server <profile-name>
(Instant Access Point)(Auth Server <profile-name>)# ip <IP-address>
(Instant Access Point)(Auth Server <profile-name>)# key <key>
(Instant Access Point)(Auth Server <profile-name>)# port <port>
(Instant Access Point)(Auth Server <profile-name>)# acctport <port>
(Instant Access Point)(Auth Server <profile-name>)# nas-id <NAS-ID>
```

```
(Instant Access Point)(Auth Server <profile-name>)# nas-ip <NAS-IP-address>
(Instant Access Point)(Auth Server <profile-name>)# timeout <seconds>
(Instant Access Point)(Auth Server <profile-name>)# retry-count <number>
(Instant Access Point)(Auth Server <profile-name>)# deadtime <minutes>
(Instant Access Point)(Auth Server <profile-name>)# drp-ip  <IP-address>  <mask> vlan  <vlan>
gateway <gateway-IP-address>
(Instant Access Point)(Auth Server <profile-name>)# end
(Instant Access Point)# commit apply
```

Associate the Authentication Servers with an SSID or Wired Profile

1. Access the WLAN wizard or Wired Settings window.
   - To open the WLAN wizard, select an existing SSID in the **Network** tab, and click **edit**.
   - To open the wired settings window, click **More**>**Wired**. In the **Wired** window, select a profile and click **Edit**.

   You can also associate the authentication servers when creating a new WLAN or wired profile.
2. Click the **Security** tab.
3. If you are configuring authentication server for a WLAN SSID, under **Security** tab, slide to **Enterprise** security level.
4. Ensure that an authentication type is enabled.
5. From the **Authentication Server 1** drop-down, select the server name on which dynamic RADIUS proxy parameters are enabled. You can also create a new server with RADIUS and RADIUS proxy parameters by selecting **New**.
6. Click **Next** and then click **Finish**.
7. To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.

NOTE

You can also add an external RADIUS server by selecting New for Authentication Server when configuring a WLAN or wired profile. For more information, see Configuring Security Settings for a WLAN SSID Profile on page 94 and Configuring Security Settings for a Wired Profile on page 109.

In the CLI

To associate an authentication server to a WLAN SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name># auth-server <server-name>
(Instant Access Point)(SSID Profile <name># end
((Instant Access Point)# commit apply
```

To associate an authentication server to a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# auth-server <name>
(Instant Access Point)(wired ap profile <name>)# end
((Instant Access Point)# commit apply
```

Configuring Authentication Parameters for Virtual Controller Management Interface

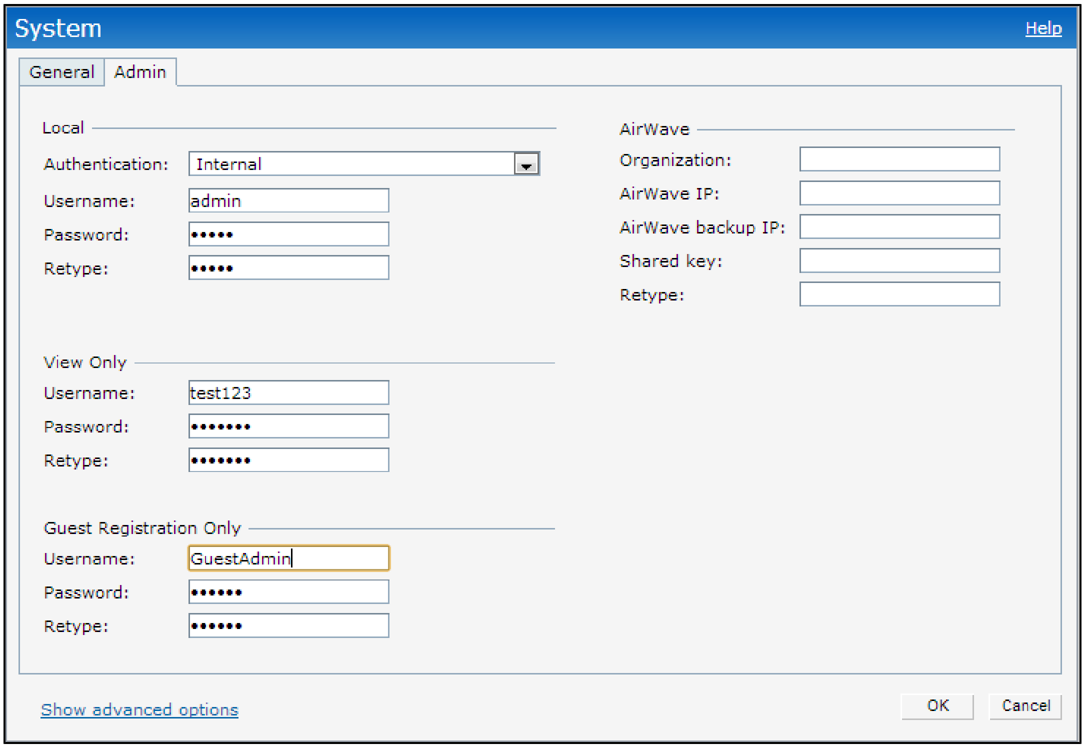
You can configure authentication settings to access to the Virtual Controller management user interface in the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at top right corner of the Instant main window. The **System** window appears.

2. Select the **Admin** tab. The **Admin** tab details are displayed. The following figure shows the contents of the **Admin** tab:

Figure 49 *Admin Tab: Management Authentication Parameters*



Local

Authentication: Internal

Username: admin

Password: •••••

Retype: •••••

View Only

Username: test123

Password: •••••••

Retype: •••••••

Guest Registration Only

Username: GuestAdmin

Password: ••••••

Retype: ••••••

AirWave

Organization:

AirWave IP:

AirWave backup IP:

Shared key:

Retype:

3. Under Local, select any of the following options from the **Authentication** drop-down list:

- **Internal**– Select this option to specify a single set of user credentials. Enter the **Username** and **Password** for accessing the Virtual Controller Management User Interface.
- **RADIUS Server**– Specify one or two RADIUS servers to authenticate clients. If two servers are configured, users can use them in primary or backup mode or load balancing mode. To enable load balancing, select **Enabled** from the **Load balancing** drop-down list.
- **RADIUS server w/ fallback to internal**– Select this option to use both internal and external servers. When enabled, the authentication switches to **Internal** if there is no response from the RADIUS server (RADIUS server timeout). To complete this configuration, perform the following steps:

   a. To enable load balancing, select **Enabled** from the **Load balancing** drop-down list.

   b. Specify a **Username** and **Password**.

   c. Retype the password to confirm.

4. Click **OK**.

In the CLI

To configure management authentication settings:

```
(Instant Access Point)(config)# mgmt-auth-server <server1>
(Instant Access Point)(config)# mgmt-auth-server <server2>
(Instant Access Point)(config)# mgmt-auth-server-load-balancing
(Instant Access Point)(config)# mgmt-auth-server-local-backup
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Configuring 802.1X Authentication for a Network Profile

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

The steps involved in 802.1X authentication are as follows:

1. The NAS requests authentication credentials from a wireless client.
2. The wireless client sends authentication credentials to the NAS.
3. The NAS sends these credentials to a RADIUS server.
4. The RADIUS server checks the user identity and authenticates the client if the user details are available 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 appropriate credentials.
5. After the client is authenticated, the RADIUS server forwards the encryption key to the NAS. The encryption key is used for encrypting or decrypting traffic sent to and from the client.

NOTE

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

Configuring 802.1X authentication for a Wireless Network Profile

You can configure 802.1X authentication for a wireless network profile in the Instant UI or CLI.

In the Instant UI

To enable 802.1X authentication for a wireless network:

1. In the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable 802.1X authentication and click **edit**.
2. In the **Edit <profile-name>** or **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. In the **Security** tab, specify the following parameters for the **Enterprise** security level:
   a. Select any of the following options from the **Key management** drop-down list.
      - WPA-2 Enterprise
      - WPA Enterprise
      - Both (WPA-2 & WPA)
      - Dynamic WEP with 802.1X
4. If you do not want to use a session key from the RADIUS Server to derive pair wise unicast keys, set **Session Key for LEAP** to **Enabled**.
5. To terminate the EAP portion of 802.1X authentication on the IAP instead of the RADIUS server, set **Termination** to **Enabled**.

   By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the AP acts as a relay for this exchange. When **Termination** is enabled, the IAP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server.
6. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see Configuring Security Settings for a WLAN SSID Profile on page 94
7. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure 802.1X authentication for a wireless network:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# type {<Employee>|<Voice>}
(Instant Access Point)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip|wpa-tkip,wpa2-aes|dynam
ic-wep}
(Instant Access Point)(SSID Profile <name>)# leap-use-session-key
(Instant Access Point)(SSID Profile <name>)# termination
(Instant Access Point)(SSID Profile <name>)# external-server
(Instant Access Point)(SSID Profile <name>)# auth-server <server-name>
(Instant Access Point)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant Access Point)(SSID Profile <name>)# auth-survivability
(Instant Access Point)(SSID Profile <name>)# exit
(Instant Access Point)(config)# auth-survivability cache-time-out <hours>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Configuring 802.1X authentication for Wired Profiles

You can configure 802.1X authentication for a wired profile in the Instant UI or CLI.

In the Instant UI

To enable 802.1X authentication for a wired profile:

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable 802.1X authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. In the **Security** tab, select **Enabled** from the **802.1X authentication** drop-down list.
5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see Configuring Security Settings for a Wired Profile on page 109
6. Click **Next** to define access rules, and then click **Finish** to apply the changes.
7. Assign the profile to an Ethernet port. For more information, see Assigning a Profile to Ethernet Ports on page 113.

In the CLI

To enable 802.1X authentication for a wired profile:

```
(Instant Access Point) (config)# wired-port-profile <name>
(Instant Access Point) (wired ap profile <name>)# type {<employee> |<guest>}
(Instant Access Point) (wired ap profile <name>)# dot1x
(Instant Access Point) (wired ap profile <name>)# auth-server <server1>
(Instant Access Point) (wired ap profile <name>)# auth-server <server1>
(Instant Access Point) (wired ap profile <name>)# server-load-balancing
(Instant Access Point) (wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant Access Point) (wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring MAC Authentication for a Network Profile

MAC authentication can be used alone or it can be combined with other forms of authentication such as WEP authentication. However, it is recommended that you do not use the MAC-based authentication.

This section describes the following procedures:

- Configuring MAC Authentication for Wireless Network Profiles on page 158
- Configuring MAC Authentication for Wireless Network Profiles on page 158

Configuring MAC Authentication for Wireless Network Profiles

You can configure MAC authentication for a wired profile in the Instant UI or CLI.

In the Instant UI

To enable MAC Authentication for a wireless network:

1. In the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable MAC authentication and click **edit**.
2. In the **Edit <profile-name>** or **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. In the **Security** tab, select **Enabled** from the **MAC authentication** drop-down list, for **Personal** or **Open** security level.
4. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see Configuring Security Settings for a WLAN SSID Profile on page 94
5. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure a WLAN SSID profile in the CLI:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# type {<Employee> | <Voice>| <Guest>}
(Instant Access Point)(SSID Profile <name>)# mac-authentication
(Instant Access Point)(SSID Profile <name>)# external-server
(Instant Access Point)(SSID Profile <name>)# auth-server <server-name1>
(Instant Access Point)(SSID Profile <name>)# auth-server <server-name2>
(Instant Access Point)(SSID Profile <name>)# server-load-balancing
(Instant Access Point)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring MAC Authentication for Wired Profiles

You can configure MAC authentication for a wired profile in the Instant UI or CLI.

In the Instant UI

To enable MAC authentication for a wired profile:

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which for which you want to enable MAC authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. In the **Security** tab, select **Enabled** from the **MAC authentication** drop-down list.
5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see Configuring Security Settings for a Wired Profile on page 109
6. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To enable MAC authentication for a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# type {<employee> |<guest>}
(Instant Access Point)(wired ap profile <name>)# mac-authentication
```

```
(Instant Access Point)(wired ap profile <name>)# auth-server <server-1>
(Instant Access Point)(wired ap profile <name>)# auth-server <server-2>
(Instant Access Point)(wired ap profile <name>)# server-load-balancing
(Instant Access Point)(wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring MAC Authentication with 802.1X Authentication

This section describes the following procedures:

- Configuring MAC and 802.1X Authentication for a Wireless Network Profile on page 159
- Configuring MAC and 802.1X Authentication for Wired Profiles on page 159

Configuring MAC and 802.1X Authentication for a Wireless Network Profile

You can configure MAC authentication with 802.1X authentication for wireless network profile using Instant UI or CLI.

In the Instant UI

To configure both MAC and 802.1X authentication for a wireless network:

1. In the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable MAC and 802.1X authentication and click **edit**.
2. In the **Edit <profile-name>** or **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. In the **Security** tab, ensure that the required parameters for MAC authentication and 802.1X authentication are configured.
4. Select the **Perform MAC authentication before 802.1X** check box to use 802.1X authentication only when the MAC authentication is successful.
5. Select the check box **MAC authentication fail-thru** to use 802.1X authentication even when the MAC authentication fails.
6. Click **Next** and then click **Finish** to apply the changes.

In the CLI

To configure both MAC and 802.1X authentication for a wireless network:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# type {<Employee> | <Voice>| <Guest>}
(Instant Access Point)(SSID Profile <name>)# mac-authentication
(Instant Access Point)(SSID Profile <name>)# l2-auth-failthrough
(Instant Access Point)(SSID Profile <name>)# auth-server <server-name1>
(Instant Access Point)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant Access Point)(SSID Profile <name>)# auth-survivability
(Instant Access Point)(SSID Profile <name>)# exit
(Instant Access Point)(config)# auth-survivability cache-time-out <hours>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Configuring MAC and 802.1X Authentication for Wired Profiles

You can configure MAC and 802.1X authentication for a wired profile in the Instant UI or CLI.

In the Instant UI

To enable MAC and 802.1X authentication for a wired profile:

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which for which you want to enable MAC authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. In the **Security** tab, enable the following options:
   - Select **Enabled** from the **MAC authentication** drop-down list.
   - Select **Enabled** from the **802.1X authentication** drop-down list.
   - Select **Enabled** from the **MAC authentication fail-thru** drop-down list.
5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see Configuring Security Settings for a Wired Profile on page 109
6. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To enable MAC and 802.1X authentication for a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile "<name>")# type {<employee> |<guest>}
(Instant Access Point)(wired ap profile "<name>")# mac-authentication
(Instant Access Point)(wired ap profile "<name>")# dot1x
(Instant Access Point)(wired ap profile "<name>")# l2-auth-failthrough
(Instant Access Point)(wired ap profile "<name>")# auth-server <name>
(Instant Access Point)(wired ap profile "<name>")# server-load-balancing
(Instant Access Point)(wired ap profile "<name>")# radius-reauth-interval <Minutes>
(Instant Access Point)(wired ap profile "<name>")# end
(Instant Access Point)# commit apply
```

Configuring MAC Authentication with Captive Portal Authentication

This authentication method has the following features:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
- If the captive portal splash page type is **none**, MAC authentication is disabled.
- MAC authentication only role– You can use the WLAN wizard to configure the **mac-auth-only** role in the role-based access rule configuration section when MAC authentication is enabled with captive portal authentication.

Configuring MAC Authentication with Captive Portal Authentication

You can configure the MAC authentication with Captive Portal authentication for a network profile using the Instant UI or CLI.

In the Instant UI

1. Select an existing wireless or wired profile for which you want to enable MAC with Captive Portal authentication. Depending on the network profile selected, the **Edit <WLAN-Profile>** or **Edit Wired Network** window is displayed.

NOTE

You can configure MAC authentication with Captive Portal authentication, in the **Access** tab of the **New WLAN** and **New Wired Network** windows when configuring a new profile.

2. In the **Access** tab, specify the following parameters for a network with **Role-Based** rules:
   a. Select the **Enforce Machine Authentication** check box when MAC authentication is enabled for Captive Portal. If the MAC authentication fails, the Captive Portal authentication role is assigned to the client.
   b. For wireless network profile, select **Enforce MAC Auth Only Role** check box when MAC authentication is enabled for Captive Portal. After successful MAC authentication, MAC auth only role is assigned to the client.
3. Click **Next** and then click **Finish** to apply the changes.

In the CLI

To configure MAC authentication with Captive Portal authentication for a wireless profile:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# type <Guest>
(Instant Access Point)(SSID Profile <name>)# mac-authentication
(Instant Access Point)(SSID Profile <name>)# captive-portal <type> exclude-uplink <type>
(Instant Access Point)(SSID Profile <name>)# set-role-machine-auth <machine-authentication> <u
ser-authentication>
(Instant Access Point)(SSID Profile <name>)# set-role-mac-auth <MAC-authentication-only>
(Instant Access Point)(SSID Profile <name>)#  end
(Instant Access Point)# commit apply
```

To configure MAC authentication with Captive Portal authentication for a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# type <guest>
(Instant Access Point)(wired ap profile <name>)# mac-authentication
(Instant Access Point)(wired ap profile <name>)# captive-portal <type>
(Instant Access Point)(wired ap profile <name>)# captive-portal <type> exclude-uplink {<3G>| <
4G>| <Wifi> | Ethernet}
(Instant Access Point)(wired ap profile <name>)# set-role-machine-auth <machine-only> <user-on
ly>
(Instant Access Point)(wired ap profile <name>)# set-role-mac-auth <mac-only>
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring WISPr Authentication

Instant supports the following smart clients:

- iPass
- Boingo

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

NOTE

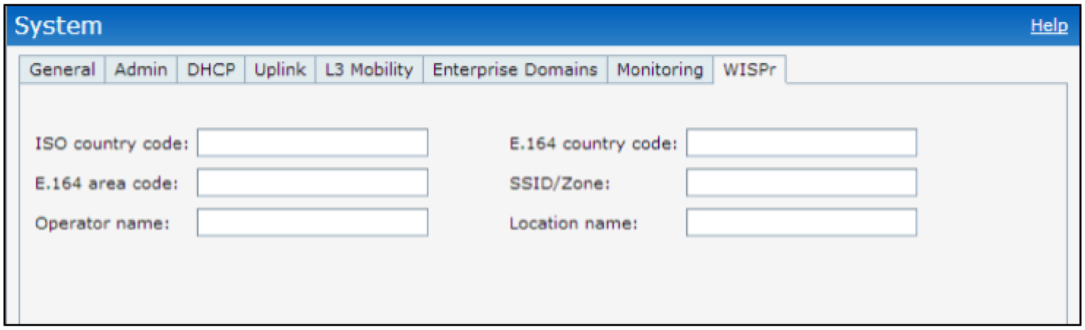
WISPr authentication is supported only for the **Internal - Authenticated** and **External - RADIUS Server** captive portal authentication.
Select the **Internal - Authenticated** or the **External - RADIUS Server** option from the **Splash page type** drop-down menu to configure WISPr authentication for a WLAN profile.

You can configure WISPr authentication using Instant UI or CLI.

In the Instant UI

1. Click the **System** link at the top-right corner of the Instant main window. The **System** window is displayed.
2. Click **Show advanced options**.
3. Click **WISPr** tab. The **WISPr** tab contents are displayed. The following figure shows the **WISPr** tab contents:

Figure 50 *Configuring WISPr Authentication*



4. Enter the ISO Country Code for the WISPr Location ID in the **ISO Country Code** text box.
5. Enter the E.164 Area Code for the WISPr Location ID in the **E.164 Area Code** text box.
6. Enter the operator name of the Hotspot in the **Operator Name** text box.
7. Enter the E.164 Country Code for the WISPr Location ID in the **E.164 Country Code** text box.
8. Enter the SSID/Zone section for the WISPr Location ID in the **SSID/Zone** text box.
9. Enter the name of the Hotspot location in the **Location Name** text box. If no name is defined, the name of the IAP to which the user is associated is used.
10. Click **OK** to apply the changes.

The WISPr RADIUS attributes and configuration parameters are specific to the RADIUS server used by your ISP for the WISPr authentication. Contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU Websites (www.iso.org and http://www.itu.int).

A Boingo smart client uses a NAS identifier in the format <CarrierID>_<VenueID> for location identification. To support Boingo clients, ensure that you configure the NAS identifier parameter in the Radius server profile for the WISPr server.

In the CLI

```
(Instant Access Point)(config)# wlan wispr-profile
(Instant Access Point)(WISPr)# wispr-location-id-ac
(Instant Access Point)(WISPr)# wispr-location-id-cc
(Instant Access Point)(WISPr)# wispr-location-id-isocc
(Instant Access Point)(WISPr)# wispr-location-id-network
(Instant Access Point)(WISPr)# wispr-location-name-location
(Instant Access Point)(WISPr)# wispr-location-name-operator-name
(Instant Access Point)(WISPr)# end
(Instant Access Point)# commit apply
```

Blacklisting Clients

The client blacklisting denies connection to the blacklisted clients. When a client is blacklisted, it is not allowed to associate with an IAP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force client disconnection.

This section describes the following procedures:

- Blacklisting Clients Manually on page 163
- Blacklisting Users Dynamically on page 163

Blacklisting Clients Manually

Manual blacklisting adds the MAC address of a client to the blacklist. These clients are added into a permanent blacklist. These clients are not allowed to connect to the network unless they are removed from the blacklist.

Adding a Client to the Blacklist

You can add a client to the blacklist manually using Instant UI or CLI.

In the Instant UI

1. Click the **Security** link from the top right corner of the Instant main window.
2. Click the **Blacklisting** tab.
3. Under the **Manual Blacklisting**, click **New** .
4. Enter the MAC address of the client to be blacklisted in the **MAC address to add** text box.
5. Click **OK**. The **Blacklisted Since** tab displays the time at which the current blacklisting has started for the client.
6. To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklisting**, and then click **Delete**.

In the CLI

To blacklist a client:

```
(Instant Access Point)(config)# blacklist-client <MAC-Address>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To view the blacklisted clients:

```
(Instant Access Point)# show blacklist-client

Blacklisted Clients
-------------------
MAC                Reason        Timestamp  Remaining time(sec)  AP name
---                ------        ---------  -------------------  -------
00:1c:b3:09:85:15  user-defined  17:21:29   Permanent            -
```

Blacklisting Users Dynamically

The clients can be blacklisted dynamically when they exceed the authentication failure threshold or when a blacklisting rule is triggered as part of the authentication process.

Authentication Failure Blacklisting

When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically blacklisted by an IAP.

Session Firewall Based Blacklisting

In session firewall based blacklisting, an ACL rule is used to enable the option for automation blacklisting. when the ACL rule is triggered, it sends out blacklist information and the client is blacklisted.

Configuring Blacklist Duration

You can set the blacklist duration using Instant UI or CLI.

In the Instant UI

To set a blacklist duration:

1. Click the **Security** link from the top right corner of the Instant main window.
2. Click the **Blacklisting** tab.

3. Under Dynamic Blacklisting:
4. For **Auth failure blacklist time**, duration in seconds after which the clients that exceed the authentication failure threshold must be blacklisted.
5. For **PEF rule blacklisted time**, enter the duration in seconds after which the clients can be blacklisted due to an ACL rule trigger.

You can configure a maximum number of authentication failures by the clients, after which a client must be blacklisted. For more information on configuring maximum authentication failure attempts, see Configuring Security Settings for a WLAN SSID Profile on page 94

To enable session firewall based blacklisting, click **New** and navigate to **WLAN Settings > VLAN > Security > Access** window, and enable the **Blacklist** option of the corresponding ACL rule.

In the CLI

To dynamically blacklist clients:

```
(Instant Access Point)(config)# auth-failure-blacklist-time <seconds>
(Instant Access Point)(config)# blacklist-time <seconds>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To view the blacklisted clients:

```
(Instant Access Point)# show blacklist-client config

Blacklist Time               :60
Auth Failure Blacklist Time  :60
Manually Blacklisted Clients
----------------------------
MAC  Time
---  ----
Dynamically Blacklisted Clients
-------------------------------
MAC  Reason  Timestamp  Remaining time(sec)  AP IP
---  ------  ---------  -------------------  -----
Dyn Blacklist Count  :0
```

Uploading 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.

Instant supports the following certificate files:

- Auth server or Captive portal server certificate: PEM format with passphrase (PSK)
- CA certificate: PEM or DER format

In the current release, IAP supports uploading of a customized certificate for internal Captive portal server.

This section describes the following procedures:

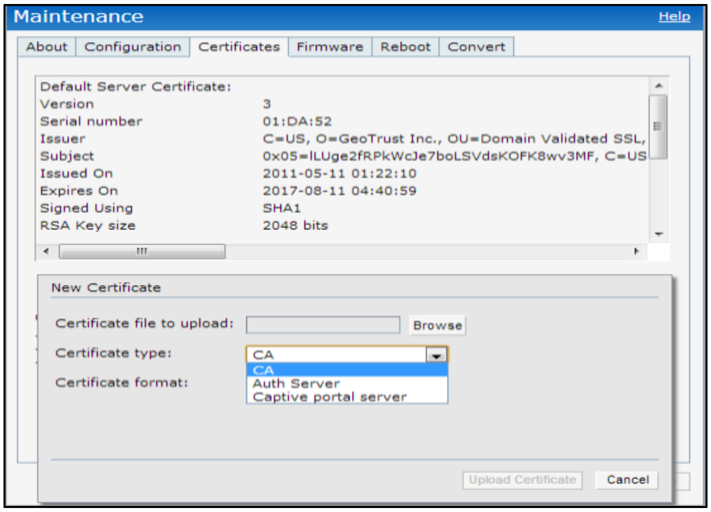
- Loading Certificates using Instant UI on page 165
- Loading Certificates using Instant CLI
- Loading Certificates using AirWave on page 165

Loading Certificates using Instant UI

To load a certificate in the Instant UI:

1. Click the **Maintenance** link at the top right corner of the Instant main window.
2. Click the **Certificates** tab. The **Certificates** tab contents are displayed. The following figure shows the **Certificates** window:

Figure 51 *Maintenance Window: Certificates Tab*



```
Default Server Certificate:
Version                 3
Serial number           01:DA:52
Issuer                  C=US, O=GeoTrust Inc., OU=Domain Validated SSL,
Subject                 0x05=lLUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US
Issued On               2011-05-11 01:22:10
Expires On              2017-08-11 04:40:59
Signed Using            SHA1
RSA Key size            2048 bits
```

New Certificate

Certificate file to upload:

Certificate type: CA

Certificate format:

3. To upload a certificate, click **Upload New Certificate**. The **New Certificate** window appears.
4. Browse and select the file to upload.
5. Select any of the following types of certificate from the **Certificate type** drop-down list:

- CA—CA certificates validate the client's certificate.
- Auth Server—The authentication server certificate verifies the server's identity to the client.
- Captive portal server—Captive portal server certificate verifies internal Captive portal server's identity to the client.

6. Select the certificate format from the **Certificate format** drop-down list.
7. If you have selected **Auth Server** or **Captive portal server** type, enter a passphrase in **Passphrase** and reconfirm. The default password is **whatever**. If the certificate does not include a passphrase, there is no passphrase required.
8. Click **Browse** and select the appropriate certificate file, and click **Upload Certificate**. The **Certificate Successfully Installed** message is displayed.

Loading Certificates using Instant CLI

To upload a certificate:

```
(Instant Access Point)# copy tftp {<ip-address> <filename> cpserver cert <password> format
{p12|pem} |system {1xca [format {der|pem}]|1xcert <passsword>[format {p12|pem}]}
```

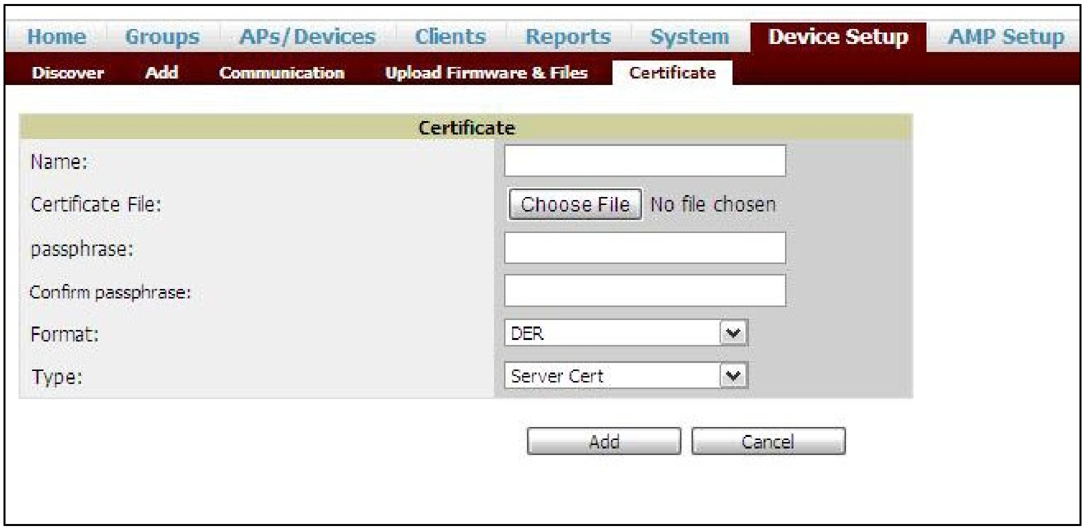
Loading Certificates using AirWave

You can manage certificates using the AirWave. The AMP directly provisions the certificates and performs basic certificate verification (such as certificate type, format, version, serial number and so on), before accepting the certificate and uploading to an IAP network. The AMP packages the text of the certificate into an HTTPS message and sends it to the Virtual Controller. After the VC receives this message, it draws the certificate content from the message, converts it to the right format and saves it on the RADIUS server.

To load a certificate in AirWave:

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

Figure 52 *Loading Certificate via AirWave*



Certificate

Name:

Certificate File: No file chosen

passphrase:

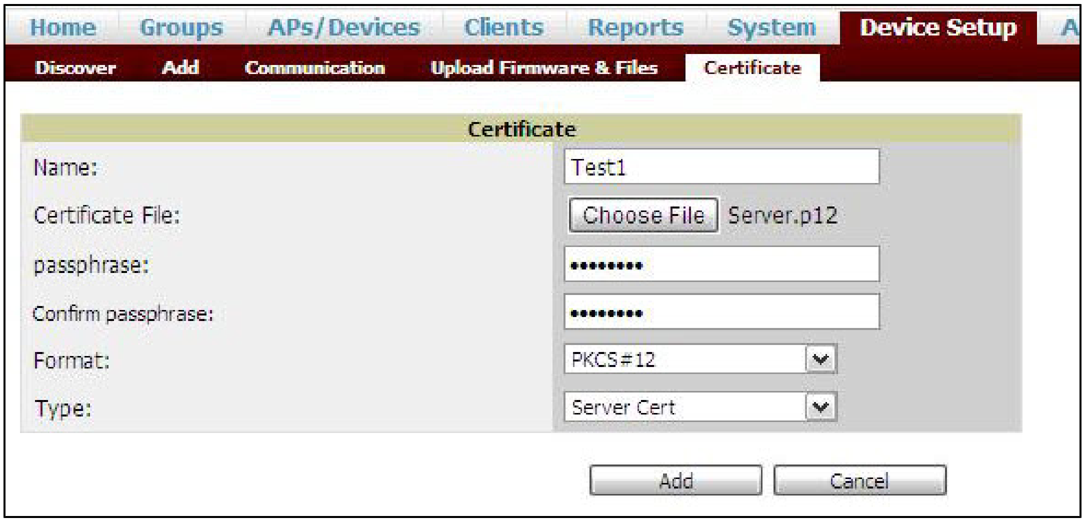
Confirm passphrase:

Format: DER

Type: Server Cert

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

Figure 53 *Server Certificate*



Certificate

Name: Test1

Certificate File: Server.p12

passphrase: ••••••••

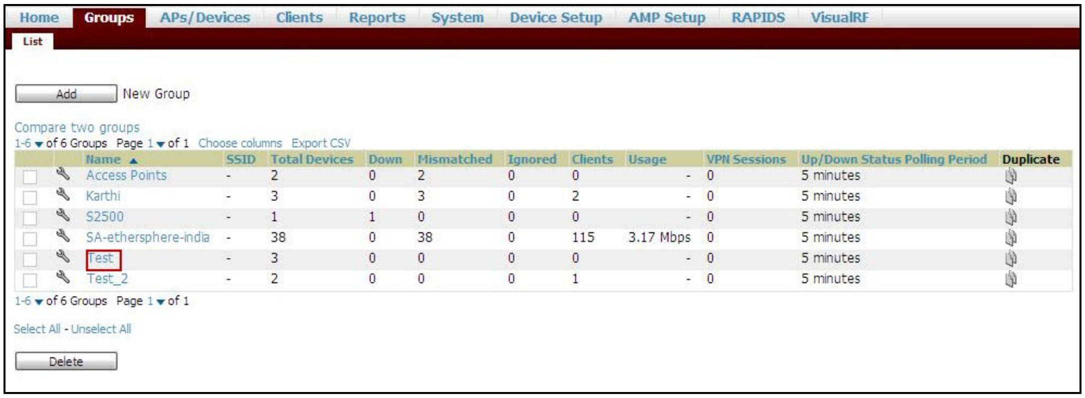
Confirm passphrase: ••••••••

Format: PKCS#12

Type: Server Cert

4. After you upload the certificate, navigate to **Groups,** click the Instant **Group** and then select **Basic**. The Group name appears only if you have entered the **Organization** name in the Instant UI. For more information, see Configuring Organization String on page 271 for further information.

Figure 54 *Selecting the Group*



		Name ▲	SSID	Total Devices	Down	Mismatched	Ignored	Clients	Usage	VPN Sessions	Up/Down Status Polling Period	Duplicate
□		Access Points	-	2	0	2	0	0	-	0	5 minutes	
□		Karthi	-	3	0	3	0	2	-	0	5 minutes	
□		S2500	-	1	1	0	0	0	-	0	5 minutes	
□		SA-ethersphere-india	-	38	0	38	0	115	3.17 Mbps	0	5 minutes	
□		Test	-	3	0	0	0	0	-	0	5 minutes	
□		Test_2	-	2	0	0	0	1	-	0	5 minutes	

The **Virtual Controller Certificate** section displays the certificates (CA cert and Server).

5. Click **Save** to apply the changes only to AirWave. Click **Save and Apply** to apply the changes to the IAP.
6. To clear the certificate options, click **Revert**.

Chapter 12
Roles and Policies

This chapter describes the procedures for configuring user roles, role assignment, and firewall policies.

- Firewall Configuration on page 169
- Access Control List Rules on page 173
- Configuring User Roles on page 180
- Configuring Derivation Rules on page 182

Firewall Configuration

Instant firewall provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using Instant firewall, you can enforce network access policies that define access to the network, areas of the network that users may access, and the performance thresholds of various applications.

Instant supports a role-based stateful firewall. Instant firewall recognizes flows in a network and keeps track of the state of sessions. Instant firewall manages packets according to the first rule that matches packet. The firewall logs on the IAPs are generated as syslog messages. Instant firewall also supports the Application Layer Gateway (ALG) functions such as SIP, Vocera, Alcatel NOE, and Cisco Skinny protocols.

Configuring ALG Protocols

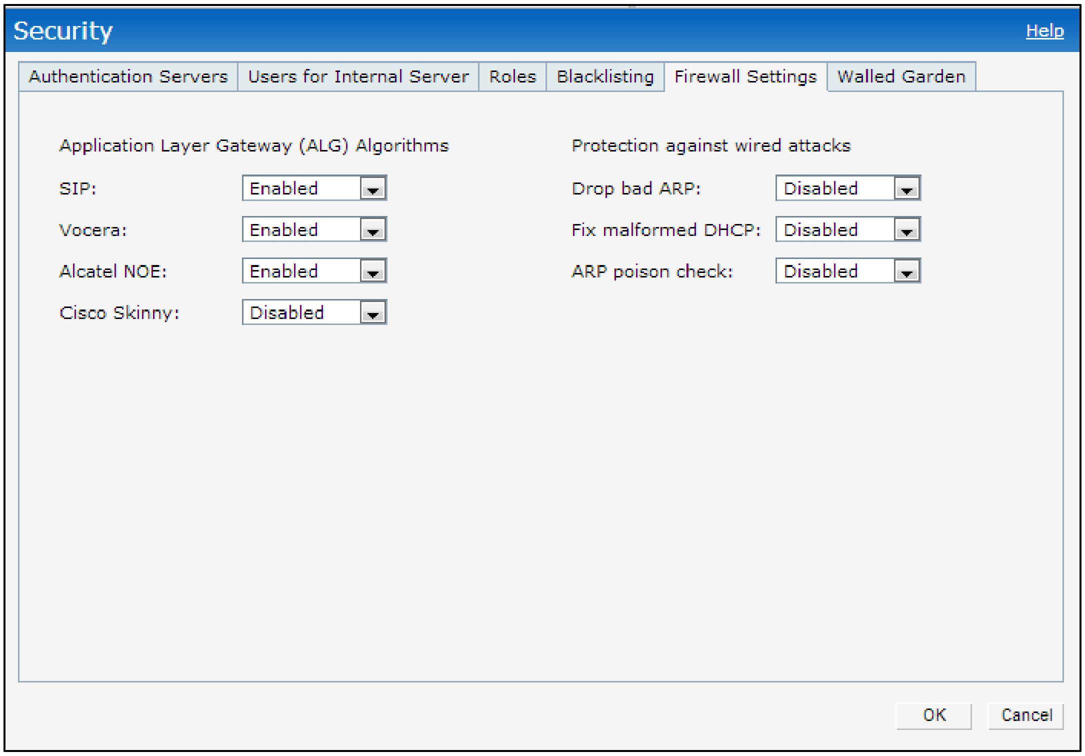
You can enable or disable protocols for Application Layer Gateway (ALG) in Instant using Instant UI or CLI.

In the Instant UI

To configure protocols for ALG:

1. Click the **Security** link at the top right corner of Instant main window.
2. Click the **Firewall Settings** tab. The **Firewall Settings** tab contents are displayed. The following figure shows the contents of the **Firewall Settings** tab:

Figure 55 *Firewall Settings—ALG Protocols*



Application Layer Gateway (ALG) Algorithms

SIP: Enabled

Vocera: Enabled

Alcatel NOE: Enabled

Cisco Skinny: Disabled

Protection against wired attacks

Drop bad ARP: Disabled

Fix malformed DHCP: Disabled

ARP poison check: Disabled

3. Select **Enabled** from the corresponding drop-down lists to enable SIP, VOCERA, Alcatel NOE, and Cisco skinny protocols.
4. Click **OK**.

When the protocols for ALG are **Disabled** the changes do not take effect affect until the existing user sessions are expired. Reboot the IAP and the client, or wait for few minutes for changes to affect.

In the CLI

To configure protocols for ALG:

```
(Instant Access Point)(config)# alg
(Instant Access Point)(ALG)# sccp-disable
(Instant Access Point)(ALG)# no sip-disable
(Instant Access Point)(ALG)# no ua-disable
(Instant Access Point)(ALG)# no vocera-disable
(Instant Access Point)(ALG)# end
(Instant Access Point)# commit apply
```

To view the ALG configuration:

```
(Instant Access Point)# show alg

Current ALG
-----------
ALG      Status
---      ------
sccp     Disabled
sip      Enabled
ua       Enabled
vocera   Enabled
```

Configuring Firewall Settings for Protection from ARP Attacks

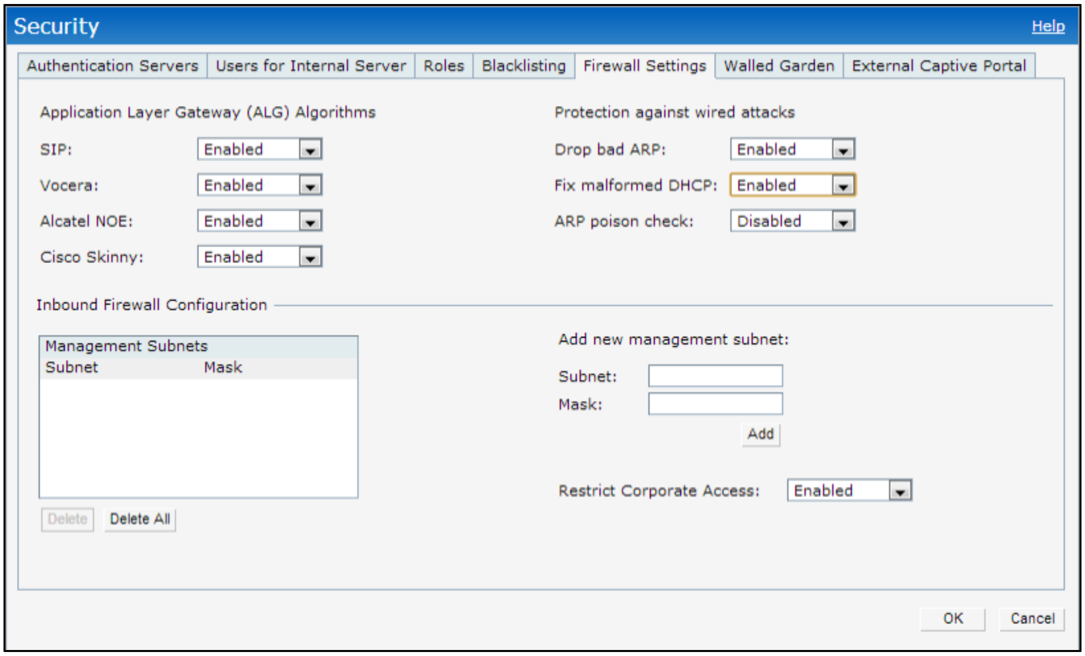
You can configure firewall settings to protect the network against attacks using Instant using Instant UI or CLI.

In the Instant UI

To configure firewall settings:

1. Click the **Security** link at the top right corner of Instant main window.
2. Click the **Firewall Settings** tab. The **Firewall Settings** tab contents are displayed.
3. To configure protection against security attacks, select the following check boxes:
   - Select **Drop bad ARP** to enable the IAP to drop the fake ARP packets.
   - Select **Fix malformed DHCP** to the IAP to fix the malformed DHCP packets.
   - Select **ARP poison check** to enable the IAP to trigger an alert notifying the user about the ARP poisoning that may have been caused by the rogue APs.

Figure 56 *Firewall Settings —Protection Against Wired Attacks*



Application Layer Gateway (ALG) Algorithms

SIP: Enabled

Vocera: Enabled

Alcatel NOE: Enabled

Cisco Skinny: Enabled

Protection against wired attacks

Drop bad ARP: Enabled

Fix malformed DHCP: Enabled

ARP poison check: Disabled

Inbound Firewall Configuration

Management Subnets	
Subnet	Mask

Add new management subnet:

Subnet:

Mask:

Restrict Corporate Access: Enabled

4. Click **OK.**

In the CLI

To configure firewall settings to prevent attacks

```
(Instant Access Point)(config)# attack
(Instant Access Point)(ATTACK)# drop-bad-arp-enable
(Instant Access Point)(ATTACK)# fix-dhcp-enable
(Instant Access Point)(ATTACK)# poison-check-enable
(Instant Access Point)(ATTACK)# end
(Instant Access Point)# commit apply
```

To view the configuration status:

```
(Instant Access Point)# show attack config

Current Attack
--------------
Attack        Status
------        ------
drop-bad-arp  Enabled
fix-dhcp      Enabled
poison-check  Enabled
```

To view the attack statistics

```
(Instant Access Point)# show attack stats
```

```
attack counters
--------------------------------------
Counter                                Value
-------                                -------
arp packet counter                     0
drop bad arp packet counter            0
dhcp response packet counter           0
fixed bad dhcp packet counter          0
send arp attack alert counter          0
send dhcp attack alert counter         0
arp poison check counter               0
garp send check counter                0
```

Managing Inbound Traffic

Instant now supports enhanced inbound firewall by allowing the configuration of management subnets and restricting corporate access through an uplink switch.

To allow flexibility in firewall configuration, Instant supports the following features:

- Configurable Management Subnets
- Restricted corporate access

Configuring Management Subnets

You can configure subnets to ensure that the IAP management is carried out only from these subnets. When the management subnets are configured, Telnet, SSH, and UI access is restricted to these subnets only.

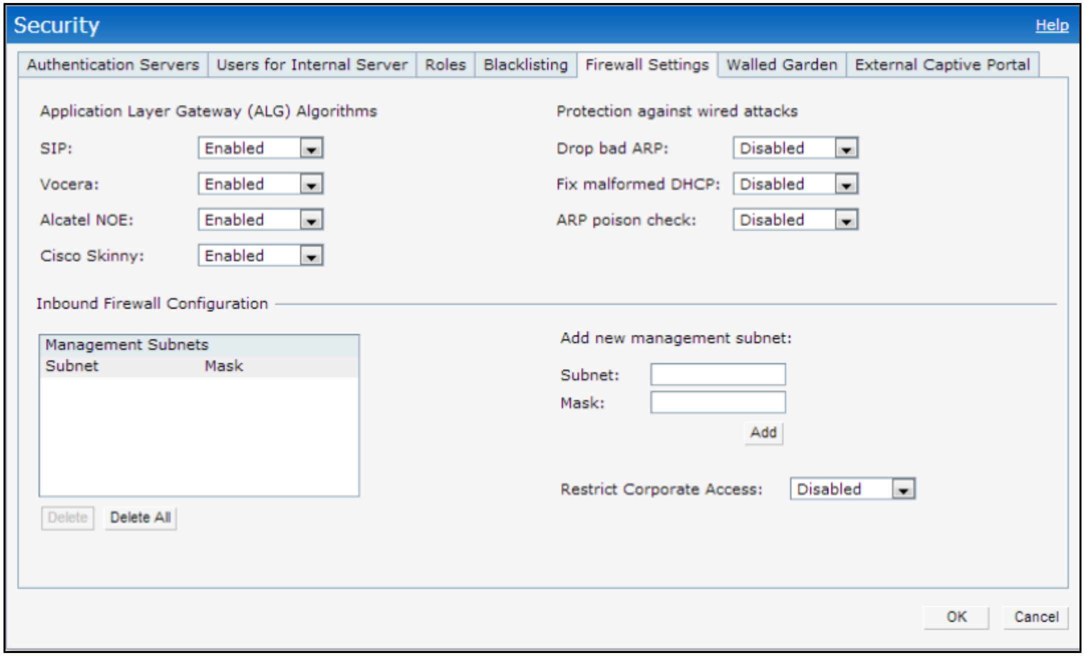
You can configure management subnets by using the Instant UI or CLI.

In the Instant UI

To configure management subnets:

1. Navigate to **Security**> **Firewall Settings**. The **Firewall Settings** tab contents are displayed.

Figure 57 *Firewall Settings—Management Subnets*



Application Layer Gateway (ALG) Algorithms

SIP: Enabled

Vocera: Enabled

Alcatel NOE: Enabled

Cisco Skinny: Enabled

Protection against wired attacks

Drop bad ARP: Disabled

Fix malformed DHCP: Disabled

ARP poison check: Disabled

Inbound Firewall Configuration

Management Subnets	
Subnet	Mask

Add new management subnet:

Subnet:

Mask:

Restrict Corporate Access: Disabled

2. To add a new management subnet:
   - Enter the subnet address in **Subnet**.

  - Enter the subnet mask in **Mask.**
  - Click **Add**.

3. To add multiple subnets, repeat step 2.
4. Click **OK**.

In the CLI

To configure a management subnet:

```
(Instant Access Point)(config) # restricted-mgmt-access <subnet-IP-address> <subnet-mask>
(Instant Access Point)(config) # end
(Instant Access Point)# commit apply
```

Configuring Restricted Access to Corporate Network

You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master IAP, including clients connected to a slave IAP. You can configure restricted corporate access by using the Instant UI or CLI.

In the Instant UI

To configure restricted corporate access:

1. Navigate to **Security**> **Firewall Settings**. The **Firewall Settings** (see Figure 57) tab contents are displayed.
2. Select **Enabled** from the **Restrict Corporate Access**.
3. Click **OK**.

In the CLI

To configure restricted management access:

```
(Instant Access Point)(config) # restrict-corp-access
(Instant Access Point)(config) # end
(Instant Access Point)# commit apply
```

Access Control List Rules

You can use Access Control List (ACL) rules to either permit or deny data packets passing through the IAP. You can also limit packets or bandwidth available to a set of user roles by defining access rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses.

You can create access rules to allow or block data packets that match the criteria defined in an access rule. You can create rules for either inbound traffic or outbound traffic. Inbound rules explicitly allow or block the inbound network traffic that matches the criteria in the rule. Outbound rules explicitly allow or block the network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to an IP address through the firewall.

The IAP clients are associated with user roles, which determine the client’s network privileges and the frequency at which clients re-authenticate. Instant supports the following types of ACLs:

- ACLs that permit or deny traffic based on the source IP address of the packet.
- ACLs that permit or deny traffic based on source or destination IP address, source or destination port number.

NOTE

You can configure of up to 64 access control rules for a firewall policy.

Configuring Access Rules

You can configure access rules using Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard or Wired settings window:
   - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure access rules for a wired profile, **More**>**Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab.
3. Slide to **Network-based** using the scroll bar to specify access rules for the network.
4. Click **New** to add a new rule. The **New Rule** window is displayed.
5. In the **New Rule** window, specify the following parameters:

Table 30: *Access Rule Configuration Parameters*

Field	Description
Rule type	Select a rule type, for example **Access control** from the drop-down list.
Action	Select any of following attributes: ● Select **Allow** to allow access users based on the access rule. ● Select **Deny** to deny access to users based on the access rule. ● Select **Destination-NAT** to allow changes to destination IP address. ● Select **Source-NAT** to allow changes to the source IP address.
Service	Select a service from the list of available services. You can allow or deny access to any or all of the following services based on your requirement: ● **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 ● **cfgm-tcp**– ● **cups**–Common UNIX Printing System ● **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 ● **noe**–Alcatel NOE service ● **noe-oxo**–

Table 30: *Access Rule Configuration Parameters*

Field	Description
	- **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 - **sips**–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 - **snmp**–Simple network management protocol - **snmp-trap**–Simple network management protocol-trap - **svp**–Software Validation Protocol - **syslog**–Syslog - **telnet**–Telnet network protocol - **tftp**– Trivial file transfer protocol - **vocera**–VOCERA service
Destination	Select a destination option. You can allow or deny access to any the following destinations based on your requirements. - **To all destinations**– Access is allowed or denied to all destinations. - **To a particular server**–Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. - **Except to a particular server**–Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. - **To a network**–Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. - **Except to a network**–Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. - **To domain name**–Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the **Domain Name** text box.
Log	Select this check box if you want a log entry to be created when this rule is triggered. Instant firewall supports firewall based logging function. Firewall logs on the IAPs are generated as syslog messages.
Blacklist	Select the **Blacklist** check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Clients on page 162.
Classify media	Select the **Classify media** check box to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows: - Video: Priority 5 (Critical) - Voice: Priority 6 (Internetwork Control)
Disable scanning	Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled, For more information, see Configuring Radio Settings for an IAP on page 226.
DSCP tag	Select the **DSCP tag** check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0 to 63. To assign a higher priority, specify a higher value.

Table 30: *Access Rule Configuration Parameters*

Field	Description
802.1p priority	Select the **802.1p priority** check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

6. Click **OK** and then click **Finish**.

In the CLI

To configure access rules:

```
(Instant Access Point)(config)# wlan access-rule <access-rule-name>
(Instant Access Point)(Access Rule <Name>)# rule <dest> <mask> <match> <protocol> <start-port>
<end-port> {permit |deny | src-nat | dst-nat {<IP-address> <port> | <port>}}[<option1…option
9>]
(Instant Access Point)(Access Rule <Name>)# end
(Instant Access Point)# commit apply
```

Configuring Network Address Translation

Network Address Translation (NAT) is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and private (local network), which allows translation of private network IP addresses to a public address space.

Instant supports the NAT mechanism to allow a routing device to use the translation tables to map the private addresses into a single IP address and packets are sent from this address, so that they appear to originate from the routing device. Similarly, if the packets are sent to the private IP address, the destination address is translated as per the information stored the translation tables of the routing device.

Configuring a Source NAT Access Rule

The source NAT action in access rules allows the user to override the routing profile entries. For example, when a routing profile is configured to use 0.0.0.0/0 , the client traffic on an SSID in L3 mode access to the corporate network is sent to the tunnel. When an access rule is configured with **Source NAT** action, the users can specify the service, protocol, or destination to which the source NAT is applied.

You can also configure source based routing to allow client traffic on one SSID to reach the Internet through the corporate network, while the other SSID can be used as an alternate uplink. You can create an access rule to perform source NAT by using the Instant UI or CLI.

In the Instant UI

To configure a source NAT access rule:

1. Navigate to the WLAN wizard or Wired settings window:
   - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure access rules for a wired profile, **More**>**Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab.
3. To configure access rules for the network, slide to **Network-based**. To configure access rules for user roles, slide to **Role-based** .
4. To create a new rule for the network, click **New**. To create an access rule for a user role, select the user role and then click **New**. The **New Rule** window is displayed.
5. In the **New Rule** window:

6. Select **Access control** from the **Rule type** drop-down list.
7. Select **Source-NAT** from the **Action** drop-down list, to allow changes to the source IP address.
8. Select a service from the list of available services.
9. Select the required option from the **Destination** drop-down.
10. If required, enable other parameters such as **Log**, **Blacklist**, **Classify media**, **Disable scanning**, **DSCP tag**, and **802.1p priority**.
11. Click **OK** and then click **Finish**.

In the CLI

To configure source NAT access rule:

```
(Instant Access Point)(config)# wlan access-rule <access_rule>
(Instant Access Point)(Access Rule "<access_rule>")# rule <dest> <mask> <match> <protocol> <sp
ort> <eport> src-nat
(Instant Access Point)(Access Rule "<access_rule>")# end
(Instant Access Point)# commit apply
```

Configuring Source-Based Routing

To allow different forwarding policies for different SSIDs, you can configure source-based routing. The source-based routing configuration overrides the routing profile configuration and allows any destination or service to be configured to have direct access to the Internet (bypassing VPN tunnel) based on the ACL rule definition. When source-based routing is enabled, the Virtual Controller performs source NAT by using its uplink IP address.

To configure source-based routing:

1. Ensure that an L3 subnet with the netmask, gateway, VLAN, and IP address is configured, For more information on configuring L3 subnet, see Configuring L3-Mobility on page 208.
2. Ensure that the source IP address is associated with the IP address configured for the L3 subnet.
3. Create an access rule for the SSID profile with Source NAT action as described in Configuring Source-Based Routing on page 177. The source NAT pool is configured and source based routing entry is created.

Configuring a Destination NAT Access Rule

Instant supports configuration of the destination NAT rule, which can be used to redirect traffic to the specified IP address and destination port. Destination-NAT configuration is supported only in the bridge mode without VPN.

You can configure a destination-NAT access rule by using the Instant UI or CLI.

In the Instant UI

To configure an destination NAT access rule:

1. Navigate to the WLAN wizard or Wired settings window:
   - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure access rules for a wired profile, **More**>**Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab.
3. To configure access rules for the network, slide to **Network-based**. To configure access rules for user roles, slide to **Role-based** .
4. To create a new rule for the network, click **New**. To create an access rule for a user role, select the user role and then click **New**. The **New Rule** window is displayed.
5. In the **New Rule** window:
6. Select **Access control** from the **Rule type** drop-down list.

7. Select **destination-NAT** from the **Action** drop-down list, to allow changes to the source IP address.
8. Specify the IP address and port details.
9. Select a service from the list of available services.
10. Select the required option from the **Destination** drop-down.
11. If required, enable other parameters such as **Log**, **Blacklist**, **Classify media**, **Disable scanning**, **DSCP tag**, and **802.1p priority**.
12. Click **OK** and then click **Finish**.

In the CLI

To configure destination NAT access rule:

```
(Instant Access Point)(config)# wlan access-rule <access_rule>
(Instant Access Point)(Access Rule "<access_rule>")# rule <dest> <mask> <match> <protocol> <sp
ort> <eport> dst-nat ip <IP-address> [<port>]
(Instant Access Point)(Access Rule "<access_rule>")# end
(Instant Access Point)# commit apply
```

Configuration Examples for Access Rules

This section provides procedures to create the following access rules.

- Allow POP3 Service to a Particular Server on page 178
- Allow TCP Service to a Particular Network on page 178
- Deny FTP Service except to a Particular Server on page 179
- Deny bootp Service except to a Particular Network on page 179

Allow POP3 Service to a Particular Server

To configure POP3 service to a particular server:

1. Select an existing wireless or wired profile. Depending on the network profile selected, the **Edit <WLAN-Profile>** or **Edit Wired Network** window is displayed.

NOTE

You can also configure access rules in the **Access** tab of the **New WLAN** and **New Wired Network** windows when configuring a new profile.

2. In the **Access** tab, slide to **Network-based** using the scroll bar to specify access rules for the network.
3. Click **New** to add a new rule. The **New Rule** window is displayed.
   a. Select **Allow** from the **Action** drop-down list.
   b. Select **pop3** from the **Service** drop-down list.
   c. Select **to a particular server** from the **Destination** drop-down list and enter appropriate IP address in the IP text box.
   d. Click **OK**.
4. Click **Finish**.

Allow TCP Service to a Particular Network

To allow TCP service to a particular server:

1. Select an existing wireless or wired profile. Depending on the network profile selected, the **Edit <WLAN-Profile>** or **Edit Wired Network** window is displayed.

NOTE

You can also configure access rules in the **Access** tab of the **New WLAN** and **New Wired Network** windows when configuring a new profile.

2. In the **Access** tab, slide to **Network-based** using the scroll bar to specify access rules for the network.
3. Click **New** to add a new rule. The **New Rule** window is displayed.
   a. Select **Allow** from the **Action** drop-down list.
   b. Select **Custom** from the **Service** drop-down list.
      - Select TCP from the Protocol drop-down list.
      - Enter appropriate port number in the **Ports** text box.
   c. 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.
   d. Click **OK.**
4. Click **Finish**.

Deny FTP Service except to a Particular Server

To define deny FTP service access rule except to a particular server:

1. Select an existing wireless or wired profile. Depending on the network profile selected, the **Edit <WLAN-Profile>** or **Edit Wired Network** window is displayed.

NOTE

You can also configure access rules in the **Access** tab of the **New WLAN** and **New Wired Network** windows when configuring a new profile.

2. In the **Access** tab, slide to **Network-based** using the scroll bar to specify access rules for the network.
3. Click **New** to add a new rule. The **New Rule** window is displayed.
   a. Select **Deny** from the **Action** drop-down list.
   b. Select **ftp** from the **Service** drop-down list.
   c. Select **except to a particular server** from the **Destination** drop-down list and enter appropriate IP address in the **IP** text box.
   d. Click **OK.**
4. Click **Finish**.

Deny bootp Service except to a Particular Network

To define deny bootp service access rule except to a network:

1. Select an existing wireless or wired profile. Depending on the network profile selected, the **Edit <WLAN-Profile>** or **Edit Wired Network** window is displayed.

NOTE

You can also configure access rules in the **Access** tab of the **New WLAN** and **New Wired Network** windows when configuring a new profile.

2. In the **Access** tab, slide to **Network-based** using the scroll bar to specify access rules for the network.
3. Click **New** to add a new rule. The **New Rule** window is displayed.
   a. Select **Deny** from the **Action** drop-down list.
   b. Select **bootp** from the **Service** drop-down list.
   c. Select **except to a network** from the **Destination** drop-down list.
      - Enter the appropriate IP address in the IP text box.
      - Enter the appropriate netmask in the Netmask text box.
   d. Click **OK.**

4. Click **Finish**.

Configuring User Roles

Every client in the Instant network is associated with a user role, which determines the client's network privileges, the frequency of reauthentication, and the applicable bandwidth contracts. The user role configuration on an IAP involves the following procedures:

- Creating a User Role on page 180
- Assigning Bandwidth Contracts to User Roles
- Configuring Machine and User Authentication Roles on page 181

Creating a User Role

You can create a user role by using Instant UI or CLI.

In the Instant UI

To create a user role:

1. Click the **Security** at the top right corner of Instant main window. The **Security** window is displayed.
2. Click **Roles** tab. The Roles tab contents are displayed.
3. Under Roles, click **New**.
4. Enter a name for the new role and click **OK**.

NOTE

You can also create a user role when configuring wireless or wired network profiles. For more information, see Configuring Access Rules for a WLAN SSID Profile on page 99 and Configuring Access Rules for a Wired Profile on page 110

In the CLI

To configure user roles and access rules:

```
(Instant Access Point)(config)# wlan access-rule <access-rule-name>
(Instant Access Point)(Access Rule <Name>)# rule <dest> <mask> <match> <protocol> <start-port>
<end-port> {permit |deny | src-nat | dst-nat {<IP-address> <port> | <port>}}[<option1…option
9>]
```

Assigning Bandwidth Contracts to User Roles

The administrators can manage bandwidth utilization by assigning maximum bandwidth rates, or bandwidth contracts to user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the IAP) or downstream (IAP to clients) traffic for a user role. The bandwidth contract will not be applicable to the user traffic on the bridged out (same subnet) destinations. For example, if clients are connected to an SSID, you can restrict the upstream bandwidth rate allowed for each user to 512 Kbps.

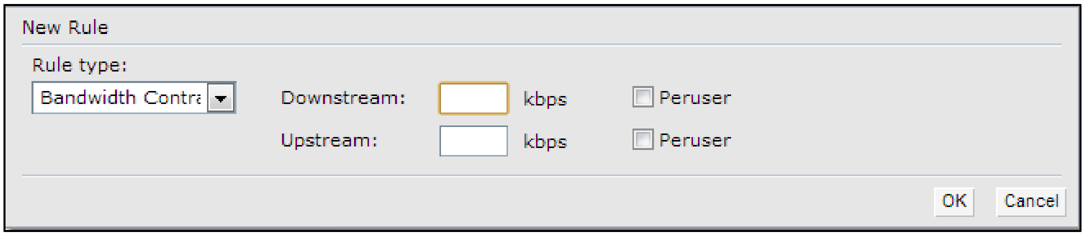
By default, all users that belong to the same role share a configured bandwidth rate for upstream or downstream traffic. The assigned bandwidth will be served and shared among all the users. You can also assign bandwidth per user to provide every user a specific bandwidth within a range of 1 to 65535 Kbps. If there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.

NOTE

In the earlier releases, bandwidth contract could be assigned per SSID. In the current release, the bandwidth contract can also be assigned for each SSID user. If the bandwidth contract is assigned for an SSID in Instant 6.2.1.0-3.4.0.0 image and when the IAP is upgraded to 6.3.1.1-4.0 release version, the bandwidth configuration per SSID will be treated as per-user downstream bandwidth contract for that SSID.

Assigning Bandwidth Contracts in the InstantUI

1. Click the **Security** at the top right corner of Instant main window. The **Security** window is displayed.
2. Click **Roles** tab. The **Roles** tab contents are displayed.
3. Create a new role or select an existing role.
4. Under Access Rules, click **New**. The **New Rule** window is displayed.
5. Select **Bandwidth Contract** from the **Rule Type** drop-down.



New Rule

Rule type: Bandwidth Contra

6. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select the **Peruser** checkbox.
7. Click **OK**.
8. Associate the user role to a WLAN SSID or wired profile.

You can also create a user role and assign bandwidth contracts while configuring an SSID or wired profile.

Assigning a bandwidth contract using Instant CLI:

To assign a bandwidth contract in the CLI:

```
(Instant Access Point)(config)# wlan access-rule <name>
(Instant Access Point) (Access Rule <name>)# bandwidth-limit {downstream <kbps>| upstream <kbp
s>| peruser { downstream <kbps>| upstream <kbps>}}
(Instant Access Point) (Access Rule <name>)# end
(Instant Access Point) # commit apply
```

To associate the access rule to a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# access-rule-name <access-rule-name>
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point) # commit apply
```

Configuring Machine and User Authentication Roles

You can assign different rights to clients based on whether their hardware device supports machine authentication. Machine Authentication is only supported on Windows devices, so this can be used to distinguish between Windows devices and other devices such as iPads.

You can create any of the following types of rules:

- Machine Auth only role - This indicates a Windows machine with no user logged in. The device supports machine authentication and has a valid RADIUS account, but a user has not yet logged in and authenticated.
- User Auth only role - This indicates a known user or a non-Windows device. The device does not support machine auth or does not have a RADIUS account, but the user is logged in and authenticated.

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

You can configure machine authentication with role-based access control using Instant UI or CLI.

In the Instant UI

To configure machine authentication with role-based access control, perform the following steps:

1. In the **Access** tab of the WLAN (**New WLAN** or **Edit <WLAN-profile>**) or Wired Network configuration (**New Wired Network** or **Edit Wired Network**) window, under **Roles**, create **Machine auth only** and **User auth only** roles.
2. Configure access rules for these roles by selecting the role, and applying the rule. For more information on configuring access rules, see Configuring Access Rules on page 173.
3. Select **Enforce Machine Authentication** and select the **Machine auth only** and **User auth only** roles.
4. Click **Finish** to apply these changes.

In the CLI

To configure machine and user authentication roles for a WLAN SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name># set-role-machine-auth <machine-authentication-onl
y> <user-authentication-only>
(Instant Access Point)(SSID Profile <name># end
(Instant Access Point)# commit apply
```

To configure machine and user authentication roles for wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# set-role-machine-auth <machine-authenticatio
n-only> <user-authentication-only>
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring Derivation Rules

Instant allows you to configure role and VLAN derivation-rules. You can configure these rules to assign a user role or VLAN to the clients connecting to an SSID or a wired profile.

Understanding Role Assignment Rule

When an SSID or wired profile is created, a default role for the clients connecting this SSID or wired profile is assigned. You can assign a user role to the clients connecting to an SSID by any of the following methods. The role assigned by some methods may take precedence over the roles assigned by the other methods.

RADIUS VSA Attributes

The user role can be derived from Aruba Vendor-Specific Attributes (VSA) for RADIUS server authentication. The role derived from an Aruba VSA takes precedence over roles defined by other methods.

MAC-Address Attribute

The first three octets in a MAC address are known as Organizationally Unique Identifier (OUI), and are purchased from the Institute of Electrical and Electronics Engineers, Incorporated (IEEE) Registration Authority. This identifier uniquely identifies a vendor, manufacturer, or other organization (referred to by the IEEE as the “assignee”) globally and effectively reserves a block of each possible type of derivative identifier (such as MAC addresses) for the exclusive use of the assignee.

IAPs use the OUI part of a MAC address to identify the device manufacturer and can be configures to assign a desired role for users who have completed 802.1X authentication and MAC authentication. The user role can be derived from the user attributes after a client associates with an AP. You can configure rules that assign a user role to clients that match a MAC address based criteria. For example, you can assign a voice role any client with a MAC address starting a0:a1:a2.

Roles Based on Client Authentication

The user role can be the default user role configured for an authentication method, such as 802.1x authentication. For each authentication method, you can configure a default role for clients who are successfully authenticated using that method.

DHCP Option and DHCP Fingerprinting

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

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

Table 31: *Validated DHCP Fingerprint*

Device	DHCP Option	DHCP Fingerprint
Apple iOS	Option 55	370103060F77FC
Android	Option 60	3C64686370636420342E302E3135
Blackberry	Option 60	3C426C61636B4265727279
Windows 7/Vista Desktop	Option 55	37010f03062c2e2f1f2179f92b
Windows XP(SP3, Home, Professional)	Option 55	37010f03062c2e2f1f21f92b
Windows Mobile	Option 60	3c4d6963726f736f66742057696e646f777320434500
Windows 7 Phone	Option 55	370103060f2c2e2f
Apple Mac OSX	Option 55	370103060f775ffc2c2e2f

Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client.

NOTE

When creating more than one role assignment rule, the first matching rule in the rule list is applied.

You can create a role assignment rules by using the Instant UI or CLI.

In the Instant UI

1. Navigate to the WLAN wizard or Wired settings window:
   - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure access rules for a wired profile, **More**>**Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab.
3. Under **Role Assignment Rules**, click **New**. The **New Role Assignment** window allows you to define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server.

4. Select the attribute from the **Attribute** drop-down list that the rule it matches against. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA on page 141.
5. Select the operator from the **Operator** drop-down list. The following types of operators are supported:
   - **contains**– The rule is applied only if the attribute value contains the string specified in *Operand*.
   - **Is the role**– The rule is applied if the attribute value is the role.
   - **equals**– The rule is applied only if the attribute value is equal to the string specified in *Operand*.
   - **not-equals**– The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
   - **starts-with**– The rule is applied only if the attribute value starts with the string specified in *Operand*.
   - **ends-with**– The rule is applied only if the attribute value ends with string specified in *Operand*.
   - **matches-regular-expression**– The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.
6. Enter the string to match in the **String** text box.
7. Select the appropriate role from the **Role** drop-down list.
8. Click **OK**.

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

In the CLI

To configure role assignment rules for a WLAN SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-wi
th|ends-with|contains|matches-regular-expression} <operator><role>|value-of}
(Instant Access Point)(SSID Profile <name># end
(Instant Access Point)# commit apply
```

To configure role assignment rules for a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(wired ap profile <name>)# set-role <attribute>{{equals|not-equal|start
s-with|ends-with|contains}<operator> <role>| value-of}
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Example

```
(Instant Access Point)(config)# wlan ssid-profile Profile1
(Instant Access Point)(SSID Profile "Profile1")# set-role mac-address-and-dhcp-options matche
s-regular-expression \bring\b Profile1
(Instant Access Point)(SSID Profile"Profile1")# end
(Instant Access Point)# commit apply
```

Understanding VLAN Assignment

You can assign VLANs to a client based on the following configuration conditions:

- The default VLAN configured for the WLAN can be assigned to a client.
- If VLANs are configured for a WLAN SSID or an Ethernet port profile, the VLAN for client can be derived before the authentication, from the rules configured for these profiles.
- If a rule derives a specific VLAN, it is prioritized over the user roles that may have a VLAN configured.

- The user VLANs can be derived from the default roles configured for 802.1X authentication or MAC authentication.
- After client authentication, the VLAN can be derived from Vendor Specific Attributes (VSA) for RADIUS server authentication.
- The DHCP-based VLANs can be derived for Captive Portal authentication.

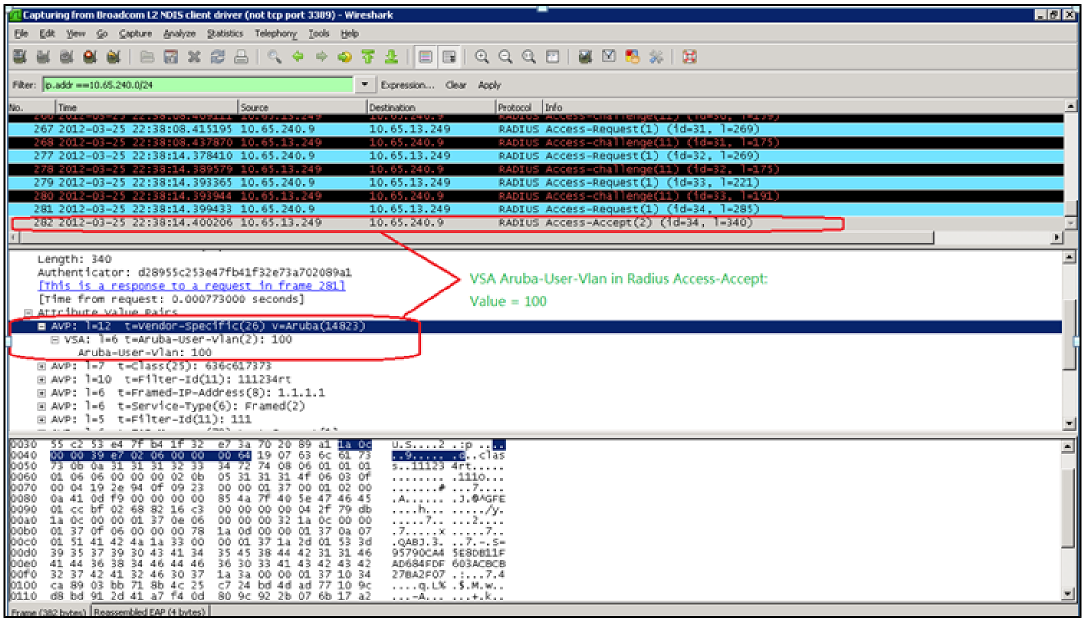
NOTE

Instant supports role derivation based on DHCP option for Captive Portal authentication. When the Captive Portal authentication is successful, the role derivation based on DHCP option assigns a new user role to the guest users, instead of the pre-authenticated role.

Vendor Specific Attributes (VSA)

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

Figure 58 *RADIUS Access-Accept packets with VSA*


Capturing from Broadcom L2 NDIS client driver (not tcp port 3389) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: ip.addr ==10.65.240.0/24
Expression... Clear Apply
Frame (382 bytes) Reassembled EAP (4 bytes)

```
No.  Time                       Source          Destination     Protocol Info
267 2012-03-25 22:38:08.415195 10.65.240.9    10.65.13.249    RADIUS Access-Request(1) (id=31, l=269)
268 2012-03-25 22:38:08.437870 10.65.13.249   10.65.240.9     RADIUS Access-challenge(11) (id=31, l=175)
277 2012-03-25 22:38:14.378410 10.65.240.9    10.65.13.249    RADIUS Access-Request(1) (id=32, l=269)
278 2012-03-25 22:38:14.389579 10.65.13.249   10.65.240.9     RADIUS Access-challenge(11) (id=32, l=175)
279 2012-03-25 22:38:14.393365 10.65.240.9    10.65.13.249    RADIUS Access-Request(1) (id=33, l=221)
280 2012-03-25 22:38:14.393944 10.65.13.249   10.65.240.9     RADIUS Access-challenge(11) (id=33, l=191)
281 2012-03-25 22:38:14.399433 10.65.240.9    10.65.13.249    RADIUS Access-Request(1) (id=34, l=285)
282 2012-03-25 22:38:14.400206 10.65.13.249   10.65.240.9     RADIUS Access-Accept(2) (id=34, l=340)
```

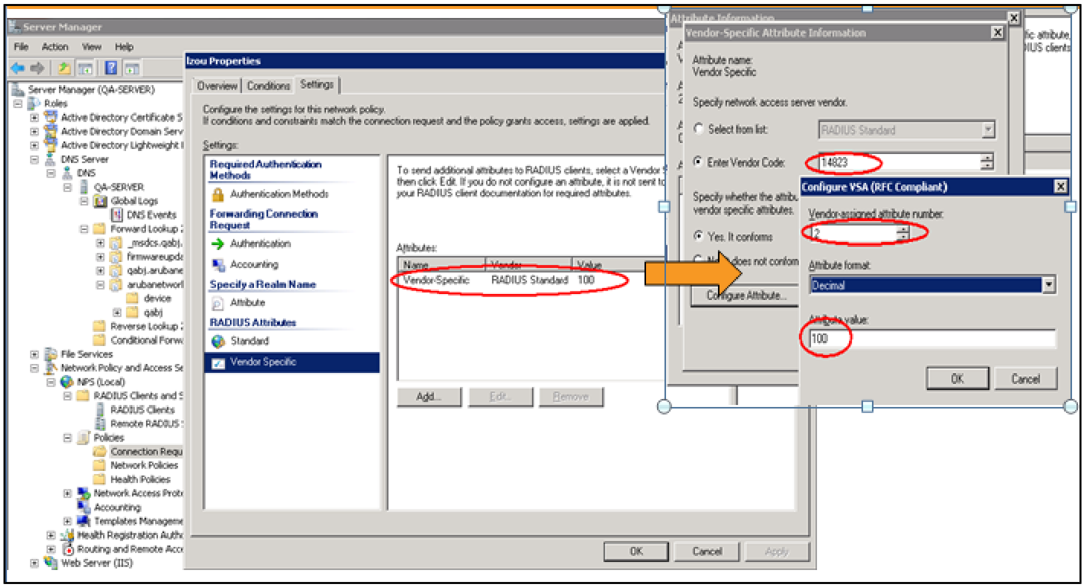
```
    Length: 340
    Authenticator: d28955c253e47fb41f32e73a702089a1
    [This is a response to a request in frame 281]
    [Time from request: 0.000773000 seconds]
  ⊟ Attribute Value Pairs
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Aruba(14823)
      ⊟ VSA: l=6 t=Aruba-User-Vlan(2): 100
          Aruba-User-Vlan: 100
    ⊞ AVP: l=7  t=Class(25): 636c617373
    ⊞ AVP: l=10  t=Filter-Id(11): 111234rt
    ⊞ AVP: l=6  t=Framed-IP-Address(8): 1.1.1.1
    ⊞ AVP: l=6  t=Service-Type(6): Framed(2)
    ⊞ AVP: l=5  t=Filter-Id(11): 111
```

VSA Aruba-User-Vlan in Radius Access-Accept:

Value = 100

```
0030  55 c2 53 e4 7f b4 1f 32  e7 3a 70 20 89 a1 1a 0c   U.S....2 .:p ....
0040  00 00 39 e7 02 06 00 00  00 64 19 07 63 6c 61 73   ..9..... .d..clas
0050  73 0b 0a 31 31 31 32 33  34 72 74 08 06 01 01 01   s..11123 4rt.....
0060  01 06 06 00 00 00 02 0b  05 31 31 31 4f 06 03 0f   ........ .111o...
0070  00 04 19 2e 94 0f 09 23  00 00 01 37 00 01 02 00   .......# ...7....
0080  0a 41 0d f9 00 00 00 00  85 4a 7f 40 5e 47 46 45   .A...... .J.@^GFE
0090  01 cc bf 02 68 82 16 c3  00 00 00 00 04 2f 79 db   ....h... ...../y.
00a0  1a 0c 00 00 01 37 0e 06  00 00 00 32 1a 0c 00 00   .....7.. ...2....
00b0  01 37 0f 06 00 00 00 78  1a 0d 00 00 01 37 0a 07   .7.....x .....7..
00c0  01 51 41 42 4a 1a 33 00  00 01 37 1a 2d 01 53 3d   .QABJ.3. ..7.-.S=
00d0  39 35 37 39 30 43 41 34  35 45 38 44 42 31 31 46   95790CA4 5E8DB11F
00e0  41 44 36 38 34 46 44 46  36 30 33 41 43 42 43 42   AD684FDF 603ACBCB
00f0  32 37 42 41 32 46 30 37  1a 3a 00 00 01 37 10 34   27BA2F07 .:...7.4
0100  ca 89 03 bb 71 8b 4c 25  c7 24 bd 4d ad 77 10 9c   ....q.L% .$.M.w..
0110  d8 bd 91 2d 41 a7 f4 0d  80 9c 92 2b 07 6b 17 a2   ...-A... ...+.k..
```

Figure 59 *Configure VSA on a RADIUS Server*



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a Vendor S then click Edit. If you do not configure an attribute, it is not sent to your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	100

Attribute name:
Vendor Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

● Enter Vendor Code: 14823

Specify whether the attribu vendor specific attributes.

● Yes. It conforms

○ No. It does not conform

Vendor-assigned attribute number: 2

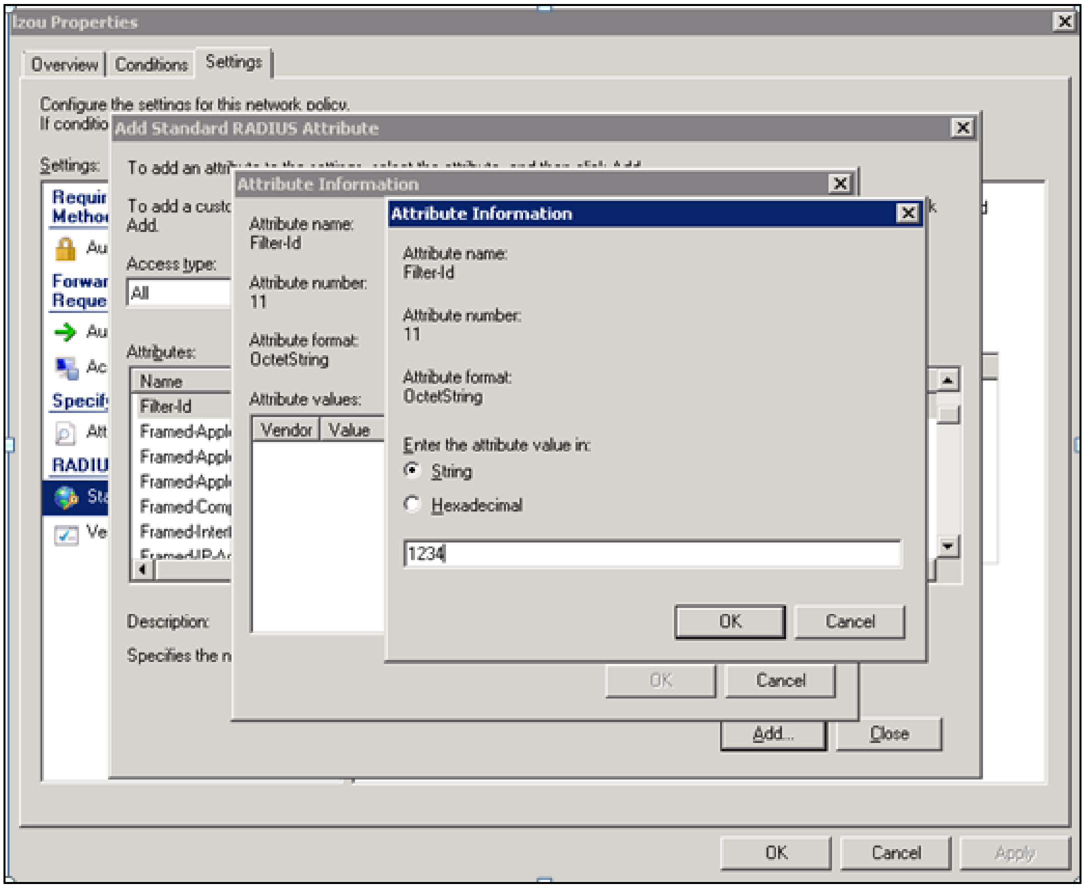
Attribute format: Decimal

Attribute value: 100

VLAN Assignment Based on Derivation Rules

When an external RADIUS server is used for authentication, the RADIUS server may return a reply message for authentication. If the RADIUS server supports return attributes, and sets an attribute value to the reply message, the IAP can analyze the return message and match attributes with a user pre-defined VLAN derivation rule. If the rule is matched, the VLAN value defined by the rule is assigned to the user. For a complete list of RADIUS server attributes, see Supported VSAs on page 142.

Figure 60 *Configuring RADIUS Attributes on the RADIUS Server*



Configure the settings for this network policy.
If conditio

To add an attri

To add a custo
Add.

Access type:
All

Specifies the n

Attribute name:
Filter-Id

Attribute number:
11

Attribute format:
OctetString

Attribute name:
Filter-Id

Attribute number:
11

Attribute format:
OctetString

Enter the attribute value in:
● String
○ Hexadecimal

1234

User Role

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

VLANs Created for an SSID

If the VSA and VLAN derivation rules are not matching, and the User Role does not contain a VLAN, the user VLAN can be derived by VLANs configured for an SSID or Ethernet port profile.

Configuring VLAN Derivation Rules

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

You can configure VLAN derivation rules for an SSID profile by using the Instant UI or CLI.

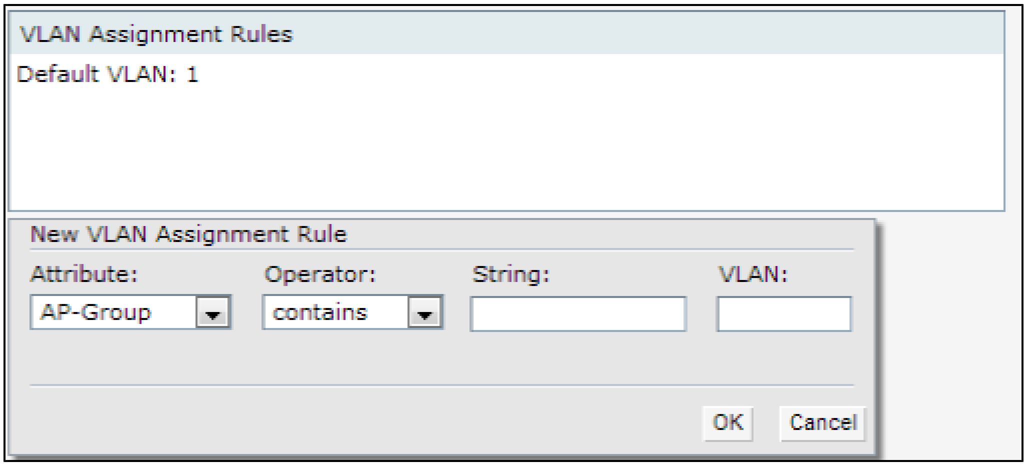
In the Instant UI

1. Perform the following steps:

- To configure VLAN derivation rule for a WLAN SSID profile, Click **Network**>**New**>**New WLAN**>**VLAN** or **Network**>**edit**>**Edit <WLAN-profile>**>**VLAN**. Select the **Dynamic** option under the **Client VLAN assignment**.
- To configure VLAN derivation rule for a wired network profile, click **Wired**>**New**>**New Wired Network**>**VLAN** or **Wired**>**Edit**>**Edit Wired Network**>**VLAN**.

2. Click **New** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server.

Figure 61 *VLAN Assignment Rule Window*



VLAN Assignment Rules

Default VLAN: 1

New VLAN Assignment Rule

Attribute: AP-Group

Operator: contains

String:

VLAN:

3. Select the attribute from the **Attribute** drop-down list. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA on page 141.
4. Select the operator from the **Operator** drop-down list. The following types of operators are supported:
   - **contains**– The rule is applied only if the attribute value contains the string specified in *Operand*.
   - **equals**– The rule is applied only if the attribute value is equal to the string specified in *Operand*.
   - **not-equals** – The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
   - **starts-with** – The rule is applied only if the attribute value starts with the string specified in *Operand*.
   - **ends-with** – The rule is applied only if the attribute value ends with string specified in *Operand*.
   - **matches-regular-expression** – The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.
5. Enter the string to match in the **String** field.
6. Select the appropriate VLAN ID from the **VLAN** drop-down list.
7. Click **OK**.
8. Ensure that all other required parameters are configured.
9. Click **Finish** to apply the changes.

In the CLI

To create a VLAN assignment rule for WLAN SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals|starts-wit
h|ends-with|contains|matches-regular-expression}<operator><VLAN-ID>|value-of}
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

To configure a VLAN assignment rule for a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <nname>
(Instant Access Point)(wired ap profile <name>)# set-vlan <attribute>{equals|not-equals|start
s-with|ends-with|contains}<operator><VLAN-ID>|value-of}
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Example

```
(Instant Access Point)(config)# wlan ssid-profile Profile1
(Instant Access Point)(SSID Profile "Profile1")# set-vlan mac-address-and-dhcp-options matche
s-regular-expression ..link 100
(Instant Access Point)(SSID Profile "Profile1")# end
(Instant Access Point)# commit apply
```

Using Advanced Expressions in Role and VLAN Derivation Rules

For complex policies of role and VLAN derivation using device DHCP fingerprints, you can use a regular expression to match against the combined string of the MAC address and the DHCP options. The combined string is formed by concatenating the hexadecimal presentation of the MAC address and all of the DHCP options sent by a particular device. The regular expression is a powerful pattern description language that can be used to perform advanced pattern matching of the above string.

If the combined device fingerprint string matches the specified regular expression, the role or vlan can be set to the WLAN client.

The following table lists some of the most commonly used regular expressions, which can be used in user role and user VLAN derivation rules:

Operator	Description
.	Matches any character. For example, l..k matches lack, lark, link, lock, look, Lync and so on.
\	Matches the character that follows the backslash. For example, \192.\.0\.. matches IP addresses ranges that starting with 192.0, such as 192.0.1.1. The expression looks only for the single characters that match.
[ ]	Matches any one character listed between the brackets. For example, [bc]lock matches block and clock.
\b	Matches the words that begin and end with the given expression. For example, \bdown matches downlink, linkdown, shutdown.
\B	Matches the middle of a word. For example, \Bvice matches services, devices, serviceID, deviceID, and so on.
^	Matches the characters at starting position in a string. For example, ^bcd matches bcde or bcdf, but not abcd.
[^]	Matches any characters that are not listed between the brackets. For example, [^u]link matches downlink, link, but not uplink.
?	Matches any one occurrence of the pattern. For example, ?est matches best, nest, rest, test and so on.
$	Matches the end of an input string. For example, eth$ matches Eth, but not Ethernet.
*	Matches the declared element multiple times if it exists. For example, eth* matches all occurrences of eth, such as Eth, Ethernet, Eth0 and so on.

Operator	Description
+	Matches the declared element one or more times. For example, aa+ matches occurrences of aa and aaa.
( )	Matches nested characters. For example, (192)* matches any number of the character string 192.
|	Matches the character patterns on either side of the vertical bar. You can use this expression to construct a series of options.
\<	Matches the beginning of the word. For example, \<wire matches wired, wireless and so on.
\>	Matches the end of the word. For example, \>list matches blacklist, whitelist, and so on.
{n}	Where n is an integer" Matches the declared element exactly the n times. For example, {2}link matches uplink, but not downlink.
{n,}	Where n is an integer" Matches the declared element at n times. For example, {2,}ink matches downlink, but not uplink.

For information on how to use regular expressions in role and VLAN derivation rules, see the following topics:

- Configuring VLAN Derivation Rules on page 186
- Creating a Role Derivation Rule on page 183

Configuring a User Role for VLAN Derivation

This section describes the following procedures:

- Creating a User VLAN Role on page 189
- Assigning User VLAN Roles to a Network Profile on page 190

Creating a User VLAN Role

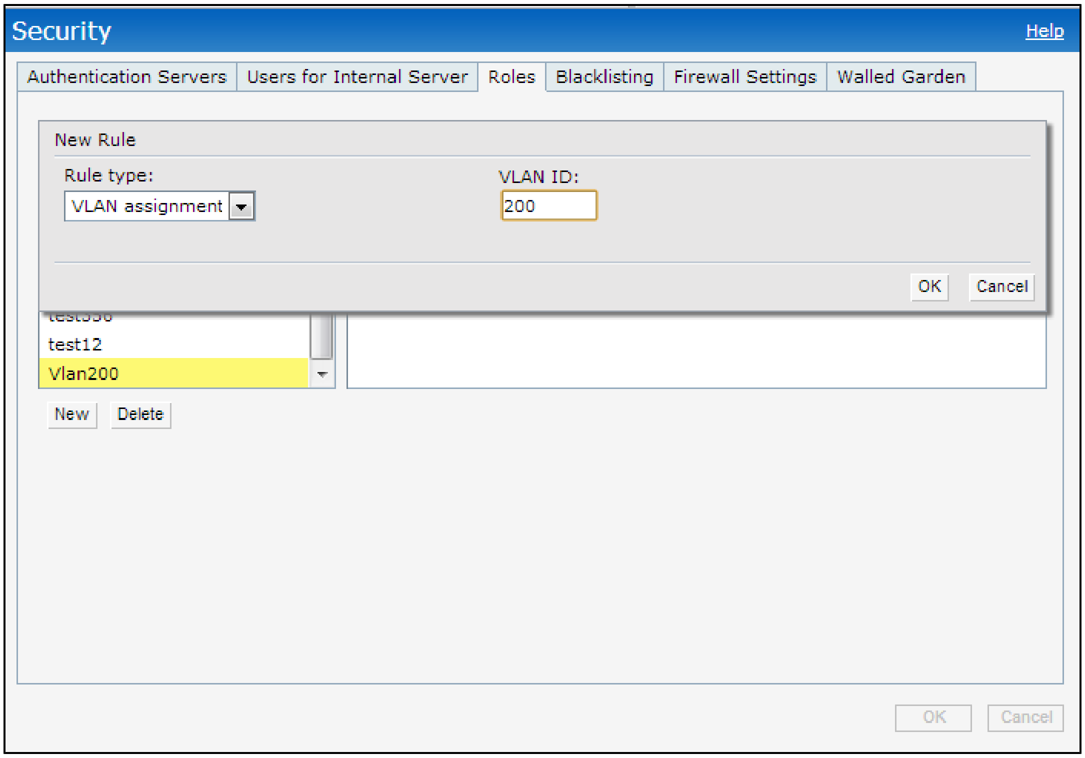
You can create a user role for VLAN derivation using the Instant UI or CLI

In the Instant UI

To configure a user role for VLAN derivation:

1. Click the **Security** at the top right corner of Instant main window.
2. Click **Roles** tab. The Roles tab contents are displayed.
3. Under Roles, click **New**.
4. Enter a name for the new role and click **OK**.
5. Under the **Access rules**, click **New**.
6. Select the **Rule type** as **VLAN assignment**.
7. Enter the ID of the VLAN in the **VLAN ID** text box. The following figure shows an example of a user VLAN role:

Figure 62 *Configuring User Role for VLAN Derivation*



Rule type: VLAN assignment

VLAN ID: 200

8. Click **OK**.

In the CLI

To create a VLAN role:

```
(Instant Access Point)(config)# wlan access-rule <rule-name>
(Instant Access Point)(Access Rule <rule-name>)# vlan 200
(Instant Access Point)(Access Rule <rule-name>)# end
(Instant Access Point)# commit apply
```

Assigning User VLAN Roles to a Network Profile

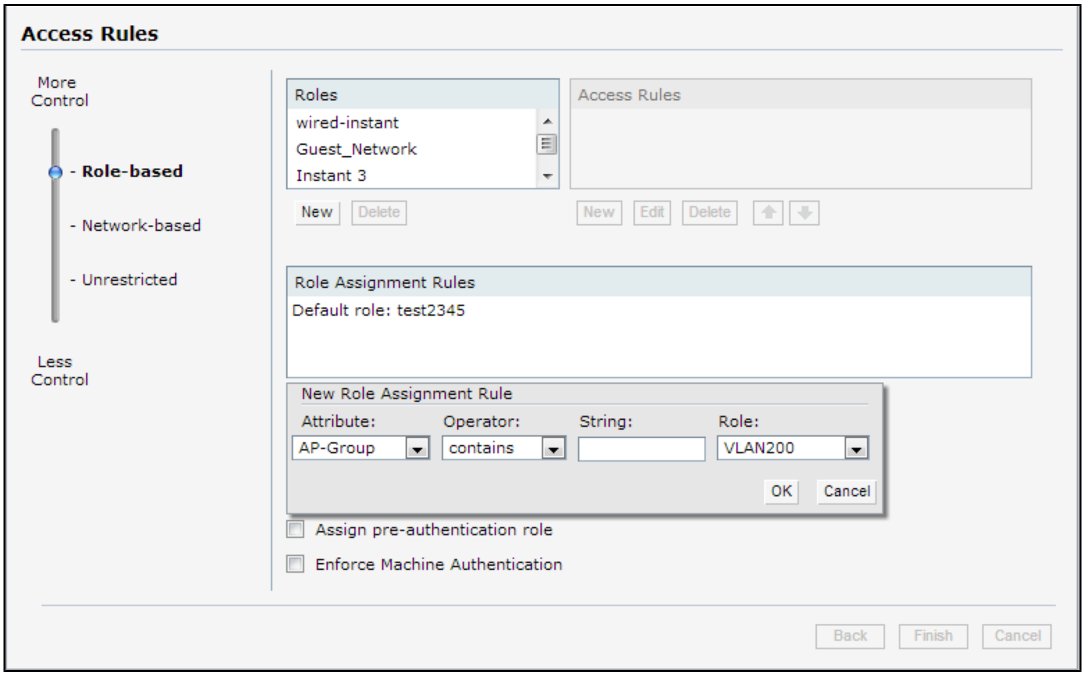
You can configure user VLAN roles for a network profile using Instant UI or CLI.

In the Instant UI

To assign a user VLAN role:

1. Click **Network**>**New**>**New WLAN**>**Access** or **Network**>**edit**>**Edit <WLAN-profile>**>**Access**.
2. Ensure that the slider is at the **Role-based** option.
3. Click **New** under the **New Role Assignment** and configure the following parameters:
   a. Select the attribute from the **Attribute** drop-down list.
   b. Select the operator to match from the **Operator** drop-down list.
   c. Enter the string to match in the **String** text box.
   d. Select the role to be assigned from the **Role** text box. The following figure shows an example for the VLAN role assignment:

Figure 63 *User VLAN Role Assignment*



Access Rules

Roles
wired-instant
Guest_Network
Instant 3

Role Assignment Rules
Default role: test2345

New Role Assignment Rule
Attribute: AP-Group
Operator: contains
String:
Role: VLAN200

☐ Assign pre-authentication role
☐ Enforce Machine Authentication

4. Click **OK**.

In the CLI

To assign VLAN role to a WLAN profile:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# set-role <attribute>{{equals <operator> <role>| n
ot-equals <operator> <role> | starts-with <operator> <role> | ends-with <operator> <role> |con
tains <operator> <role>}|value-of}
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

Chapter 13
Uplink Configuration

This chapter provides the following information:

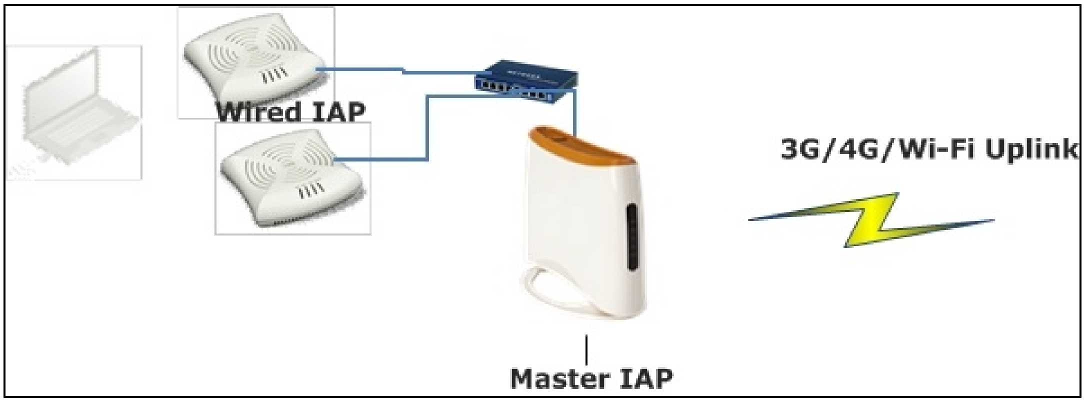
- Uplink Interfaces on page 193
- Ethernet Uplink on page 194
- 3G/4G Uplink on page 196
- Wi-Fi Uplink on page 200
- Uplink Preferences and Switching on page 201

Uplink Interfaces

Instant network supports Ethernet, 3G and 4G USB modems, and the Wi-Fi uplink to provide access to the corporate Instant network. The 3G/4G USB modems and the Wi-Fi uplink can be used to extend the connectivity to places where an Ethernet uplink cannot be configured. It also provides a reliable backup link for the Ethernet based Instant network.

The following figure illustrates a scenario in which the IAPs join the Virtual Controller as slave IAPs through a wired or mesh Wi-Fi uplink:

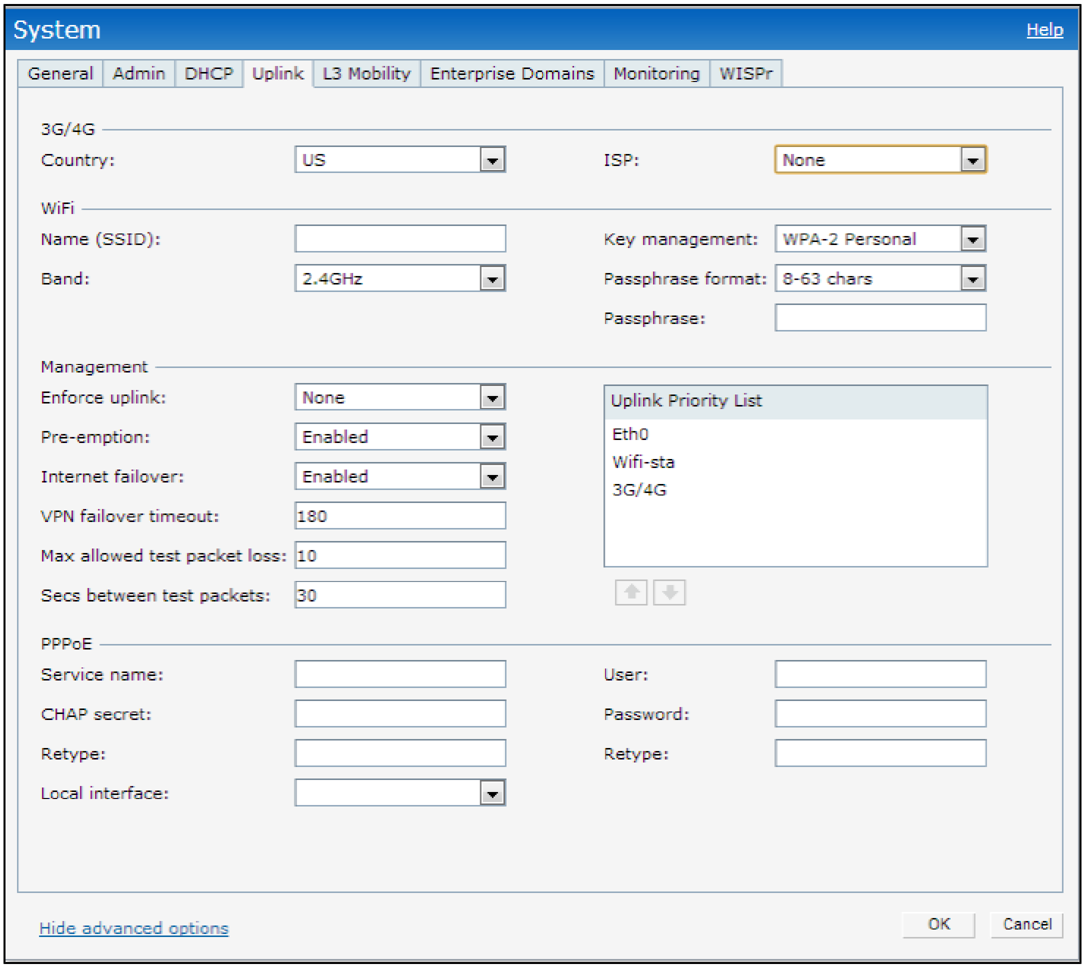
Figure 64 *Uplink Types*



The following types of uplinks are supported on Instant:

- Ethernet Uplink
- 3G/4G Uplink
- Wi-Fi Uplink

The following figure shows the window for configuring uplinks in the Instant UI:



System

3G/4G

Country: US

ISP: None

WiFi

Name (SSID):

Key management: WPA-2 Personal

Band: 2.4GHz

Passphrase format: 8-63 chars

Passphrase:

Management

Enforce uplink: None

Pre-emption: Enabled

Internet failover: Enabled

VPN failover timeout: 180

Max allowed test packet loss: 10

Secs between test packets: 30

Uplink Priority List

Eth0
Wifi-sta
3G/4G

PPPoE

Service name:

User:

CHAP secret:

Password:

Retype:

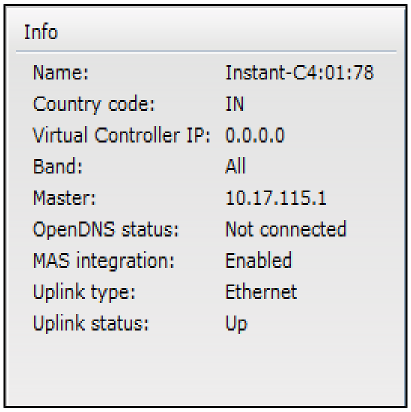
Retype:

Local interface:

Ethernet Uplink

The Ethernet 0 port on an IAP is enabled as an uplink port by default. You can view the type of uplink and the status of the uplink in the Instant in the **Info** tab.

Figure 65 *Uplink Status*



Info

Name:	Instant-C4:01:78
Country code:	IN
Virtual Controller IP:	0.0.0.0
Band:	All
Master:	10.17.115.1
OpenDNS status:	Not connected
MAS integration:	Enabled
Uplink type:	Ethernet
Uplink status:	Up

Ethernet uplink supports the following types of configuration in this Instant release.

- PPPoE
- DHCP
- Static IP

You can use PPPoE for your uplink connectivity in both IAP and IAP-VPN deployments. PPPoE is supported only in a single AP deployment.

Uplink redundancy with the PPPoE link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections. The IAP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP). Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After configuring PPPoE, reboot the IAP for the configuration to affect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during IAP boot and if the configuration is correct, Ethernet is used for the uplink connection.

When PPPoE is used, do not configure Dynamic RADIUS Proxy and IP address of the Virtual Controller. An SSID created with default VLAN is not supported with PPPoE uplink.

You can also configure an alternate Ethernet uplink to enable uplink failover when an Ethernet port fails.

Configuring PPPoE Uplink Profile

You can configure PPPOE settings from the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at the top right corner of the Instant main window. The **System** window is displayed.
2. Click the **Show advanced options** link. The advanced options are displayed.
3. In the **Uplink** tab, perform the following steps in the **PPPoE** section:
   a. Enter the **PPPoE service name** provided by your service provider in the **Service name** field.
   b. In the **CHAP secret** and **Retype** fields, enter the secret key used for Challenge Handshake Authentication Protocol (CHAP) authentication. You can use a maximum of 34 characters for the CHAP secret key.
   c. Enter the user name for the PPPoE connection in the **User** field.
   d. In the **Password** and **Retype** fields, enter a password for the PPPoE connection and confirm it.
4. To set a local interface for the PPPoE uplink connections, select a value from the **Local Configuration** drop-down. The selected DHCP scope will be used as a local interface on the PPPoE interface and the Local,L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and allows the entire Local,L3 DHCP subnet to be allocated to clients.

The options in the **Local Configuration** drop-down appear only if a Local,L3 DHCP scope is configured on the IAP.

5. Click **OK**.
6. Reboot the IAP for the configuration to affect.

In the CLI

To configure a PPPoE uplink connection:

```
(Instant Access Point)(config) # pppoe-uplink-profile
(Instant Access Point)(pppoe-uplink-profile)# pppoe-svcname <service-name>
(Instant Access Point)(pppoe-uplink-profile)# pppoe-username <username>
(Instant Access Point)(pppoe-uplink-profile)# pppoe-passwd <password>
(Instant Access Point)(pppoe-uplink-profile)# pppoe-chapsecret <password>
(Instant Access Point)(pppoe-uplink-profile)# pppoe-unnumbered-local-l3-dhcp-profile <dhcp-pro
file>
```

```
(Instant Access Point)(pppoe-uplink-profile)# end
(Instant Access Point)# commit apply
```

To view the PPPoE configuration:

```
(Instant Access Point)# show pppoe config

PPPoE Configuration
-------------------
Type                     Value
----                     -----
User                     testUser
Password                 3c28ec1b82d3eef0e65371da2f39c4d49803e5b2bc88be0c
Service name             internet03
CHAP secret              8e87644deda9364100719e017f88ebce
Unnumbered dhcp profile  dhcpProfile1
```

To view the PPPoE status:

```
(Instant Access Point)# show pppoe status

pppoe uplink state:Suppressed.
```

3G/4G Uplink

Instant supports the use of 3G/4G USB modems to provide the Internet backhaul to an Instant network. The 3G/4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the RAPs to automatically choose the available network in a specific region.

The 3G and 4G LTE USB modems can be provisioned on RAP-3WN/3WNP, RAP-108, and RAP-155/155P.

Types of Modems

Instant supports the following three types of 3G modems:

- **True Auto Detect**– Modems of this type can be used only in one country and for a specific ISP. The parameters are configured automatically and hence no configuration is necessary.
- **Auto-detect + ISP/country**– Modems of this type require the user to specify the Country and ISP. The same modem is used for different ISPs with different parameters configured for each of them.
- **No Auto-detect**– Modems of this type are used only if they share the same Device-ID, Country, and ISP details. You need to configure different parameters for each of them. These modems work with Instant when the appropriate parameters are configured.

The following table lists the types of supported 3G modems:

Table 32: *List of Supported 3G Modems*

Modem Type	Supported 3G Modems
True Auto Detect	● USBConnect 881 (Sierra 881U) ● Quicksilver (Globetrotter ICON 322) ● UM100C (UTstarcom) ● Icon 452 ● Aircard 250U (Sierra) ● USB 598 (Sierra) ● U300 (Franklin wireless) ● U301 (Franklin wireless) ● USB U760 for Virgin (Novatel)

Table 32: *List of Supported 3G Modems*

Modem Type	Supported 3G Modems
	• USB U720 (Novatel/Qualcomm) • UM175 (Pantech) • UM150 (Pantech) • UMW190(Pantech) • SXC-1080 (Qualcomm) • Globetrotter ICON 225 • UMG181 • NTT DoCoMo L-05A (LG FOMA L05A) • NTT DoCoMo L-02A • ZTE WCDMA Technologies MSM (MF668?) • Fivespot (ZTE) • c-motech CNU-600 • ZTE AC2736 • SEC-8089 (EpiValley) • Nokia CS-10 • NTT DoCoMo L-08C (LG) • NTT DoCoMo L-02C (LG) • Novatel MC545 • Huawei E220 for Movistar in Spain • Huawei E180 for Movistar in Spain • ZTE-MF820 • Huawei E173s-1 • Sierra 320 • Longcheer WM72 • U600 (3G mode)
Auto-detect + ISP/country	• Sierra USB-306 (HK CLS/1010 (HK)) • Sierra 306/308 (Telstra (Aus)) • Sierra 503 PCIe (Telstra (Aus)) • Sierra 312 (Telstra (Aus)) • Aircard USB 308 (AT&T's Shockwave) • Compass 597(Sierra) (Sprint) • U597 (Sierra) (Verizon) • Tstick C597(Sierra) (Telecom(NZ)) • Ovation U727 (Novatel) (Sprint) • USB U727 (Novatel) (Verizon) • USB U760 (Novatel) (Sprint) • USB U760 (Novatel) (Verizon) • Novatel MiFi 2200 (Verizon Mifi 2200) • Huawei E272, E170, E220 (ATT) • Huawei E169, E180,E220,E272 (Vodafone/SmarTone (HK)) • Huawei E160 (O2(UK)) • Huawei E160 (SFR (France)) • Huawei E220 (NZ and JP) • Huawei E176G (Telstra (Aus)) • Huawei E1553, E176 (3/HUTCH (Aus)) • Huawei K4505 (Vodafone/SmarTone (HK)) • Huawei K4505 (Vodafone (UK)) • ZTE MF656 (Netcom (norway)) • ZTE MF636 (HK CSL/1010) • ZTE MF633/MF636 (Telstra (Aus)) • ZTE MF637 (Orange in Israel) • Huawei E180, E1692,E1762 (Optus (Aus)) • Huawei E1731 (Airtel-3G (India)) • Huawei E3765 (Vodafone (Aus))

Table 32: *List of Supported 3G Modems*

Modem Type	Supported 3G Modems
	● Huawei E3765 (T-Mobile (Germany) ● Huawei E1552 (SingTel) ● Huawei E1750 (T-Mobile (Germany)) ● UGM 1831 (TMobile) ● Huawei D33HW (EMOBILE(Japan)) ● Huawei GD01 (EMOBILE(Japan)) ● Huawei EC150 (Reliance NetConnect+ (India)) ● KDDI DATA07(Huawei) (KDDI (Japan)) ● Huawei E353 (China Unicom) ● Huawei EC167 (China Telecom) ● Huawei E367 (Vodafone (UK)) ● Huawei E352s-5 (T-Mobile (Germany))
No auto-detect	● Huawei D41HW ● ZTE AC2726

Table 33: *4G Supported Modem*

Modem Type	Supported 4G Modem
True Auto Detect	● Pantech UML290 ● Ether-lte

> When UML290 runs in auto detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Configuring Cellular Uplink Profiles

You can configure 3G or 4G uplinks using the Instant UI or CLI.

In the Instant UI

1. Click the **System** link at the upper right corner of the Instant main window. The **System** window is displayed.
2. In the **System** window, click the **show advanced settings** link. The advanced options are displayed.
3. Click the **Uplink** tab and perform any of the following steps:
   - To configure a 3G or 4G uplink automatically, select the **Country** and **ISP**. The parameters are automatically populated.
   - To configure a 3G or 4G uplink manually, perform the following steps:

     a. Obtain the modem configuration parameters from the local IT administrator or the modem manufacturer.

     b. Enter the type of the 3G/4G modem driver type:

        - For 3G – Enter the type of 3G modem in the **USB type** text box.
        - For 4G – Enter the type of 4G modem in the **4G USB type** text box.

     c. Enter the device ID of modem in the **USB dev** text box.

   d. Enter the TTY port of the modem in the **USB tty** text box.
   e. Enter the parameter to initialize the modem in the **USB init** text box.
   f. Enter the parameter to dial the cell tower in the **USB dial** text box.
   g. Enter the username used to dial the ISP in the **USB user** text box.
   h. Enter the password used to dial the ISP in the **USB password** text box.
   i. Enter the parameter used to switch a modem from the storage mode to modem mode in the **USB mode switch** text box.

4. To configure 3G/4G switch network, provide the driver type for the 3G modem in the **USB type** text box and the driver type for 4G modem in the **4G USB type** text box.
5. Click **OK**.
6. Reboot the IAP for changes to affect.

NOTE

In the Instant UI, you can view the list of country and ISP in the **Country** and **ISP** drop-down lists. You can either use the country or ISP to configure the modem, or configure the individual modem parameters manually. If you cannot view the list of country or ISP from the drop-down list, configure the modem parameters manually. Contact your IT administrator or the manufacturer of your modem to obtain the parameter details.

In the CLI

To configure a 3G cellular uplink profile:

```
(Instant Access Point)(config) # cellular-uplink-profile
(Instant Access Point)(cellular-uplink-profile)# usb-type <3G-usb-type>
(Instant Access Point)(cellular-uplink-profile)# modem-country <country>
(Instant Access Point)(cellular-uplink-profile)# modem-isp <service-provider-name>
(Instant Access Point)(cellular-uplink-profile)# usb-auth-type <usb_authentication_type>
(Instant Access Point)(cellular-uplink-profile)# end
(Instant Access Point)# commit apply
```

To configure a 4G cellular uplink profile:

```
(Instant Access Point)(config) # cellular-uplink-profile
(Instant Access Point)(cellular-uplink-profile)# 4g-usb-type <4g-usb>
(Instant Access Point)(cellular-uplink-profile)# modem-country <country>
(Instant Access Point)(cellular-uplink-profile)# modem-isp <service-provider-name>
(Instant Access Point)(cellular-uplink-profile)# usb-auth-type <usb_authentication_type>
(Instant Access Point)(cellular-uplink-profile)# end
(Instant Access Point)# commit apply
```

To switch a modem from the storage mode to modem mode:

```
(Instant Access Point)(config)# cellular-uplink-profile
(Instant Access Point)(cellular-uplink-profile)# usb-modeswitch <usb-modem>
```

To configure 3G/4G switch network

```
(Instant Access Point)(config) # cellular-uplink-profile
(Instant Access Point)(cellular-uplink-profile)# usb-type <3G-usb-type>
(Instant Access Point)(cellular-uplink-profile)# 4g-usb-type <4g-usb>
(Instant Access Point)(cellular-uplink-profile)# modem-country <country>
(Instant Access Point)(cellular-uplink-profile)# modem-isp <service-provider-name>
(Instant Access Point)(cellular-uplink-profile)# usb-auth-type <usb-authentication_type>
(Instant Access Point)(cellular-uplink-profile)# usb-user <username>
(Instant Access Point)(cellular-uplink-profile)# usb-passwd <password>
(Instant Access Point)(cellular-uplink-profile)# usb-dev <device-ID>
(Instant Access Point)(cellular-uplink-profile)# usb-tty <tty-port>
(Instant Access Point)(cellular-uplink-profile)# usb-init <Initialization-parameter>
(Instant Access Point)(cellular-uplink-profile)# usb-dial <dial-parameter>
(Instant Access Point)(cellular-uplink-profile)# end
(Instant Access Point)# commit apply
```

To view the cellular configuration:

```
(Instant Access Point)# show cellular config

USB Plugged in: Vendor_ID=0 Product_ID=0

cellular configure
------------------
Type            Value
----            -----
4g-usb-type     pantech-lte
usb-type
usb-dev         test
usb-tty
usb-init
usb-user
usb-passwd
usb-auth-type   PAP
usb-dial        usb-init
usb-modeswitch
modem-isp       verison
modem-country   India
Supported Country list
----------------------
Country list
------------
Supported ISP list
------------------
ISP list
--------
```

To view the cellular status:

```
(Instant Access Point)# show cellular status

cellular status
---------------
card         detect       link
----         ------       ----
Not-present  Not-detect  Linkdown
```

Wi-Fi Uplink

The Wi-Fi uplink is supported for all the IAP models, but only the master IAP uses this uplink. The Wi-Fi allows uplink to open, PSK-CCMP, and PSK-TKIP SSIDs.

- For single radio IAPs, the radio serves wireless clients and the Wi-Fi uplink.
- For dual radio IAPs, both radios can be used to serve clients but only one of them can be used for the Wi-Fi uplink.

NOTE

When the Wi-Fi uplink is in use, the client IP is assigned by the internal DHCP server.

Configuring a Wi-Fi Uplink Profile

The following configuration conditions apply to the Wi-Fi uplink:

- To bind or unbind the Wi-Fi uplink on the 5 GHz band, reboot the IAP.
- If the Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two links are mutually exclusive.
- For IAPs to connect to an ArubaOS based WLAN using Wi-Fi uplink, the mobilitycontroller must run ArubaOS 6.2.1.0 or later.

To provision an IAP with the Wi-Fi Uplink, complete the following steps:

1. If you are configuring a Wi-Fi uplink after restoring factory settings on an IAP, connect the IAP to an Ethernet cable to allow the IAP to get the IP address. Otherwise, go to step 2.
2. Click the **System** link at the top right corner of the Instant main window. The **System** window is displayed.
3. Click the **Show advanced options** link. The advanced options are displayed.
4. Click the **Uplink** tab.
5. Under Wi-Fi, enter the name of the wireless network that is used for the Wi-Fi uplink in the **Name (SSID)** text box.
6. Select the type of key for uplink encryption and authentication from the **Key management** drop-down list. If the uplink wireless router uses mixed encryption, WPA-2 is recommended for the Wi-Fi uplink.
7. From the **band** drop-down list. Select the band in which the Virtual Controller currently operates. The following options are available:
   - 2.4GHz (default)
   - 5 GHz
8. Select a passphrase format from the **Passphrase format** drop-down list. The following options are available:
   - 8 - 63 alphanumeric characters
   - 64 hexadecimal characters

NOTE

Ensure that the hexadecimal password string is exactly 64 digits in length.

9. Enter a pre-shared key (PSK) passphrase in the **Passphrase** text box and click **OK**.

You can view the W-Fi configuration and uplink status in the CLI. To view the configuration status in the CLI:

```
(Instant Access Point)# show wifi-uplink status

configured     :NO

(Instant Access Point)# show wifi-uplink config

ESSID           :
Cipher Suite    :
Passphrase      :
Band            :

(Instant Access Point)# show wifi-uplink auth log

----------------------------------------------------------------------
wifi uplink auth configuration:
----------------------------------------------------------------------
----------------------------------------------------------------------
wifi uplink auth log:
----------------------------------------------------------------------
[1116]2000-01-01 00:00:45.625: Global control interface '/tmp/supp_gbl'
```

Uplink Preferences and Switching

This topic describes the following procedures:

- Enforcing Uplinks on page 202
- Setting an Uplink Priority on page 202
- Enabling Uplink Preemption on page 203

- Switching Uplinks Based on VPN and Internet Availability on page 203
- Viewing Uplink Status and Configuration on page 204

Enforcing Uplinks

The following configuration conditions apply to the uplink enforcement:

- When an uplink is enforced, the IAP uses the specified uplink regardless of uplink preemption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured and uplink is enabled on the wired profiles, the IAP tries to find an alternate Ethernet link based on the priority configured.
- When no uplink is enforced and preemption is not enabled, and if the current uplink fails, the IAP tries to find an available uplink based on the priority configured.
- When no uplink is enforced and preemption is enabled, and if the current uplink fails, the IAP tries to find an available uplink based on in the priority configured. If current uplink is active, the IAP periodically tries to use a higher priority uplink and switches to the higher priority uplink even if the current uplink is active.

You can enforce a specific uplink on an IAP by using the Instant UI or CLI.

In the Instant UI

To enforce an uplink:

1. Click the **System** > **show advanced settings** > **Uplink**. The **Uplink** tab contents are displayed.
2. Under **Uplink Management**, select the type of uplink from the **Enforce Uplink** drop-down list. If Ethernet uplink is selected, the **Port** field is displayed.
3. Specify the Ethernet interface port number.
4. Click **OK**. The selected uplink is enforced on the IAP.

In the CLI

To enforce an uplink:

```
(Instant Access Point)(config)# uplink
(Instant Access Point)(uplink)# enforce {cellular|ethernet|wifi|none}
(Instant Access Point)(uplink)# end
(Instant Access Point)# commit apply
```

Setting an Uplink Priority

You can set an uplink priority by using the Instant UI or CLI.

In the Instant UI

1. Click the **System** > **show advanced settings** > **Uplink**. The **Uplink** tab contents are displayed.
2. Under **Uplink Priority List**, select the uplink, and click the icons at the bottom of the **Uplink Priority List** section, to increase or decrease the priority. By default, the Eth0 uplink is set as a high priority uplink.
3. Click **OK**. The selected uplink is prioritized over other uplinks.

In the CLI

To set an uplink priority:

```
(Instant Access Point)(config)# uplink
(Instant Access Point)(uplink)# uplink-priority {cellular <priority> | ethernet <priority>|[po
rt <Interface-number> <priority>]|wifi <priority>}
(Instant Access Point)(uplink)# end
(Instant Access Point)# commit apply
```

For example, to set a priority for Ethernet uplink:

```
(Instant Access Point)(uplink)# uplink-priority ethernet port 0 1
(Instant Access Point)(uplink)# end
(Instant Access Point)# commit apply
```

Enabling Uplink Preemption

The following configuration conditions apply to uplink preemption:

- Preemption can be enabled only when no uplink is enforced.
- When preemption is disabled and the current uplink goes down, the IAP tries to find an available uplink based on the uplink priority configuration.
- When preemption is enabled and if the current uplink is active, the IAP periodically tries to use a higher priority uplink, and switches to a higher priority uplink even if the current uplink is active.

You can enable uplink preemption using Instant UI or CLI.

In the Instant UI

1. Click the **System** > **show advanced settings** > **Uplink**. The **Uplink** tab contents are displayed.
2. Under **Uplink Management**, ensure that the **Enforce Uplink** is set to none.
3. Select **Enabled** from the **Pre-emption** drop-down list.
4. Click **OK**.

In the CLI

To enable uplink preemption:

```
(Instant Access Point)(config)# uplink
(Instant Access Point)(uplink)# preemption
(Instant Access Point)(uplink)# end
(Instant Access Point)# commit apply
```

Switching Uplinks Based on VPN and Internet Availability

The default priority for uplink switchover is Ethernet and then 3G/4G. The IAP can switch to the lower priority uplink if the current uplink is down.

Switching Uplinks Based on VPN Status

Instant supports switching uplinks based on the VPN status when deploying multiple uplinks (Ethernet, 3G/4G, and Wi-Fi). When VPN is used with multiple backhaul options, the IAP switches to an uplink connection based on the VPN connection status, instead of only using the Ethernet or the physical backhaul link.

The following configuration conditions apply to uplink switching:

- If the current uplink is Ethernet and the VPN connection is down, the IAP tries to reconnect to VPN. The retry time depends on the fast failover configuration and the primary or backup VPN tunnel. If this fails, the IAP waits for the VPN failover timeout and selects a different uplink such as 3G/4G or Wi-Fi.
- If the current uplink is 3G or Wi-Fi, and Ethernet has a physical link, the IAP periodically suspends user traffic to try and connect to the VPN on the Ethernet. If the IAP succeeds, the IAP switches to Ethernet. If the IAP does not succeed, it restores the VPN connection to the current uplink.

NOTE

This feature is automatically enabled when VPN is configured on the IAP. IAPmonitors the VPN status and when the VPN connection is not available for 3 minutes, the uplink switches to another available connection (if a low priority uplink is detected and the uplink preference is set to none).

Switching Uplinks Based on Internet Availability

You can configure Instant to switch uplinks based on Internet availability.

When the uplink switchover based on Internet availability is enabled, the IAP continuously sends ICMP packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the public Internet is not reachable from the current uplink, the IAP switches to a different connection.

You can set preferences for uplink switching using Instant UI and CLI.

In the Instant UI

To configure uplink switching:

1. Click the **System** > **show advanced settings** > **Uplink**. The **Uplink** tab contents are displayed.
2. Under **Uplink Management**, configure the following parameters:
   - **VPN failover timeout** – To configure uplink switching based on VPN status, specify the duration to wait for an uplink switch. The default duration is set to 180 seconds.
   - **Internet failover** – To configure uplink switching based on Internet availability, perform the following steps:

     a. Select **Enabled** from the **Internet failover** drop-down list.

     b. Specify the required values for **Max allowed test packet loss** and **Secs between test packets**.

     c. Click **OK**.

> NOTE
>
> When **Internet failover** is enabled, the IAP ignores the VPN status, although uplink switching based on VPN status is enabled.

In the CLI

To enable uplink switching based on VPN status:

```
(Instant Access Point)(config)# uplink
(Instant Access Point)(uplink)# failover-vpn-timeout <seconds>
(Instant Access Point)(uplink)# end
(Instant Access Point)# commit apply
```

To enable uplink switching based on Internet availability:

```
(Instant Access Point)(config)# uplink
(Instant Access Point)(uplink)# failover-internet
(Instant Access Point)(uplink)# failover-internet-pkt-lost-cnt <count>
(Instant Access Point)(uplink)# failover-internet-pkt-send-freq <frequency>
(Instant Access Point)(uplink)# end
(Instant Access Point)# commit apply
```

Viewing Uplink Status and Configuration

To view the uplink status and configuration in the CLI:

```
Instant Access Point# show uplink status

Uplink preemption           :enable
Uplink enforce              :none
Ethernet uplink bond0        :DHCP
Uplink Table
------------
Type      State  Priority  In Use
----      -----  --------  ------
eth0      UP     0         Yes
Wifi-sta  LOAD   6         No
3G/4G     INIT   7         No
Internet failover           :disable
Max allowed test packet loss:10
Secs between test packets   :30
```

```
VPN failover timeout (secs) :180
ICMP pkt sent        :0
ICMP pkt lost        :0
Continuous pkt lost  :0
VPN down time        :0

Instant Access Point# show uplink config

Uplink preemption           :enable
Uplink enforce              :none
Ethernet uplink bond0        :DHCP
Internet failover           :disable
Max allowed test packet loss:10
Secs between test packets   :30
VPN failover timeout (secs) :180
```

This chapter provides the following information:

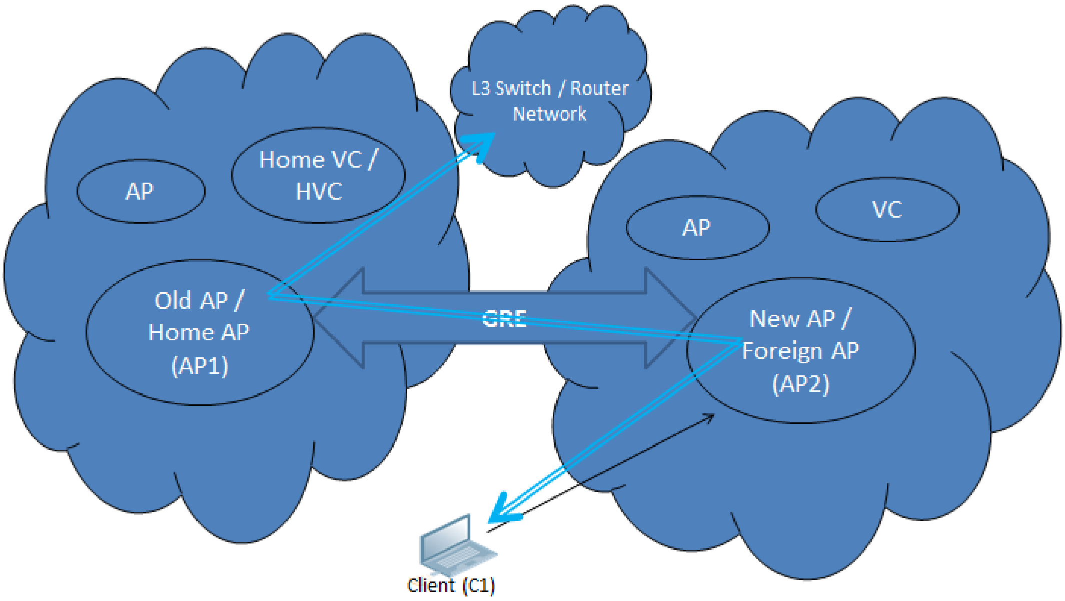
Layer-3 Mobility Overview

IAPs form a single Instant network when they are in the same Layer-2 (L2) domain. As the number of clients increase, multiple subnets are required to avoid broadcast overhead. In such a scenario, a client must be allowed to roam away from the Instant network to which it first connected (home network) to another network supporting the same WLAN access parameters (foreign network) and continue its existing sessions.

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

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

Figure 66 *Routing of traffic when the client is away from its home network*



When a client first connects to an Instant network, a message is sent to all configured Virtual Controller IP addresses to see if this is an L3 roamed client. On receiving an acknowledgement from any of the configured Virtual Controller IP addresses, the client is identified as an L3 roamed client. If the AP has no GRE tunnel to this home network, a new tunnel is formed to an AP (home AP) from the client's home network.

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

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

Configuring L3-Mobility

To configure a mobility domain, you have to specify the list of all Instant networks that form the mobility domain. To allow clients to roam seamlessly among all the APs, specify the Virtual Controller IP for each foreign subnet. You may include the local Instant or Virtual Controller IP address, so that the same configuration can be used across all Instant networks in the mobility domain.

It is recommended that you configure all client subnets in the mobility domain. When client subnets are configured:

- If a client is from a local subnet, it is identified as a local client. When a local client starts using the IP address, the L3 roaming is terminated.
- If the client is from a foreign subnet, it is identified as a foreign client. When a foreign client starts using the IP address, the L3 roaming is set up.

Home Agent Load Balancing

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

Configuring a Mobility Domain for Instant

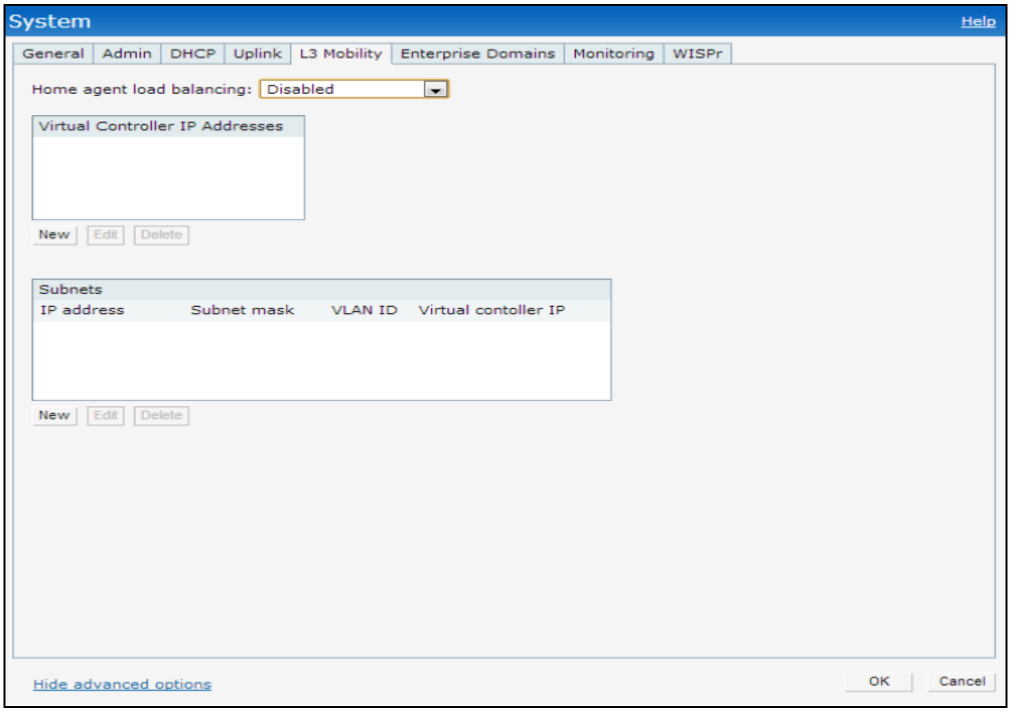
You can configure L3 mobility domain by using Instant UI or CLI.

In the Instant UI

To configure a mobility domain, perform the following steps:

1. Click the **System** link at top right corner of the Instant main window. The **System** window appears.
2. Click the **Show advanced options** link. The advanced options are displayed.
3. Click **L3 Mobility**. The L3 Mobility window is displayed.

Figure 67 *L3 Mobility Window*



Home agent load balancing: Disabled

1. Select **Enabled** from the **Home agent load balancing** drop-down list. By default, home agent load balancing is disabled.
2. Click **New** in the **Virtual Controller IP Addresses** section, add the IP address of a Virtual Controller that is part of the mobility domain, and click **OK**.
3. Repeat Step 2 to add the IP addresses of all Virtual Controllers that form the L3 mobility domain.
4. Click **New** in the **Subnets** section and specify the following:
    a. Enter the client subnet in the **IP address** text box.
    b. Enter the mask in the **Subnet mask** text box.
    c. Enter the VLAN ID in the home network in the **VLAN ID** text box.
    d. Enter the home VC IP address for this subnet in the **Virtual Controller IP** text box.
5. Click **OK**.

In the CLI

To configure a mobility domain:

```
(Instant Access Point)(config)# l3-mobility
(Instant Access Point)(L3-mobility)# home-agent-load-balancing
(Instant Access Point)(L3-mobility)# virtual-controller <IP-address>
(Instant Access Point)(L3-mobility)# subnet <IP-address> <subnet-mask> <VLAN-ID> <virtual-cont
roller-IP-address>
(Instant Access Point)(L3-mobility)# end
(Instant Access Point)# commit apply
```

This chapter provides the following information:

- Understanding Spectrum Data on page 211
- Configuring Spectrum Monitors and Hybrid IAPs on page 216

Understanding Spectrum Data

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

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

The spectrum monitor is supported on IAP-104, IAP-105, IAP-134 and IAP-135 radios.

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

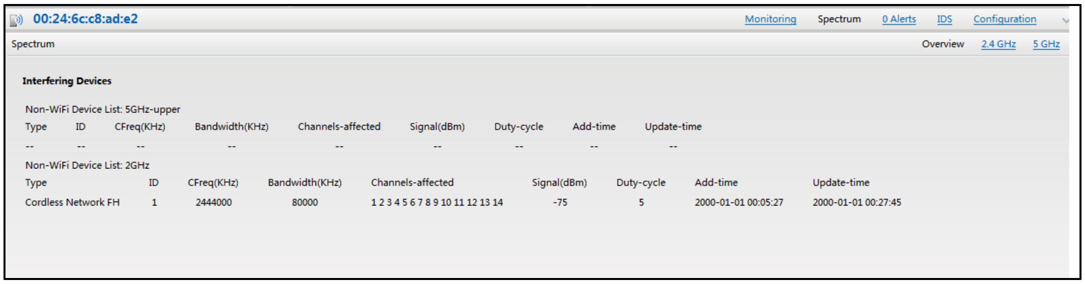
- Device List
- Non Wi-Fi Interferers
- Channel Metrics
- Channel Details
- Spectrum Alerts

Device List

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

To view the device list, click **Spectrum** in the dashboard. The following figure shows an example of the device list details.

Figure 68 *Device List*



Interfering Devices

Non-WiFi Device List: 5GHz-upper

Type	ID	CFreq(KHz)	Bandwidth(KHz)	Channels-affected	Signal(dBm)	Duty-cycle	Add-time	Update-time
--	--	--	--	--	--	--	--	--

Non-WiFi Device List: 2GHz

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

Device Summary and Channel Information shows the details of the information that is displayed:

Table 34: *Device Summary and Channel Information*

Column	Description
Type	Device type. This parameter can be any of the following: ● audio FF (fixed frequency) ● bluetooth ● cordless base FH (frequency hopper) ● cordless phone FF (fixed frequency) ● cordless network FH (frequency hopper) ● generic FF (fixed frequency) ● generic FH (frequency hopper) ● generic interferer ● microwave ● microwave inverter ● video ● xbox **NOTE:** For additional details about non Wi-Fi device types shown in this table, see Non Wi-Fi Interferer Types.
ID	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device.
Channels-affected	Radio channels affected by the wireless device.
Signal-strength	Strength of the signal sent from the device, in dBm.
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add-time	Time at which the device was first detected.
Update-time	Time at which the device's status was updated.

Non Wi-Fi Interferers

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

Table 35: *Non Wi-Fi Interferer Types*

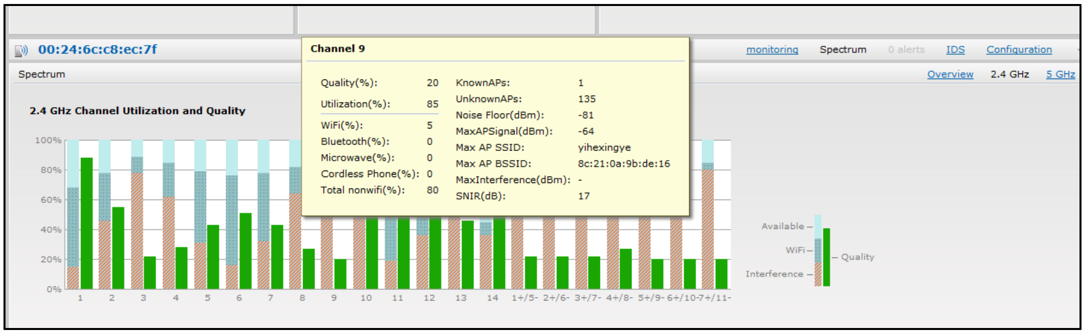
Non Wi-Fi Interferer	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed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

Non Wi-Fi Interferer	Description
Generic Interferer	Any non-frequency hopping device that does not fall into one of the other categories described in this table is classified as a *Generic Interferer*. For example a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a Generic Interferer. Similarly wide-band interfering devices may be classified as Generic Interferers.

Channel Details

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

Figure 69 *Channel Details*



Channel 9

Quality(%):	20	KnownAPs:	1
Utilization(%):	85	UnknownAPs:	135
WiFi(%):	5	Noise Floor(dBm):	-81
Bluetooth(%):	0	MaxAPSignal(dBm):	-64
Microwave(%):	0	Max AP SSID:	yihexingye
Cordless Phone(%):	0	Max AP BSSID:	8c:21:0a:9b:de:16
Total nonwifi(%):	80	MaxInterference(dBm):	-
		SNIR(dB):	17

Channel Details Information shows the information that you can view in the channel details graph.

Table 36: *Channel Details Information*

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Quality(%)	Current relative quality of the channel.
Utilization(%)	The percentage of the channel being used.
Wi-Fi (%)	The percentage of the channel currently being used by Wi-Fi devices.
Type	Device type.
Total nonwifi (%)	The percentage of the channel currently being used by non Wi-Fi devices.
Known APs	Number of valid APs identified on the radio channel.
UnKnown APs	Number of invalid or rogue APs identified on the radio channel.
Channel Util (%)	Percentage of the channel currently in use.
Max AP Signal (dBm)	Signal strength of the AP that has the maximum signal strength on a channel.

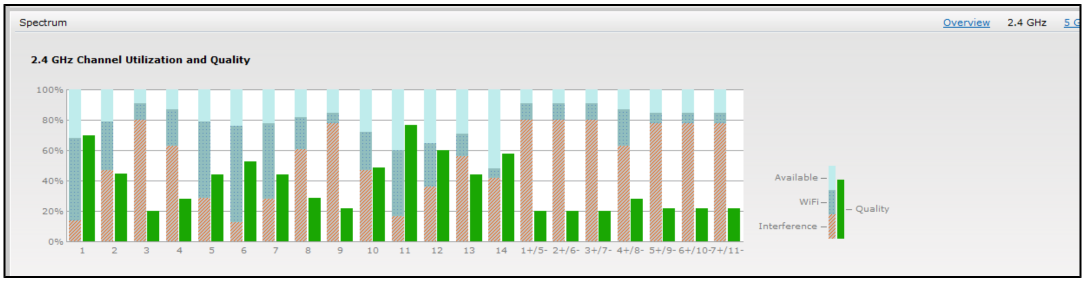
Column	Description
Max Interference (dBm)	Signal strength of the non Wi-Fi device that has the highest signal strength.
SNIR (db)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Channel Metrics

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

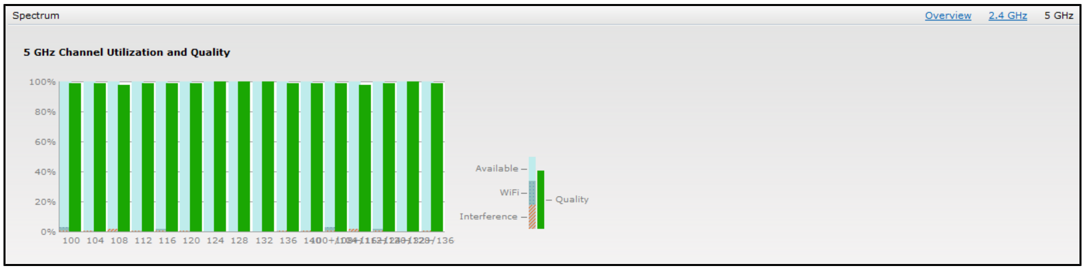
To view this graph, click **2.4 GHz** in the **Spectrum** section of the dashboard.

Figure 70 *Channel Metrics for the 2.4 GHz Radio Channel*



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

Figure 71 *Channel Metrics for the 5 GHz Radio Channel*



Channel Metrics shows the information displayed in the channel metrics graph.

Table 37: *Channel Metrics*

Column	Description
Channel	A 2.4 GHz or 5 GHz radio channel.

Column	Description
Quality(%)	Current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands, as determined by the percentage of packet retries, the current noise floor, and the duty cycle for non Wi-Fi devices on that channel.
Availability(%)	The percentage of the channel currently available for use.
Utilization(%)	The percentage of the channel being used.
WiFi Util(%)	The percentage of the channel currently being used by Wi-Fi devices.
Interference Util(%)	The percentage of the channel currently being used by non Wi-Fi interference + Wi-Fi ACI (Adjacent Channel Interference)

Spectrum Alerts

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

Configuring Spectrum Monitors and Hybrid IAPs

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

Converting an IAP to a Hybrid IAP

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

You can convert IAPs in an Instant network to hybrid mode using Instant UI or CLI.

In the Instant UI

To convert an IAP to a hybrid IAP:

1. Click the **RF** link at the top right corner of the Instant UI.
2. Click **Show advanced options** to view the **Radio** tab.
3. To enable a spectrum monitor on the 802.11g radio band, in the 2.4 GHz radio profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
4. To enable a spectrum monitor on the 802.11a radio band, in the 5 GHz radio profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
5. Click **OK**.

In the CLI

To configure 2.4 GHz radio settings:

```
(Instant Access Point)(config)# rf dot11g-radio-profile
(Instant Access Point)(RF dot11 g Radio Profile)# spectrum-monitor
```

To configure 5 GHz radio settings:

```
(Instant Access Point)(config)# rf dot11a-radio-profile
(Instant Access Point)(RF dot11a Radio Profile)# spectrum-monitor
```

Converting an IAP to a Spectrum Monitor

In spectrum mode, spectrum monitoring is performed on entire bands. However for the 5 GHz radio, spectrum monitoring is performed on only one of the three bands:

- 5 GHz - lower
- 5 GHz - middle
- 5 GHz - higher

By default, spectrum monitoring is performed on a higher band of the 5 GHz radio.

You can configure an IAP to function as a standalone spectrum monitor using Instant UI or CLI.

In the Instant UI

To convert an IAP to a spectrum monitor:

1. In the **Access Points** tab, click the AP that you want to convert to a spectrum monitor. The **edit** link appears.
2. Click the **edit** link. The **Edit Access Point** window appears.
3. Click the **Radio** tab.
4. From the **Access Mode** drop-down list, select **Spectrum Monitor**.
5. Click **OK**.
6. Reboot the IAP for the changes to affect.
7. To enable spectrum monitoring for any other band for the 5 GHz radio:
   a. Click the **RF** link at the upper right corner of the Instant UI.
   b. Click **Show advanced options** to view the **Radio** tab.
   c. For the 5 GHz radio, specify the spectrum band you want that radio to monitor by selecting **Lower**, **Middle**, or **Higher** from the **Standalone spectrum band** drop-down list.
   d. Click **OK**.

In the CLI

To convert an IAP to a spectrum monitor:

```
(Instant Access Point)# wifi0-mode {<access>|<monitor>|<spectrum-monitor>}
(Instant Access Point)# wifi1-mode {<access>|<monitor>|<spectrum-monitor>}
```

To enable spectrum monitoring for any other band for the 5 GHz radio:

```
(Instant Access Point)(config)# rf dot11a-radio-profile
Instant Access Point (RF dot11a Radio Profile)# spectrum-band <type>
```

To view the radio configuration:

```
Instant Access Point# show radio config
2.4 GHz:
Legacy Mode:disable
Beacon Interval:100
802.11d/802.11h:disable
Interference Immunity Level:2
Channel Switch Announcement Count:0
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable

5.0 GHz:
Legacy Mode:disable
```

```
Beacon Interval:100
802.11d/802.11h:disable
Interference Immunity Level:2
Channel Switch Announcement Count:0
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Standalone Spectrum Band:5ghz-upper
```

Chapter 16
Adaptive Radio Management

This chapter provides the following information:

- ARM Overview on page 219
- Configuring ARM Features on an IAP on page 221
- Configuring Radio Settings for an IAP on page 226

ARM Overview

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, n, and ac client types to inter operate at the highest performance levels.

Channel or Power Assignment

The channel or power assignment 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 the ongoing operations when RF conditions change.

Voice Aware Scanning

The Voice Aware scanning feature prevents an IAP supporting an active voice call from scanning for other channels in the RF spectrum and allows n IAP to resume scanning when there are no active voice calls. This significantly improves the voice quality when a call is in progress and simultaneously delivers the automated RF management functions. By default, this feature is enabled.

Load Aware Scanning

The Load Aware Scanning 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. By default, this feature is enabled.

Band Steering Mode

The Band Steering feature assigns the dual-band capable clients to 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. For more information, Configuring ARM Features on an IAP on page 221.

Client Match

The ARM client match feature continually monitors a client's RF neighborhood to provide ongoing client bandsteering and load balancing, and enhanced AP reassignment for roaming mobile clients. This feature supersedes the legacy bandsteering and spectrum load balancing features, which, unlike client match, do not trigger IAP changes for clients already associated to an IAP.

NOTE

Legacy 802.11a/b/g access points do not support the client match feature. When client match is enabled on 802.11n capable access points, the client match feature overrides any settings configured for the legacy bandsteering, station handoff assist or load balancing features. 802.11ac-capable access points do not support the legacy bandsteering, station hand off or load balancing settings, so these access points must be managed using client match.

When the client match feature is enabled on an IAP, the IAP measures the RF health of its associated clients. If one of the three mismatch conditions described below are met, clients are moved from one AP to another for better performance and client experience. In the current release, the client match feature is supported only within an IAP cluster.

The following client or IAP mismatch conditions are managed by the client match feature:

- Dynamic Load Balancing: Client match balances clients across IAPs on different channels, based upon the client load on the IAPs and the SNR levels the client detects from an underutilized IAP. If an IAP radio can support additional clients, the IAP will participate in client match load balancing and clients can be directed to that IAP radio, subject to predefined SNR thresholds.
- Sticky Clients: The client match feature also helps mobile clients that tend to stay associated to an IAP despite low signal levels. IAPs using client match continually monitor the client's RSSI as it roams between IAPs, and move the client to an IAP when a better radio match can be found. This prevents mobile clients from remaining associated to an APs with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that IAP.
- Band Steering: IAPs using the client match feature monitor the RSSI for clients that advertise a dual-band capability. If a client is currently associated to a 2.4 GHz radio and the AP detects that the client has a good RSSI from the 5 GHz radio, the controller will attempt to steer the client to the 5 GHz radio, as long as the 5 GHz RSSI is not significantly worse than the 2.4 GHz RSSI, and the IAP retains a suitable distribution of clients on each of its radios.

By default, the client match feature is disabled. For information on client match configuration on an IAP, see Configuring ARM Features on an IAP on page 221.

NOTE

In the Instant 6.3.1.1-4.0 release, spectrum load balancing is integrated with the client match feature. Client match allows the APs in a cluster to be divided into several logical AP RF neighborhood called domains, which share the same clients. The Virtual Controller determines the distribution of clients and balances client load across channels, regardless of whether the AP is responding to the wireless clients' probe requests.

Airtime Fairness Mode

The Airtime Fairness 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 the clients from monopolizing resources.

Access Point Control

The following access point control features are supported:

- **Customize Valid Channels** – You can customize **Valid 5 GHz channels** and **Valid 2.4 GHz channels** for 20MHz and 40MHz channels in the IAP. The administrators can configure the ARM channels in the channel width window. The valid channels automatically show in the **static channel assignment** window.
- **Minimum 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. A higher power level setting may be constrained by the local regulatory requirements and AP capabilities. If the minimum transmission EIRP setting

configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting. The default value is for minimum transmit power is 18 dBm.

- **Maximum 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. If the maximum transmission EIRP configured on an AP is not supported by the AP model, the value is reduced to the highest supported power setting. The default value for maximum transmit power is 127 dBm.
- **Client Aware** – When **Enabled**, ARM does not change channels for the APs with active clients, except for high priority events such as radar or excessive noise. This feature must 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, which change may disrupt current client traffic for a while. 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 a BSSID.

- **Scanning** – When ARM is enabled, the IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and reports to the IAP. This scanning report includes WLAN coverage, interference, and intrusion detection data.
- **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 sends reports to a Virtual Controller on network (WLAN) coverage, interference, and intrusion detection.

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 its ARM-assigned channel to provide a snapshot of the current RF health state.

Configuring ARM Features on an IAP

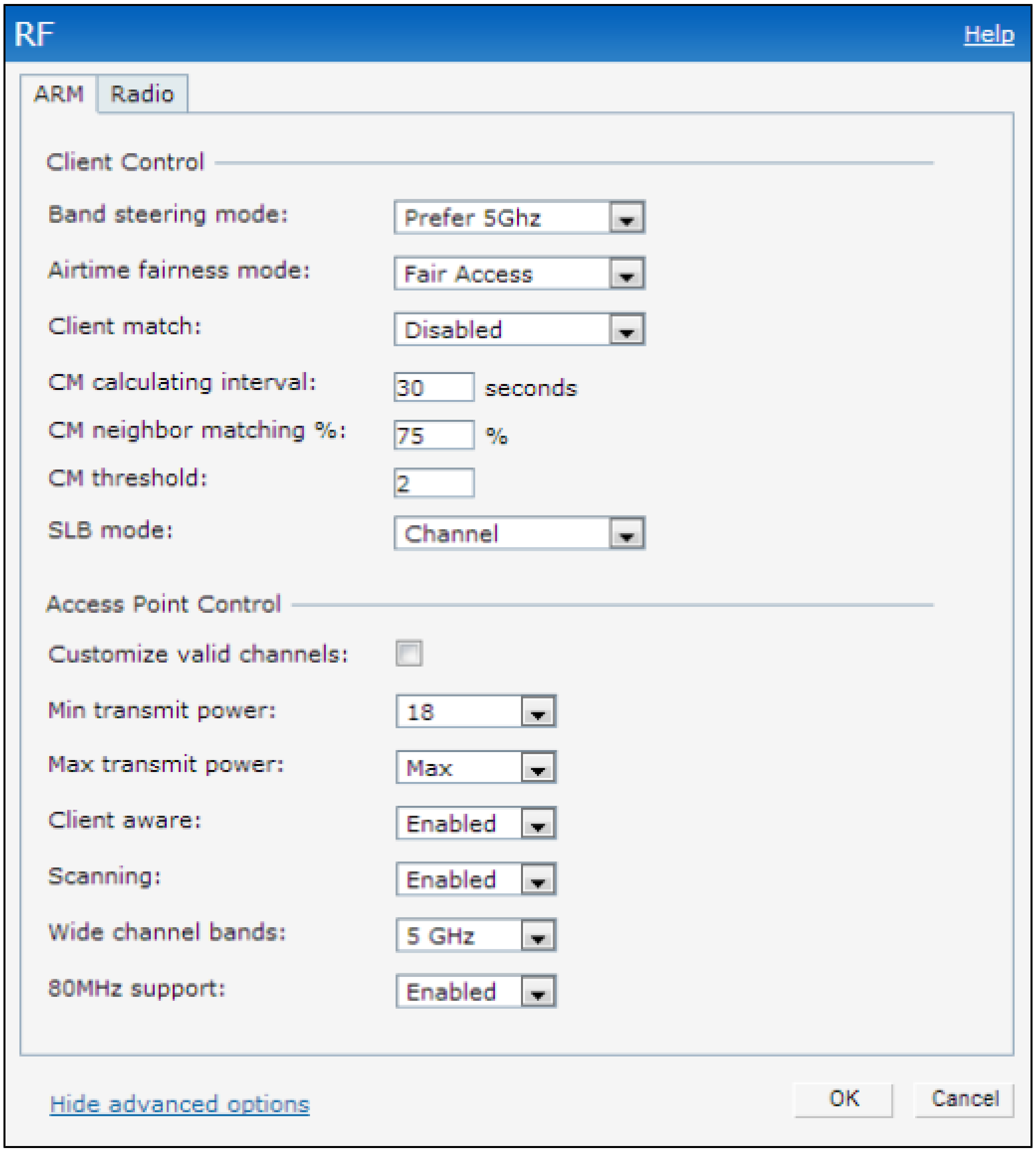
You can configure ARM features such as band steering, spectrum load balancing, and airtime fairness mode either using Instant UI or CLI.

In the Instant UI

To configure ARM:

1. Click the **RF** link at the top right corner of the Instant main window.
2. Click **Show advanced options**. The ARM tab details are displayed.

Figure 72 *RF Window - ARM Tab*



Client Control

Band steering mode: Prefer 5Ghz

Airtime fairness mode: Fair Access

Client match: Disabled

CM calculating interval: 30 seconds

CM neighbor matching %: 75 %

CM threshold: 2

SLB mode: Channel

Access Point Control

Customize valid channels: □

Min transmit power: 18

Max transmit power: Max

Client aware: Enabled

Scanning: Enabled

Wide channel bands: 5 GHz

80MHz support: Enabled

3. Configure the following parameters for **Band steering mode**:

Table 38: *Band Steering Mode - Configuration Parameters*

Parameter	Description
Prefer 5 GHz	Select this option to use band steering in 5 GHz mode. On selecting this, the IAP steers the client to 5 GHz band (if the client is 5 GHz capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.
Force 5 GHz	Select this option to enforce 5 GHz band steering mode on the IAPs.
Balance Bands	Select this option is selected, the IAP tries to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40MHz while the 2.5 GHz band operates in 20MHz.
Disabled	Select this option if you want to allow the clients to select the band to use.

4. For **Airtime fairness mode**, specify any of the following values:

Table 39: *Airtime Fairness Mode - Configuration Parameters*

Parameter	Description
Default Access	Select this option to provide access based on client requests. When **Air Time Fairness** is set to default access, per user and per SSID bandwidth limits are not enforced.
Fair Access	Select this option to allocate Airtime evenly across all the clients.
Preferred Access	Select this option to set a preference where 11n clients are assigned more airtime than 11a/11g. The 11a/11g clients get more airtime than 11b. The ratio is 16:4:1.

5. For **Spectrum load balancing**, specify the following parameters:

Table 40: *Spectrum Load Balancing - Configuration Parameters*

Parameter	Description
Client match	Select **Enabled** to enable the **Client match** feature on APs. When enabled, client count will be balanced among all the channels in the same band. For more information, see Client Match on page 219.
CM calculating interval	Specify a value for the calculating interval of Client match. The value specified for **CM calculating interval** determines the interval at which client match is calculated. The interval is specified in seconds and the default value is 30 seconds. You can specify a value within the range of 10-600.
CM neighbor matching %	Specify a value for **CM neighbor matching %**. This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of client match. You can specify a percentage value within the range of 20-100. The default value is 75%.
CM threshold	Specify a value for **CM threshold**. This number takes acceptance client count difference among all the channels of Client match into account. When the client load on an AP reaches or exceeds the threshold in comparison, client match is enabled on that AP. You can specify a value within range of 1-20. The default value is 2.
SLB mode	Select a mode from the **SLB mode** drop-down. The SLB mode determines the balancing strategy for client match. The following options are available: ● Channel ● Radio ● Channel + Radio

6. For **Access Point Control**, specify the following parameters:

Table 41: *Access Point Control - Configuration Parameters*

Parameter	Description
Customize Valid Channels	Select this check box to customize valid channels for 2,4 GHz and 5 GHz. By default, the AP uses valid channels as defined by the Country Code (regulatory domain). On selecting the **Customize Valid Channels** check box, a list of valid channels for both 2.4.GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default.
Minimum Transmit Power	Specify the minimum transmission power. The value specified for **Minimum Transmit Power** indicates the minimum Effective Isotropic Radiated Power (EIRP) from 3 to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting. The default value is for minimum transmit power is 18 dBm.
Maximum Transmit Power	Specify the maximum transmission power. The value specified for **Maximum Transmit Power** indicates the maximum Effective Isotropic Radiated Power (EIRP) from 3 to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on an AP is not supported by the AP model, the value is reduced to the highest supported power setting. The default value for maximum transmit power is 127 dBm.
Client aware	Select **Enabled** to allow ARM to control channel assignments for the APs with active clients. When the **Client aware** mode is set to **Disabled**, the IAP may change to a more optimal channel, which change may disrupt current client traffic. The **Client aware** option is **Enabled** by default.
Scanning	Select **Enabled** so that the IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and reports to the IAP. This scanning report includes WLAN coverage, interference, and intrusion detection data.
Wide Channel Bands	Select a band to allow the APs to be placed in 40Mhz (wide band) channels. The **Wide channel band** allows administrators to configure 40 MHz channels in the 2.4 GHz and 5.0 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. 40 MHz channel effectively doubles the frequency bandwidth available for data transmission. For high performance, you can select 5GHz. If the AP density is low, enable in the 2.4GHz band.
80 MHz Support	Enables or disables the use of 80 MHz channels on APs. This feature allows ARM to assign 80 MHz channels on APs with 5GHz radios, which support a very high throughput. This setting is enabled by default. **NOTE:** Only the APs that support 802.11ac can be configured with 80 MHz channels.

7. Reboot the IAP.
8. Click **OK**.

In the CLI

To configure ARM features on an IAP with 5 GHz radio:

```
(Instant Access Point)(config)# arm
(Instant Access Point)(ARM)# a-channels <5GHz-channels>
(Instant Access Point)(ARM)# min-tx-power <power>
(Instant Access Point)(ARM)# max-tx-power <power>
(Instant Access Point)(ARM)# band-steering-mode {<Prefer 5 GHz>| <Force 5 GHz>|<Balance Bands>
|<Disabled>}
(Instant Access Point)(ARM)# air-time-fairness-mode {<Default Access>| <Fair Access> | <Prefer
red Access>}
```

```
(Instant Access Point)(ARM)# client-aware
(Instant Access Point)(ARM)# wide-bands {<5GHz>|<2GHz>|<All>|<None>}
(Instant Access Point)(ARM)# scanning
(Instant Access Point)(ARM)# client-match calc-interval <seconds>
(Instant Access Point)(ARM)# client-match calc-threshold <threshold>
(Instant Access Point)(ARM)# client-match nb-matching <percentage>
(Instant Access Point)(ARM)# client-match slb-mode 1
(Instant Access Point)(ARM)# 80mhz-support
(Instant Access Point)(ARM)# end
(Instant Access Point)# commit apply
```

To view ARM configuration:

```
(Instant Access Point)# show arm config

Minimum Transmit Power            :18
Maximum Transmit Power            :127
Band Steering Mode        :prefer-5ghz
Client Aware              :enable
Scanning                  :enable
Wide Channel Bands        :5ghz
80Mhz Support             :enable
Air Time Fairness Mode    :fair-access
Client Match              :disable
CM NB Matching Percent    :75
CM Calculating Interval   :30
CM SLB Threshold          :2
CM SLB Balancing Mode     :channel based
CM max client match req   :5
CM max adoption           :5
Custom Channels           :No
2.4 GHz Channels
----------------
Channel  Status
-------  ------
1        enable
2        disable
3        disable
4        disable
5        disable
6        enable
7        disable
8        disable
9        disable
10       disable
11       enable
12       disable
13       disable
1+       enable
2+       disable
3+       disable
4+       disable
5+       disable
6+       disable
7+       enable
5.0 GHz Channels
----------------
Channel  Status
-------  ------
36       enable
40       enable
44       enable
```

```
48      enable
52      enable
56      enable
60      enable
64      enable
149     enable
153     enable
157     enable
161     enable
165     enable
36+     enable
44+     enable
52+     disable
60+     disable
149+    enable
157+    enable
36E     enable
52E     enable
149E    enable
```

Configuring Radio Settings for an IAP

You can configure 2.4 GHz and 5 GHz radio settings for an IAP either using Instant UI or CLI.

In the Instant UI

To configure radio settings:

1. Click the **RF** link at the top right corner of the Instant main window.
2. Click **Show advanced options**. The advanced options are displayed.
3. Click the **Radio** tab.
4. Under the channel 2.4.GHz or 5GHz or both, configure the following parameters.

Table 42: *Radio Configuration Parameters*

Parameter	Description
Legacy only	Select **Enabled** to run the radio in non-802.11n mode. This option is set to **Disabled** by default.
802.11d / 802.11h	Select **Enabled** to allow the radio to advertise its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This option is set to **Disabled** by default.
Beacon interval	Enter the Beacon period for the IAP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the access point. You can specify a value within the range of 60-500. The default value is 100 milliseconds.
Interference immunity level	Select to increase the immunity level to improve performance in high-interference environments. The default immunity level is 2. ● **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

Parameter	Description
	detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ● **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. **NOTE:** Increasing the immunity level makes the AP to lose a small amount of range.
Channel switch announcement count	Specify the count to indicate the number of channel switching announcements that must be sent before switching to a new channel. This allows associated clients to recover gracefully from a channel change.
Background spectrum monitoring	Select **Enabled** to allow the APs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.

5. Reboot the IAP after configuring the radio profile settings.

In the CLI

To configure 2.4 GHz radio settings:

```
(Instant Access Point)(config)# rf dot11g-radio-profile
(Instant Access Point)(RF dot11 g Radio Profile)# beacon-interval <milliseconds>
(Instant Access Point)(RF dot11 g Radio Profile)# legacy-mode
(Instant Access Point)(RF dot11 g Radio Profile)# spectrum-monitor
(Instant Access Point)(RF dot11 g Radio Profile)# dot11h
(Instant Access Point)(RF dot11 g Radio Profile)# interference-immunity <level>
(Instant Access Point)(RF dot11 g Radio Profile)# csa-count <count>
(Instant Access Point)(RF dot11 g Radio Profile)# max-distance <count>
(Instant Access Point)(RF dot11 g Radio Profile)# end
(Instant Access Point)# commit apply
```

To configure 5 GHz radio settings:

```
(Instant Access Point)(config)# rf dot11a-radio-profile
(Instant Access Point)(RF dot11a Radio Profile)# beacon-interval <milliseconds>
(Instant Access Point)(RF dot11a Radio Profile)# legacy-mode
(Instant Access Point)(RF dot11a Radio Profile)# spectrum-monitor
(Instant Access Point)(RF dot11a Radio Profile)# spectrum-band <type>
(Instant Access Point)(RF dot11a Radio Profile)# dot11h
(Instant Access Point)(RF dot11a Radio Profile)# interference-immunity <level>
(Instant Access Point)(RF dot11a Radio Profile)# max-distance <count>
(Instant Access Point)(RF dot11a Radio Profile)# csa-count <count>
(Instant Access Point)(RF dot11 g Radio Profile)# end
(Instant Access Point)# commit apply
```

To view the radio configuration:

```
(Instant Access Point)# show radio config

Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:0
MAX Distance:600
```

```
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable

5.0 GHz:
Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:2
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Standalone Spectrum Band:5ghz-upper
```

The 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.

The IDS feature in the Instant network enables you to detect rogue APs, interfering APs, and other devices that can potentially disrupt network operations.

This chapter describes the following procedures:

- Detecting and Classifying Rogue APs on page 229
- OS Fingerprinting on page 229
- Configuring Wireless Intrusion Protection and Detection Levels on page 230
- Configuring IDS Using CLI on page 234

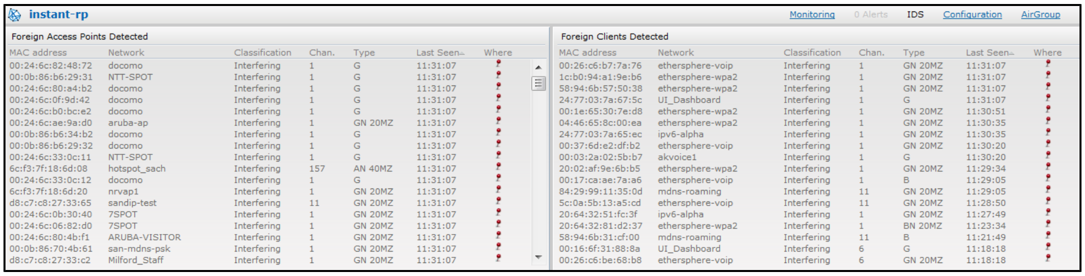
Detecting and Classifying Rogue APs

A rogue AP is an unauthorized AP plugged into the wired side of the network.

An interfering AP is an AP 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, because it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

To detect the rogue APs, click the **IDS** link in the Instant main window. The built-in IDS scans for access points that are not controlled by the Virtual Controller. These are listed and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

Figure 73 *Intrusion Detection*



Foreign Access Points Detected

MAC address	Network	Classification	Chan.	Type	Last Seen	Where
00:24:6c:82:48:72	docomo	Interfering	1	G	11:31:07	📍
00:0b:86:b6:29:31	NTT-SPOT	Interfering	1	G	11:31:07	📍
00:24:6c:80:a4:b2	docomo	Interfering	1	G	11:31:07	📍
00:24:6c:0f:9d:42	docomo	Interfering	1	G	11:31:07	📍
00:24:6c:b0:bc:e2	docomo	Interfering	1	G	11:31:07	📍
00:24:6c:ae:9a:d0	aruba-ap	Interfering	1	GN 20MZ	11:31:07	📍
00:0b:86:b6:34:b2	docomo	Interfering	1	G	11:31:07	📍
00:0b:86:b6:29:32	docomo	Interfering	1	G	11:31:07	📍
00:24:6c:33:0c:11	NTT-SPOT	Interfering	1	G	11:31:07	📍
6c:f3:7f:18:6d:08	hotspot_sach	Interfering	157	AN 40MZ	11:31:07	📍
00:24:6c:33:0c:12	docomo	Interfering	1	G	11:31:07	📍
6c:f3:7f:18:6d:20	nrvap1	Interfering	1	GN 20MZ	11:31:07	📍
d8:c7:c8:27:33:65	sandip-test	Interfering	11	GN 20MZ	11:31:07	📍
00:24:6c:0b:30:40	7SPOT	Interfering	1	GN 20MZ	11:31:07	📍
00:24:6c:06:82:d0	7SPOT	Interfering	1	GN 20MZ	11:31:07	📍
00:24:6c:80:4b:f1	ARUBA-VISITOR	Interfering	1	GN 20MZ	11:31:07	📍
00:0b:86:70:4b:61	san-mdns-psk	Interfering	1	GN 20MZ	11:31:07	📍
d8:c7:c8:27:33:c2	Milford_Staff	Interfering	1	GN 20MZ	11:31:07	📍

Foreign Clients Detected

MAC address	Network	Classification	Chan.	Type	Last Seen	Where
00:26:c6:b7:7a:76	ethersphere-voip	Interfering	1	GN 20MZ	11:31:07	📍
1c:b0:94:a1:9e:b6	ethersphere-wpa2	Interfering	1	GN 20MZ	11:31:07	📍
58:94:6b:57:50:38	ethersphere-wpa2	Interfering	1	GN 20MZ	11:31:07	📍
24:77:03:7a:67:5c	UI_Dashboard	Interfering	1	G	11:31:07	📍
00:1e:65:30:7e:d8	ethersphere-wpa2	Interfering	1	GN 20MZ	11:30:51	📍
04:46:65:8c:00:ea	ethersphere-wpa2	Interfering	1	GN 20MZ	11:30:35	📍
24:77:03:7a:65:ec	ipv6-alpha	Interfering	1	GN 20MZ	11:30:35	📍
00:37:6d:e2:df:b2	ethersphere-voip	Interfering	1	GN 20MZ	11:30:20	📍
00:03:2a:02:5b:b7	akvoice1	Interfering	1	G	11:30:20	📍
20:02:af:9e:6b:b5	ethersphere-wpa2	Interfering	1	GN 20MZ	11:29:34	📍
00:17:ca:ae:7a:a6	ethersphere-voip	Interfering	1	B	11:29:05	📍
84:29:99:11:35:0d	mdns-roaming	Interfering	11	GN 20MZ	11:29:05	📍
5c:0a:5b:13:a5:cd	ethersphere-voip	Interfering	11	GN 20MZ	11:28:50	📍
20:64:32:51:fc:3f	ipv6-alpha	Interfering	1	GN 20MZ	11:27:49	📍
20:64:32:81:d2:37	ethersphere-wpa2	Interfering	1	BN 20MZ	11:23:34	📍
58:94:6b:31:cf:00	mdns-roaming	Interfering	11	B	11:21:49	📍
00:16:6f:31:88:8a	UI_Dashboard	Interfering	6	G	11:18:18	📍
00:26:c6:be:68:b8	ethersphere-voip	Interfering	6	GN 20MZ	11:18:18	📍

OS Fingerprinting

The OS Fingerprinting feature gathers information about the client that is connected to the 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 Instant network by default. The following operating systems are identified by Instant:

- Windows 7
- Windows Vista

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

Configuring Wireless Intrusion Protection and Detection Levels

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 Aruba network, the WIP can be configured on the IAP.

You can configure the following options:

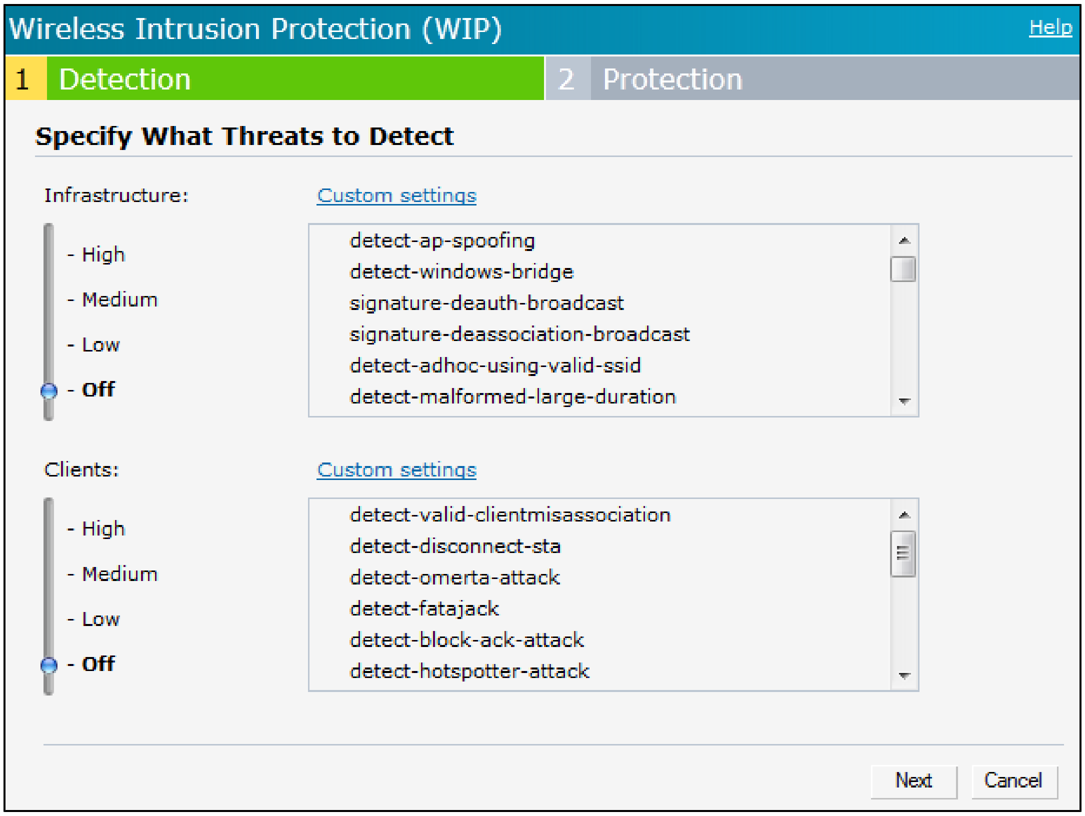
- **Infrastructure Detection Policies**– Specifies the policy for detecting wireless attacks on access points
- **Client Detection Policies**– Specifies the policy for detecting wireless attacks on clients
- **Infrastructure Protection Policies**– Specifies the policy for protecting access points from wireless attacks.
- **Client Protection Policies**– Specifies the policy for protecting clients from wireless attacks.
- **Containment Methods**– Prevents unauthorized stations from connecting to your Instant network.

Each of these options contains several default levels that enable different sets of policies. An administrator can customize enable or disable these options accordingly.

The detection levels can be configured using the **IDS** window. To view the IDS window, click **More**>**IDS** link at the top right corner of the Instant main window. The following levels of detection can be configured in the WIP Detection page:

- **Off**
- **Low**
- **Medium**
- **High**

Figure 74 *Wireless Intrusion Detection*



Specify What Threats to Detect

Infrastructure:

- High
- Medium
- Low
- ● Off

detect-ap-spoofing
detect-windows-bridge
signature-deauth-broadcast
signature-deassociation-broadcast
detect-adhoc-using-valid-ssid
detect-malformed-large-duration

Clients:

- High
- Medium
- Low
- ● Off

detect-valid-clientmisassociation
detect-disconnect-sta
detect-omerta-attack
detect-fatajack
detect-block-ack-attack
detect-hotspotter-attack

The following table describes the detection policies enabled in the Infrastructure Detection **Custom settings** field.

Table 43: *Infrastructure Detection Policies*

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

Table 43: *Infrastructure Detection Policies*

Detection Level	Detection Policy
	• 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 enabled in the Client Detection **Custom settings** field.

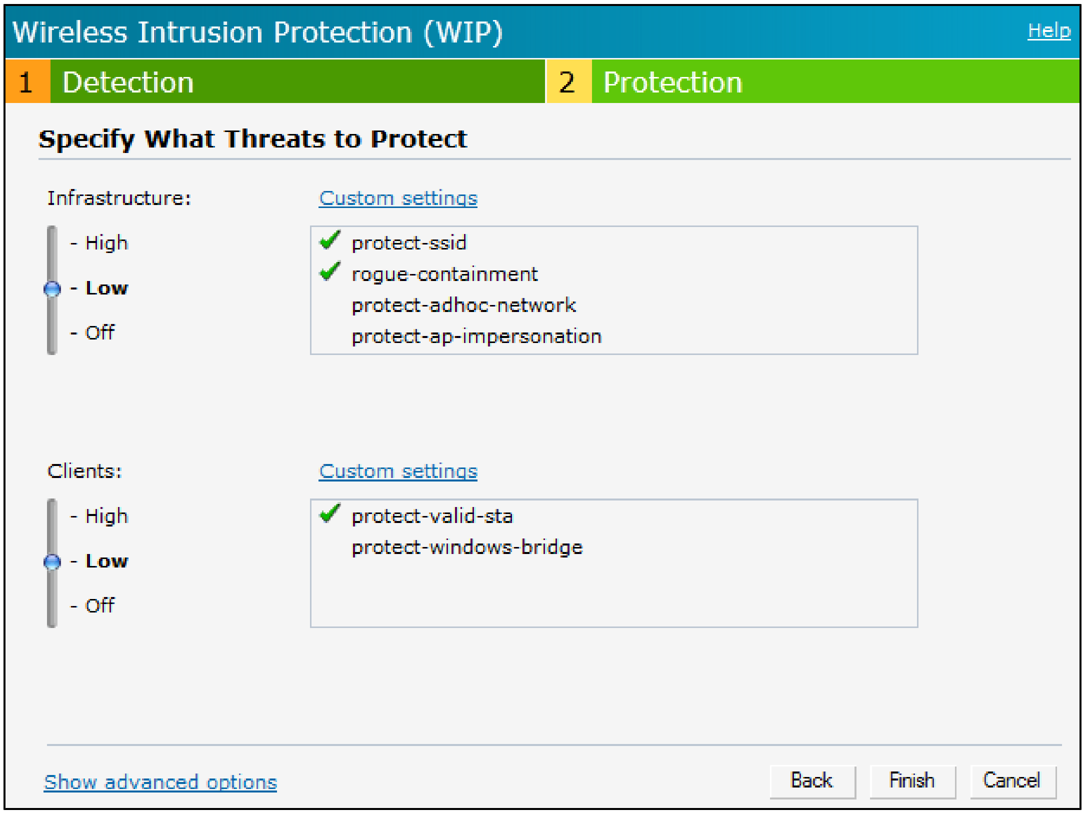
Table 44: *Client Detection Policies*

Detection Level	Detection Policy
Off	All detection policies are disabled.
Low	• Detect Valid Station Misassociation
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

The following levels of detection can be configured in the WIP Protection page:

- **Off**
- **Low**
- **High**

Figure 75 *Wireless Intrusion Protection*



Wireless Intrusion Protection (WIP)

Specify What Threats to Protect

Infrastructure: Low

- ✓ protect-ssid
- ✓ rogue-containment
- protect-adhoc-network
- protect-ap-impersonation

Clients: Low

- ✓ protect-valid-sta
- protect-windows-bridge

The following table describes the protection policies that are enabled in the Infrastructure Protection **Custom settings** field.

Table 45: *Infrastructure Protection Policies*

Protection Level	Protection Policy
Off	All protection 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 the Client Protection **Custom settings** field.

Table 46: *Client Protection Policies*

Protection Level	Protection Policy
Off	All protection policies are disabled
Low	Protect Valid Station
High	Protect Windows Bridge

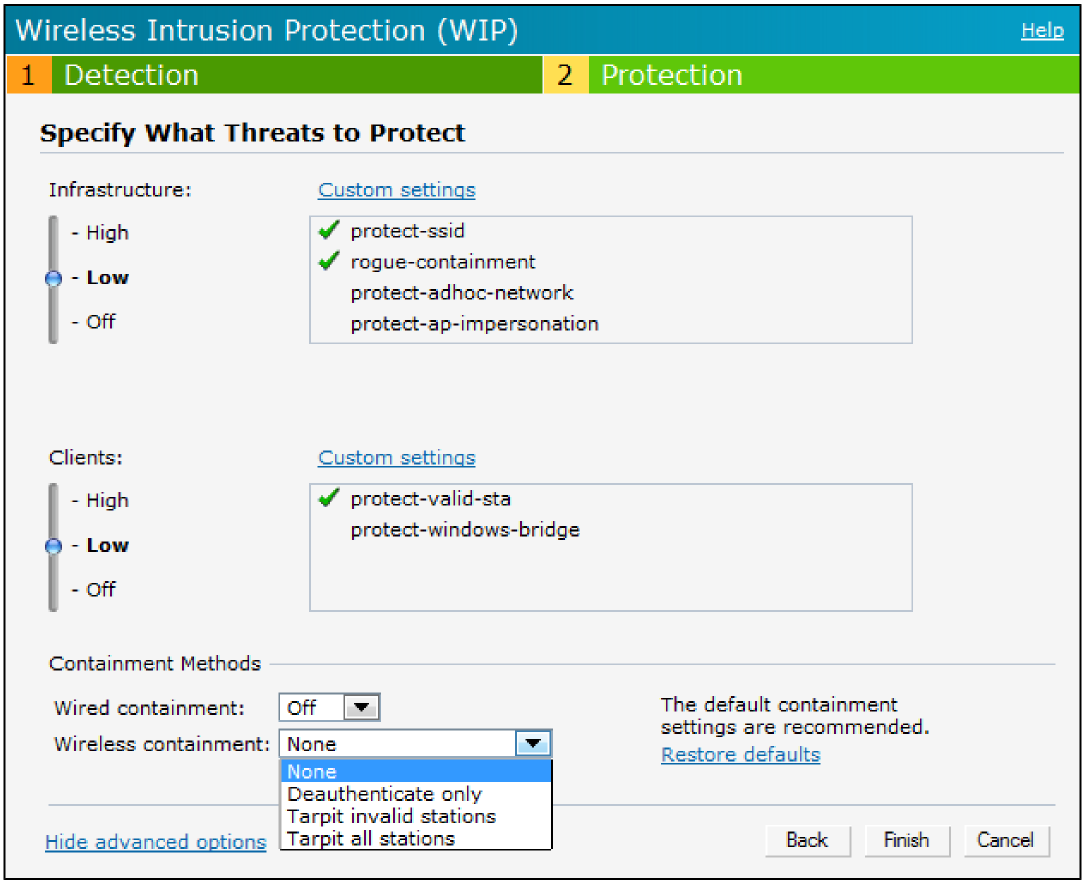
Containment Methods

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, Instant Access Points generate ARP packets on the wired network to contain wireless attacks.
- Wireless containment– When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified Access Point.
  - None– Disables all the containment mechanisms.
  - Deauthenticate only– With deauthentication containment, the Access Point or client is contained by disrupting the client association on the wireless interface.
  - Tarpit containment– With Tarpit containment, the Access Point is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the Access Point being contained.

Figure 76 *Containment Methods*



Wireless Intrusion Protection (WIP)

Specify What Threats to Protect

Infrastructure: Low

✓ protect-ssid
✓ rogue-containment
protect-adhoc-network
protect-ap-impersonation

Clients: Low

✓ protect-valid-sta
protect-windows-bridge

Containment Methods

Wired containment: Off

Wireless containment: None

The default containment settings are recommended.

Configuring IDS Using CLI

To configure IDS using CLI:

```
(Instant Access Point)(config)# ids
(Instant Access Point)(IDS)# infrastructure-detection-level <type>
(Instant Access Point)(IDS)# client-detection-level <type>
(Instant Access Point)(IDS)# infrastructure-protection-level <type>
(Instant Access Point)(IDS)# client-protection-level <type>
```

```
(Instant Access Point)(IDS)# wireless-containment <type>
(Instant Access Point)(IDS)# wired-containment
(Instant Access Point)(IDS)# detect-ap-spoofing
(Instant Access Point)(IDS)# detect-windows-bridge
(Instant Access Point)(IDS)# signature-deauth-broadcast
(Instant Access Point)(IDS)# signature-deassociation-broadcast
(Instant Access Point)(IDS)# detect-adhoc-using-valid-ssid
(Instant Access Point)(IDS)# detect-malformed-large-duration
(Instant Access Point)(IDS)# detect-ap-impersonation
(Instant Access Point)(IDS)# detect-adhoc-network
(Instant Access Point)(IDS)# detect-valid-ssid-misuse
(Instant Access Point)(IDS)# detect-wireless-bridge
(Instant Access Point)(IDS)# detect-ht-40mhz-intolerance
(Instant Access Point)(IDS)# detect-ht-greenfield
(Instant Access Point)(IDS)# detect-ap-flood
(Instant Access Point)(IDS)# detect-client-flood
(Instant Access Point)(IDS)# detect-bad-wep
(Instant Access Point)(IDS)# detect-cts-rate-anomaly
(Instant Access Point)(IDS)# detect-rts-rate-anomaly
(Instant Access Point)(IDS)# detect-invalid-addresscombination
(Instant Access Point)(IDS)# detect-malformed-htie
(Instant Access Point)(IDS)# detect-malformed-assoc-req
(Instant Access Point)(IDS)# detect-malformed-frame-auth
(Instant Access Point)(IDS)# detect-overflow-ie
(Instant Access Point)(IDS)# detect-overflow-eapol-key
(Instant Access Point)(IDS)# detect-beacon-wrong-channel
(Instant Access Point)(IDS)# detect-invalid-mac-oui
(Instant Access Point)(IDS)# detect-valid-clientmisassociation
(Instant Access Point)(IDS)# detect-disconnect-sta
(Instant Access Point)(IDS)# detect-omerta-attack
(Instant Access Point)(IDS)# detect-fatajack
(Instant Access Point)(IDS)# detect-block-ack-attack
(Instant Access Point)(IDS)# detect-hotspotter-attack
(Instant Access Point)(IDS)# detect-unencrypted-valid
(Instant Access Point)(IDS)# detect-power-save-dos-attack
(Instant Access Point)(IDS)# detect-eap-rate-anomaly
(Instant Access Point)(IDS)# detect-rate-anomalies
(Instant Access Point)(IDS)# detect-chopchop-attack
(Instant Access Point)(IDS)# detect-tkip-replay-attack
(Instant Access Point)(IDS)# signature-airjack
(Instant Access Point)(IDS)# signature-asleap
(Instant Access Point)(IDS)# protect-ssid
(Instant Access Point)(IDS)# rogue-containment
(Instant Access Point)(IDS)# protect-adhoc-network
(Instant Access Point)(IDS)# protect-ap-impersonation
(Instant Access Point)(IDS)# protect-valid-sta
(Instant Access Point)(IDS)# protect-windows-bridge
(Instant Access Point)(IDS)# end
(Instant Access Point)# commit apply
```

This chapter provides the following information:

Content Filtering

The Content Filtering feature allows you to create Internet access policies that allow or deny user access to Websites based on Website categories and security ratings. With this feature, you can:

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

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

NOTE

Regardless of whether content filtering is disabled or enabled, the DNS requests to http://instant.arubanetworks.com are always resolved internally on Instant.

Enabling Content Filtering

The content filtering configuration applies to all IAPs in the network and the service is enabled or disabled globally across the wireless or wired network profiles.

You can enable content filtering for an SSID when configuring or modifying a wireless or wired network using Instant UI or CLI.

Enabling Content Filtering for a Wireless Profile

To enable content filtering for a wireless SSID, perform the following steps:

In the Instant UI

1. Select a wireless profile in the **Networks** tab and then click the **edit** link. The window for editing the WLAN SSID profile is displayed.
2. Click **Show advanced options**.
3. Select **Enabled** from the **Content Filtering** drop-down list and click **Next** to continue.

You can also enable content filtering while adding a new wireless profile. For more information, see Configuring WLAN Settings for an SSID Profile on page 90.

In the CLI

To enable content filtering on a WLAN SSID:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name>)# content-filtering
```

```
(Instant Access Point)(SSID Profile <name>)# end
(Instant Access Point)# commit apply
```

Enabling Content Filtering for a Wired Profile

To enable content filtering for a wired profile, perform the following steps:

In the Instant UI

1. Click the **Wired** link under **More** at the top right corner of the Instant main window. The **Wired** window appears.
2. In the **Wired** window, select the wired profile to modify.
3. Click **Edit**. The **Edit Wired Network** window is displayed.
4. In the **Wired Settings** tab, select **Enabled** from the **Content Filtering** drop-down list and click **Next** to continue.

In the CLI

To enable content filtering for a wired profile in the CLI:

```
(Instant Access Point)(config)# wired-port-profile test
(Instant Access Point)(wired ap profile <name>)# content-filtering
(Instant Access Point)(wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Configuring Enterprise Domains

The enterprise domain names list displays the DNS domain names that are valid on the enterprise network. This list is used to determine how client DNS requests should be routed. When **Content Filtering** is enabled, the DNS request of the clients is verified and the domain names that do not match the names in the list are sent to the open DNS server.

You can configure an enterprise domain using Instant UI or CLI.

In the Instant UI

To manually add a domain:

1. Navigate to **System**> **General**, click **Show advanced options** >**Enterprise Domains**. The **Enterprise Domain** tab contents are displayed.
2. Click **New** and enter a **New Domain Name**
3. Click **OK** to apply the changes.

To delete a domain, select the domain and click **Delete** to remove the domain name from the list.

In the CLI

To configure an enterprise domain:

```
(Instant Access Point)(config)# internal-domains
(Instant Access Point)(domain)# domain-name <name>
(Instant Access Point)(domain)# end
(Instant Access Point)# commit apply
```

Configuring OpenDNS Credentials

When configured, the OpenDNS credentials are used by Instant to access OpenDNS to provide enterprise-level content filtering. You can configure OpenDNS credentials using Instant UI or CLI.

In the Instant UI

To configure OpenDNS credentials:

1. Click **More**> **Services**>**OpenDNS**. The **OpenDNS** tab contents are displayed.
2. Enter the **Username** and **Password** to enable access to OpenDNS.
3. Click **OK** to apply the changes.

In the CLI

To configure OpenDNS credentials:

```
(Instant Access Point)(config)# opendns <username <password>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

This chapter provides the following information:

- Configuring DHCP Scopes on page 241
- Configuring DHCP Server for Client IP Assignment on page 248

Configuring DHCP Scopes

The Virtual Controller supports different modes of DHCP address assignment. With each DHCP address assignment mode, various client traffic forwarding modes are associated. For more information client traffic forwarding modes for IAP-VPN, see L2/L3 Forwarding Modes on page 263.

You can configure Distributed,L2, Distributed,L3, Local or NAT DHCP, Local,L3, and Centralized L2 DHCP scopes using the Instant UI or CLI.

This section describes the following procedures:

- Configuring Distributed DHCP Scopes on page 241
- Configuring Centralized DHCP Scope on page 244
- Configuring Local and Local,L3 DHCP Scopes on page 246

Configuring Distributed DHCP Scopes

Instant allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

Instant supports the following distributed DHCP scopes:

- **Distributed, L2** – In this mode, the Virtual Controller acts as the DHCP server, but the default gateway is in the data center. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the Virtual Controller controls a scope that is a subset of the complete IP Address range for the subnet distributed across all the branches. This DHCP Assignment mode is used with the L2 forwarding mode.
- **Distributed, L3** – In this mode, the Virtual Controller acts as the DHCP server and the default gateway. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the Virtual Controller is configured with a unique subnet and a corresponding scope.

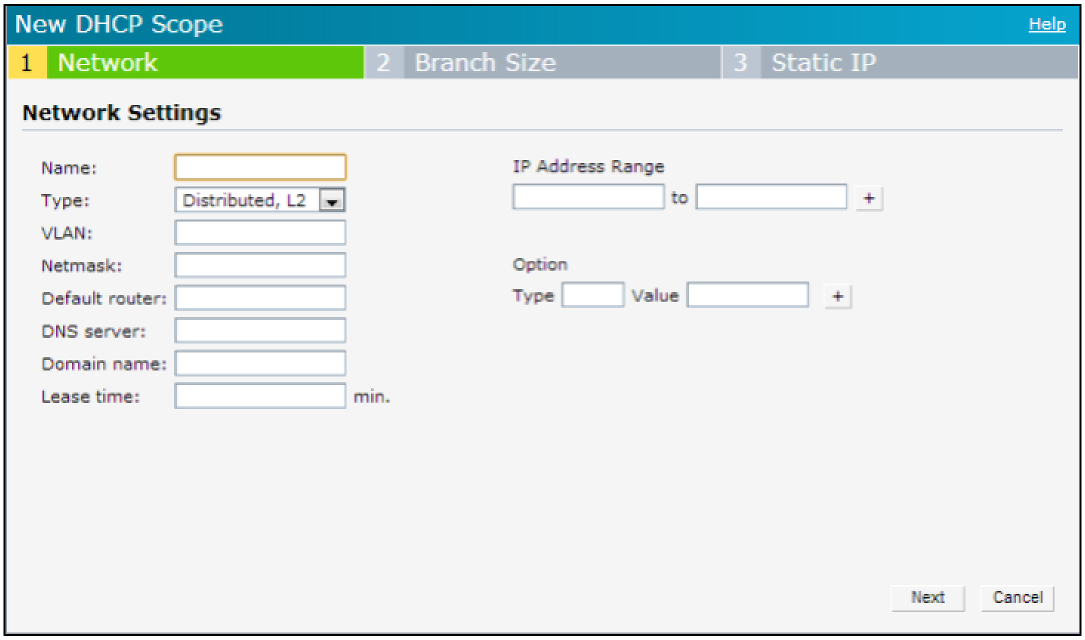
You can configure distributed DHCP scopes such as Distributed, L2 or Distributed,L3 by using the Instant UI or CLI.

In the Instant UI

To configure distributed DHCP scopes such as Distributed,L2 or Distributed,L3:

1. Click **More**>**DHCP**. The **DHCP Server** window is displayed.
2. To configure a distributed DHCP mode, click **New** under **Distributed DHCP Scopes**. The **New DHCP Scope** window is displayed. The following figure shows the contents of the **New DHCP Scope** window.

Figure 77 *New DHCP Scope: Distributed DHCP Mode*



New DHCP Scope

Network Settings

Name:

Type: Distributed, L2

VLAN:

Netmask:

Default router:

DNS server:

Domain name:

Lease time: min.

IP Address Range

to

Option

Type Value

3. Based on type of distributed DHCP scope, configure the following parameters:

Table 47: *Distributed DHCP Mode: Configuration Parameters*

Name	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ● **Distributed, L2**– On selecting **Distributed, L2**, the Virtual Controller acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. ● **Distributed, L3**– On selecting **Distributed, L3**, the Virtual Controller acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 93 and Configuring VLAN for a Wired Profile on page 108
Netmask	If **Distributed, L2** is selected for type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Default router	If **Distributed, L2** is selected for type of DHCP scope, specify the IP address of the default router.
DNS Server	If required, specify the IP address of a DNS server.
Domain Name	If required, specify the domain name.
Lease Time	Specify a lease time for the client in minutes.
IP Address Range	Specify a range of IP addresses to use. To add another range, click the + icon. You can specify up to four different ranges of IP addresses. ● For Distributed,L2 mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is

Table 47: *Distributed DHCP Mode: Configuration Parameters*

Name	Description
	performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. - For Distributed,L3 mode, you can configure any discontiguous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count. **NOTE:** You can allocate multiple branch IDs (BID) per subnet. The IAP generates a subnet name from the DHCP IP configuration, which the controller can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with BID 0, which is mapped directly to the configured static subnet.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. To add multiple DHCP options, click the + icon. You can add up to eight DHCP options.

4. Click **Next**.
5. Specify the number of clients to use per branch. The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The IAP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.
6. Click **Next**. The **Static IP** tab is displayed. Specify the number of first and last IP addresses to reserve in the subnet.
7. Click **Finish**.

In the CLI

To configure Distributed,L2 DHCP scope:

```
(Instant Access Point)(config)# ip dhcp <profile-name>
(Instant Access Point)(DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L2>
(Instant Access Point)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant Access Point)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant Access Point)(DHCP Profile <profile-name>)# default-router <IP-address>
(Instant Access Point)(DHCP Profile <profile-name>)# client-count <number>
(Instant Access Point)(DHCP Profile <profile-name>)# dns-server <name>
(Instant Access Point)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant Access Point)(DHCP Profile <profile-name>)# lease-time <minutes>
(Instant Access Point)(DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(Instant Access Point)(DHCP Profile <profile-name>)# reserve {first|last} <count>
(Instant Access Point)(DHCP Profile <profile-name>)# option <type> <value>
(Instant Access Point)(DHCP Profile <profile-name>)# end
(Instant Access Point))# commit apply
```

To configure Distributed,L3 DHCP scope:

```
(Instant Access Point)(config)# ip dhcp <profile-name>
(Instant Access Point)(DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L3>
(Instant Access Point)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant Access Point)(DHCP Profile <profile-name>)# client-count <number>
(Instant Access Point)(DHCP Profile <profile-name>)# dns-server <name>
(Instant Access Point)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant Access Point)(DHCP Profile <profile-name>)# lease-time <minutes>
```

```
(Instant Access Point)(DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(Instant Access Point)(DHCP Profile <profile-name>)# reserve {first | last} <count>
(Instant Access Point)(DHCP Profile <profile-name>)# option <type> <value>
(Instant Access Point)(DHCP Profile <profile-nae>)# end
(Instant Access Point))# commit apply
```

Configuring Centralized DHCP Scope

The Centralized DHCP scope supports L2 and L3 clients.

When a centralized DHCP scope is configured:

- The Virtual Controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP Server.
- For L2 clients, the Virtual Controller bridges the DHCP traffic to the controller over the VPN/GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN/GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the controller.
- For L3 clients, the Virtual Controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the controller in the corporate network and reachable through the IPSec tunnel. The centralized L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

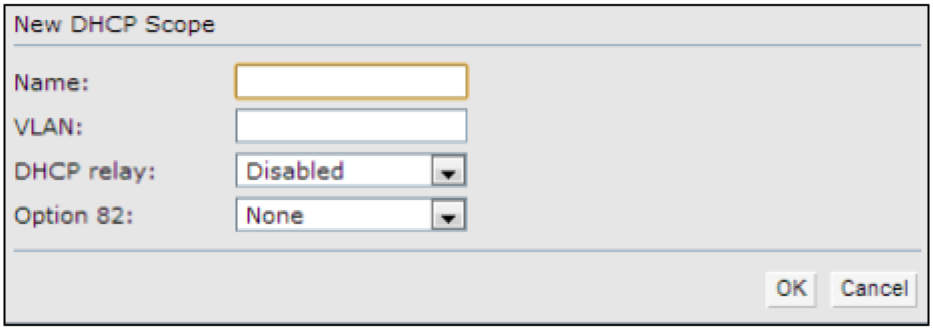
You can configure Centralized DHCP scope by using the Instant UI or CLI.

In the Instant UI

To configure a centralized DHCP scope:

1. Click **More**>**DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a **Centralized** DHCP scopes, click **New** under **Centralized DHCP Scopes**. The **New DHCP Scope** window is displayed. The following figure shows the contents of the **New DHCP Scope** window.

Figure 78 *New DHCP Scope: Centralized DHCP Scope*



New DHCP Scope

Name:

VLAN:

DHCP relay: Disabled

Option 82: None

3. Based on type of DHCP scope, configure the following parameters:

Table 48: *DHCP Mode: Configuration Parameters*

Name	Description
Name	Enter a name for the DHCP scope.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 93 and Configuring VLAN for a Wired Profile on page 108
DHCP relay	Select **Enabled** to allow the IAPs to intercept the broadcast packets and relay DHCP

Table 48: *DHCP Mode: Configuration Parameters*

Name	Description
	requests.
Helper address	Enter the IP address of the DHCP server.
VLAN IP	Specify the VLAN IP address of the DHCP relay server.
VLAN Mask	Specify the VLAN subnet mask of the DHCP relay server.
Option82	This option is available only if Centralized is selected. Select **Alcatel** to enable DHCP Option 82 to allow clients to send DHCP packets with the Option 82 string. The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following: ● Remote Circuit ID; X AP-MAC; SSID; SSID-Type ● Remote Agent; X IDUE-MAC

4. Click **OK**.

The Option 82 is specific to Alcatel and is not configurable in this version of Instant.

The following table describes the behavior of DHCP Relay Agent and Option 82 in the IAP.

Table 49: *DHCP Relay and Option 82*

DHCP Relay	Option 82	Behavior
Enabled	Enabled	DHCP packet relayed with the ALU-specific Option 82 string
Enabled	Disabled	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	Enabled	DHCP packet not relayed, but broadcast with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcast without the ALU-specific Option 82 string

In the CLI

To configure Centralized DHCP scope for L2 clients:

```
(Instant Access Point)(config)# ip dhcp <profile-name>
(Instant Access Point)(DHCP Profile <profile-name>)# server-type <centralized>
(Instant Access Point)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant Access Point)(DHCP Profile <profile-name>)# option82 alu
(Instant Access Point)(DHCP Profile <profile-name>)# end
(Instant Access Point))# commit apply
(Instant Access Point))# commit apply
```

To configure Centralized DHCP scope for L3 clients:

```
(Instant Access Point)(config)# ip dhcp <profile-name>
(Instant Access Point)(DHCP Profile <profile-name>)# server-type <centralized>
(Instant Access Point)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant Access Point)(DHCP Profile <profile-name>)# dhcp-relay
(Instant Access Point)(DHCP Profile <profile-name>)# dhcp-server <DHCP-relay-server>
(Instant Access Point)(DHCP Profile <profile-name>)# vlan-ip <DHCP IP address> mask <VLAN mas
k>
(Instant Access Point)(DHCP Profile <profile-name>)# end
```

```
(Instant Access Point))# commit apply
```

Configuring Local and Local,L3 DHCP Scopes

You can configure Local and Local,L3 DHCP scopes by using the Instant UI or CLI.

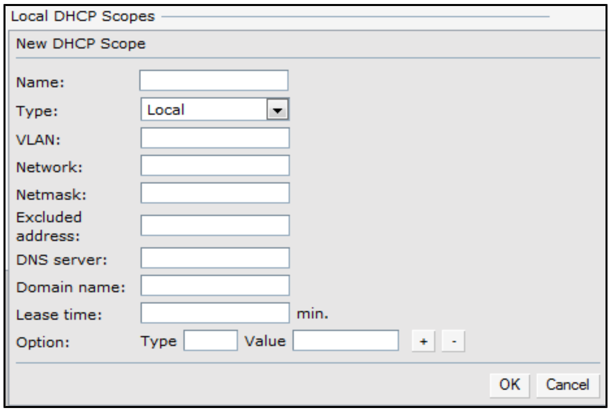
- **Local** – In this mode, the Virtual Controller acts as both the DHCP Server and the default gateway. The configured subnet and the corresponding DHCP scope are independent of subnets configured in other IAP clusters. The Virtual Controller assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPSec tunnel or through the uplink. This DHCP assignment mode is used for the NAT forwarding mode.
- **Local, L3**– In this mode, the Virtual Controller acts as a DHCP server and the gateway, and assigns an IP address from the local subnet. The IAP routes the packets sent by clients on its uplink. This mode does not provide corporate access through the IPsec tunnel. This DHCP assignment mode is used with the L3 forwarding mode.

In the Instant UI

To configure a Local or Local,L3 DHCP scope:

1. Click **More**>**DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a **Local** or **Local,L3** DHCP scopes, click **New** under **Local DHCP Scopes**. The **New DHCP Scope** window is displayed. The following figure shows the contents of the **New DHCP Scope** window.

Figure 79 *New DHCP Scope: Other DHCP scopes*



Local DHCP Scopes

New DHCP Scope

Name:

Type: Local

VLAN:

Network:

Netmask:

Excluded address:

DNS server:

Domain name:

Lease time: min.

Option: Type Value + -

OK Cancel

3. Based on type of DHCP scope, configure the following parameters:

Table 50: *DHCP Mode: Configuration Parameters*

Name	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ● **Local**– On selecting **Local**, the DHCP server for local branch network is used for keeping the scope of the subnet local to the IAP. In the NAT mode, the traffic is forwarded through the IPSec tunnel or the uplink. ● **Local, L3**–On selecting **Local, L3**, the Virtual Controller acts as a DHCP server and gateway. In this mode, the IAP routes the packets sent by clients and also adds a route on the controller, after the VPN tunnel is set up during the registration of the subnet.

Table 50: *DHCP Mode: Configuration Parameters*

Name	Description
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 93 and Configuring VLAN for a Wired Profile on page 108
Network	Specify the network to use.
Net Mask	If **Local** or **Local,L3** is selected, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Excluded address	If **Local,L3** is selected, specify the IP address to exclude, The value entered in the field determines the exclusion range of the subnet. Based on the size of the subnet, the IP addresses that come before or after the IP address value specified in this field are excluded.
DNS Server	If required, specify the IP address of a DNS server for the **Local** and **Local,L3** scopes.
Domain Name	If required, specify the domain name for the **Local** and **Local,L3** scopes.
Lease Time	Specify a lease time for the client in minutes.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, and 161. To add multiple DHCP options, click the + icon.

4. Click **OK**.

In the CLI

To configure Local DHCP scope:

```
(Instant Access Point)(config)# ip dhcp <profile-name>
(Instant Access Point)(DHCP Profile <profile-name>)# server-type <Local>
(Instant Access Point)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant Access Point)(DHCP Profile <profile-name>)# subnet <IP-address>
(Instant Access Point)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant Access Point)(DHCP Profile <profile-name>)# dns-server <name>
(Instant Access Point)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant Access Point)(DHCP Profile <profile-name>)# lease-time <minutes>
(Instant Access Point)(DHCP Profile <profile-name>)# option <type> <value>
(Instant Access Point)(DHCP Profile <profile-name>)# end
(Instant Access Point))# commit apply
```

To configure Local,L3 DHCP scope:

```
(Instant Access Point)(config)# ip dhcp <profile-name>
(Instant Access Point)(DHCP Profile <profile-name>)# server-type <Local,L3>
(Instant Access Point)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant Access Point)(DHCP Profile <profile-name>)# subnet <IP-address>
(Instant Access Point)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant Access Point)(DHCP Profile <profile-name>)# exclude-address <IP-address>
(Instant Access Point)(DHCP Profile <profile-name>)# dns-server <name>
(Instant Access Point)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant Access Point)(DHCP Profile <profile-name>)# lease-time <minutes>
(Instant Access Point)(DHCP Profile <profile-name>)# option <type> <value>
(Instant Access Point)(DHCP Profile <profile-name>)# end
(Instant Access Point))# commit apply
```

Configuring DHCP Server for Client IP Assignment

The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the Virtual Controller. You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. The largest address pool supported is 2048. The default size of the IP address pool is 512.

When the DHCP server is configured and if the **Client IP assignment** parameter for an SSID profile is set to **Virtual Controller Assigned**, the Virtual Controller assigns the IP addresses to the WLAN or wired clients. By default, the IAP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks.
In the current release, the IAP typically selects the 172.31.98.0/23 subnet. If the IP address of the IAP is within the 172.31.98.0/23 subnet, the IAP selects the 10.254.98.0/23 subnet. However, this mechanism does not guarantee that it would avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to Aruba Instant 6.2.1.0-3.4, manually configure the DHCP pool by following the steps described in this section.

You can configure a domain name, DNS server and DHCP server for client IP assignment using Instant UI or CLI.

In the Instant UI

1. Click the **System** link at top right corner of the Instant main window. The **System** window appears.
2. In the **DHCP** tab, enter the domain name of the client in the **Domain name** text box.
3. Enter the IP addresses of the DNS servers separated by comma(,) in the **DNS server** text box.
4. Enter the duration of the DHCP lease in the **Lease time** text box.
5. Select **Minutes**, **Hours**, or **Days** for the lease time from the drop-down list next to **Lease time**. The default lease time is 0.
6. Enter the network in the **Network** text box.
7. Enter the mask in the **Mask** text box.

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

8. Click **OK** to apply the changes.

In the CLI

To configure a DHCP pool:

```
(Instant Access Point)(config)# ip dhcp pool
(Instant Access Point)(DHCP)# domain-name <domain>
(Instant Access Point)(DHCP)# dns-server <DNS-IP-address>
(Instant Access Point)(DHCP)# lease-time <lease-time>
(Instant Access Point)(DHCP)# subnet <IP-address>
(Instant Access Point)(DHCP)# subnet-mask <subnet-mask>
```

To view the DHCP database:

```
(Instant Access Point)# show ip dhcp database

DHCP Subnet          :192.0.2.0
DHCP Netmask         :255.255.255.0
DHCP Lease Time(m)   :20
DHCP Domain Name     :example.com
DHCP DNS Server      :192.0.2.1
```

This chapter describes the following VPN configuration procedures:

- Understanding VPN Features on page 249
- Configuring a Tunnel from an IAP to Aruba Mobility Controller on page 249
- Configuring Routing Profiles on page 260

Understanding VPN Features

As IAPs use a Virtual Controller architecture, the IAP network does not require a physical controller to provide the configured WLAN services. However, a physical controller is required for terminating Virtual Private Networks (VPN) tunnels from the IAP networks at branch locations or datacenters, where the Aruba controller acts as a VPN concentrator.

When VPN is configured, the IAP acting as the Virtual Controller creates a VPN tunnel to an Aruba Mobility Controller in your corporate office. The controller acts as a VPN end-point and does not supply the IAP with any configuration.

The VPN features are recommended for:

- Enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
- Branch offices that require multiple APs.
- Individuals working from home, connecting to the VPN.

The survivability feature of IAPs with the VPN connectivity of RAPs allows you to provide corporate connectivity to non-corporate networks.

Configuring a Tunnel from an IAP to Aruba Mobility Controller

IAP supports the configuration of tunneling protocols such as Generic Routing Encapsulation (GRE), IPsec, and L2TPv3. This section describes the procedure for configuring VPN host settings on an IAP to enable communication with a remote Controller:

- Configuring an Aruba IPSec Tunnel on page 249
- Enabling Automatic Configuration of Aruba GRE Tunnel on page 251
- Manually Configuring a GRE Tunnel on page 253
- Configuring an L2TPv3 Tunnel on page 254

Configuring an Aruba IPSec Tunnel

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPSec tunnel to the Aruba Controller secures corporate data. You can configure an Aruba IPSec tunnel from Virtual Controller using Instant UI or CLI.

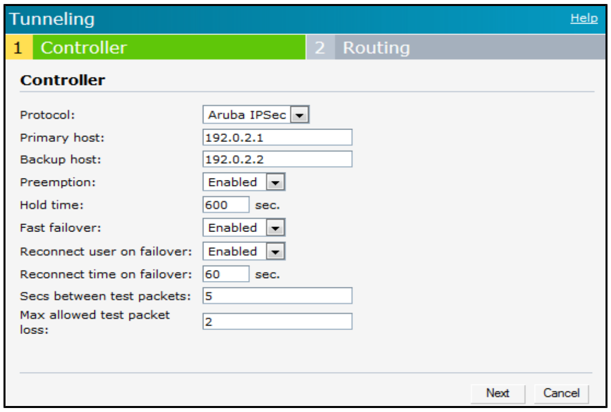
In the Instant UI

To configure a tunnel using IPSec Protocol:

1. Click the **More**>**VPN** link at the top right corner of the Instant UI. The **Tunneling** window is displayed.
2. Select **Aruba IPSec** from the **Protocol** drop-down list.

3. Enter the IP address or fully qualified domain name (FQDN) for the main VPN/IPSec endpoint in the **Primary host** field.
4. Enter the IP address or FQDN for the backup VPN/IPSec endpoint in the **Backup host** field. This entry is optional. When you specify the primary and backup host details, the other fields are displayed
5. Specify the following parameters. A sample configuration is shown in Figure 80.
   a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list . This step is optional.
   b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold-time. The default value for **Hold time** is 600 seconds.
   c. To allow the IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** from the **Fast failover** drop-down list. When fast failover is enabled and if the primary tunnel fails, the IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
   d. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the IAP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the IAP will send one packet to the controller at every 5 seconds.
   e. Enter a value for **Max allowed test packet loss**, to define a number for lost packets, after which the IAP can determine that the VPN connection is unavailable. The default value is 2.
   f. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect user on failover** to **Enabled**.
   g. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect time on failover** within a range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.

Figure 80 *Aruba IPSec Configuration*



Controller

Protocol: Aruba IPSec
Primary host: 192.0.2.1
Backup host: 192.0.2.2
Preemption: Enabled
Hold time: 600 sec.
Fast failover: Enabled
Reconnect user on failover: Enabled
Reconnect time on failover: 60 sec.
Secs between test packets: 5
Max allowed test packet loss: 2

6. Click **Next** to continue. When the IPsec tunnel configuration is completed, the packets that are sent from and received by an IAP are encrypted.

In the CLI

To configure an Aruba IPSec VPN tunnel:

```
(Instant Access Point)(config)# vpn primary <name>
(Instant Access Point)(config)# vpn backup <name>
(Instant Access Point)(config)# vpn fast-failover
(Instant Access Point)(config)# vpn hold-time <seconds>
(Instant Access Point)(config)# vpn preemption
(Instant Access Point)(config)# vpn monitor-pkt-send-freq <frequency>
(Instant Access Point)(config)# vpn monitor-pkt-lost-cnt <count>
```

```
(Instant Access Point)(config)# vpn reconnect-user-on-failover
(Instant Access Point)(config)# vpn reconnect-time-on-failover <down_time>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Example

```
(Instant Access Point)(config)# vpn primary 192.0.2.18
(Instant Access Point)(config)# vpn backup  192.0.2.18
(Instant Access Point)(config)# vpn fast-failover
(Instant Access Point)(config)# vpn preemption

(Instant Access Point)(config)# ip dhcp distl2
(Instant Access Point)(DHCP Profile "distL2")# server-type Distributed,L2
(Instant Access Point)(DHCP Profile "distL2")# server-vlan 2
(Instant Access Point)(DHCP Profile "distL2")# ip-range 10.15.205.0 10.15.205.255
(Instant Access Point)(DHCP Profile "distL2")# subnet-mask 255.255.255.0
(Instant Access Point)(DHCP Profile "distL2")# lease-time 86400
(Instant Access Point)(DHCP Profile "distL2")# default-router 10.15.205.254
(Instant Access Point)(DHCP Profile "distL2")# dns-server 10.13.6.110,10.1.1.50
(Instant Access Point)(DHCP Profile "distL2")# domain-name arubanetworks.com
(Instant Access Point)(DHCP Profile "distL2")# client-count 5

(Instant Access Point)(config)# ip dhcp local
(Instant Access Point)(DHCP Profile "local")# server-type Local
(Instant Access Point)(DHCP Profile "local")# server-vlan 200
(Instant Access Point)(DHCP Profile "local")# subnet 172.16.200.1
(Instant Access Point)(DHCP Profile "local")# subnet-mask 255.255.255.0
(Instant Access Point)(DHCP Profile "local")# lease-time 86400
(Instant Access Point)(DHCP Profile "local")# dns-server 10.13.6.110,10.1.1.50
(Instant Access Point)(DHCP Profile "local")# domain-name arubanetworks.com
```

To view VPN configuration:

```
Instant Access Point# show vpn config
```

Enabling Automatic Configuration of Aruba GRE Tunnel

Aruba GRE is an Aruba proprietary tunnel protocol for encapsulating multicast, broadcast, and L2 packets between Aruba Controllers and IAPs. The automatic GRE features uses the IPSec connection between IAP and Aruba Controller to send the control information for setting up a GRE tunnel. When automatic GRE configuration is enabled, a single IPSec tunnel between the IAP cluster and Aruba Controller and one or several GRE tunnels are created based on the Per-AP tunnel configuration on the IAP. When this feature is enabled on the IAP, no manual configuration is required on Aruba Controller to create the GRE tunnel.

NOTE

Automatic configuration of GRE tunnel is supported only on Aruba Controllers. This feature is not supported on controllers running ArubaOS 6.3.x.x or lowe versions.

You can configure an IAP to automatically set up a Aruba GRE tunnel from the IAP to Aruba Controller by using Instant UI or CLI.

In the Instant UI

1. Click the **More**>**VPN** link at the top right corner of the Instant UI. The **Tunneling** window is displayed.
2. Select **Aruba GRE** from the **Protocol** drop-down list.
3. Enter the IP address or FQDN for the main VPN/IPSec endpoint in the **Primary host** field.
4. Enter the IP address or FQDN for the backup VPN/IPSec endpoint in the **Backup host** field. This entry is optional. When you enter Primary host IP address, Backup host IP address, other fields are displayed.
5. Specify the following parameters. A sample configuration is shown in Figure 81.

a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list. This step is optional.

b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold time. The default value for **Hold time** is 600 seconds.

c. To allow the IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** or **Disabled** from the **Fast failover** drop-down list. If the primary tunnel fails, the IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect user on failover** to **Enabled**.

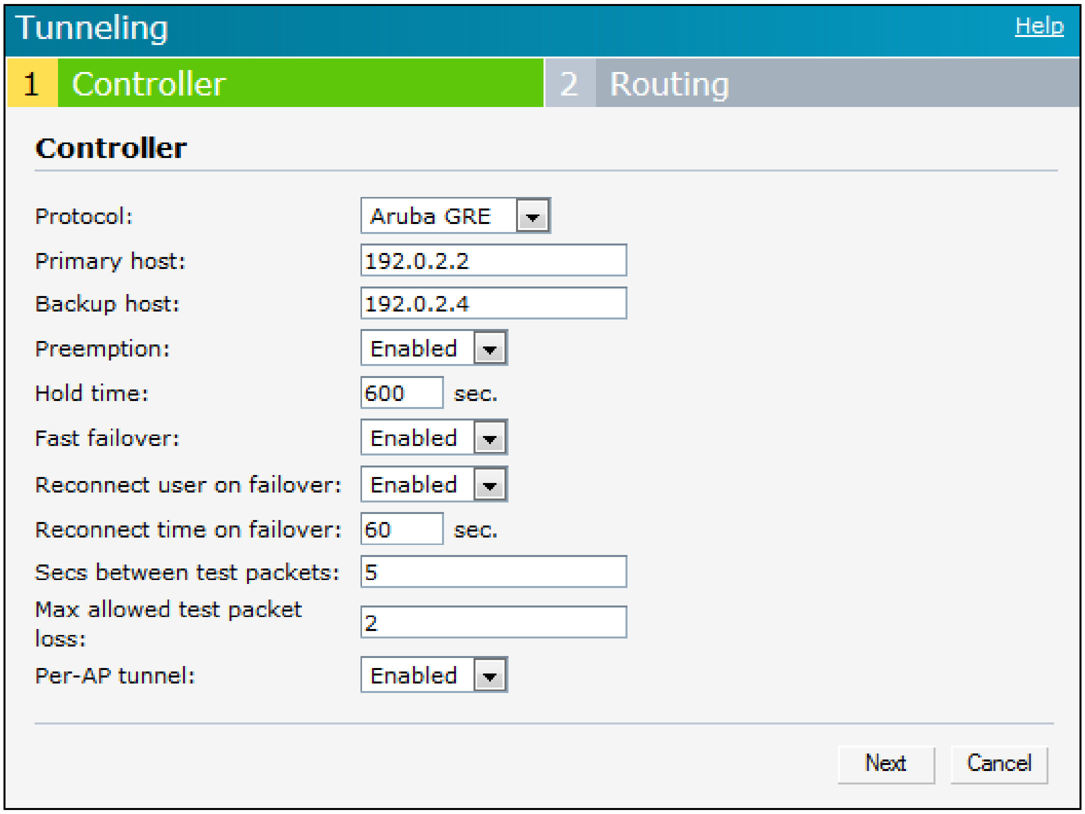
e. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect time on failover** within the range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.

f. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the IAP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the IAP will send one packet to the controller at every 5 seconds.

g. Enter a value for **Max allowed test packet loss**, to define a number for lost packets, after which the IAP can determine that the VPN connection is unavailable. The default value is 2.

h. Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. The administrator can enable this option to create a GRE tunnel from each IAP to the VPN/GRE Endpoint rather than the tunnels created just from the master IAP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the IAP itself and need not be forwarded through the master IAP.

Figure 81 *Aruba GRE Configuration*



Controller

Protocol:	Aruba GRE
Primary host:	192.0.2.2
Backup host:	192.0.2.4
Preemption:	Enabled
Hold time:	600 sec.
Fast failover:	Enabled
Reconnect user on failover:	Enabled
Reconnect time on failover:	60 sec.
Secs between test packets:	5
Max allowed test packet loss:	2
Per-AP tunnel:	Enabled

6. Click **Next** to continue.

In the CLI

To enable automatic confieguration of the GRE tunnel:

```
(Instant Access Point)(config)# vpn gre-outside
(Instant Access Point)(config)# vpn primary <name/IP-address>
(Instant Access Point)(config)# vpn backup <<name/IP-address>>
(Instant Access Point)(config)# vpn fast-failover
(Instant Access Point)(config)# vpn hold-time <seconds>
(Instant Access Point)(config)# vpn preemption
(Instant Access Point)(config)# vpn monitor-pkt-send-freq <frequency>
(Instant Access Point)(config)# vpn monitor-pkt-lost-cnt <count>
(Instant Access Point)(config)# vpn reconnect-user-on-failover
(Instant Access Point)(config)# vpn reconnect-time-on-failover <down_time>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To view VPN configuration details:

```
   Instant Access Point# show vpn config
```

Manually Configuring a GRE Tunnel

You can also manually configure a GRE tunnel by configuring the GRE tunnel parameters on the IAP and controller. This procedure describes the steps involved in manual configuration of GRE tunnel from Virtual Controller by using Instant UI or CLI.

During the manual GRE setup, you can either use the Virtual Controller IP or the IAP IP to create the GRE tunnel at the controller side depending upon the following IAP settings:

- If a Virtual Controller IP is configured and if Per-AP tunnel is disabled, then the Virtual Controller IP is used to create the GRE tunnel.
- If a Virtual Controller IP is not configured or if Per-AP tunnel is enabled, then the IAP IP is used to create the GRE tunnel.

For information on the GRE tunnel configuration on Controller, see *ArubaOS User Guide*.

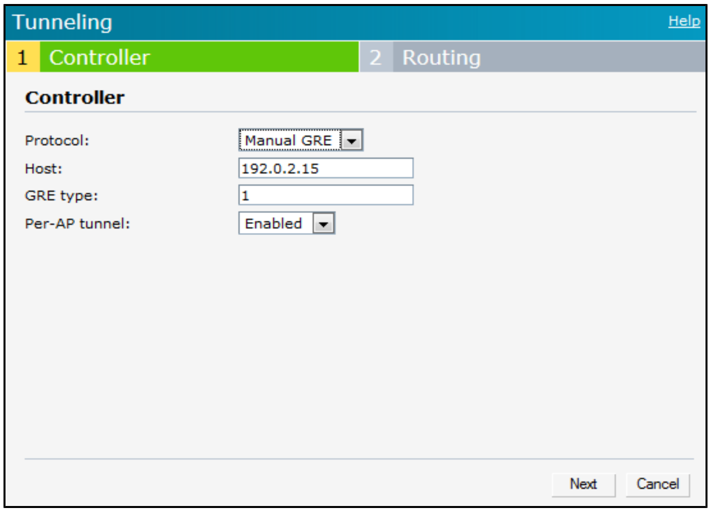
In the Instant UI

1. Click the **More**>**VPN** link at the top right corner of the Instant UI. The **Tunneling** window is displayed.
2. Select **Manual GRE** from the **Protocol** drop-down list.
3. Specify the following parameters. A sample configuration is shown in Figure 82.
   a. Enter the IP address or the FQDN for the main VPN/GRE endpoint.
   b. Enter the value for GRE type parameter.
   c. Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. The administrator can enable this option to create a GRE tunnel from each IAP to the VPN/GRE Endpoint rather than the tunnels created just from the master IAP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the IAP itself and need not be forwarded through the master IAP.

NOTE

By default, the **Per-AP tunnel** option is disabled.

Figure 82 *Manual GRE Configuration*



Controller

Protocol: Manual GRE

Host: 192.0.2.15

GRE type: 1

Per-AP tunnel: Enabled

4. Click **Next** to continue. When the GRE tunnel configuration is completed on both the IAP and Aruba Controller, the packets sent from and received by an IAP are encapsulated, but not encrypted.

In the CLI

To configure a manual GRE VPN tunnel:

```
(Instant Access Point)(config)# gre primary <name>
(Instant Access Point)(config)# gre type <type>
(Instant Access Point)(config)# gre per-ap-tunnel
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To view VPN configuration details:

```
Instant Access Point# show vpn config
```

Configuring an L2TPv3 Tunnel

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows IAP to act as L2TP Access Concentrator (LAC) and tunnel all wireless clients L2 traffic from AP to L2TP Network Server (LNS). In a centralized L2 model, the VLAN on the corporate side are extended to remote branch sites. Wireless clients associated to IAP gets the IP address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel. In this release, L2TPv3 supports following:

- Instant supports tunnel and session configuration, and uses Control Message Authentication (RFC 3931) for tunnel and session establishment. Each L2TPv3 tunnel supports one data connection and this connection is termed as an L2TPv3 session.
- Each IAP supports tunneling over UDP only.
- If primary LNS is down, then it will failover to the backup LNS. L2TPv3 has one tunnel profile and under this, one primary peer and a backup peer are configured. If the primary tunnel creation fails or if the primary tunnel gets deleted, the backup starts. Following two failover modes are supported:
    - Preemptive: In this mode, if the primary comes up when the backup is active, the backup tunnel is deleted and primary will be the only active tunnel. If you configure the tunnel to be preemptive, and when the primary tunnel goes down, it will start the persistence timer which tries to bring up the primary tunnel.
    - Non-Preemptive: In this mode, when the back tunnel is established after primary tunnel goes down, it does not make the primary tunnel active again.
- L2TPV3 configuration is supported on the following IAPs:
    - RAP-108

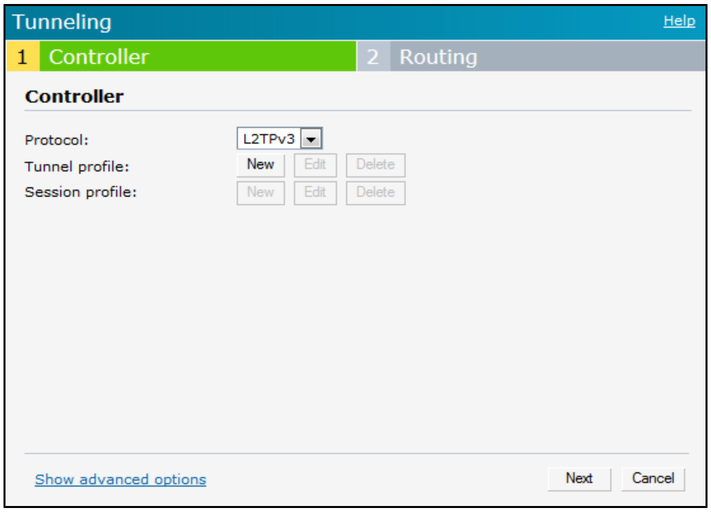
- RAP-109
- IAP-135

You can configure an L2TPv3 tunnel from Virtual Controller using Instant UI or CLI.

In the Instant UI

1. Click the **More**>**VPN** link at the top right corner of the Instant UI. The **Tunneling** window is displayed.

Figure 83 *L3TPv3 Tunneling*



Tunneling

1 Controller

2 Routing

Controller

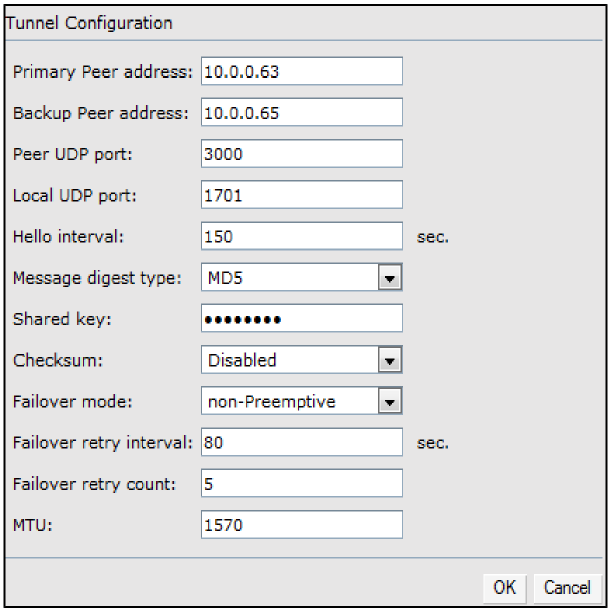
Protocol: L2TPv3

Tunnel profile:

Session profile:

2. Select **L2TPv3** from the Protocol drop-down list.
3. Configure the tunnel profile:
   a. Enter the tunnel name to be used for tunnel creation.

Figure 84 *Tunnel Configuration*



Tunnel Configuration

Primary Peer address: 10.0.0.63

Backup Peer address: 10.0.0.65

Peer UDP port: 3000

Local UDP port: 1701

Hello interval: 150 sec.

Message digest type: MD5

Shared key: ••••••••

Checksum: Disabled

Failover mode: non-Preemptive

Failover retry interval: 80 sec.

Failover retry count: 5

MTU: 1570

   b. Enter the primary server IP address.
   c. Enter the remote end backup tunnel IP address. This is an optional field and required only when backup server is configured
   d. Enter the remote end UDP port number. The default value is 1701.
   e. Enter the interval at which the hello packets are sent through the tunnel. The default value is 60 seconds.

f. Select the message digest as MD5 or SHA used for message authentication.

g. Enter a shared key for the message digest. This key should match with the tunnel end point shared key.

h. If required, select the failover mode as Primary or Backup (when backup server is available).

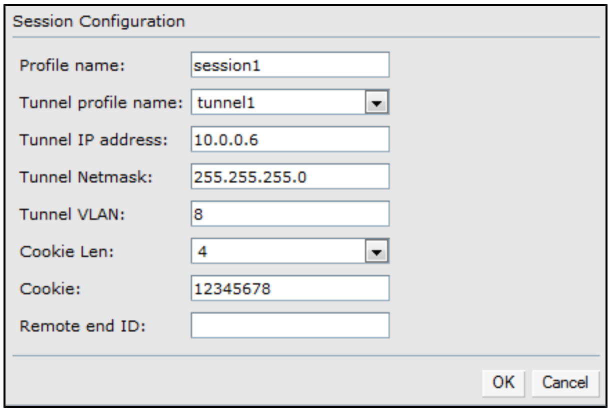
i. Specify a value for tunnel MTU value if required. The default value is 1460.

j. Click **OK**.

4. Configure the session profile:

   a. Enter the session name to be used for session creation.

Figure 85 *Session Configuration*



Session Configuration

Profile name:	session1
Tunnel profile name:	tunnel1
Tunnel IP address:	10.0.0.6
Tunnel Netmask:	255.255.255.0
Tunnel VLAN:	8
Cookie Len:	4
Cookie:	12345678
Remote end ID:	

   b. Enter the tunnel profile name where the session will be associated.

   c. Configure tunnel IP address with corresponding network mask and VLAN ID. This is required to reach AP from a corporate network. For example, SNMP polling.

   d. Select the cookie length and enter a cookie value corresponding to the length. By default, the cookie length is not set.

   e. Click **OK**.

5. Click **Next** to continue.

In the CLI

To configure a L2TPv3 VPN tunnel:

```
(Instant Access Point)(config)# l2tpv3 tunnel <l2tpv3_tunnel_profile>
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# backup peer-address <p
eer_ip_addr_tunnel>
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# checksum
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# failover-mode <preempt
ive/non-preemptive>
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# failover-retry-count <
retry_count>
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# failover-retry-interva
l <interval_in_seconds>
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# hello-timeout <interva
l_in_seconds>
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# local-port <local_udp_
port_number>
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# message-digest-type <d
igest_algorithm>
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# mtu <tunnel_MTU_size>
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# peer-port <peer_udp_po
rt_number>
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# primary peer-address <
peer_ip_addr_tunnel>
```

```
(Instant Access Point) (L2TPv3 Tunnel Profile <l2tpv3_tunnel_profile>)# secret-key <secret_ke
y>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To configure a L2TPv3 session:

```
(Instant Access Point)(config)# l2tpv3 session <l2tpv3_session_profile>
(Instant Access Point) (L2TPv3 Tunnel Profile <2tpv3_session_profile>)# cookie len <cookie_len
gth> value <cookie_value>
(Instant Access Point) (L2TPv3 Tunnel Profile <2tpv3_session_profile>)# l2tpv3 tunnel <l2tpv3_
tunnel_name_to_associate>
(Instant Access Point) (L2TPv3 Tunnel Profile <2tpv3_session_profile>)# tunnel-ip <local_ip_ad
dr_tunnel> mask <tunnel_mask_ip_addr> vlan <vlan_ID>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Example

```
(Instant Access Point)(config)# l2tpv3 tunnel test_tunnel
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel")# primary peer-address 10.0.0.65
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel")# backup peer-address 10.0.0.63
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel")# no checksum
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel")# failover-mode non-preemptive
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel")# failover-retry-count 5
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel")# failover-retry-interval 80
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel")# hello-timeout 150
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel")# mtu 1570
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel")# peer-port 3000
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel")# secret-key test123
(Instant Access Point)(L2TPv3 Tunnel Profile "test_tunnel")# end
(Instant Access Point) # commit apply

(Instant Access Point) (config) # l2tpv3 session test_session
(Instant Access Point) (L2TPv3 Session Profile "test_session")# cookie len 4 value 12345678
(Instant Access Point) (L2TPv3 Session Profile "test_session")# l2tpv3 tunnel test_tunnel
(Instant Access Point) (L2TPv3 Session Profile "test_session")# tunnel-ip 1.1.1.1 mask 255.255
.255.0 vlan 5
(Instant Access Point)(L2TPv3 Tunnel Profile "test_tunnel")# end
(Instant Access Point) # commit apply
```

To view L2TPv3 configuration:

```
(Instant Access Point)# show l2tpv3 config
L2TPV3 Tunnel configuration
---------------------------
Tunnel Profile  Primary Peer   Backup Peer   Peer UDP Port  Local UDP Port  Hello Interval  Ho
st Name         MTU   Message Digest Type  secret Key                        Failover Mode   F
ailover Retry Count  Retry Interval  Checksum
--------------  -------------  ------------  -------------  --------------  --------------  --
-------         ---   -------------------  ----------                        -------------   -
-------------------  --------------  --------
test_tunnel     10.0.0.63      10.0.0.65      3000                 1701               150       In
stant-C4:42:98  1570       MD5                625beed39fa4ff3424edb3082ede48fa  non-preemptive
 5                     80              Disabled
L2TPV3 Session configuration
----------------------------
Session Name  Tunnel Name  Local tunnel IP  Tunnel Mask    Tunnel Vlan  Session Cookie Length
Session Cookie  Session Remote End ID
------------  -----------  ---------------  -----------    -----------  ---------------------
--------------  ---------------------
test_session               1.1.1.1          255.255.255.0  5            0
0               0
```

To view L2TPv3 global configuration:

```
(Instant Access Point)# show l2tpv3 global parameter

L2TPV3 Global configuration
---------------------------
Host Name
----------
Instant-C4:42:98
```

To view L2TPV3 session status:

```
(Instant Access Point)# show l2tpv3 session status

Session 1821009927 on tunnel 858508253:-
type: LAC Incoming Call, state: ESTABLISHED
created at:  Jul  2 04:58:45 2013
administrative name: 'test_session' (primary)
created by admin: YES, peer session id: 12382
session profile name: test_session_primary
data sequencing required: OFF
use data sequence numbers: OFF
Peer configuration data:-
data sequencing required: OFF
framing types:
data rx packets: 16, rx bytes: 1560, rx errors: 0 rx cookie error 0
data tx packets: 6, tx bytes: 588, tx errors: 0
```

To view L2TPV3 tunnel status:

```
(Instant Access Point)# show l2tpv3 tunnel status

Tunnel 858508253, from 10.13.11.29 to 10.13.11.157:-
state: ESTABLISHED
created at:  Jul  2 04:58:25 2013
administrative name: 'test_tunnel' (primary)
created by admin: YES, tunnel mode: LAC, persist: YES
local host name: Instant-C4:42:98
peer tunnel id: 1842732147, host name: aruba1600pop636635.hsbtst2.aus
UDP ports: local 1701, peer 3000
session limit: 0, session count: 1
tunnel profile: test_tunnel_primary, peer profile: default
session profile: default
hello timeout: 150, retry timeout: 80, idle timeout: 0
rx window size: 10, tx window size: 10, max retries: 5
use udp checksums: OFF
do pmtu discovery: OFF, mtu: 1460
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI
peer vendor name: Katalix Systems Ltd. Linux-2.6.32-358.2.1.el6.x86_64 (x86_64)
peer protocol version: 1.0, firmware 0
peer rx window size: 10
Transport status:-
ns/nr: 98/97, peer 98/96
cwnd: 10, ssthresh: 10, congpkt_acc: 9
Transport statistics:-
out-of-sequence control/data discards: 0/0
ACKs tx/txfail/rx: 0/0/96
retransmits: 0, duplicate pkt discards: 0, data pkt discards: 0
hellos tx/txfail/rx: 94/0/95
control rx packets: 193, rx bytes: 8506
control tx packets: 195, tx bytes: 8625
```

```
data rx packets: 0, rx bytes: 0, rx errors: 0
data tx packets: 6, tx bytes: 588, tx errors: 0
establish retries: 0
```

To view L2TPv3 tunnel config:

```
(Instant Access Point)# show l2tpv3 tunnel config

Tunnel profile test_tunnel_primary
l2tp host name: Instant-C4:42:98
local UDP port: 1701
peer IP address: 10.0.0.65
peer UDP port: 3000
hello timeout 150, retry timeout 80, idle timeout 0
rx window size 10, tx window size 10, max retries 5
use UDP checksums: OFF
do pmtu discovery: OFF, mtu: 1570
framing capability: SYNC ASYNC
bearer capability: DIGITAL ANALOG
use tiebreaker: OFF
peer profile: NOT SET
session profile: NOT SET
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI

Tunnel profile test_tunnel_backup
l2tp host name: aruba1600pop658509.hsb-dev4.aus
local UDP port: 1701
peer IP address: 10.13.11.157
peer UDP port: 1701
hello timeout 60, retry timeout 1, idle timeout 0
rx window size 10, tx window size 10, max retries 5
use UDP checksums: OFF
do pmtu discovery: OFF, mtu: 1460
framing capability: SYNC ASYNC
bearer capability: DIGITAL ANALOG
use tiebreaker: OFF
peer profile: NOT SET
session profile: NOT SET
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI
```

To view L2TPv3 system statistics:

```
(Instant Access Point)# show l2tpv3 system statistics

L2TP counters:-
Total messages sent: 99, received: 194, retransmitted: 0
illegal: 0, unsupported: 0, ignored AVPs: 0, vendor AVPs: 0
Setup failures: tunnels: 0, sessions: 0
Resource failures: control frames: 0, peers: 0
tunnels: 0, sessions: 0
Limit exceeded errors: tunnels: 0, sessions: 0
Frame errors: short frames: 0, wrong version frames: 0
unexpected data frames: 0, bad frames: 0
Internal: authentication failures: 0, message encode failures: 0
no matching tunnel discards: 0, mismatched tunnel ids: 0
no matching session_discards: 0, mismatched session ids: 0
total control frame send failures: 0, event queue fulls: 0
Message counters:-
Message          RX Good           RX Bad               TX
ILLEGAL              0                 0                0
SCCRQ                0                 0                1
```

```
SCCRP               1                 0                0
SCCCN               0                 0                1
STOPCCN             0                 0                0
RESERVED1           0                 0                0
HELLO              95                 0               95
OCRQ                0                 0                0
OCRP                0                 0                0
OCCN                0                 0                0
ICRQ                0                 0                1
ICRP                1                 0                0
ICCN                0                 0                1
RESERVED2           0                 0                0
CDN                 0                 0                0
WEN                 0                 0                0
SLI                 0                 0                0
```

Configuring Routing Profiles

Instant can terminate a single VPN connection on an Aruba Mobility Controller. The Routing profile defines the corporate subnets which need to be tunneled through IPSec.

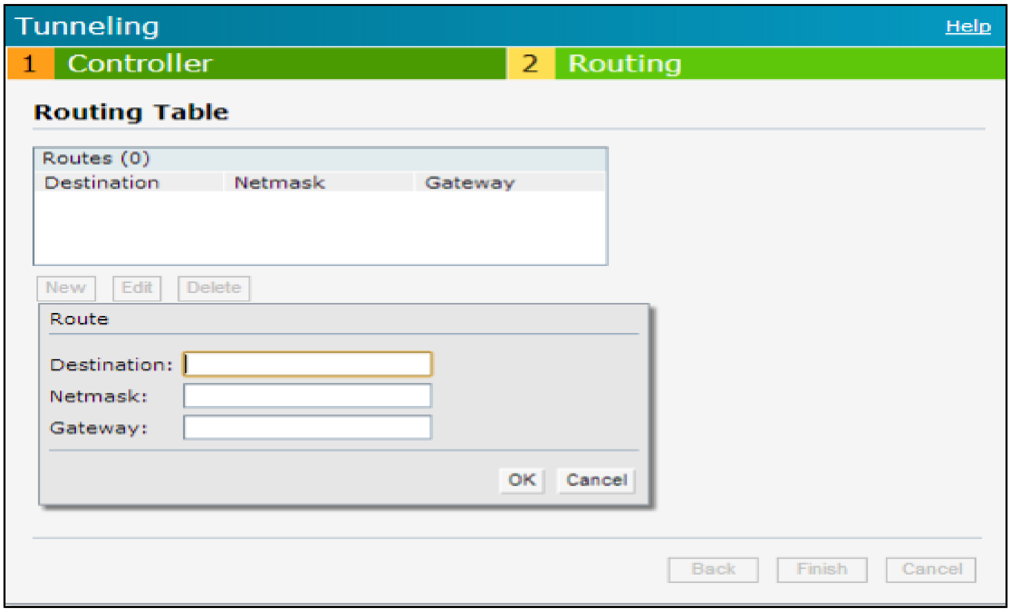
You can configure routing profiles to specify a policy based on routing into the VPN tunnel using Instant UI or CLI.

In the Instant UI

To configure a routing profile:

1. Click **Routing** in the **Tunneling** window. The routing details are displayed.
2. Click **New**. The route parameters to configure are displayed.

Figure 86 *Tunneling— Routing*



3. Update the following parameters:
   - **Destination**– Specify the destination network that is reachable through the VPN tunnel.
   - **Netmask**– Specify the subnet mask of network that is reachable through the VPN tunnel.
   - **Gateway**– Specify the gateway to which traffic must be routed. This IP address must be the controller IP address on which the VPN connection is terminated.
4. Click **OK**.

5. Click **Finish**.

In the CLI

```
(Instant Access Point)(config)# routing-profile
(Instant Access Point)(Routing-profile)# route <destination> <mask> <gateway>
(Instant Access Point)(Routing-profile)# end
(Instant Access Point)# commit apply
```

Chapter 21
IAP-VPN Configuration

Aruba controllers provide an ability to terminate the IPSec and GRE VPN tunnels from the IAP and provide corporate connectivity to the branch network.

This section describes the following topics:

- Overview on page 263
- VPN Configuration on page 266
- Viewing Branch Status on page 267

Overview

This section provides a brief summary of the features supported by the controllers to allow VPN termination from an IAP.

Termination of IPSec and GRE VPN Tunnels

IAPs can terminate VPN tunnels on Controllers. The IAP cluster creates an IPSec or GRE VPN tunnel from the Virtual Controller to a Mobility Controller in your corporate office. The controller only acts an IPSec or GRE VPN end-point and it does not configure the IAP. For more information on how to create an IPSec or GRE VPN tunnel, see VPN Configuration on page 249.

L2/L3 Forwarding Modes

The Virtual Controller enables different DHCP pools (various assignment modes) in addition to allocating IP subnets for each branch. The Virtual Controller allows different modes of forwarding of traffic from the clients on a VLAN with a VPN tunnel. The forwarding modes are associated with various modes of DHCP address assignment modes. For more information on DHCP assignment modes and configuring DHCP scope for IAP-VPN, see Configuring DHCP Scopes on page 241.

The following DHCP modes are supported:

- **NAT Mode**: In this mode, the source IP for all client traffic is translated. The traffic destined for the corporate network is translated using the VPN tunnel IP address of the IAP and is forwarded through the IPsec VPN tunnel. The traffic destined for the non-corporate network is translated using the IP address of the IAP and is forwarded through the uplink.

  When the NAT mode is used for forwarding client traffic, hosts on the corporate network cannot establish connections to the clients on the IAP, because the source address of the clients is translated.
- **L2 Switching Mode**: In this mode, the traffic destined for the corporate network is bridged through the VPN tunnel to the controller and the destined for the non-corporate network is translated using the IP address of the IAP and is forwarded through the uplink.

  When an IAP registers with the controller, and is configured to use the L2 DHCP address assignment mode, the controller automatically adds the VPN tunnel associated to this IAP into the VLAN multicast table. This allows the clients connecting to the L2 mode VLAN to be part of the same L2 broadcast domain on the controller.
- **L3 Routing Mode:** In this mode, the traffic destined for the corporate network is routed through the VPN tunnel to the controller and the traffic destined for the non corporate network is translated using the IP address of the IAP and is forwarded through the uplink.

  When an IAP registers with the controller and is configured to use the L3 DHCP address assignment mode, the Mobility Controller adds a route on the controller, enabling routing of traffic from the corporate network to clients on this subnet in the branch.

IAP-VPN Scalability Limits

ArubaOS provides enhancements to the scalability limits for the IAP-VPN branches terminating on the controller. The following table provides the IAP-VPN scalability information for various controller platforms:

Table 51: *IAP-VPN Scalability*

Platforms	Branches	Routes	L3 Mode Users	NAT Users	Total L2 Users
3200	1000	1000	N/A	N/A	64000
3400	2000	2000			64000
3600	8000	8000			64000
M3	8000	8000			64000
7210	8000	8000			64000
7220	16000	16000			128000
7240	32000	32000			128000

- **Branches**–The number of IAP-VPN branches that can be terminated on a given controller platform.
- **Routes**–The number of L3 routes supported on the controller.
- **L3 mode and NAT mode users**–The number of trusted users supported on the controller. There is no scale impact on the controller. They are limited only by the number of clients supported per IAP.
- **L2 mode users**–The number of L2 mode users are limited to 128000 for 7220and 7240 and 64000 across all platforms.

OSPF Configuration

OSPF (Open Shortest Path First) is a dynamic Interior Gateway routing Protocol (IGP) based on IETF RFC 2328. The premise of OSPF is that the shortest or fastest routing path is used. The implementation of OSPFv2 allows controllers to deploy effectively in a Layer 3 topology. The controllers can act as default gateway for all clients and forward user packets to the upstream router.

Each IAP-VPN can be defined a separate subnet derived from corporate intranet pool to allow IAP-VPN devices to work independently. For sample topology and configuration, see *ArubaOS User Guide*.

To redistribute IAP-VPN routes into the OSPF process, use the following command :

```
(host)(config) # router ospf redistribute rapng-vpn
```

To verify if the redistribution of the IAP-VPN is enabled, use following command:

```
(host) #show ip ospf redistribute
Redistribute RAPNG
```

To configure aggregate route for IAP-VPN routes, use the following command:

```
(host) (config) # router ospf aggregate-route rapng-vpn
```

To view the aggregated routes for IAP-VPN routes, use the following command:

```
(host) #show ip ospf rapng-vpn aggregate-routes
RAPNG VPN aggregate routes
--------------------------
Prefix Mask Contributing routes Cost
------ ---- ------------------- ----
201.201.200.0 255.255.252.0 5 268779624
100.100.2.0 255.255.255.0 1 10
```

To verify the details of configured aggregated route, use the following command:

```
(host) # show ip ospf rapng-vpn aggregated-routes <net> <mask>
(host) #show ip ospf rapng-vpn aggregate-routes 100.100.2.0 255.255.255.0
Contributing routes of RAPNG VPN aggregate route
------------------------------------------------
Prefix Mask Next-Hop Cost
------ ---- -------- ----
100.100.2.64 255.255.255.224 5.5.0.10 10
```

To view all the redistributed routes:

```
(host) #show ip ospf database
OSPF Database Table
-------------------
Area ID    LSA Type      Link ID        Adv Router     Age   Seq#         Checksum
-------    --------      -------        ----------     ---   ----         --------
0.0.0.15   ROUTER        9.9.9.9        9.9.9.9        159   0x80000016   0xee92
0.0.0.15   ROUTER        10.15.148.12   10.15.148.12   166   0x80000016   0x4c0d
0.0.0.15   NETWORK       10.15.148.12   10.15.148.12   167   0x80000001   0x9674
0.0.0.15   NSSA          12.12.2.0      9.9.9.9        29    0x80000003   0x7b54
0.0.0.15   NSSA          12.12.12.0     9.9.9.9        164   0x80000008   0x63a
0.0.0.15   NSSA          12.12.12.32    9.9.9.9        164   0x80000008   0x7b8
0.0.0.15   NSSA          50.40.40.0     9.9.9.9        164   0x80000007   0x8ed4
0.0.0.15   NSSA          51.41.41.128   9.9.9.9        164   0x80000007   0x68f6
0.0.0.15   NSSA          53.43.43.32    9.9.9.9        164   0x80000007   0x2633
0.0.0.15   NSSA          54.44.44.16    9.9.9.9        164   0x80000007   0x353
N/A        AS_EXTERNAL   12.12.2.0      9.9.9.9        29    0x80000003   0x8c06
N/A        AS_EXTERNAL   12.12.12.0     9.9.9.9        169   0x80000001   0x25e4
N/A        AS_EXTERNAL   12.12.12.32    9.9.9.9        169   0x80000001   0x2663
N/A        AS_EXTERNAL   50.40.40.0     9.9.9.9        169   0x80000001   0xab80
N/A        AS_EXTERNAL   51.41.41.128   9.9.9.9        169   0x80000001   0x85a2
N/A        AS_EXTERNAL   53.43.43.32    9.9.9.9        169   0x80000001   0x43de
N/A        AS_EXTERNAL   54.44.44.16    9.9.9.9        169   0x80000001   0x20fe
```

To verify if the redistributed routes are installed or not.

```
(host) #show ip route
Codes: C - connected, O - OSPF, R - RIP, S - static
M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN
Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 10.15.148.254 to network 0.0.0.0 at cost 1
S*    0.0.0.0/0  [1/0] via 10.15.148.254*
V    12.12.2.0/24 [10/0] ipsec map
V    12.12.12.0/25 [10/0] ipsec map
V    12.12.12.32/27 [10/0] ipsec map
V    50.40.40.0/24 [10/0] ipsec map
V    51.41.41.128/25 [10/0] ipsec map
V    53.43.43.32/27 [10/0] ipsec map
V    54.44.44.16/28 [10/0] ipsec map
C    9.9.9.0/24 is directly connected, VLAN9
C    10.15.148.0/24 is directly connected, VLAN1
C    43.43.43.0/24 is directly connected, VLAN132
C    42.42.42.0/24 is directly connected, VLAN123
C    44.44.44.0/24 is directly connected, VLAN125
C    182.82.82.12/32 is an ipsec map 10.15.149.69-182.82.82.12
C    182.82.82.14/32 is an ipsec map 10.17.87.126-182.82.82.14
```

VPN Configuration

The following VPN configuration steps on the controller, enable IAPs to terminate their VPN connection on the controller:

Whitelist Database Configuration

The whitelist database is a list of the MAC addresses of the IAPs that are allowed to establish VPN connections with the Mobility Controller. This list can be either stored in the Mobility Controller or on an external server.

Controller Whitelist Database

You can use the following CLI command to configure the whitelist database entry if the controller is acting as the whitelist database:

```
(host) #whitelist-db rap add mac-address 00:11:22:33:44:55 ap-group test
```

The **ap-group** parameter is not used for any configuration, but needs to be configured. The parameter can be any valid string.

External Whitelist Database

If an external server is used as the location for the whitelist database, add the MAC addresses of the valid IAPs in the external database or external directory server and then configure a RADIUS server to authenticate the IAPs using the entries in the external database or external directory server.

If you are using Windows 2003 server, perform the following steps to configure the external whitelist database on it. There are equivalent steps available for Windows Server 2008 and other RADIUS servers.

1. Add the MAC addresses for all the IAPs in the Active Directory of the RADIUS server:
   a. Open the **Active Directory and Computers** window, add a new user and specify the MAC address (without the colon delimiter) of the IAP for the user name and password.
   b. Right-click the user that you have just created and click **Properties**.
   c. In the **Dial-in** tab, select **Allow access** in the **Remote Access Permission** section and click **OK**.
   d. Repeat Step a through Step b for all IAPs.
2. Define the remote access policy in the Internet Authentication Service:
   a. In the **Internet Authentication Service** window, select **Remote Access Policies**.
   b. Launch the wizard to configure a new remote access policy.
   c. Define filters and select **grant remote access permission** in the **Permissions** window.
   d. Right-click the policy that you have just created and select **Properties**.
   e. In the **Settings** tab, select the policy condition, and **Edit Profile...**.
   f. In the **Advanced** tab, select **Vendor Specific**, and click **Add** to add new vendor specific attributes.
   g. Add new vendor specific attributes and click **OK**.
   h. In the **IP** tab, provide the IP address of the IAP and click **OK**.

VPN Local Pool Configuration

The VPN local pool is used to assign an IP Address to the IAP after successful XAUTH VPN.

```
(host) # ip local pool "rapngpool" <startip> <endip>
```

Role Assignment for the Authenticated IAPs

Define a role that includes a src-nat rule to allow connections to the RADIUS server and for the Dynamic Radius Proxy in the IAP to work. This role is assigned to IAPs after successful authentication.

```
(host) (config) #ip access-list session iaprole
```

```
(host) (config-sess-iaprole)#any host <radius-server-ip> any src-nat
(host) (config-sess-iaprole)#any any any permit
(host) (config-sess-iaprole)#!
(host) (config) #user-role iaprole
(host) (config-role) #session-acl iaprole
```

VPN Profile Configuration

The VPN profile configuration defines the server used to authenticate the IAP (internal or an external server) and the role assigned to the IAP after successful authentication.

```
(host) (config) #aaa authentication vpn default-iap
(host) (VPN Authentication Profile "default-iap") #server-group default
(host) (VPN Authentication Profile "default-iap") #default-role iaprole
```

For information about the VPN profile configuration on the IAP, see VPN Configuration on page 249.

Viewing Branch Status

To view the details of the branch information connected to the controller, execute the **show iap table** command.

Example

This example shows the details of the branches connected to the controller:

```
(host) #show iap table long

IAP Branch Table
----------------
Name             VC MAC Address     Status   Inner IP       Assigned Subnet  Assigned Vlan
----             --------------     ------   --------       ---------------  -------------
Tokyo-CB:D3:16   6c:f3:7f:cc:42:f8  DOWN     0.0.0.0
Paris-CB:D3:16   6c:f3:7f:cc:3d:04  UP       10.15.207.140  10.15.206.99/29  2
LA               6c:f3:7f:cc:42:25  UP       10.15.207.111  10.15.206.24/29  2
Munich           d8:c7:c8:cb:d3:16  DOWN     0.0.0.0
London-c0:e1     6c:f3:7f:c0:e1:b1  UP       10.15.207.120  10.15.206.64/29  2
Instant-CB:D3    6c:f3:7f:cc:42:1e  DOWN     0.0.0.0
Delhi            6c:f3:7f:cc:42:ca  DOWN     0.0.0.0
Singapore        6c:f3:7f:cc:42:cb  UP       10.15.207.122  10.15.206.120/29 2


Key        Bid(Subnet Name)
---        ----------------
b3c65c...
b3c65c...
b3c65c...  2(10.15.205.0-10.15.205.250,5),1(10.15.206.1-10.15.206.252,5)
a2a65c...  0
b3c65c...  7(10.15.205.0-10.15.205.250,5),8(10.15.206.1-10.15.206.252,5)
b3c65c...
b3c65c...  1(10.15.205.0-10.15.205.250,5),2(10.15.206.1-10.15.206.252,5)
b3c65c...  14(10.15.205.0-10.15.205.250,5),15(10.15.206.1-10.15.206.252,5)
```

The output of this command provides the following information:

Table 52: *Branch Details*

Parameter	Description
Name	Displays the name of the branch.

Parameter	Description
`VC MAC Address`	Displays the MAC address of the Virtual Controller of the branch.
`Status`	Displays the current status of the branch (UP/DOWN).
`Inner IP`	Displays the internal VPN IP of the branch.
`Assigned Subnet`	Displays the subnet mask assigned to the branch.
`Assigned Vlan`	Displays the VLAN ID assigned to the branch.
`Key`	Displays the key for the branch, which is unique to each branch.
`Bid(Subnet Name)`	Displays the Branch ID (BID) of the subnet. ● In the example above, the controller displays bid-per-subnet-per-branch i.e., for "LA" branch, BID "2" for the ip-range "10.15.205.0-10.15.205.250" with client count per branch "5"). If a branch has multiple subnets, it can have multiple BIDs. ● Branches that are in **UP** state and do not have a **Bid(Subnet Name)** means that the IAP is connected to a controller, which did not assign any BID for any subnet. In the above example, "Paris-CB:D3:16" branch is **UP** and does not have a **Bid(Subnet Name)** information. This means that either the IAP is connected to a backup controller or connected to a primary controller without any distributed L2 or L3 subnets.

NOTE

The **show iap table** command output does not display the **Key** and **Bid(Subnet Name)** details.

This chapter provides the following information:

AirWave Features

AirWave is a powerful tool and easy-to-use network operations system that manages Aruba wireless, wired, and remote access networks, as well as wired and wireless infrastructures from a wide range of third-party manufacturers. With its easy-to-use interface, AirWave provides real-time monitoring, proactive alerts, historical reporting, and fast, efficient troubleshooting. It also offers tools that manage RF coverage, strengthen wireless security, and demonstrate regulatory compliance.

The IAPs communicate with AirWave using the using the HTTPS protocol. This allows an AirWave server to be deployed in the cloud across a NAT device, such as a router. This AirWave features available in the Instant network are described in the following sections.

Image Management

AirWave allows you to manage firmware updates on WLAN devices by defining a minimum acceptable firmware version for each make and model of a device. It remotely distributes the firmware image to the WLAN devices that require updates, and it schedules the firmware updates such that updating is completed without requiring you to manually monitor the devices.

The following models can be used to upgrade the firmware:

- Automatic– In this model, the Virtual Controller 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 for each Virtual Controller or set the 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.

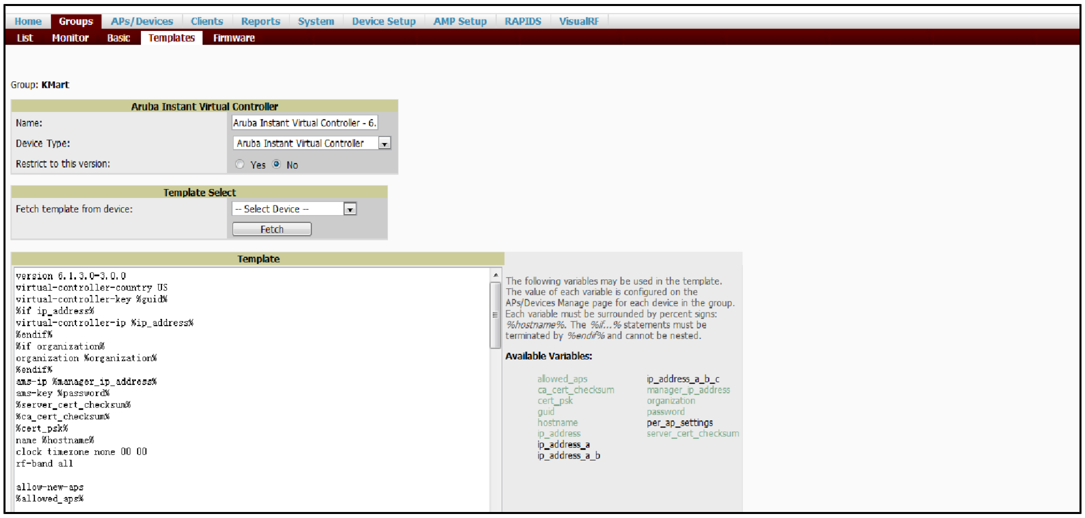
NOTE

In the AirWave User Interface (UI), you can select either **Manage Read/Write** or **Monitor-only+Firmware Upgrades** as management modes. When the Management level is set to **Manage Read/Write**, the Instant UI is in read-only mode. If Airwave Management Level is set to **Monitor-only+Firmware Upgrades** mode, the Instant UI changes to the read-write mode.

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 the following figure. 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 incorrectly configured devices.

Figure 87 *Template-based Configuration*



Group: **KMart**

Aruba Instant Virtual Controller

Name:	Aruba Instant Virtual Controller - 6.
Device Type:	Aruba Instant Virtual Controller
Restrict to this version:	○ Yes ● No

Template Select

Fetch template from device: -- Select Device --

Template

```
version 6.1.3.0-3.0.0
virtual-controller-country US
virtual-controller-key %guid%
%if ip_address%
virtual-controller-ip %ip_address%
%endif%
%if organization%
organization %organization%
%endif%
ams-ip %manager_ip_address%
ams-key %password%
%server_cert_checksum%
%ca_cert_checksum%
%cert_psk%
name %hostname%
clock timezone none 00 00
rf-band all

allow-new-aps
%allowed_aps%
```

The following variables may be used in the template. The value of each variable is configured on the APs/Devices Manage page for each device in the group. Each variable must be surrounded by percent signs: *%hostname%*. The *%if...%* statements must be terminated by *%endif%* and cannot be nested.

Available Variables:

allowed_aps
ca_cert_checksum
cert_psk
guid
hostname
ip_address
ip_address_a
ip_address_a_b
ip_address_a_b_c
manager_ip_address
organization
password
per_ap_settings
server_cert_checksum

Trending Reports

AirWave saves up to 14 months of actionable information, including network performance data and user roaming patterns, so you can analyze how network usage and performance trends have changed over time. It also provides detailed capacity reports with which you can plan the capacity and appropriate strategies for your organization.

Intrusion Detection System

AirWave provides advanced, rules-based rogue classification. It automatically detects rogue APs irrespective of their location in the network and 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

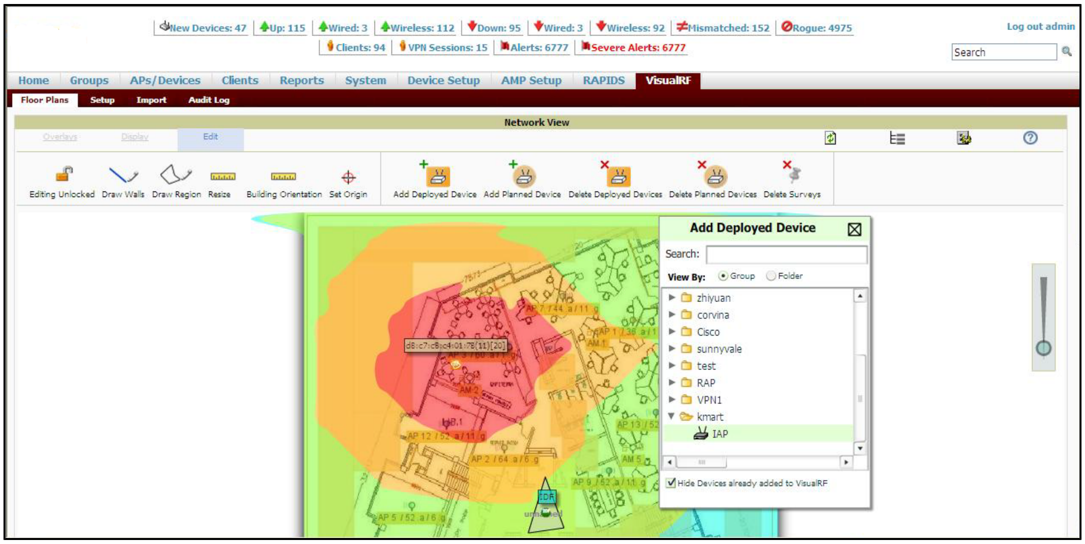
AirWave supports Wireless Intrusion Detection System (WIDS) Event Reporting, which is provided by Instant. This includes WIDS classification integration with the RAPIDS (Rogue Access Point Detection Software) module. RAPIDS is a powerful and easy-to-use tool for automatic detection of unauthorized wireless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

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

RF Visualization Support for Instant

AirWave supports RF visualization for Instant. The VisualRF module provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. VisualRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every Instant device in range. VisualRF provides graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network.

Figure 88 *Adding an IAP in VisualRF*



PSK-based and Certificate-based Authentication

On the DHCP server, two formats for option 43 are supported:

- **<organization>,<ams-ip>,<ams-key>**– If you choose this format, the IAP authenticates the AirWave Management Platform server using the Pre-Shared Key (PSK) login process.
- **<organization>,<ams-domain>**– If you choose this format, the IAP resolves the AirWave Management platform domain name into one or two IP address as AirWave Primary or AirWave Primary and AirWave Backup, and then IAP will start a certificate-based authentication with AirWave Management platform server, instead of the PSK login. When the AirWave Management platform domain name is used, the IAP performs certificate-based authentication with AirWave Management platform server. The IAP initiates an SSL connection with the AirWave server. The AirWave server verifies the signature and public key certificate from IAP. If the signature matches, the AirWave responds to the IAP with the login request.

Configuring AirWave

Before configuring the AirWave, ensure that you have the following information:

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

This section describes the following procedures:

- Configuring Organization String on page 271
- Configuring for AirWave Discovery through DHCP on page 273
- Alternate Method for Defining Vendor-Specific DHCP Options on page 276

Configuring Organization String

The Organization string is a set of colon-separated strings created by the AirWave administrator to accurately represent the deployment of each Instant system. This string is defined by the installation personnel on the site.

You can use any of the following strings:

- 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"

You can also assign additional strings to create a hierarchy of sub folders under the folder named "Org". For example:

- subfolder1 for a folder under the "Org" folder
- subfolder2 for a folder under subfolder1

Shared Key

The Shared Secret key is an optional field used by the administrator to manually authorize the first Virtual Controller for an organization. Any string is acceptable.

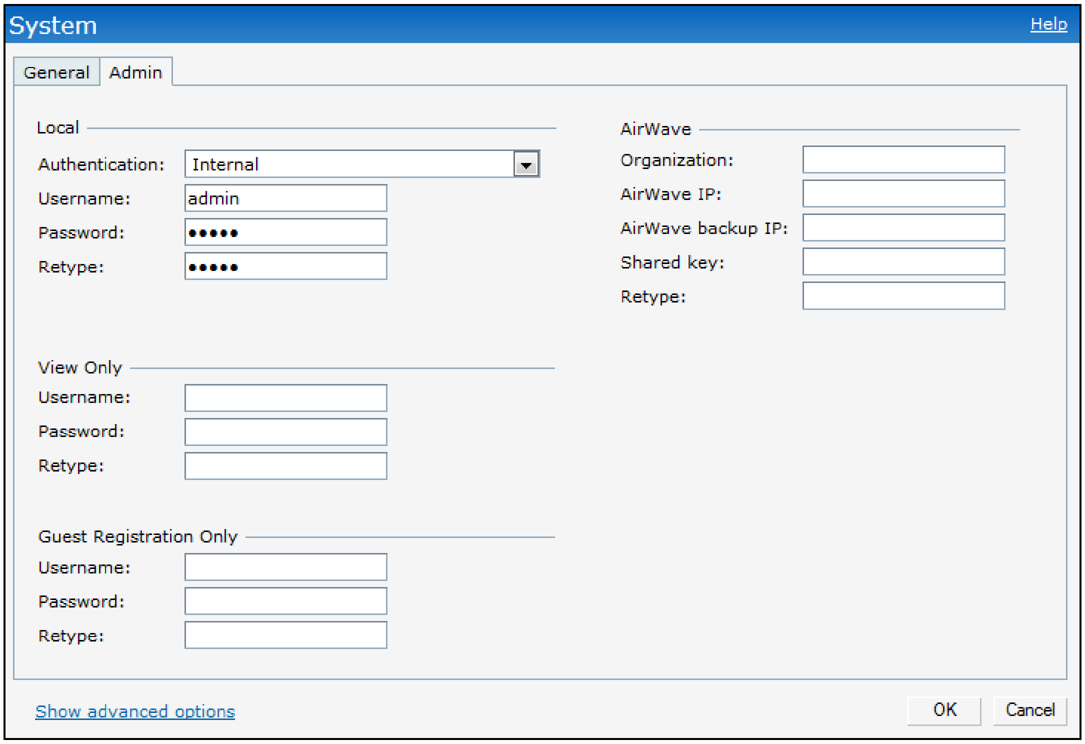
Configuring AirWave Information

You can configure AirWave information using Instant UI or CLI.

In the Instant UI

1. Click the AirWave **Set Up Now** link in the bottom-middle region of the Instant UI window. The **System** window is displayed with the AirWave parameters in the **Admin** tab.

Figure 89 *Configuring AirWave*



System

Local

Authentication: Internal

Username: admin

Password: •••••

Retype: •••••

View Only

Username:

Password:

Retype:

Guest Registration Only

Username:

Password:

Retype:

AirWave

Organization:

AirWave IP:

AirWave backup IP:

Shared key:

Retype:

2. Enter the name of your organization in the **Organization** name text box. The name defined for organization will be displayed under the **Groups** tab in the AirWave user interface.
3. Enter the IP address or domain name of the AirWave server in the **AirWave IP** text box.
4. Enter the IP address or domain name of a backup AirWave server in the **AirWave backup IP** text box. The backup server provides connectivity when the primary server is down. If the IAP cannot send data to the primary server, the Virtual Controller switches to the backup server automatically.
5. Enter the shared key in the **Shared key** text box and reconfirm. This shared key is used for configuring the first AP in the Instant network.
6. Click **OK**.

In the CLI

To configure AirWave information in Instant:

```
(Instant Access Point)(config)# organization <name>
(Instant Access Point)(config)# ams-ip <IP-address or domain name>
(Instant Access Point)(config)# ams-backup-ip <IP-address or domain name>
(Instant Access Point)(config)# ams-key <key>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Configuring for AirWave Discovery through DHCP

The AirWave can be discovered through DHCP server. You can configure this only if AirWave was not configured earlier or if you have deleted the precedent configuration.

On the DHCP server, the format for option 60 is “ **InstantAP**“, and the two formats for option 43 are “**<organization>,<ams-ip>,<ams-key>**” and “**<organization>,<ams-domain>**” .

If you use the format **<organization>,<ams-ip>,<ams-key>** the PSK-based authentication is used to access the AirWave Management Platform server.

If you use the format **<organization>,<ams-domain>**, the IAP resolves the domain name into two IP address as AirWave Primary AirWave Backup, and then IAP will start a certificate-based authentication with AirWave Management platform server, instead of the PSK login.

NOTE

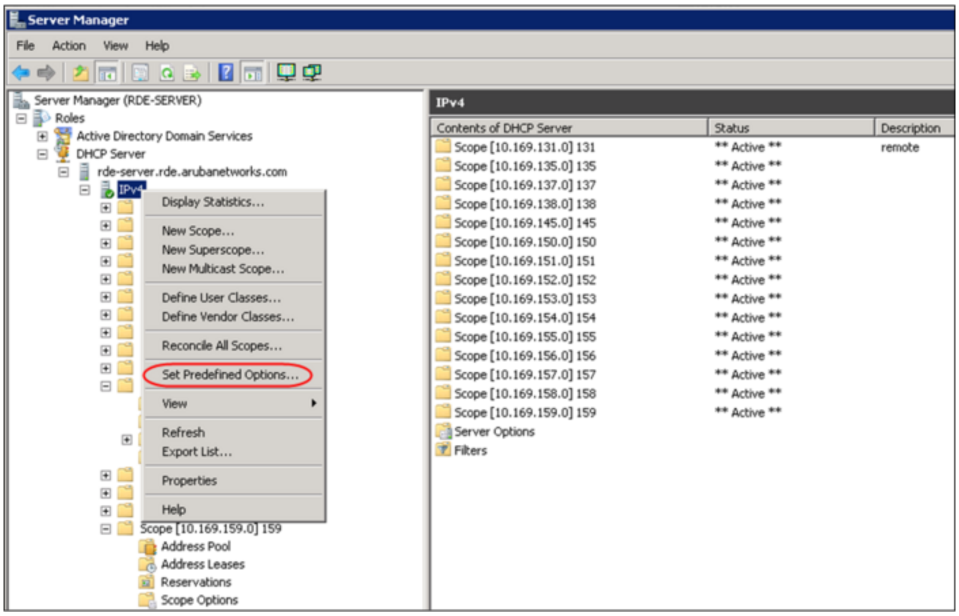
For option 43 when you choose to enter the domain name, the IP address and key will not be available.

Standard DHCP option 60 and 43 on Windows Server 2008

In networks that are not using DHCP option 60 and 43, it is easy to use the standard DHCP options 60 and 43 for an AP or IAP. For APs, these options can be used to indicate the master controller or the local controller. For IAPs, these options can be used to define the AirWave IP, group, password, and domain name.

1. From a server running Windows Server 2008 navigate to **Server Manager**> **Roles**> **DHCP sever** >**domain DHCP Server** (rde-server.rde.arubanetworks.com) **> IPv4**.
2. Right-click **IPv4** and select **Set Predefined Options**.

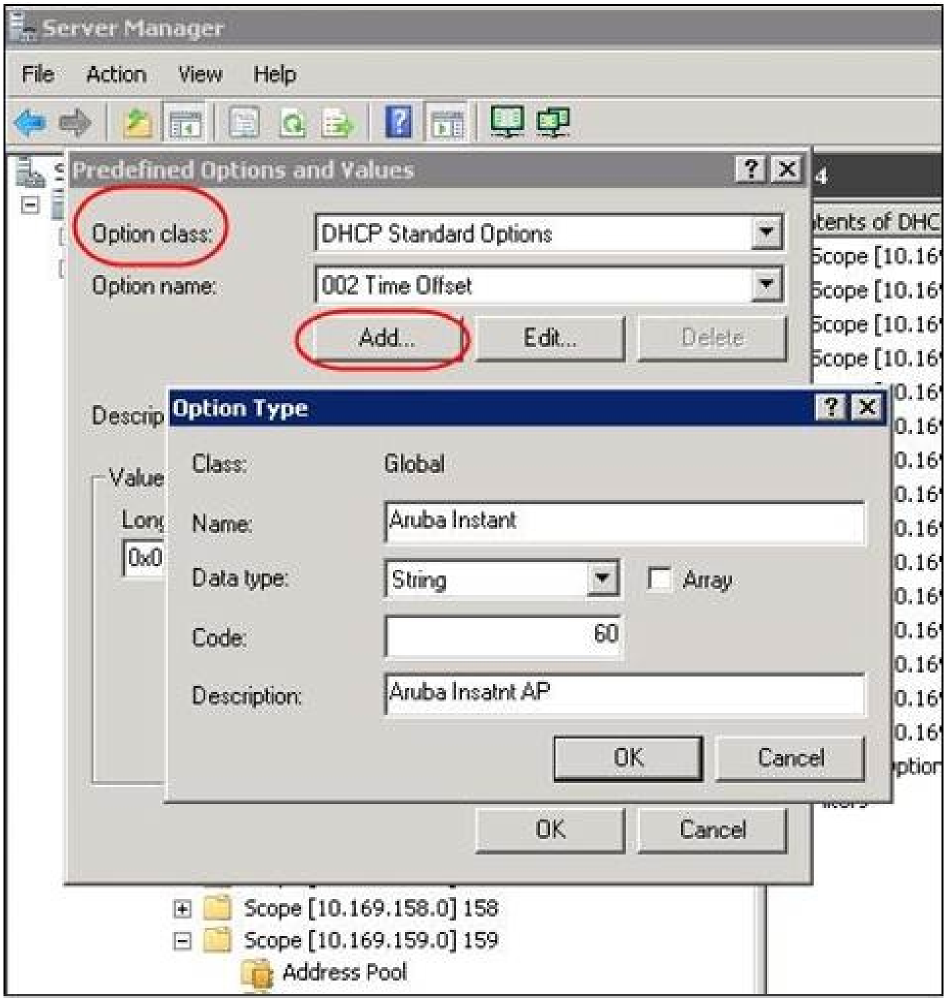
Figure 90 *Instant and DHCP options for AirWave: Set Predefined Options*



Contents of DHCP Server	Status	Description
Scope [10.169.131.0] 131	** Active **	remote
Scope [10.169.135.0] 135	** Active **	
Scope [10.169.137.0] 137	** Active **	
Scope [10.169.138.0] 138	** Active **	
Scope [10.169.145.0] 145	** Active **	
Scope [10.169.150.0] 150	** Active **	
Scope [10.169.151.0] 151	** Active **	
Scope [10.169.152.0] 152	** Active **	
Scope [10.169.153.0] 153	** Active **	
Scope [10.169.154.0] 154	** Active **	
Scope [10.169.155.0] 155	** Active **	
Scope [10.169.156.0] 156	** Active **	
Scope [10.169.157.0] 157	** Active **	
Scope [10.169.158.0] 158	** Active **	
Scope [10.169.159.0] 159	** Active **	
Server Options		
Filters		

3. Select **DHCP Standard Options** in the **Option class** drop-down list and then click **Add**.
4. Enter the following information:
   - Name– Instant
   - Data Type– String
   - Code–60
   - Description–Instant AP

Figure 91 *Instant and DHCP options for AirWave: Predefined Options and Values*



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 002 Time Offset

Option Type

Class: Global

Name: Aruba Instant

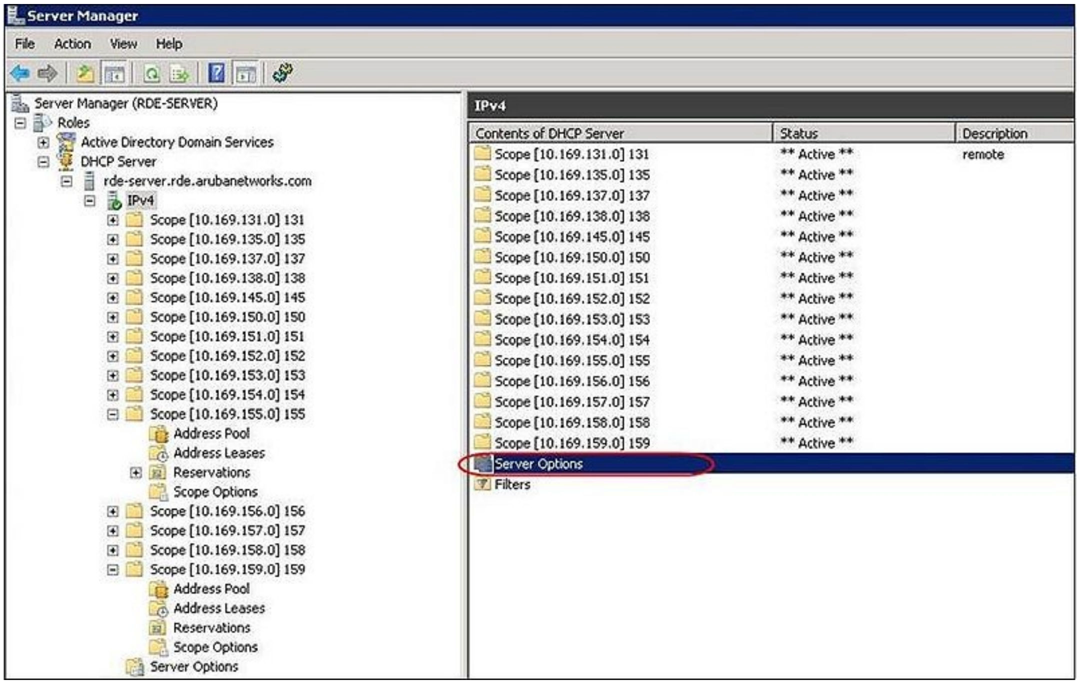
Data type: String ☐ Array

Code: 60

Description: Aruba Insatnt AP

5. Navigate to **Server Manager** and select **Server Options** in the **IPv4** window. (This sets the value globally. Use options on a per-scope basis to override the global options.)
6. Right-click **Server Options** and select the configuration options.

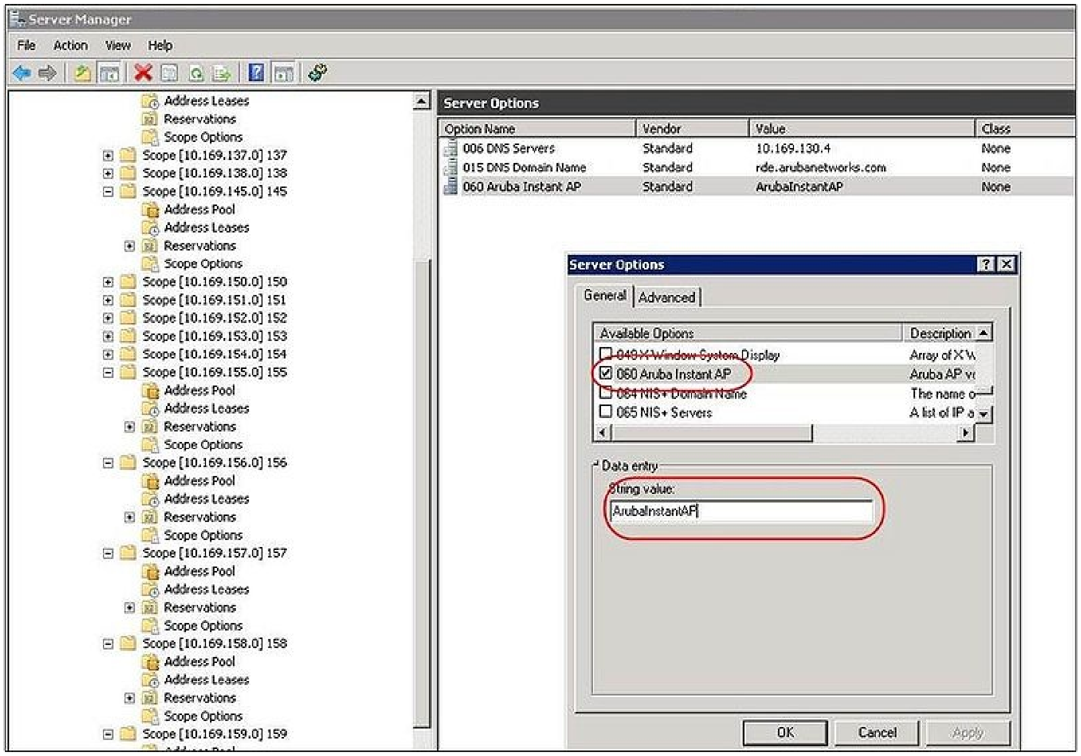
Figure 92 *Instant and DHCP options for AirWave: Server Options*



Contents of DHCP Server	Status	Description
Scope [10.169.131.0] 131	** Active **	remote
Scope [10.169.135.0] 135	** Active **	
Scope [10.169.137.0] 137	** Active **	
Scope [10.169.138.0] 138	** Active **	
Scope [10.169.145.0] 145	** Active **	
Scope [10.169.150.0] 150	** Active **	
Scope [10.169.151.0] 151	** Active **	
Scope [10.169.152.0] 152	** Active **	
Scope [10.169.153.0] 153	** Active **	
Scope [10.169.154.0] 154	** Active **	
Scope [10.169.155.0] 155	** Active **	
Scope [10.169.156.0] 156	** Active **	
Scope [10.169.157.0] 157	** Active **	
Scope [10.169.158.0] 158	** Active **	
Scope [10.169.159.0] 159	** Active **	
Server Options		
Filters		

7. Select **060 Aruba Instant AP** in the **Server Options** window and enter **ArubaInstantAP** in the String Value.

Figure 93 *Instant and DHCP options for AirWave—060 IAP in Server Options*



Option Name	Vendor	Value	Class
006 DNS Servers	Standard	10.169.130.4	None
015 DNS Domain Name	Standard	rde.arubanetworks.com	None
060 Aruba Instant AP	Standard	ArubaInstantAP	None

Available Options	Description
□ ~~049 X Window System~~ Display	Array of X W
☑ 060 Aruba Instant AP	Aruba AP vc
□ ~~064 NIS+ Domain Name~~	The name o
□ 065 NIS+ Servers	A list of IP a

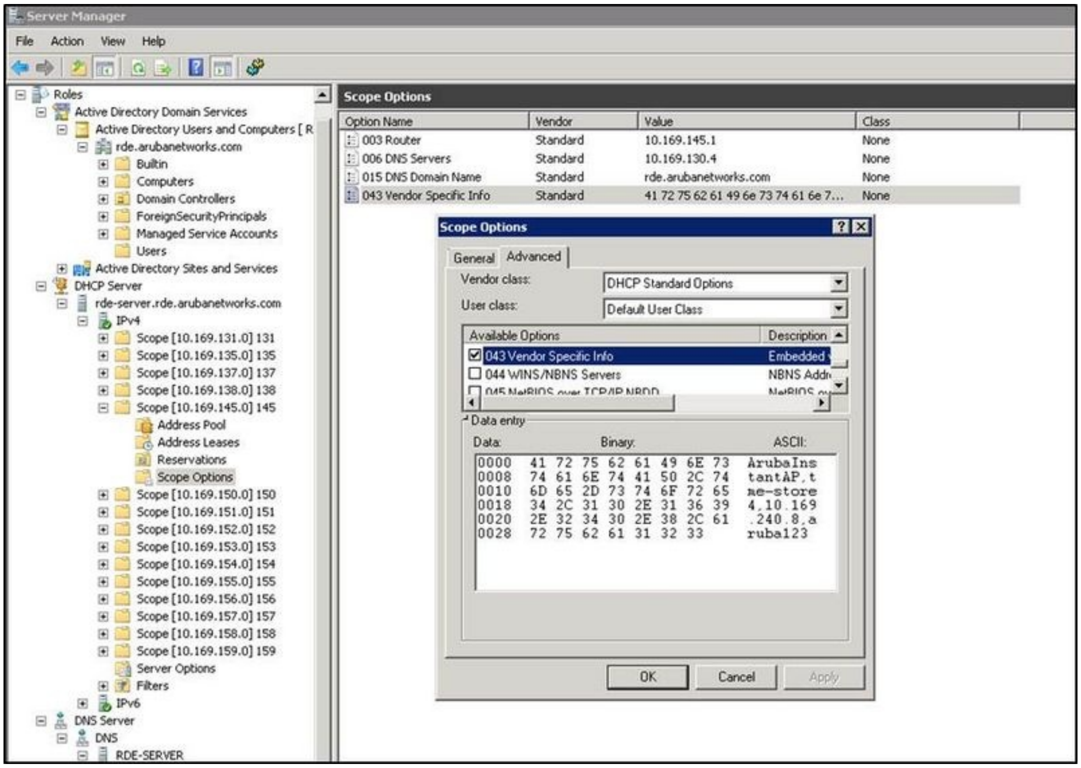
Data entry

String value: ArubaInstantAP

8. Select **043 Vendor Specific Info** and enter a value for either of the following in ASCII field:

- **airwave-orgn, airwave-ip, airwave-key**; for example: Aruba,192.0.2.20, 12344567
- **airwave-orgn, airwave-domain**; for example: Aruba, aruba.support.com

Figure 94 *Instant and DHCP options for AirWave— 043 Vendor Specific Info*



Scope Options

Option Name	Vendor	Value	Class
003 Router	Standard	10.169.145.1	None
006 DNS Servers	Standard	10.169.130.4	None
015 DNS Domain Name	Standard	rde.arubanetworks.com	None
043 Vendor Specific Info	Standard	41 72 75 62 61 49 6e 73 74 61 6e 7...	None

Vendor class: DHCP Standard Options

User class: Default User Class

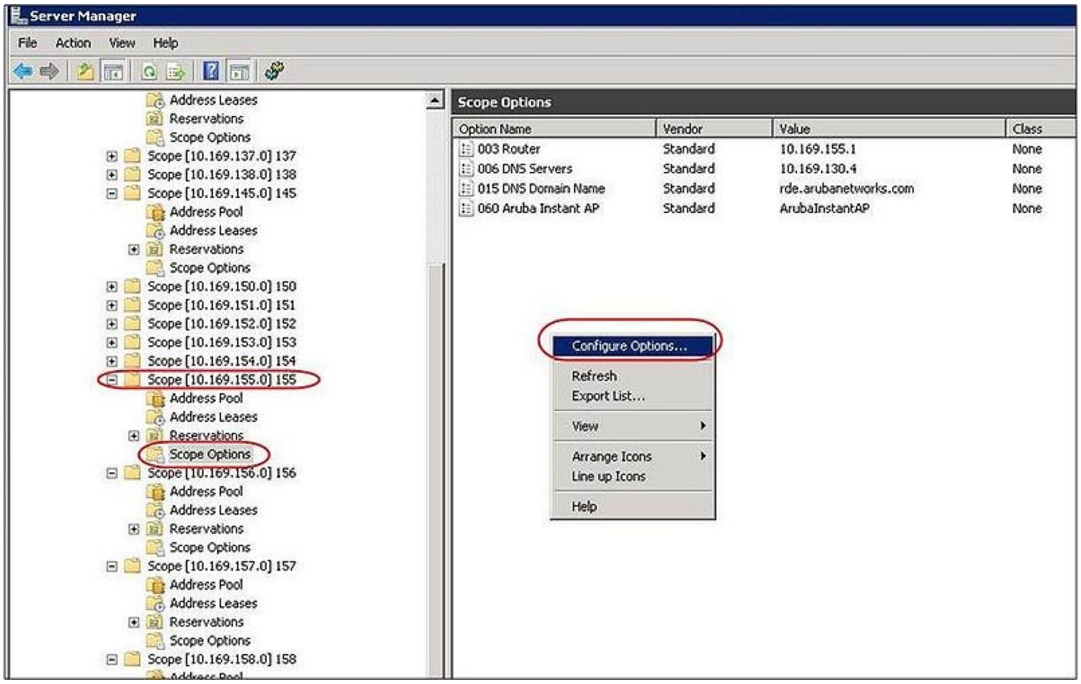
Available Options	Description
☑ 043 Vendor Specific Info	Embedded
□ 044 WINS/NBNS Servers	NBNS Addr
□ 045 NetBIOS over TCP/IP NBDD	NetBIOS ov

Data entry

```
Data:          Binary:                    ASCII:
0000   41 72 75 62 61 49 6E 73   ArubaIns
0008   74 61 6E 74 41 50 2C 74   tantAP,t
0010   6D 65 2D 73 74 6F 72 65   me-store
0018   34 2C 31 30 2E 31 36 39   4,10.169
0020   2E 32 34 30 2E 38 2C 61   .240.8,a
0028   72 75 62 61 31 32 33      ruba123
```

This creates a DHCP option 60 and 43 on a global basis. You can do the same on a per-scope basis. The per-scope option overrides the global option.

Figure 95 *Instant and DHCP options for AirWave: Scope Options*



Scope Options

Option Name	Vendor	Value	Class
003 Router	Standard	10.169.155.1	None
006 DNS Servers	Standard	10.169.130.4	None
015 DNS Domain Name	Standard	rde.arubanetworks.com	None
060 Aruba Instant AP	Standard	ArubaInstantAP	None

Alternate Method for Defining Vendor-Specific DHCP Options

This section describes how to add vendor-specific DHCP options for Instant APs in a network that already uses DHCP options 60 and 43 for other services. Some networks use DHCP standard options 60 and 43 to provide the

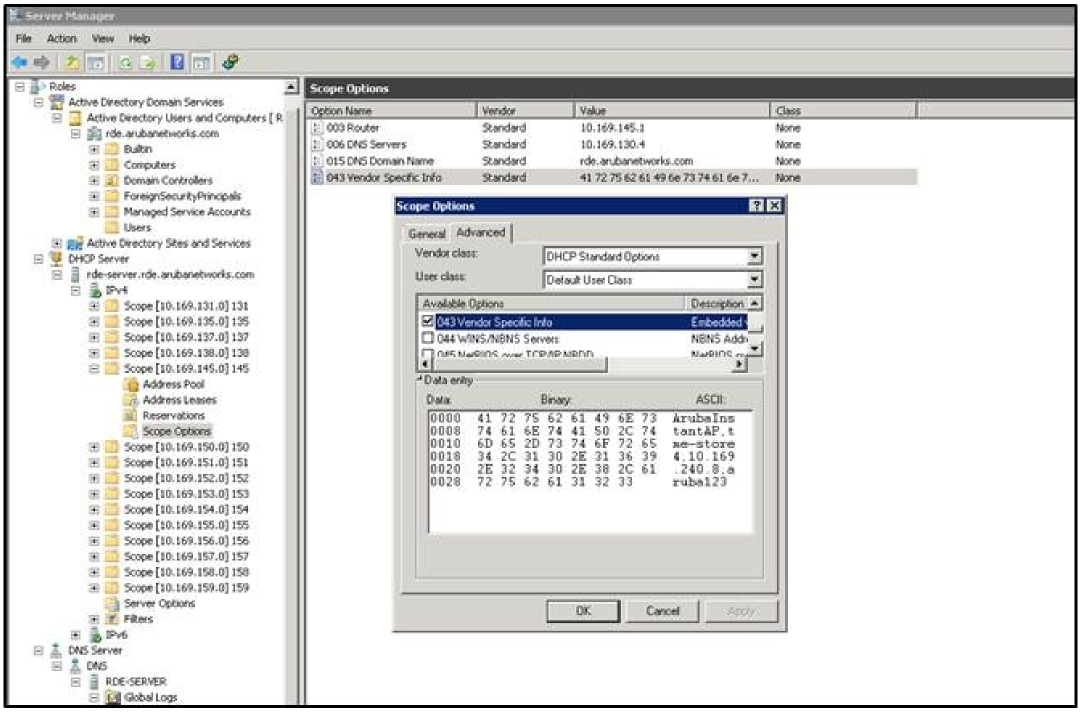
DHCP clients information about certain services such as PXE. In such an environment, the standard DHCP options 60 and 43 cannot be used for Aruba APs.

This method describes how to set up a DHCP server to send option 43 with AirWave information to Instant IAP. This section assumes that option 43 is sent per scope, because option 60 is being shared by other devices as well.

> NOTE
>
> The DHCP scope must be specific to Instant, and the PXE devices that use options 60 and 43 must not connect to the subnet defined by this scope. This is because you can specify only one option 43 for a scope, and if other devices that use option 43 connect to this subnet, they are presented with Instant-specific information.

1. In server 2008, navigate to **Server Manager > Roles > DHCP Server > Domain DHCP Server** (rde-server.rde.arubanetworks.com) **> IPv4**.
2. Select a scope (subnet). Scope (10.169.145.0)145 is selected in the example shown in the figure below.
3. Right-click and select **Advanced,** and then specify the following options:
   - Vendor class– DHCP Standard Options
   - User class– Default User Class
   - Available options– Select 043 Vendor-Specific Info
   - String Value– ArubaInstantAP, tme-store4, 10.169.240.8, Aruba123 (which is the AP description, organization string, AirWave IP address or domain name, Pre-shared key, for AirWave)

Figure 96 *Vendor Specific DHCP options*



Scope Options

Option Name	Vendor	Value	Class
003 Router	Standard	10.169.145.1	None
006 DNS Servers	Standard	10.169.130.4	None
015 DNS Domain Name	Standard	rde.arubanetworks.com	None
043 Vendor Specific Info	Standard	41 72 75 62 61 49 6e 73 74 61 6e 7...	None

Vendor class: DHCP Standard Options

User class: Default User Class

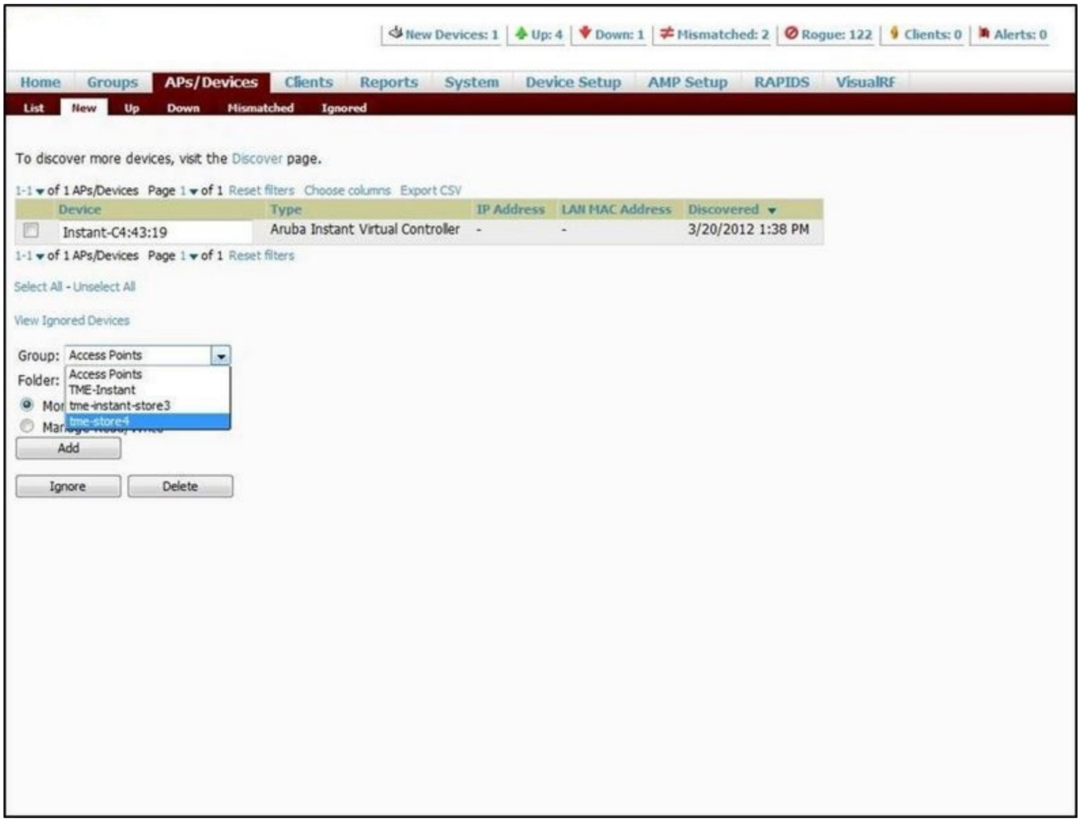
Available Options	Description
☑ 043 Vendor Specific Info	Embedded
□ 044 WINS/NBNS Servers	NBNS Addr
□ 045 NetBIOS over TCP/IP NBDD	NetBIOS

Data entry

```
Data:          Binary:                    ASCII:
0000   41 72 75 62 61 49 6E 73   ArubaIns
0008   74 61 6E 74 41 50 2C 74   tantAP,t
0010   6D 65 2D 73 74 6F 72 65   me-store
0018   34 2C 31 30 2E 31 36 39   4,10.169
0020   2E 32 34 30 2E 38 2C 61   .240.8,a
0028   72 75 62 61 31 32 33      ruba123
```

Upon completion, the IAP shows up as a new device in AirWave, and a new group called **tme-store4** is created. Navigate to **APs/Devices > New > Group** to view this group.

Figure 97 *AirWave — New Group*



To discover more devices, visit the Discover page.

1-1 of 1 APs/Devices Page 1 of 1 Reset filters Choose columns Export CSV

	Device	Type	IP Address	LAN MAC Address	Discovered
□	Instant-C4:43:19	Aruba Instant Virtual Controller	-	-	3/20/2012 1:38 PM

1-1 of 1 APs/Devices Page 1 of 1 Reset filters

Select All - Unselect All

View Ignored Devices

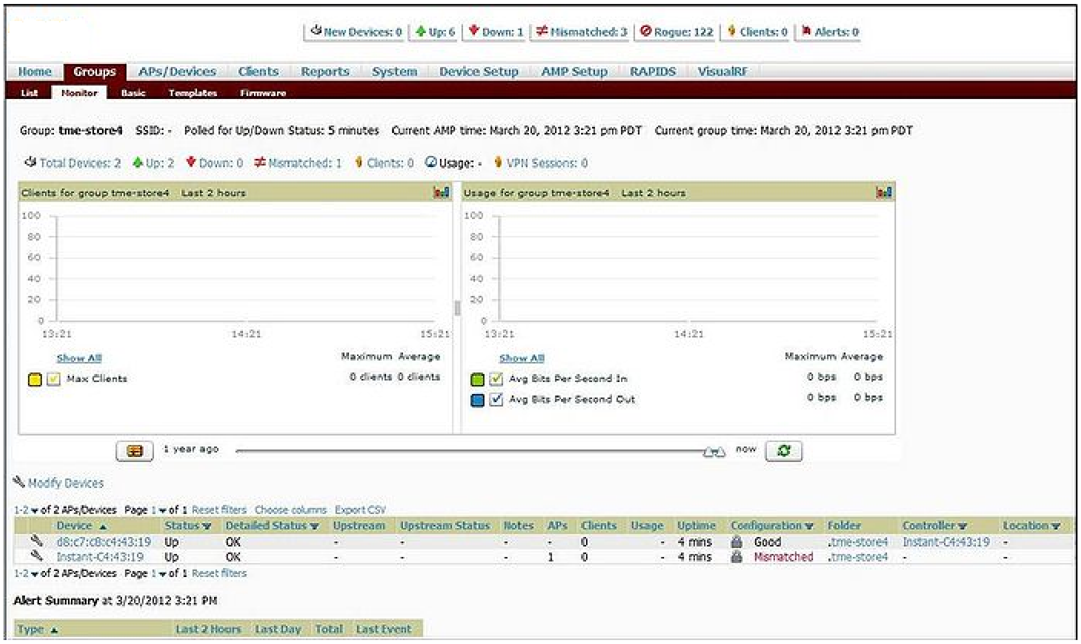
Group: Access Points

Folder:

● Mon

○ Mar

Figure 98 *AirWave —Monitor*



Group: tme-store4 SSID: - Polled for Up/Down Status: 5 minutes Current AMP time: March 20, 2012 3:21 pm PDT Current group time: March 20, 2012 3:21 pm PDT

Total Devices: 2 Up: 2 Down: 0 Mismatched: 1 Clients: 0 Usage: - VPN Sessions: 0

1-2 of 2 APs/Devices Page 1 of 1 Reset filters Choose columns Export CSV

	Device	Status	Detailed Status	Upstream	Upstream Status	Notes	APs	Clients	Usage	Uptime	Configuration	Folder	Controller	Location
	d8:c7:c8:c4:43:19	Up	OK	-	-	-	-	0	-	4 mins	Good	.tme-store4	Instant-C4:43:19	-
	Instant-C4:43:19	Up	OK	-	-	-	1	0	-	4 mins	Mismatched	.tme-store4	-	-

1-2 of 2 APs/Devices Page 1 of 1 Reset filters

Alert Summary at 3/20/2012 3:21 PM

Type	Last 2 Hours	Last Day	Total	Last Event

The Aruba Central user interface provides a standard web-based interface that allows you to configure and monitor multiple Aruba Instant networks from anywhere with a connection to the internet. Central supports all the Instant Access Points (IAPs) running 6.2.1.0-3.3.0.0 or later versions.

Using Central, individual users can manage their own wireless network. This user interface is accessible through a standard web browser and can be launched using various browsers. Aruba Central uses a secure HTTPs connection and provides a strong mutual authentication mechanism using certificates for all communication with IAPs. These certificates ensure the highest level of protection.

Provisioning an IAP using Central

After you subscribe and register an IAP, log in to the Central dashboard to manage your IAP using the URL, https://portal.central.arubanetworks.com.

The Central user interface is categorized into the following sections:

1. Monitoring
2. Configuration
3. Reporting
4. Maintenance

These sections are layered under groups. The configuration details of the IAPs are defined at a group level. Any IAP joining a group inherits the configuration defined for the group. After you create a group, navigate to the Configuration section and create a new SSID. Aruba Central supports zero touch provisioning which allows the network administrators to configure the IAPs even before the hardware arrives.

After you power on the IAP and connect to the uplink port, you will see the IAP under the default group in the Aruba Central user interface. You can choose to move the IAP to a different group that you created. The configuration defined in this group is automatically applied to the IAP.

Maintaining the Subscription List

Aruba Central maintains a subscription list for the IAPs. If an IAP is not included in this list, Central identifies it as an unauthorized IAP and prevents it from joining the network. The service providers use Aruba Central to track the subscription of each IAP based on its serial number and MAC address.

Following are the types of subscription status that can be listed for the IAPs:

- Active - Central allows the IAP to join the network.
- Expired - Central denies the IAP from joining the network.

NOTE

  - If the status of a master IAP changes from active to expired, the virtual controller is set to factory defaults and reboots.
  - If the status of a slave IAP changes from active to expired, the virtual controller sets the slave IAP to factory defaults and reboots the IAP.

- Unknown - Central does not allow the IAP to join the network, however it gives an option to retry the connection.

The list maintained by Aruba Central is different from the list maintained by the end-users. So, Central can prevent an IAP from joining the network when the subscription expires, even if the IAP is present in the subscription list maintained by the end-user.

NOTE

The subscription list is dynamic and gets updated each time an IAP is included in Central.

Firmware Maintenance

For a multi-class IAP network, ensure the IAP can download software images from the Aruba Cloud-based Image Service. You may also need to configure HTTP proxy settings on the IAP if they are required for Internet access in your network. For more information about image upgrade and HTTP proxy configuration, see sections Image Management Using Cloud Server on page 72 and Configuring HTTP Proxy on an IAP on page 72.

This chapter provides the following information:

AirGroup Overview

AirGroup is a unique enterprise-class capability that leverages zero configuration networking to enable Bonjour® services such as Apple® AirPrint and AirPlay from mobile devices in an efficient manner. Apple AirPlay and AirPrint services are based on the Bonjour protocol are essential services in campus Wi-Fi networks.

Zero configuration networking enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home. Bonjour is the trade name for the zero configuration implementation introduced by Apple. It is supported by most of the Apple product lines, including the Mac OS X operating system, iPhone, iPod Touch, iPad, Apple TV, and AirPort Express.

Bonjour can be installed on computers running Microsoft Windows® and is supported by the new network-capable printers. Bonjour is also included with popular software programs such as Apple iTunes, Safari, and iPhoto. Bonjour uses multicast DNS (mDNS) to locate devices and the services offered by these devices. The AirGroup solution supports both wired and wireless devices. Wired devices, which support the Bonjour services are made part of AirGroup when the VLANs of the devices are terminated on the Virtual Controller.

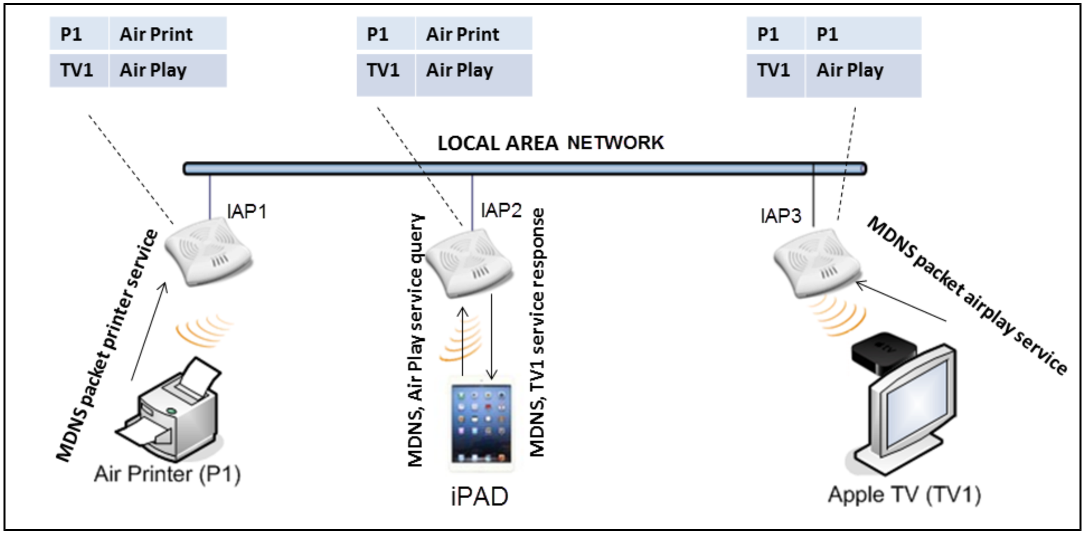
AirGroup also supports ClearPass Policy Manager (CPPM).

- Users can register their personal devices and define a group of users who can to share the registered devices.
- Administrators can register and manage an organization's shared devices such as printers and conference room Apple TVs. An administrator can grant global access to each device, or restrict access according to the username, role, or user location.

The distributed AirGroup architecture allows each IAP to handle Bonjour queries and responses individually instead of overloading a Virtual Controller with these tasks. This results in a scalable AirGroup solution.

As shown in the following figure, the IAP1 discovers Air Printer (P1) and IAP3 discovers Apple TV (TV1). IAP1 advertises information about its connected P1 device to the other IAPs that isIAP2 and IAP3. Similarly, IAP3 advertises TV1 device to IAP1 and IAP2. This type of distributed architecture allows any IAP to respond to its connected devices locally. In this example, the iPad connected to IAP2 obtains direct response from the same IAP about the other Bonjour-enabled services in the network.

Figure 99 *- AirGroup Architecture*



NOTE

AirGroup is not supported on a 3G uplink.

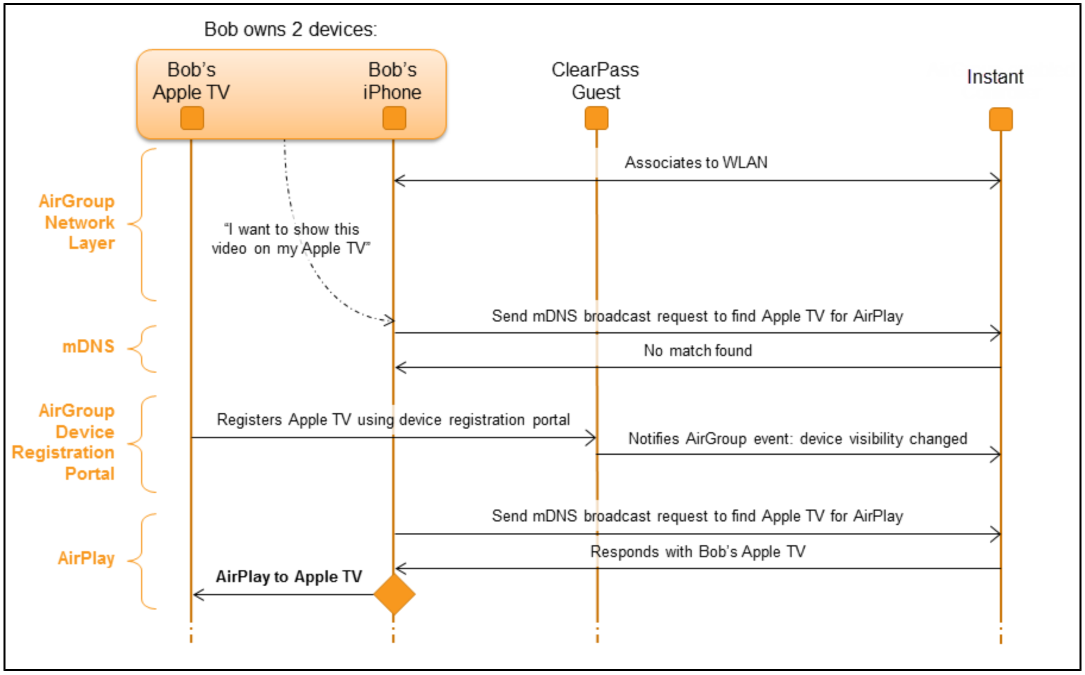
AirGroup with Instant

AirGroup capabilities are available as a feature in Aruba WLANs where Wi-Fi data is distributed among Instant APs. When an Aruba WLAN is powered by Instant and CPPM, AirGroup begins to function.

An AirGroup device can be registered by an administrator or a guest user.

1. The AirGroup administrator gives an end user the AirGroup operator role which authorizes the user to register the users' device–such as an Apple TV on the CPPM platform.
2. Instant maintains information for all mDNS services. Instant queries CPPM to map each device’s access privileges to available services.
3. Instant responds back to the query made by a device based on contextual data such as user role, username, and location.

Figure 100 *AirGroup Enables Personal Device Sharing*


Bob owns 2 devices:
Bob's Apple TV
Bob's iPhone
ClearPass Guest
Instant
AirGroup Network Layer
mDNS
AirGroup Device Registration Portal
AirPlay
Associates to WLAN
"I want to show this video on my Apple TV"
Send mDNS broadcast request to find Apple TV for AirPlay
No match found
Registers Apple TV using device registration portal
Notifies AirGroup event: device visibility changed
Send mDNS broadcast request to find Apple TV for AirPlay
Responds with Bob's Apple TV
AirPlay to Apple TV

AirGroup Solution

In large universities and enterprise networks, it is common for Bonjour-capable devices to connect to the network across VLANs. As a result, user devices such as an iPad on a specific VLAN cannot discover an Apple TV that resides on another VLAN. As the addresses used by the protocol are link-scope multicast addresses, each query or advertisement can only be forwarded on its respective VLAN, but not across different VLANs.

Broadcast and multicast traffic are usually filtered out from a wireless LAN network to preserve the airtime and battery life. This inhibits the performance of Bonjour services as they rely on multicast traffic. Aruba addresses this multicast DNS (mDNS) challenge with AirGroup technology.

AirGroup leverages key elements of Aruba's solution portfolio including operating system software for Instant, CPPM , and the VLAN-based or role-based filtering options offered by Bonjour services. AirGroup maintains seamless connectivity between clients and services across VLANs and SSIDs. The mDNS packet traffic is minimized thereby preserving valuable wired network bandwidth and WLAN airtime.

The following table summarizes the filtering options:

Table 53: *AirGroup Filtering Options*

Features	Instant Deployment Models	
	Integrated	**Integrated with CPPM**
Allow mDNS to propagate across subnets/VLANs	Yes	Yes
Limit multicast mDNS traffic on the network	Yes	Yes
VLAN based mDNS service policy enforcement	Yes	Yes
User-role based mDNS service policy enforcement	Yes	Yes
Portal to self register personal leaves	No	Yes

Table 53: *AirGroup Filtering Options*

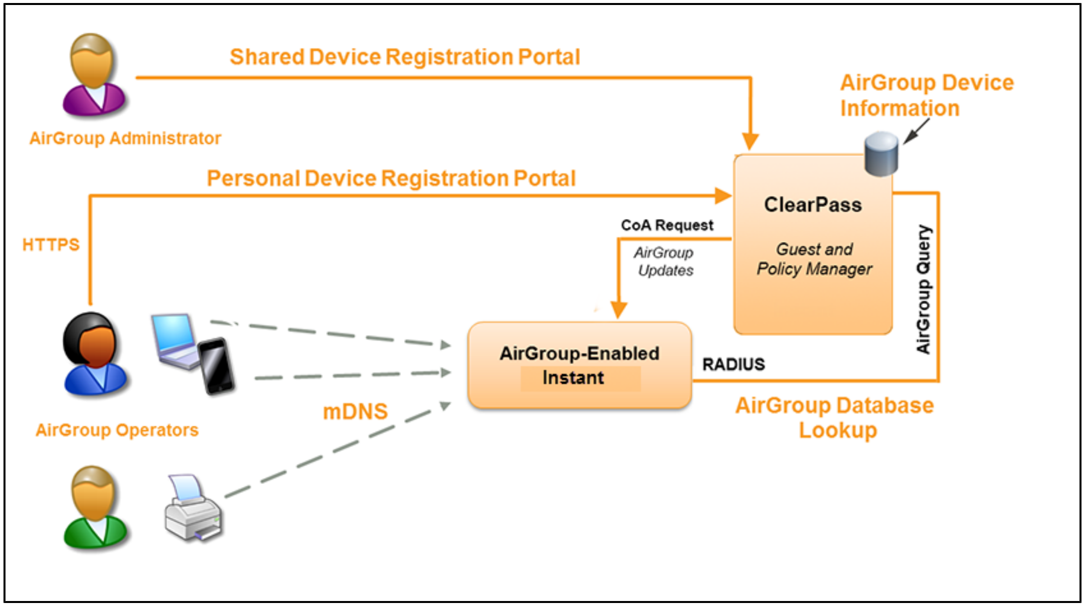
Features	Instant Deployment Models	
Device owner based policy enforcement	No	Yes
Location based policy enforcement	No	Yes
Shared user list based policy enforcement	No	Yes
Shared role list based policy enforcement	No	Yes

AirGroup also enables context awareness for services across the network:

- AirGroup is aware of personal devices. For example, an Apple TV in a dorm room can be associated with the student who owns it.
- AirGroup is aware of shared resources. This might be an Apple TV in a meeting room or a printer in a supply room that is available to certain users, such as the marketing department. Or, in a classroom, teachers can use AirPlay to wirelessly project a laptop screen onto an HDTV monitor using an Apple TV.
- AirGroup is aware of the location of services when CPPM support is enabled. For example, depending on proximity, an iPad would be presented with the closest printer instead of all the printers in the building.
- When configured with Instant, AirGroup enables a client to perform a location-based discovery. For example, when a client roams from one Instant cluster to another, it can discover devices available in the new cluster to which the client is currently connected.

The following figure shows a higher-education environment with shared, local, and personal services available to mobile devices. With AirGroup, the context-based policies determine the Bonjour services that can be accessed by an end-user’s mobile device.

Figure 101 - *AirGroup in a Higher-Education Environment*



AirGroup Features

AirGroup supports the following features:

- AirGroup sends unicast responses to mDNS queries and reduces mDNS traffic footprint.
- Ensure cross-VLAN visibility and availability of mDNS devices and services.
- Allow or block mDNS services for all users.

- Allow or block mDNS services based on user roles.
- Allow or block mDNS services based on VLANs.
- Match users' devices, such as iPads, to their closest Bonjour devices, such as printers. This requires CPPM support.

CPPM and ClearPass Guest Features

CPPM and ClearPass Guest support the following features:

- Registration portal for WLAN users to register their personal devices such as Apple TVs and printers.
- Registration portal for WLAN administrators to register shared devices, such as conference room Apple TVs and printers.
- Operator-defined *personal* AirGroup to specify a list of other users who can share devices with the operator.
- Administrator defined username, user role, and location attributes for shared devices.

AirGroup Components

The components that make up the AirGroup Solution include the Instant, CPPM, and ClearPass Guest. The version requirements are described in the following table:

Table 54: *Instant, CPPM, and ClearPass Guest Requirements*

Component	Minimum Version
Instant	6.2.0.0-3.2.0.0
ClearPass Guest software	3.9.7
ClearPass GuestServices plugin	0.8.7
ClearPass Guestsoftware	5.2

NOTE

Starting from ClearPass version 6.0, the ClearPass Guest and the AirGroup Services plug-in are integrated into a single platform.

AirGroup Services

The AirGroup supports zero configuration services. The services are pre-configured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services by using the Instant UI or CLI.

The following services are available for IAP clients:

- AirPlay™– Apple® AirPlay™ allows wireless streaming of music, video, and slideshows from your iOS device to Apple TV® and other devices that support the AirPlay™ feature.
- AirPrint™– Apple® AirPrint™ allows you to print from an iPad®, iPhone®, or iPod® Touch directly to any AirPrint™ compatible printers.
- iTunes– iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple® devices.
- RemoteMgmt– Use this service for remote login, remote management, and FTP utilities on Apple® devices.
- Sharing– Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple® devices.
- Chat– The iChat® (Instant Messenger) application on Apple® devices uses this service.

Configuring AirGroup and AirGroup Services on an IAP

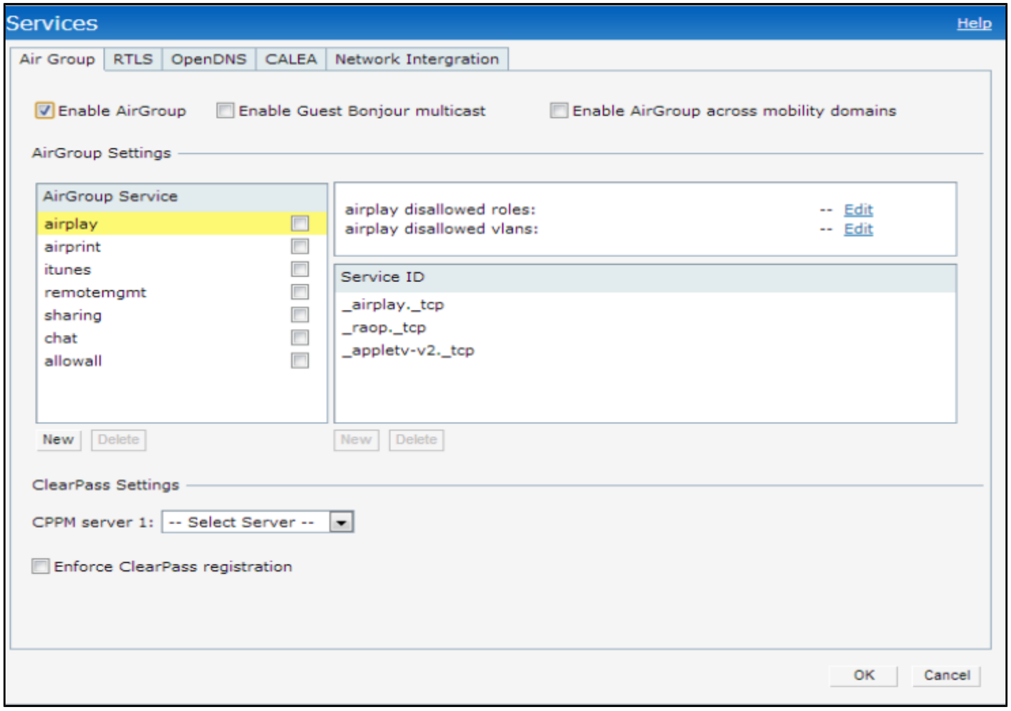
You can configure AirGroup services, using Instant UI or CLI.

In the Instant UI

To enable AirGroup and its services:

1. Click the **More**>**Services** link at the top right corner of the Instant main window.
2. Click **Air Group** tab. The **Air Group** tab details are displayed.
3. Select the **Enable Air Group** check box. The AirGroup configuration parameters are displayed.

Figure 102 *AirGroup Configuration*



☑ Enable AirGroup ☐ Enable Guest Bonjour multicast ☐ Enable AirGroup across mobility domains

AirGroup Settings

AirGroup Service	
airplay	☐
airprint	☐
itunes	☐
remotemgmt	☐
sharing	☐
chat	☐
allowall	☐

airplay disallowed roles: -- Edit
airplay disallowed vlans: -- Edit

Service ID
_airplay._tcp
_raop._tcp
_appletv-v2._tcp

ClearPass Settings

CPPM server 1: -- Select Server --

☐ Enforce ClearPass registration

4. Select **Enable Guest Bonjour multicast** to allow the users to use Bonjour services enabled in a guest VLAN. When this check box is enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN.
5. Select the **Enable Air Group across mobility domains** check box to enable Inter cluster mobility. Instant supports two types assignment modes:
   - Intra Cluster - In the Intra Cluster model, the IAP does not share the mDNS database information with the other clusters.
   - Inter Cluster - In the Inter Cluster model, the IAP shares the mDNS database information with the other clusters. The DNS records in the Virtual Controller can be shared with the all the Virtual Controllers configured for L3 Mobility.

   By default, this feature is disabled. To define clusters, go to **System**> **L3 Mobility** tab.
6. Select the required AirGroup services. The service IDs associated with an AirGroup service are also displayed. To add any service, click **New** and add. To allow all services, select **allowall**.
7. Based on the services configured, you can block any user roles and VLAN from accessing an AirGroup service. The user roles and VLANs marked as disallowed are prevented from accessing the corresponding AirGroup service. You can create a list of disallowed user roles and VLANs for all AirGroup services configured on the IAP. For example, If the AirPlay service is selected, the **edit** links for the **airplay disallowed roles** and **airplay disallowed vlans** are displayed. Similarly, if sharing service is selected, the **edit** links for the **sharing disallowed roles** and **sharing disallowed vlans** are displayed.

- To select block user roles from accessing an AirGroup service, click the corresponding **edit** link and select the user roles for which you want to restrict access. By default, an AirGroup service is accessible by all user roles configured in your IAP cluster.
- To select VLANs from allowing access to an AirGroup service, click the corresponding **edit** link and select the VLANs to exclude. By default, the AirGroup services are accessible by users or devices in all VLANs configured in your IAP cluster.

8. **ClearPass Settings**– Use this section to configure the CPPM server, CoA server, and enforce ClearPass registering.
   - **CPPM server 1**– Indicates the ClearPass Policy Manager server information for AirGroup policy.
   - **Enforce ClearPass registering**– When enabled, only devices registered with CPPM will be discovered by Bonjour devices, based on the CPPM policy.

In the CLI

To configure AirGroup:

```
(Instant Access Point)(config)# airgroup
(Instant Access Point)(airgroup)# cppm enforce-registration
(Instant Access Point)(airgroup)# cppm-server <server>
(Instant Access Point)(airgroup)# cppm-server-dead-time <interval>
(Instant Access Point)(airgroup)# cppm-query-interval <interval>
(Instant Access Point)(airgroup)# disallow-vlan <vlan-ID>
(Instant Access Point)(airgroup)# enable-guest-multicast
(Instant Access Point)(airgroup)# multi-swarm
(Instant Access Point)(airgroup)# end
(Instant Access Point)# commit apply
```

To configure AirGroup Service

```
(Instant Access Point)(config)# airgroupservice <airgroup-service>
(Instant Access Point)(airgroup-service)# id <airgroupservice-ID>
(Instant Access Point)(airgroup-service)# description <text>
(Instant Access Point)(airgroup-service)# disallow-role <role>
(Instant Access Point)(airgroup-service)# disallow-vlan <vlan-ID>
(Instant Access Point)(airgroup-service)# end
(Instant Access Point)# commit apply
```

To view AirGroup configuration status:

```
Instant Access Point# show airgroup status
AirGroup Feature
----------------
Status
------
Disabled
AirGroup Multi Swarm
--------------------
Status
------
Disabled
AirGroup Guest Multicast
------------------------
Status
------
Disabled
CPPM Parameters
---------------
Parameter                    Value
---------                    -----
CPPM Enforce Registration    Disabled
CPPM Server query interval   10 hours
CPPM Server dead time       100 Seconds
AirGroup Service Information
----------------------------
Service      Status
-------      ------
airplay      Enabled
airprint     Disabled
itunes       Disabled
remotemgmt   Enabled
sharing      Disabled
chat         Enabled
allowall     Disabled
```

Configuring AirGroup and CPPM interface in Instant

Configure the Instant and CPPM interface to allow an AirGroup IAP and CPPM to exchange information regarding device sharing, and location. The configuration options define the RADIUS server that is used by the AirGroup RADIUS client.

The AirGroup configuration with CPPM involves the following steps:

1. Create a RADIUS service
2. Assign a Server to AirGroup
3. Configure CPPM to Enforce Registration

Creating a RADIUS Server

You can configure an external RADIUS Security window. For more information on the configuring CPPM server, see Configuring an External Server for Authentication on page 149. You can also create a RADIUS server in the **Air Group** window. Navigate to **Services> AirGroup > Clear Pass Settings > CPPM server 1>** and select **New** from the drop-down menu.

Assign a Server to AirGroup

To associate CPPM server with AirGroup, select the CPPM server from the **CPPM Server 1** drop-down.

NOTE

If two CPPM servers are configured, the CPPM server 1 acts as a primary server and the CPPM server 2 acts as a backup server.

After configuration is complete, this particular server will appear in the CoA server option. To view this server go to **Services> AirGroup >ClearPass Settings > CoA server**.

Configure CPPM to Enforce Registration

When CPPM registration is enforced, the devices registered with CPPM will be discovered by Bonjour devices, based on the CPPM policy.

Change of Authorization (CoA)

When a RADIUS server is configured with Change of Authorization (CoA) with CPPM server, the guest users are allowed to register their devices. For more information on configuring RADIUS server with CoA , see Configuring an External Server for Authentication on page 149.

NOTE

You can also create a **CoA only server** in the **Services> AirGroup > Clear Pass Settings > CoA server** window.

Chapter 25

IAP Integration with Security and Location Services Applications

This chapter describes the following procedures:

- Configuring an IAP for RTLS Support on page 290
- Configuring an IAP for Analytics and Location Engine Support on page 289
- Integrating an IAP with Palo Alto Networks Firewall on page 291

Configuring an IAP for Analytics and Location Engine Support

The Analytics and Location Engine (ALE) is designed to gather client information from the network, process it and share it through a standard API. The client information gathered by ALE can be used for analyzing a client's internet behavior for business such as shopping preferences.

ALE includes a location engine that calculates the associated and unassociated device location every 30 seconds by default. For every device on the network, ALE provides the following information through the Northbound API:

- Client user name
- IP address
- MAC address
- Device type
- Application firewall data, showing the destinations and applications used by associated devices.
- Current location
- Historical location

ALE requires the AP placement data to be able to calculate location for the devices in a network.

ALE with Instant

Instant 6.3.1.1-4.0 release supports Analytics and Location Engine (ALE). The ALE server acts as a primary interface to all third-party applications and the IAP sends client information and all status information to the ALE server.

To integrate IAP with ALE, the ALE server address must be configured on an IAP. If the ALE sever is configured with a host name, the Virtula Controller performs a mutual certificated-based authentication with ALE server, before sending any information.

NOTE

IAP-92 and IAP-93 do not support ALE integration.

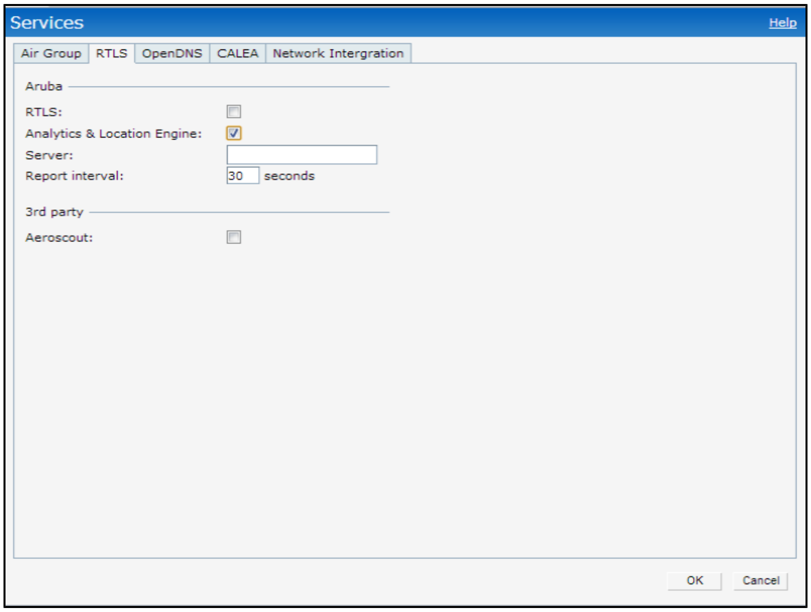
Enabling ALE Support on an IAP

You can configure an IAP for ALE support using Instant UI or CLI.

In the Instant UI

1. Click **More>Services**. The **Services** window is displayed.
2. Click the **RTLS** tab. The tab details are displayed.
3. Select the **Analytics & Location Engine** checkbox.

Figure 103 *Services Window —ALE Integration*



Aruba

RTLS: □

Analytics & Location Engine: ☑

Server:

Report interval: 30 seconds

3rd party

Aeroscout: □

4. Specify the ALE server name or IP address.
5. Specify the reporting interval within the range of 6-60 seconds. The IAP sends messages to the ALE server at the specified interval. The default interval is 30 seconds.
6. Click **OK**.

In the CLI

To enable IAP integration with the ALE server:

```
(Instant Access Point)(config)# ale-server <server-name| IP-address>
(Instant Access Point)(config)# ale-report-interval <seconds>
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Verifying ALE Configuration on an IAP

To view the configuration details:

```
(Instant Access Point)# show ale config
```

To verify the configuration status

```
(Instant Access Point)# show ale status
```

Configuring an IAP for RTLS Support

Instant supports the real-time tracking of devices when integrated with AirWave Management Platform, or third-party Real Time Location Server such as Aeroscout Real Time Location Server. With the help of the RTLS, the devices can be monitored in real-time or through history.

You can configure RTLS using Instant UI or CLI.

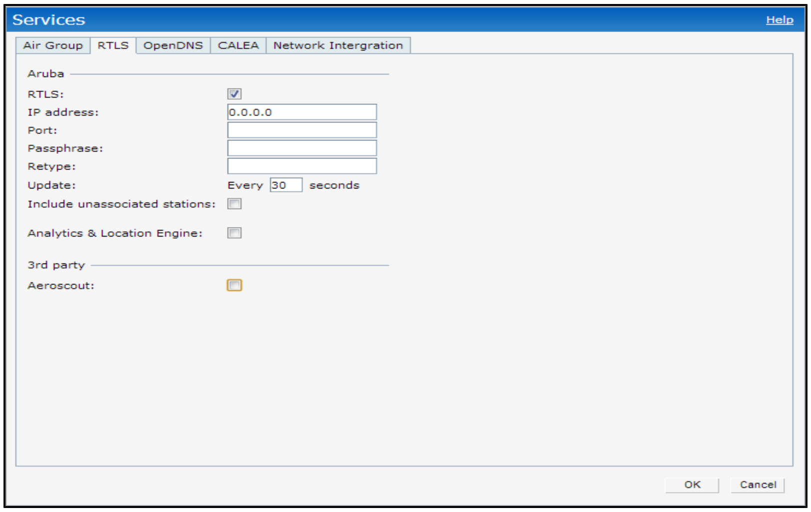
In the Instant UI

To configure Aruba RTLS:

1. Click the **More**>**Services** link at the top right corner of the Instant main window. The **Services** window is displayed.

2. Click the **RTLS** tab. The following figure shows the contents of the **RTLS** tab.
3. Select the **Aruba RTLS** check box to integrate Instant with AirWaveManagement platform or Ekahau Real Time Location Server.

Figure 104 *RTLS Window*



Aruba

RTLS: ☑

IP address: 0.0.0.0

Port:

Passphrase:

Retype:

Update: Every 30 seconds

Include unassociated stations: □

Analytics & Location Engine: □

3rd party

Aeroscout: □

4. Specify the IP address and port to which the location reports must be sent.
5. Specify the shared secret key in the **Passphrase** text box.
6. Specify the frequency at which the Virtual Controller can send updates to the server. You can specify a value within the range of 5-3600 seconds. The default value is 5 seconds.
7. Select the **Include unassociated stations** check box to send reports on the stations that are not associated to any IAP to the Aruba RTLS server.
8. Click **OK**.

To configure third-party RTLS such as Aeroscout:

1. Select the **Aeroscout** check box to send the RFID tag information to an AeroScout RTLS.
2. Specify the IP address and port number of the AeroScout server, to which location reports must be sent.
3. Select the **Include unassociated stations** check box to send reports on the stations that are not associated to any IAP to the Aeroscout RTLS server.
4. Click **OK**.

In the CLI

To configure AirWave RTLS:

```
(Instant Access Point)(config)# airwave-rtls <IP-address> <port> <passphrase> <seconds> includ
e-unassoc-sta
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To configure Aeroscout RTLS

```
(Instant Access Point)(config)# aeroscout-rtls <IP-address> <port> include-unassoc-sta
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Integrating an IAP with Palo Alto Networks Firewall

Palo Alto Networks (PAN) next-generation firewall offers contextual security for all users for safe enabling of applications. Simple firewall beyond basic IP address or TCP port numbers only provides a subset of the enhanced security required for enterprises to secure their networks. In the context of businesses using social networking sites, legacy firewalls are not able to differentiate valid authorized users from casual social networking users.

The Palo Alto next-generation firewall is based on user ID, which provides many methods for connecting to sources of identity information and associating them with firewall policy rules. For example, it provides an option to gather user information from Active Directory or LDAP server.

Integration with Instant

The functionality provided by the PAN firewall based on user ID requires the collection of information from the network. IAP maintains the network (such as mapping IP address) and user information for its clients in the network and can provide the required information for the user ID feature on PAN firewall. Before sending the user-ID mapping information to the PAN firewall, the IAP must retrieve an API key that will be used for authentication for all APIs.

IAP and PAN firewall integration can be seamless with the XML-API that available with PAN-OS 5.0 or later.

To integrate an IAP with PAN user ID, a global profile is added. This profile can be configured on an IAP with PAN firewall information such as IP address, port, user name, password, firewall enabled or disabled status.

The IAP sends messages to PAN based on the type of authentication and client status:

- After a client completes the authentication and is assigned an ip address, IAP will send the **login** message.
- After a client is disconnected or dissociated from the IAP, the IAP sends a **logout** message.

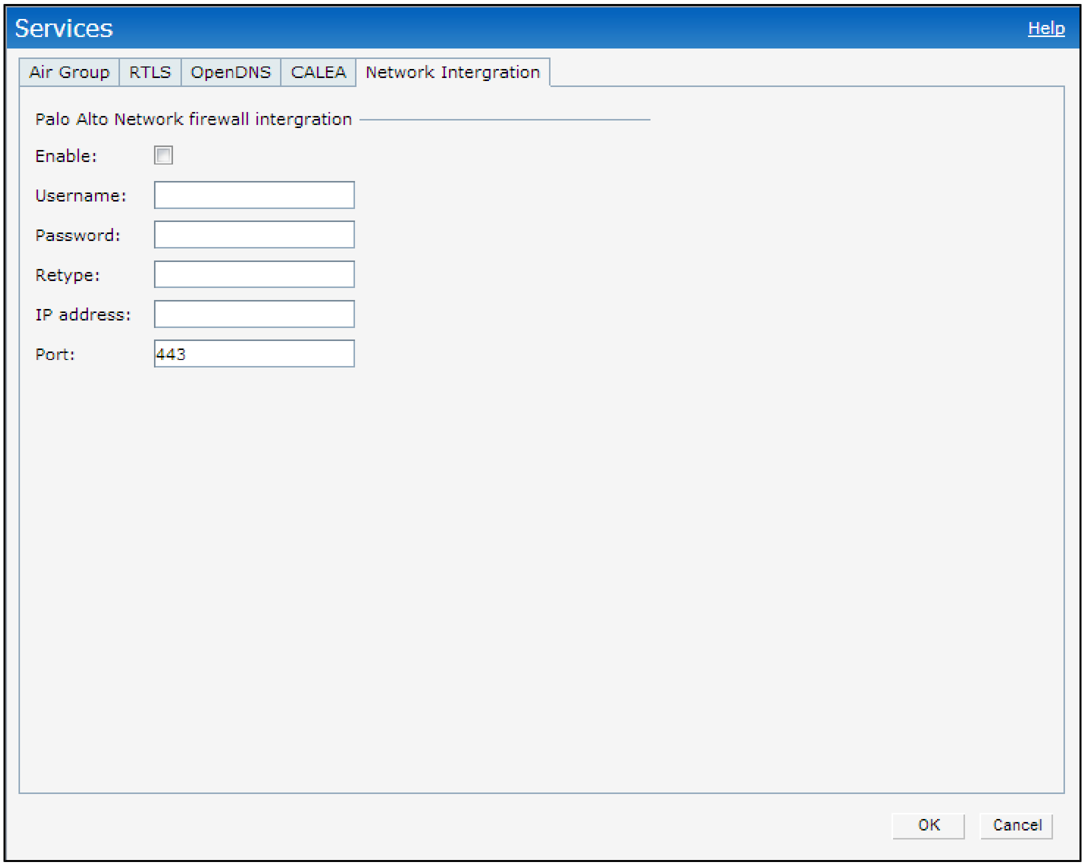
Configuring an IAP for PAN integration

You can configure an IAP for PAN firewall integration using Instant UI or CLI.

In the Instant UI

1. Click **More>Services**. The **Services** window is displayed.
2. Click **Network Integration**. The PAN firewall configuration options are displayed.

Figure 105 *Services Window—Network Integration Tab*



Palo Alto Network firewall intergration

Enable: □

Username:

Password:

Retype:

IP address:

Port: 443

3. Select the **Enable** checkbox to enable PAN firewall.
4. Specify the user name and password. Ensure that you provide user credentials of the PAN firewall administrator.
5. Enter the PAN firewall IP address.
6. Enter the port number within the range of 1–65535. The default port is 443.
7. Click **OK**.

In the CLI

To enable PAN firewall integration with the IAP:

```
(Instant Access Point)(config)# firewall-external-enforcement pan
(Instant Access Point)(firewall-external-enforcement pan)# enable
(Instant Access Point)(firewall-external-enforcement pan)# ip <ip-address>
(Instant Access Point)(firewall-external-enforcement pan)# port <port>
(Instant Access Point)(firewall-external-enforcement pan)# user <name> <password>
(Instant Access Point)(firewall-external-enforcement pan)# end
(Instant Access Point)# commit apply
```

Chapter 26
Lawful Intercept and CALEA Integration

This chapter provides the following information:

- CALEA Integration and Lawful Intercept Compliance on page 295
- Configuring IAPs for CALEA Integration on page 297

CALEA Integration and Lawful Intercept Compliance

Lawful Intercept (LI) allows the Law Enforcement Agencies (LEA) to perform an authorized electronic surveillance. Depending on the country of operation, the service providers (SPs) are required to support LI in their respective networks.

In the United States, SPs are required to ensure LI compliance based on Communications Assistance for Law Enforcement Act (CALEA) specifications.

Instant supports CALEA integration in a hierarchical and flat topology, mesh IAP network, wired and wireless networks.

NOTE

Enable this feature only if lawful interception is authorized by a Law enforcement agency.

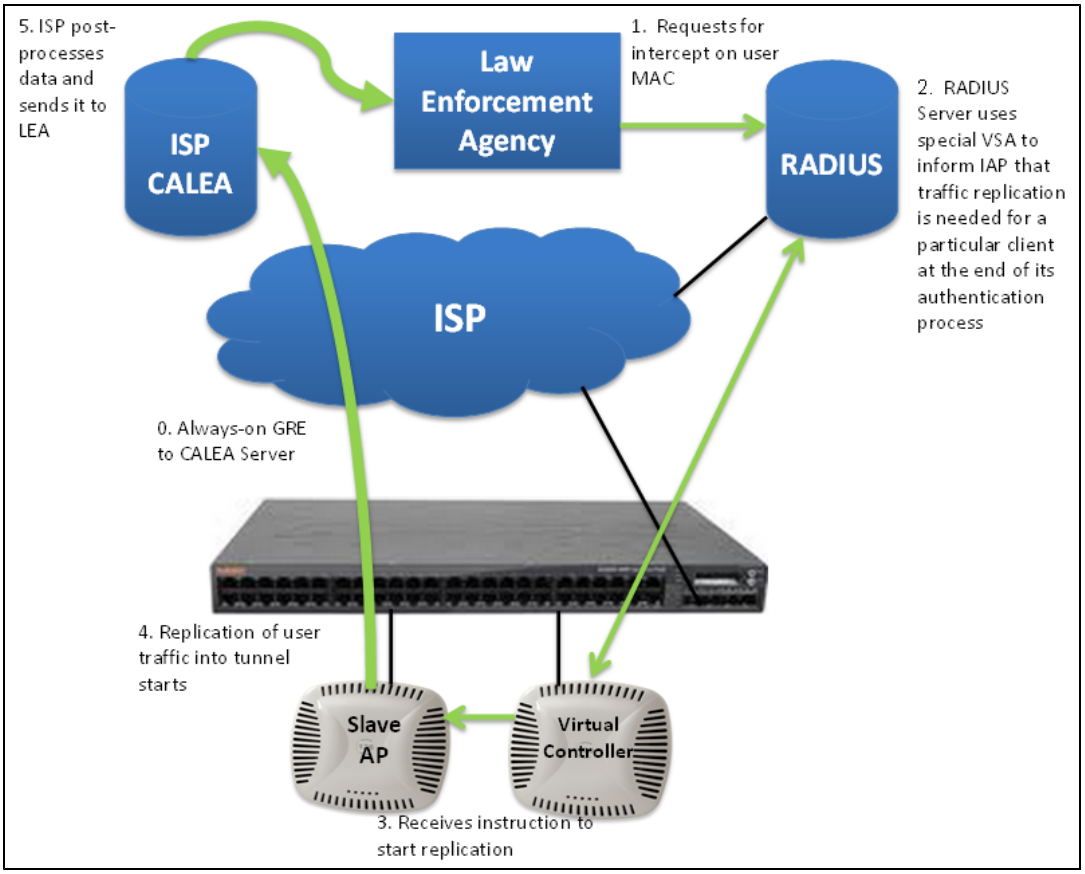
CALEA Server Integration

To support CALEA integration and ensure LI compliance, you can configure the IAPs to replicate a specific or selected client traffic and send it to a remote CALEA server.

Traffic Flow from IAP to CALEA Server

You can configure an IAP to send GRE encapsulated packets to the CALEA server and replicate client traffic within the GRE tunnel. Each IAP sends GRE encapsulated packets only for its associated or connected clients. The following figure illustrates the traffic flow from the IAP to the CALEA server.

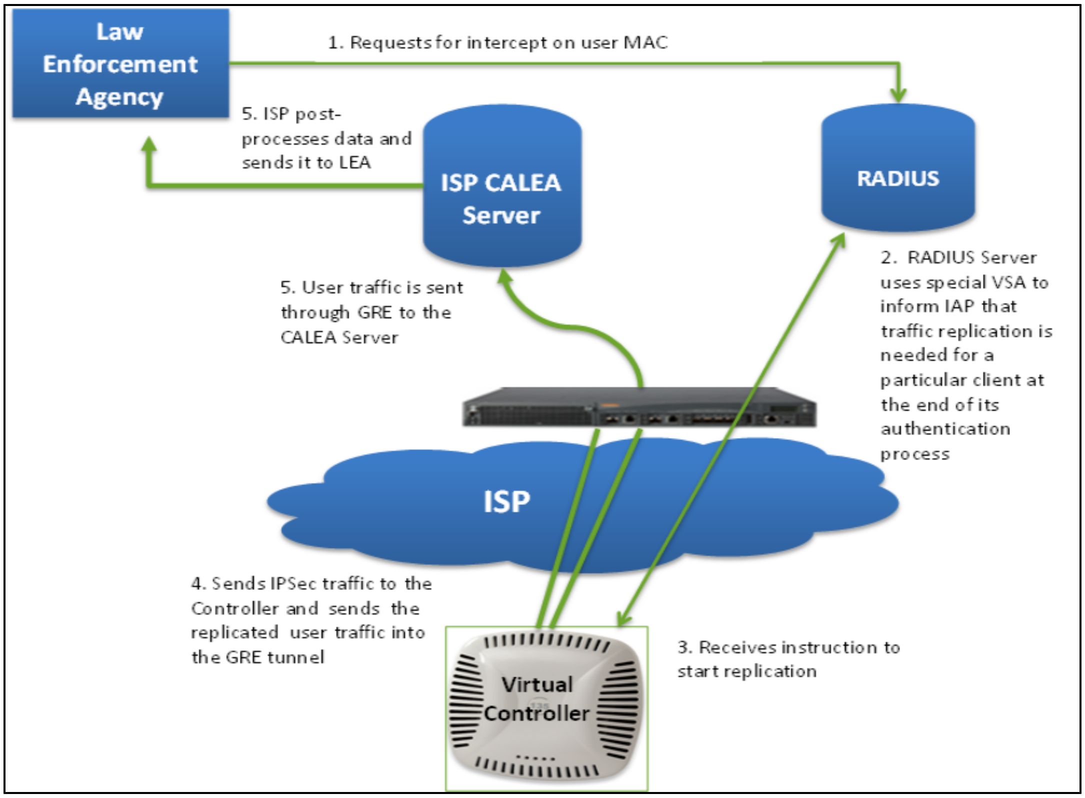
Figure 106 *IAP to CALEA Server*


5. ISP post-processes data and sends it to LEA
Law Enforcement Agency
1. Requests for intercept on user MAC
ISP CALEA
RADIUS
2. RADIUS Server uses special VSA to inform IAP that traffic replication is needed for a particular client at the end of its authentication process
ISP
0. Always-on GRE to CALEA Server
4. Replication of user traffic into tunnel starts
Slave AP
Virtual Controller
3. Receives instruction to start replication

Traffic Flow from IAP to CALEA Server through VPN

You can also deploy CALEA server with Controller and configure an additional IPSec tunnel for corporate access. When CALEA server is configured with Controller, the client traffic is replicated by the slave IAP and client data is encapsulated by GRE on slave, and routed to the master IAP. The master IAP sends the IPsec client traffic to Controller. Controller handles the IPSec client traffic while GRE data is routed to the CALEA server. The following figure illustrates the traffic flow from IAP to the CALEA server through VPN.

Figure 107 *IAP to CALEA Server through VPN*


Law Enforcement Agency
1. Requests for intercept on user MAC
5. ISP post-processes data and sends it to LEA
ISP CALEA Server
RADIUS
2. RADIUS Server uses special VSA to inform IAP that traffic replication is needed for a particular client at the end of its authentication process
5. User traffic is sent through GRE to the CALEA Server
ISP
4. Sends IPSec traffic to the Controller and sends the replicated user traffic into the GRE tunnel
Virtual Controller
3. Receives instruction to start replication

Ensure that IPSec tunnel is configured if the client data has to be routed to the ISP or CALEA server through VPN. For more information on configuring IPSec, see Configuring an Aruba IPSec Tunnel on page 249.

Client Traffic Replication

Client traffic is replicated in the following ways:

- Through RADIUS VSA– In this method, the client traffic is replicated by using RADIUS VSA to assign clients to a CALEA related user role. To enable role assignment to clients, you need to create a user role and CALEA access rule, and then assign the CALEA rule to the user role. Whenever a client that is configured to use a CALEA rule connects, a replication role is assigned.
- Through Change of Authorization (CoA)–In this method, a user session can start without replication. When the network administrator triggers a CoA from the RADIUS server, the user session is replicated. The replication is stopped when the user disconnects or by sending a CoA to change the replication role.

As the client information is shared between multiple IAPs in a cluster, the replication rules persist when clients roam within the cluster.

Configuring IAPs for CALEA Integration

To enable CALEA server integration, perform the following steps:

1. Create a CALEA profile.
2. If replication role must be assigned through RADIUS VSA, create an access rule and assign the access rule to a WLAN SSID or wired profile.
3. Verify the configuration.

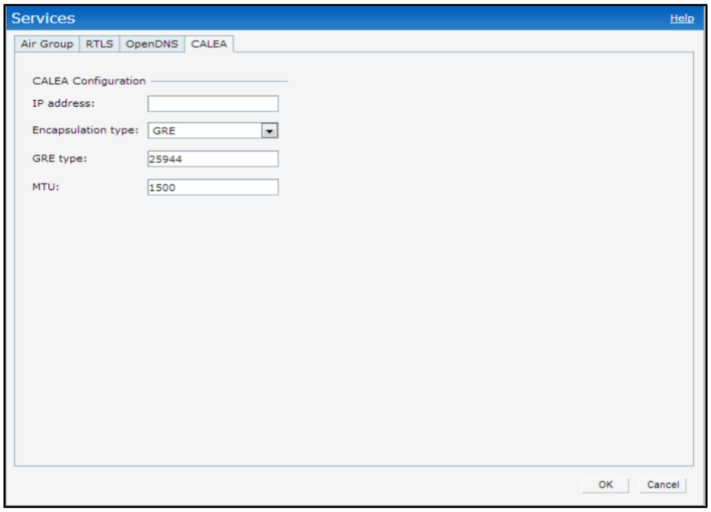
Creating a CALEA Profile

You can create a CALEA profile by using the Instant UI or CLI.

In the Instant UI

To configure a CALEA profile:

1. Click **More**>**Services** at the top right corner of the Instant main window.
2. Click **CALEA**. The **CALEA** tab details are displayed.



CALEA Configuration

IP address:

Encapsulation type: GRE

GRE type: 25944

MTU: 1500

3. Specify the following parameters:
   - **IP address**– Specify the IP address of the CALEA server.
   - **Encapsulation type**– Specify the encapsulation type. The current release of Instant supports GRE only.
   - is supported.
   - **GRE type**– Specify the GRE type.
   - **MTU**– Specify a size for the maximum transmission unit (MTU) within the range of 68–1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1500.
4. Click **OK**.

In the CLI

```
(Instant Access Point)(config)# calea
(Instant Access Point)(calea)# ip <IP-address>
(Instant Access Point)(calea)# ip mtu <size>
(Instant Access Point)(calea)# encapsulation-type <gre>
(Instant Access Point)(calea)# gre-type <type>
(Instant Access Point)(calea)# end
(Instant Access Point)# commit apply
```

Creating an Access Rule for CALEA

You can create an access rule for CALEA by using the Instant UI or CLI.

In the Instant UI

To create an access rule:

1. To add the CALEA access rule to an existing profile, select an existing wireless (**Networks** tab>**edit**) or wired (**More**>**Wired**>**Edit**) profile. To add the access rule to a new profile, click **New** under Network tab and create a WLAN profile, or click **More**>**Wired**>**New** and create a wired port profile.
2. In the **Access** tab, select the role for which you want create the access rule.
3. Under **Access Rules**, click **New**. The **New Rule** window appears.
4. Select **CALEA**.

5. Click **OK**.
6. Create a role assignment rule if required.
7. Click **Finish**.

In the CLI

To create a CALEA access rule:

```
(Instant Access Point)(config)# wlan access-rule <name>
(Instant Access Point)(Access Rule <name>)# calea
(Instant Access Point)(Access Rule <name>)# end
(Instant Access Point)# commit apply
```

To assign the CALEA rule to a user role:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name># set-role <attribute>{{equals|not-equals|starts-wit
h|ends-with|contains}<operator><role>|value-of}
(Instant Access Point)(SSID Profile <name># end
(Instant Access Point)(SSID Profile <name># commit apply
```

To associate the access rule with a wired profile:

```
(Instant Access Point)(config)# wired-port-profile <name>
(Instant Access Point)(Wired ap profile <name>)# access-rule-name <name>
(Instant Access Point)(Wired ap profile <name>)# end
(Instant Access Point)# commit apply
```

Verifying the configuration

To verify the CALEA configuration:

```
(Instant Access Point)# show calea config
```

To view the tunnel encapsulation statistics:

```
(Instant Access Point)# show calea statistics
```

Example

To enable CALEA integration:

```
(Instant Access Point)(config)# calea
(Instant Access Point)(calea)# ip 192.0.2.7
(Instant Access Point)(calea)# ip mtu 1500
(Instant Access Point)(calea)# encapsulation-type GRE
(Instant Access Point)(calea)# gre-type 255
(Instant Access Point)(calea)# end

(Instant Access Point)(config)# wlan access-rule ProfileCalea
(Instant Access Point)(Access Rule "ProfileCalea")# calea
(Instant Access Point)(Access Rule "ProfileCalea")# end
(Instant Access Point)# commit apply

(Instant Access Point)(config)# wlan ssid-profile Calea-Test
(Instant Access Point)(SSID Profile"Calea-Test")# enable
(Instant Access Point)(SSID Profile"Calea-Test")# index 0
(Instant Access Point)(SSID Profile"Calea-Test")# type employee
(Instant Access Point)(SSID Profile"Calea-Test")# essid QA-Calea-Test
(Instant Access Point)(SSID Profile"Calea-Test")# opmode wpa2-aes
(Instant Access Point)(SSID Profile"Calea-Test")# max-authentication-failures 0
(Instant Access Point)(SSID Profile"Calea-Test")# auth-server server1
(Instant Access Point)(SSID Profile"Calea-Test")# set-role Filter-Id equals 123456 calea-test
(Instant Access Point)(SSID Profile"Calea-Test")# rf-band 5.0
```

```
(Instant Access Point)(SSID Profile"Calea-Test")# captive-portal disable
(Instant Access Point)(SSID Profile"Calea-Test")# dtim-period 1
(Instant Access Point)(SSID Profile"Calea-Test")# inactivity-timeout 1000
(Instant Access Point)(SSID Profile"Calea-Test")# broadcast-filter none
(Instant Access Point)(SSID Profile"Calea-Test")# dmo-channel-utilization-threshold 90
(Instant Access Point)(SSID Profile"Calea-Test")# local-probe-req-thresh 0
(Instant Access Point)(SSID Profile"Calea-Test")# max-clients-threshold 64
(Instant Access Point)(SSID Profile"Calea-Test")# end
(Instant Access Point)(SSID Profile"Calea-Test")# commit apply
```

To verify the configuration:

```
(Instant Access Point)# show calea config


calea-ip :10.0.0.5
encapsulation-type :gre
gre-type :25944
ip mtu : 150

(Instant Access Point)# show calea statistics

Rt resolve fail : 0
Dst resolve fail: 0
Alloc failure   : 0
Fragged packets : 0
Jumbo   packets : 263
Total Tx fail   : 0
Total Tx ok     : 263
```

This chapter describes the following procedures:

- Understanding Hotspot Profiles on page 301
- Configuring Hotspot Profiles on page 302
- Sample Configuration on page 312

NOTE

In the current release, Instant supports the hotspot profile configuration only through the CLI.

Understanding Hotspot Profiles

Hotspot 2.0 is a Wi-Fi Alliance specification based on the 802.11u protocol, which allows wireless clients to discover hotspots using management frames (such as beacon, association request and association response), connect to networks, and roam between networks without additional authentication.

The Hotspot 2.0 provides the following services:

- Network discovery and selection– Allows the clients to discover suitable and available networks by advertising the access network type, roaming consortium, and venue information through the management frames. For network discovery and selection, Generic Advertisement Service (GAS) and Access Network Query Protocol (ANQP) are used.
- QOS Mapping– Provides a mapping between the network-layer QoS packet marking and over- the-air QoS frame marking based on user priority.

When a hotspot is configured in a network:

- The clients search for available hotspots using the beacon management frame.
- When a hotspot is found, client sends queries to obtain information about the type of network authentication and IP address, and IP address availability using the Generic Advertisement Service (GAS) action frames.
- Based on the response of the advertisement Server (response to the GAS Action Frames), the relevant hotspot is selected and the client attempts to associate with it.
- Based on the authentication mode used for mobility clients, the client authenticates to access the network.

Generic Advertisement Service (GAS)

GAS is a request-response protocol, which provides L2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining an 802.11 infrastructure before associating clients and allows clients to send queries to multiple 802.11 networks in parallel.

An AP can include its service provider Organization Identifier (OI) indicating the service provider identity in beacons and probe responses to clients. When a client recognizes an IAP's OI, it attempts to associate to that IAP using the security credentials corresponding to that service provider. If the client does not recognize the AP’s OI, the client sends a Generic Advertisement Service (GAS) query to the IAP to request more information about the network before associating. A client transmits a GAS Query using a GAS Initial Request frame and the IAP provides the query response or information on how to receive the query response in a GAS Initial Response frame. To transmit a GAS query for any advertisement protocol, the advertisement protocol ID must include the advertisement protocol information element with information about the advertisement protocol and its corresponding advertisement control.

Access Network Query Protocol (ANQP)

ANQP provides a range of information, such as IP address type and availability, roaming partners accessible through a hotspot, and the Extensible Authentication Protocol (EAP) method supported for authentication, for a query and response protocol. The ANQP Information Elements (IEs) provide additional data that can be sent from an IAP to the client to identify the IAP's network and service provider. If a client requests this information through a GAS query, the hotspot AP sends the ANQP capability list in the GAS Initial Response frame indicating support for the following IEs:

- Venue Name
- Domain Name
- Network Authentication Type
- Roaming Consortium List
- Network Access Identifier Realm
- 3GPP Cellular Network Data

Hotspot 2.0 Query Protocol (H2QP)

The H2QP profiles provide a range of information on hotspot 2.0 elements such as hotspot protocol and port, operating class, operator names, WAN status, and uplink and downlink metrics.

Information Elements (IEs) and Management Frames

The hotspot 2.0 configuration supports the following IEs:

- Interworking IE–Provides information about the Interworking service capabilities such as the Internet availability in a specific service provider network.
- Advertisement Protocol IE–Provides information about the advertisement protocol that a client can use for communication with the advertisement servers in a network.
- Roaming Consortium IE–Provides information about the service provider network for roaming clients, which can be used to authenticate with the AP.

The IEs are included in the following Management Frames when 802.11u is enabled:

- Beacon Frame
- Probe Request Frame
- Probe response frame
- Association Request
- Re-Association request

NAI Realm List

An NAI Realm profile identifies and describes a NAI realm to which the clients can connect. The NAI realm settings on an IAP as an advertisement profile to determine the NAI realm elements that must be included as part of a GAS Response frame.

Configuring Hotspot Profiles

To configure a hotspot profile, perform the following steps:

1. Create the required ANQP and H2QP advertisement profiles.
2. Create a hotspot profile.

3. Associate the required ANQP and H2QP advertisement profiles created in step 1 to the hotspot profile created in step 2.
4. Create a SSID Profile with enterprise security and WPA2 encryption settings and associate the SSID with the hotspot profile created in step 2.

Creating Advertisement Profiles for Hotspot Configuration

A hotspot profile contains one or several advertisement profiles. The following advertisement profiles can be configured through the Instant CLI:

- ANQP advertisement profiles
  - NAI Realm profile
  - Venue Name Profile
  - Network Authentication Profile
  - Roaming Consortium Profile
  - 3GPP Profile
  - IP Address availability Profile
  - Domain Name Profile
- H2QP advertisement profiles
  - Operator Friendly Name Profile
  - Connection Capability Profile
  - Operating Class Profile
  - WAN-Metrics Profile

Configuring an NAI Realm Profile

You configure an Network Access Identifier (NAI) Realm profile to define the NAI realm information, which can be sent as an ANQP IE in a GAS query response.

To configure a NAI profile, enter the following commands at the command prompt:

```
(Instant Access Point)(config)# hotspot anqp-nai-realm-profile <name>
(Instant Access Point)(nai-realm <name>)# nai-realm-name <name>
(Instant Access Point)(nai-realm <name>)# nai-realm-encoding {<utf8>|<rfc4282>}
(Instant Access Point)(nai-realm <name>)# nai-realm-eap-method <eap-method>
(Instant Access Point)(nai-realm <name>)# nai-realm-auth-id-1 <authentication-ID>
(Instant Access Point)(nai-realm <name>)# nai-realm-auth-id-2 <authentication-ID>
(Instant Access Point)(nai-realm <name>)# nai-realm-auth-value-1 <authentication-value>
(Instant Access Point)(nai-realm <name>)# nai-realm-auth-value-2 <authentication-value>
(Instant Access Point)(nai-realm <name>)# nai-home-realm
(Instant Access Point)(nai-realm <name>)# enable
(Instant Access Point)(nai-realm <name>)# end
(Instant Access Point)# commit apply
```

You can specify any of the following EAP methods for the **nai-realm-eap-method <eap-method>** command:

- **identity**– To use EAP Identity type. The associated numeric value is 1.
- **notification**–To allow the hotspot realm to use EAP Notification messages for authentication. The associated numeric value is 2.
- **one-time-password**–To use Authentication with a single-use password. The associated numeric value is 5.
- **generic-token-card**–To use EAP Generic Token Card (EAP-GTC). The associated numeric value is 6.
- **eap-tls**–To use EAP-Transport Layer Security. The associated numeric value is 13.
- **eap-sim**–To use EAP for GSM Subscriber Identity Modules. The associated numeric value is 18.

- **eap-ttls**–To use EAP-Tunneled Transport Layer Security. The associated numeric value is 21.
- **peap**–To use protected Extensible Authentication Protocol. The associated numeric value is 25.
- **crypto-card**– To use crypto card authentication. The associated numeric value is 28.
- **peapmschapv2**– To use PEAP with Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPV2). The associated numeric value is 29.
- **eap-aka**–To use EAP for UMTS Authentication and Key Agreement. The associated numeric value is 50.

The following table lists the possible authentication IDs and their respective values:

Table 55: *NAI Realm Profile Configuration Parameters*

Authentication ID	Authentication Value
reserved • Uses the reserved authentication method. • The associated numeric value is **0**.	–
expanded-eap • Uses the expanded EAP authentication method. • The associated numeric value is **1**.	Use expanded-eap as the authentication value.
non-eap-inner-auth • Uses non-EAP inner authentication type. • The associated numeric value is **2**.	The following authentication values apply: • **reserved**– The associated numeric value is **0**. • **pap**–The associated numeric value is **1**. • **chap**–The associated numeric value is **2**. • **mschap**–The associated numeric value is **3**. • **mschapv2**–The associated numeric value is **4**.
eap-inner-auth • Uses EAP inner authentication type. • The associated numeric value is **3**.	The following authentication values apply: • **reserved**– The associated numeric value is **0**. • **pap**–The associated numeric value is **1**. • **chap**–The associated numeric value is **2**. • **mschap**–The associated numeric value is **3**. • **mschapv2**–The associated numeric value is **4**.
exp-inner-eap • Uses the expanded inner EAP authentication method. • The associated numeric value is **4**.	Use the exp-inner-eap authentication value.
credential • Uses credential authentication. • The associated numeric value is **5**.	The following authentication values apply: • **sim**– The associated numeric value is **1**. • **usim**– The associated numeric value is **2**. • **nfc-secure**– The associated numeric value is **3**. • **hw-token**– The associated numeric value is **4**. • **softoken**– The associated numeric value is **5**. • **certificate**– The associated numeric value is **6**. • **uname-passward**–The associated numeric value is **7**. • **none**–The associated numeric value is **8**. • **reserved**–The associated numeric value is **9**. • **vendor-specific**–The associated numeric value is **10**.

Configuring a Venue Name Profile

You configure venue name profile to send venue information as an ANQP IE in a GAS query response. To configure a venue name profile, enter the following commands at the command prompt:

```
(Instant Access Point)(config)# hotspot anqp-venue-name-profile <name>
(Instant Access Point)(venue-name <name>)# venue-name <name>
(Instant Access Point)(venue-name <name>)# venue-group <group-name>
(Instant Access Point)(venue-name <name>)# venue-type <type>
(Instant Access Point)(venue-name <name>)# venue-lang-code <language>
(Instant Access Point)(venue-name <name>)# enable
(Instant Access Point)(venue-name <name>)# end
(Instant Access Point)# commit apply
```

You can specify any of the following venue groups and the corresponding venue types:

Table 56: *Venue Types*

Venue Group	Associated Venue Type Value
unspecified The associated numeric value is **0**.	
assembly The associated numeric value is **1**.	- unspecified–The associated numeric value is **0**. - arena–The associated numeric value is **1**. - stadium–The associated numeric value is **2**. - passenger-terminal–The associated numeric value is **3**. - amphitheater–The associated numeric value is **4**. - amusement-park–The associated numeric value is **5**. - place-of-worship–The associated numeric value is **6**. - convention-center–The associated numeric value is **7**. - library–The associated numeric value is **8**. - museum–The associated numeric value is **9**. - restaurant–The associated numeric value is **10**. - theater–The associated numeric value is **11**. - bar –The associated numeric value is **12**. - coffee-shop –The associated numeric value is **13**. - zoo-or-aquarium –The associated numeric value is **14**. - emergency-cord-center–The associated numeric value is **15**.
business The associated numeric value is **2**.	- unspecified–The associated numeric value is **0**. - doctor–The associated numeric value is **1** - bank–The associated numeric value is **2** - fire-station–The associated numeric value is **3** - police-station–The associated numeric value is **4** - post-office–The associated numeric value is **6** - professional-office–The associated numeric value is **7** - research-and-dev-facility–The associated numeric value is **8** - attorney-office–The associated numeric value is **9**
educational The associated numeric value is **3**.	- unspecified–The associated numeric value is **0**. - school-primary–The associated numeric value is **1**. - school-secondary–The associated numeric value is **2**. - univ-or-college–The associated numeric value is **3**.
factory-and-industrial The associated numeric value is **4**.	- unspecified–The associated numeric value is **0**. - factory–The associated numeric value is **1**.
institutional	- unspecified–The associated numeric value is **0**. - hospital–The associated numeric value is **1**.

Venue Group	Associated Venue Type Value
The associated numeric value is **5**.	- long-term-care–The associated numeric value is **2**. - alc-drug-rehab–The associated numeric value is **3**. - group-home–The associated numeric value is **4**. - prison-or-jail–The associated numeric value is **5**.
mercantile The associated numeric value is **6**.	- unspecified–The associated numeric value is **0**. - retail-store–The associated numeric value is **1**. - grocery-market–The associated numeric value is **2**. - auto-service-station–The associated numeric value is **3**. - shopping-mall–The associated numeric value is **4**. - gas-station–The associated numeric value is **5**
residential The associated numeric value is **7**.	- unspecified–The associated numeric value is **0**. - private-residence–The associated numeric value is **1**. - hotel–The associated numeric value is **3** - dormitory–The associated numeric value is **4** - boarding-house–The associated numeric value is **5**.
storage The associated numeric value is **8**.	unspecified–The associated numeric value is **0**.
utility-misc The associated numeric value is **9**.	unspecified–The associated numeric value is **0**.
vehicular The associated numeric value is **10**	- unspecified–The associated numeric value is **0**. - automobile-or-truck–The associated numeric value is **1**. - airplane–The associated numeric value is **2**. - bus–The associated numeric value is **3**. - ferry–The associated numeric value is **4**. - ship –The associated numeric value is **5**. - train –The associated numeric value is **6**. - motor-bike–The associated numeric value is **7**.
outdoor The associated numeric value is **11**.	- unspecified–The associated numeric value is **0** - muni-mesh-network–The associated numeric value is **1**. - city-park–The associated numeric value is **2**. - rest-area–The associated numeric value is **3**. - traffic-control–The associated numeric value is **4** - bus-stop–The associated numeric value is **5** - kiosk –The associated numeric value is **6**

Configuring a Network Authentication Profile

You can configure a network authentication profile to define the authentication type used by the hotspot network. To configure a network authentication profile, enter the following commands at the command prompt:

```
(Instant Access Point)(config)# hotspot anqp-nwk-auth-profile <name>
(Instant Access Point)(network-auth <name>)# nwk-auth-type <type>
(Instant Access Point)(network-auth <name>)# url <URL>
(Instant Access Point)(network-auth <name>)# enable
(Instant Access Point)(network-auth <name>)# end
(Instant Access Point)# commit apply
```

You can specify any of the following network authentication type for the **nwk-auth-type <type>** command:

- **accept-term-and-cond**–When configured, the network requires the user to accept terms and conditions. This option requires you to specify a redirection URL string as an IP address, FQDN or URL.
- **online-enrollment**–When configured, the network supports the online enrollment.

- **http-redirect**–When configured, additional information on the network is provided through HTTP/HTTPS redirection.
- **dns-redirect**–When configured, additional information on the network is provided through DNS redirection. This option requires you to specify a redirection URL string as an IP address, FQDN, or URL.

Configuring a Roaming Consortium Profile

You can configure a roaming consortium profile to send the roaming consortium information as an ANQP IE in a GAS query response. To configure a roaming consortium profile, enter the following commands at the command prompt:

```
(Instant Access Point)(config)# hotspot anqp-roam-cons-profile <name>
(Instant Access Point)(roaming-consortium <name>)# roam-cons-oi <roam-cons-oi>
(Instant Access Point)(roaming-consortium <name>)# roam-cons-oi-len <roam-cons-oi-len>
(Instant Access Point)(roaming-consortium <name>)# enable
(Instant Access Point)(roaming-consortium <name>)# end
(Instant Access Point)# commit apply
```

Specify a hexadecimal string of 3 to 5 octets for **roam-cons-oi <roam-cons-oi>**.

Based on the OI specified, you can specify the following parameters for the length of OI in **roam-cons-oi-len <roam-cons-oi-len>**.

- For 0: 0 Octets in the OI (Null)
- For 3: OI length is 24-bit (3 Octets)
- For 5: OI length is 36-bit (5 Octets)

Configuring a 3GPP Profile

You can configure a 3rd Generation Partnership Project (3GPP) profile to define information for the 3G Cellular Network for hotspots.

To configure a 3GPP profile, enter the following commands at the command prompt:

```
(Instant Access Point)(config)# hotspot anqp-3gpp-profile <name>
(Instant Access Point)(3gpp <name>)# 3gpp-plmn1 <plmn-ID>
(Instant Access Point)(3gpp <name>)# enable
(Instant Access Point)(3gpp <name>)# end
(Instant Access Point)# commit apply
```

The Public Land Mobile Network (PLMN) ID is a combination of the mobile country code and network code. You can specify up to 6 PLMN IDs for a 3GPP profile.

Configuring an IP Address Availability Profile

You can configure the available IP address types to send information on IP address availability as an ANQP IE in a GAS query response. To configure an IP address availability profile, enter the following commands at the command prompt:

```
(Instant Access Point)(config)# hotspot anqp-ip-addr-avail-profile <name>
(Instant Access Point)(IP-addr-avail <name>)# ipv4-addr-avail
(Instant Access Point)(IP-addr-avail <name>)# ipv6-addr-avail
(Instant Access Point)(IP-addr-avail <name>)# enable
(Instant Access Point)(IP-addr-avail <name>)# end
(Instant Access Point)# commit apply
```

Configuring a Domain Profile

You can configure a domain profile to send the domain names as an ANQP IE in a GAS query response. To configure a domain name profile, enter the following commands at the command prompt:

```
(Instant Access Point)(config)# hotspot anqp-domain-name-profile <name>
(Instant Access Point)(domain-name <name>)# domain-name <domain-name>
(Instant Access Point)(domain-name <name>)# enable
```

```
(Instant Access Point)(domain-name <name>)# end
(Instant Access Point)# commit apply
```

Configuring an Operator-friendly Profile

You can configure the operator-friendly name profile to define the identify the operator. To configure an H2QP operator-friendly name profile:

```
(Instant Access Point)(config)# hotspot h2qp-oper-name-profile <name>
(Instant Access Point)(operator-friendly-name <name>)# op-fr-name <op-fr-name>
(Instant Access Point)(operator-friendly-name <name>)# op-lang-code <op-lang-code>
(Instant Access Point)(operator-friendly-name <name>)# enable
(Instant Access Point)(operator-friendly-name <name>)# end
(Instant Access Point)# commit apply
```

Configuring a Connection Capability Profile

You can configure a Connection Capability profile to define information such as the hotspot IP protocols and associated port numbers that are available for communication. To configure an H2QP connection capability profile:

```
(Instant Access Point)(config) # hotspot h2qp-conn-cap-profile
(Instant Access Point)(connection-capabilities <name>)# esp-port
(Instant Access Point)(connection-capabilities <name>)# icmp
(Instant Access Point)(connection-capabilities <name>)# tcp-ftp
(Instant Access Point)(connection-capabilities <name>)# tcp-http
(Instant Access Point)(connection-capabilities <name>)# tcp-pptp-vpn
(Instant Access Point)(connection-capabilities <name>)# tcp-ssh
(Instant Access Point)(connection-capabilities <name>)# tcp-tls-vpn
(Instant Access Point)(connection-capabilities <name>)# tcp-voip
(Instant Access Point)(connection-capabilities <name>)# udp-ike2
(Instant Access Point)(connection-capabilities <name>)# udp-ipsec-vpn
(Instant Access Point)(connection-capabilities <name>)# udp-voip
(Instant Access Point)(connection-capabilities <name>)# enable
(Instant Access Point)(connection-capabilities <name>)# end
(Instant Access Point)# commit apply
```

Configuring an Operating Class Profile

You can configure an operating class profile, to list the channels on which the hotspot is capable of operating. To configure an H2QP operating class profile:

```
(Instant Access Point)(config) # hotspot h2qp-oper-class-profile <name>
(Instant Access Point)(operator-class <name>)# op-class <class-ID>
(Instant Access Point)(operator-class <name>)# enable
(Instant Access Point)(operator-class <name>)# end
(Instant Access Point)# commit apply
```

Configuring a WAN Metrics Profile

You can configure a WAN metrics profile to define information about access network characteristics such as link status and metrics. To configure a WAN metrics profile:

```
(Instant Access Point)(config)# hotspot h2qp-wan-metrics-profile <name>
(Instant Access Point)(WAN-metrics <name>)# at-capacity
(Instant Access Point)(WAN-metrics <name>)# downlink-load <load>
(Instant Access Point)(WAN-metrics <name>)# downlink-speed <speed>
(Instant Access Point)(WAN-metrics <name>)# load-duration <duration>
(Instant Access Point)(WAN-metrics <name>)# symm-link
(Instant Access Point)(WAN-metrics <name>)# uplink-load <load>
(Instant Access Point)(WAN-metrics <name>)# uplink-speed <speed>
(Instant Access Point)(WAN-metrics <name>)# wan-metrics-link-status <status>
(Instant Access Point)(WAN-metrics <name>)# end
(Instant Access Point)# commit apply
```

You can specify the following WAN downlink and uplink parameters:

- **Downlink load**– Indicates the percentage of the WAN downlink currently utilized. The default value of 0 indicates that the downlink speed is unknown or unspecified.
- **Downlink speed** –Indicates the WAN downlink speed in Kbps.
- **Uplink load**–Indicates the percentage of the WAN uplink currently utilized. The default value of 0 to indicates that the downlink speed is unknown or unspecified.
- **Uplink speed**–Indicates the WAN uplink speed in Kbps.
- **Load duration**–Indicates the duration in seconds during which the downlink utilization is measured.
- **Symmetric links**–Indicates if the uplink and downlink have the same speed.
- **WAN Link Status**– Indicates if the WAN is down (link-down), up (link-up), or in test state (link-under-test).

Creating a Hotspot Profile

To create a hotspot profile:

```
(Instant Access Point)(config)# hotspot hs-profile <name>
(Instant Access Point)(Hotspot2.0 <name>)# asra
(Instant Access Point)(Hotspot2.0 <name>)# access-network-type <type>
(Instant Access Point)(Hotspot2.0 <name>)# addtl-roam-cons-ois <roam-consortium-OIs>
(Instant Access Point)(Hotspot2.0 <name>)# comeback-mode
(Instant Access Point)(Hotspot2.0 <name>)# gas-comeback <delay-interval>
(Instant Access Point)(Hotspot2.0 <name>)# group-frame-block
(Instant Access Point)(Hotspot2.0 <name>)# hessid <hotspot-essid>
(Instant Access Point)(Hotspot2.0 <name>)# internet
(Instant Access Point)(Hotspot2.0 <name>)# p2p-cross-connect
(Instant Access Point)(Hotspot2.0 <name>)# p2p-dev-mgmt
(Instant Access Point)(Hotspot2.0 <name>)# pame-bi
(Instant Access Point)(Hotspot2.0 <name>)# query-response-length-limit <integer>
(Instant Access Point)(Hotspot2.0 <name>)# roam-cons-len-1 <integer>
(Instant Access Point)(Hotspot2.0 <name>)# roam-cons-len-2 <integer>
(Instant Access Point)(Hotspot2.0 <name>)# roam-cons-len-3 <integer>
(Instant Access Point)(Hotspot2.0 <name>)# roam-cons-oi-1 <integer>
(Instant Access Point)(Hotspot2.0 <name>)# roam-cons-oi-2 <integer>
(Instant Access Point)(Hotspot2.0 <name>)# roam-cons-oi-3 <integer>
(Instant Access Point)(Hotspot2.0 <name>)# venue-group <group>
(Instant Access Point)(Hotspot2.0 <name>)# venue-type <type>
(Instant Access Point)(Hotspot2.0 <name>)# enable
(Instant Access Point)(Hotspot2.0 <name>)# end
(Instant Access Point)#commit apply
```

The hotspot profile configuration parameters are described in the following table:

Table 57: *Hotspot Configuration Parameters*

Parameter	Description
access-network-type <type>	Specify any of the following 802.11u network types. ● **private** – This network is accessible for authorized users only. For example, home networks or enterprise networks that require user authentication. The corresponding integer value for this network type is 0. ● **private-with-guest** – This network is accessible to guest users based on guest authentication methods. For example, enterprise networks that allow guest users with captive portal authentication. The corresponding integer value for this network type is 1. ● **chargeable-public** – This network provides access to the Internet based on payment. For example, a subscription-based Internet access in a coffee shop or a hotel offering chargeable in-room Internet access service. The corresponding integer value for this network type is 2. ● **free-public** –This network is accessible to all without any charges applied. For example, a hotspot in airport or other public places that provide Internet access with no additional cost. The corresponding integer value for this network type is 3.

Table 57: *Hotspot Configuration Parameters*

Parameter	Description
	- **personal-device** – This network is accessible for personal devices. For example, a laptop or camera configured with a printer for the purpose of printing. The corresponding integer value for this network type is 4. - **emergency-services** –This network is limited to accessing emergency services only. The corresponding integer value for this network type is 5. - **test** – This network is used for test purposes only. The corresponding integer value for this network type is 14. - **wildcard** –This network indicates a wildcard network. The corresponding integer value for this network type is 15.
addtl-roam-cons-ois	Specify the number of additional roaming consortium Organization Identifiers (OIs) advertised by the AP. You can specify up to three additional OIs.
asra	Enable the Additional Steps Required for Access (asra) to indicate if additional steps are required for authentication. When enabled, the following information is sent to the client in response to an ANQP query. For ASRA, ensure that the network authentication type is associated.
comeback-mode	Enable this parameter to allow the client to obtain a GAS Request and Response as a Comeback-Request and Comeback-Response. By default, this comeback mode is disabled.
gas-comeback-delay	Specify a GAS come back delay interval in milliseconds to allow the client to retrieve the query response using a comeback request action frame when the GAS response is delayed. You can specify a value within the range of 100-2000 milliseconds and the default value is 500 milliseconds.
group-frame-block	Enable this parameter if you want to stop the AP from sending forward downstream group-addressed frames.
hessid	Specify a Homogenous Extended Service Set Identifier (HESSID) in a hexadecimal format separated by colons.
internet	Specify this parameter to allow the IAP to send an Information Element (IE) indicating that the network allows Internet access.
p2p-cross-connect	Specify this parameter to advertise support for P2P Cross Connections.
p2p-dev-mgmt	Specify this parameter to advertise support for P2P device management.
pame-bi	Specify this parameter to enable Pre-Association Message Exchange BSSID Independent (PAME-BI) bit, with which the IAP can indicate that the Advertisement Server can return a query response independent of the BSSID used in the GAS Frame exchange.
query-response-length-limit	Specify this parameter to set the maximum length of the GAS query response, in octets. You can specify a value within the range of 1-127. The default value is 127.
roam-cons-len-1 roam-cons-len-2 roam-cons-len-3	Specify the length of the organization identifier. The value of the **roam-cons-len-1**, **roam-cons-len-2**, or **roam-cons-len-3**. The roaming consortium OI is based on the following parameters: - **0**: Zero Octets in the OI (Null) - **3**: OI length is 24-bit (3 Octets) - **5**: OI length is 36-bit (5 Octets)
venue-group	Specify one of the following venue groups - assembly - business - educational

Table 57: *Hotspot Configuration Parameters*

Parameter	Description
	- factory-and-industrial - institutional - mercantile - outdoor - residential - storage - utility-and-misc - vehicular By default, the business venue group is used.
venue-type	Specify a venue type to be advertised in the ANQP IEs from IAPs associated with this hotspot profile. For more information about the supported venue types for each venue group, see Table 56.

Associating an Advertisement Profile to a Hotspot Profile

To associate a hotspot profile with an advertisement profile:

```
(Instant Access Point)(config)# hotspot hs-profile <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-protocol <protocol>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile anqp-3gpp <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile anqp-domain-name <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile anqp-ip-addr-avail <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile anqp-nai-realm <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile anqp-nwk-auth <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile anqp-roam-cons <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile anqp-venue-name <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile h2qp-conn-cap <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile h2qp-oper-class <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile h2qp-oper-name <name>
(Instant Access Point)(Hotspot2.0 <name>)# advertisement-profile h2qp-wan-metrics <name>
(Instant Access Point)(Hotspot2.0 <name>)# end
(Instant Access Point)# commit apply
```

The configuration parameters for associating an advertisement profile with a hotspot profile are described in the following table:

Table 58: *Advertisement Association Parameters*

Parameter	Description
advertisement-profile	Specify the advertisement profile to associate with this hotspot profile. For information on advertisement profiles, see Creating Advertisement Profiles for Hotspot Configuration on page 303.
advertisement-protocol	Specify the advertisement protocol types as Access Network Query Protocol (ANQP) as **anqp**.

Creating a WLAN SSID and Associating Hotspot Profile

To create a WLAN SSID with Enterprise Security and WPA2 Encryption Settings:

```
(Instant Access Point)(config)# wlan ssid-profile <name>
(Instant Access Point)(SSID Profile <name># essid <ESSID-name>
(Instant Access Point)(SSID Profile <name># type {<Employee> | <Voice>| <Guest>}
(Instant Access Point)(SSID Profile <name># vlan <vlan-ID>
(Instant Access Point)(SSID Profile <name># set-vlan <attribute>{equals|not-equals| starts-wit
h| ends-with| contains} <operator> <VLAN-ID>| value-of}
(Instant Access Point)(SSID Profile <name># opmode {wpa2-aes|wpa-tkip,wpa2-aes}
(Instant Access Point)(SSID Profile <name># blacklist
(Instant Access Point)(SSID Profile <name># mac-authentication
(Instant Access Point)(SSID Profile <name># l2-auth-failthrough
(Instant Access Point)(SSID Profile <name># termination
(Instant Access Point)(SSID Profile <name># external-server
(Instant Access Point)(SSID Profile <name># auth-server <server-name>
(Instant Access Point)(SSID Profile <name># server-load-balancing
(Instant Access Point)(SSID Profile <name># radius-accounting
(Instant Access Point)(SSID Profile <name># radius-accounting-mode {user-authentication| user-
association}
(Instant Access Point)(SSID Profile <name># radius-interim-accounting-interval <minutes>
(Instant Access Point)(SSID Profile <name># radius-reauth-interval <minutes>
(Instant Access Point)(SSID Profile <name># set-role-by-ssid
(Instant Access Point)(SSID Profile <name>)# hotspot-profile <name>
(Instant Access Point)(SSID Profile <name># end
(Instant Access Point)# commit apply
```

Sample Configuration

Step 1 - Creating ANQP and H2QP Advertisement Profile

```
(Instant Access Point)# configure terminal
(Instant Access Point)(config)#  hotspot anqp-nai-realm-profile nr1
(Instant Access Point)(nai-realm "nr1")# nai-realm-name name1
(Instant Access Point)(nai-realm "nr1")# nai-realm-encoding utf8
(Instant Access Point)(nai-realm "nr1")# nai-realm-eap-method eap-sim
(Instant Access Point)(nai-realm "nr1")# nai-realm-auth-id-1 non-eap-inner-auth
(Instant Access Point)(nai-realm "nr1")# nai-realm-auth-value-1 mschapv2
(Instant Access Point)(nai-realm "nr1")# nai-home-realm
(Instant Access Point)(nai-realm "nr1")# exit

(Instant Access Point)(config)# hotspot anqp-venue-name-profile vn1
(Instant Access Point)(venue-name "vn1")# venue-group business
(Instant Access Point)(venue-name "vn1")# venue-type business-research-and-development
(Instant Access Point)(venue-name "vn1")# venue-lang-code eng
(Instant Access Point)(venue-name "vn1")# venue-name VenueName
(Instant Access Point)(venue-name "vn1")# exit

(Instant Access Point)(config)# hotspot anqp-nwk-auth-profile na1
(Instant Access Point)(network-auth "na1")# nwk-auth-type accept-term-and-cond
(Instant Access Point)(network-auth "na1")# url www.nwkauth.com
(Instant Access Point)(network-auth "na1")# exit

(Instant Access Point)(config)# hotspot anqp-roam-cons-profile rc1
(Instant Access Point)(roaming-consortium "rc1")# roam-cons-oi-len 3
(Instant Access Point)(roaming-consortium "rc1")# roam-cons-oi 888888
(Instant Access Point)(roaming-consortium "rc1")# exit

(Instant Access Point)(config)# hotspot anqp-3gpp-profile 3g
(Instant Access Point)(3gpp "3g")# 3gpp-plmn1 40486
(Instant Access Point)(3gpp "3g")# exit

(Instant Access Point)(config)# hotspot anqp-ip-addr-avail-profile ip1
(Instant Access Point)((IP-addr-avail "ip1")# no ipv4-addr-avail
(Instant Access Point)((IP-addr-avail "ip1")# ipv6-addr-avail
(Instant Access Point)((IP-addr-avail "ip1")# exit
(Instant Access Point)(config)# hotspot anqp-domain-name-profile dn1
(Instant Access Point)(domain-name "dn1")# domain-name DomainName
(Instant Access Point)(domain-name "dn1")# exit

(Instant Access Point)(config)# hotspot h2qp-oper-name-profile on1
(Instant Access Point)(operator-friendly-name"on1")# op-lang-code eng
(Instant Access Point) operator-friendly-name"on1")# op-fr-name OperatorFriendlyName
(Instant Access Point) (operator-friendly-name"on1")# exit
```

Step 2: Creating a hotspot profile

```
(Instant Access Point)# configure terminal
(Instant Access Point)(config)# hotspot hs-profile hs1
(Instant Access Point)(Hotspot2.0 "hs1")# enable
(Instant Access Point)(Hotspot2.0 "hs1")# comeback-mode
(Instant Access Point)(Hotspot2.0 "hs1")# gas-comeback-delay 10
(Instant Access Point)(Hotspot2.0 "hs1")# no asra
(Instant Access Point)(Hotspot2.0 "hs1")# no internet
(Instant Access Point)(Hotspot2.0 "hs1")# query-response-length-limit 20
(Instant Access Point)(Hotspot2.0 "hs1")# access-network-type chargeable-public
(Instant Access Point)(Hotspot2.0 "hs1")# roam-cons-len-1 3
(Instant Access Point)(Hotspot2.0 "hs1")# roam-cons-oi-1 123456
(Instant Access Point)(Hotspot2.0 "hs1")# roam-cons-len-2 3
(Instant Access Point)(Hotspot2.0 "hs1")# roam-cons-oi-2 223355
(Instant Access Point)(Hotspot2.0 "hs1")# addtl-roam-cons-ois 0
(Instant Access Point)(Hotspot2.0 "hs1")# venue-group business
(Instant Access Point)(Hotspot2.0 "hs1")# venue-type research-and-dev-facility
(Instant Access Point)(Hotspot2.0 "hs1")# pame-bi
(Instant Access Point)(Hotspot2.0 "hs1")# group-frame-block
(Instant Access Point)(Hotspot2.0 "hs1")# p2p-dev-mgmt
(Instant Access Point)(Hotspot2.0 "hs1")# p2p-cross-connect
(Instant Access Point)(Hotspot2.0 "hs1")# end
(Instant Access Point)# commit apply
```

Step 3: Associating advertisement profiles with the hotspot profile

```
(Instant Access Point)# configure terminal
(Instant Access Point)(config)# hotspot hs-profile hs1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile anqp-nai-realm nr1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile anqp-venue-name vn1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile anqp-nwk-auth na1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile anqp-roam-cons rc1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile anqp-3gpp 3g1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile anqp-ip-addr-avail ip1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile anqp-domain-name dn1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile h2qp-oper-name on1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile h2qp-wan-metrics wm1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile h2qp-conn-cap cc1
(Instant Access Point)(Hotspot2.0 "hs1")# advertisement-profile h2qp-oper-class oc1
(Instant Access Point)(Hotspot2.0 "hs1")# exit
```

Step 4: Associate the hotspot profile with WLAN SSID:

```
(Instant Access Point)# configure terminal
(Instant Access Point)# wlan ssid-profile ssidProfile1
(Instant Access Point)(SSID Profile "ssidProfile1")# essid hsProf
(Instant Access Point)(SSID Profile "ssidProfile1")# type employee
(Instant Access Point)(SSID Profile "ssidProfile1")# vlan 200
(Instant Access Point)(SSID Profile "ssidProfile1")# opmode wpa2-aes
(Instant Access Point)(SSID Profile "ssidProfile1")# blacklist
(Instant Access Point)(SSID Profile "ssidProfile1")# mac-authentication
(Instant Access Point)(SSID Profile "ssidProfile1")# l2-auth-failthrough
(Instant Access Point)(SSID Profile "ssidProfile1")# radius-accounting
(Instant Access Point)(SSID Profile "ssidProfile1")# radius-accounting-mode user-association
(Instant Access Point)(SSID Profile "ssidProfile1")# radius-interim-accounting-interval 10
```

```
(Instant Access Point)(SSID Profile "ssidProfile1")# radius-reauth-interval 20
(Instant Access Point)(SSID Profile "ssidProfile1")# max-authentication-failures 2
(Instant Access Point)(SSID Profile "ssidProfile1")# set-role-by-ssid
(Instant Access Point)(SSID Profile "ssidProfile1")# hotspot-profile hs1
(Instant Access Point)(SSID Profile "ssidProfile1")# end
(Instant Access Point)# commit apply
```

Instant has the added ability to identify and prioritize voice and video traffic from applications such as Microsoft Office Communications Server (OCS) and Apple Facetime.

QoS for Microsoft Office OCS and Apple Facetime

Voice and video devices use a signaling protocol to establish, control, and terminate voice and video calls. These control or signaling sessions are usually permitted using pre-defined ACLs. If the control signaling packets are encrypted, the IAP cannot determine the dynamic ports are used for voice or video traffic. In these cases, the IAP has to use an ACL with the classify-media option enabled to identify the voice or video flow based on a deep packet inspection and analysis of the actual traffic.

Microsoft OCS

Microsoft Office Communications Server (OCS) uses Session Initiation Protocol (SIP) over TLS to establish, control, and terminate voice and video calls.

Apple Facetime

When an Apple device starts a Facetime video call, it initiates a TCP session to the Apple Facetime server over port 5223, then sends SIP signaling messages over a non-default port. When media traffic starts flowing, audio and video data are sent through that same port using RTP. (The audio and video packets are interleaved in the air, though individual the sessions can be uniquely identified using their payload type and sequence numbers.) The RTP header and payload also get encapsulated under the TURN ChannelData Messages. The Facetime call is terminated with a SIP BYE message that can be sent by either party.

The following table lists the ports used by Apple Facetime. Facetime users need to be assigned a role where traffic is allowed on these ports.

Table 59: *Ports Used by the Apple Facetime Application*

Port	Packet Type
53	TCP/UDP
443	TCP
3478-3497	UDP
5223	TCP
16384-16387	UDP
16393-16402	UDP

This chapter provides the following information:

Dynamic CPU Management

IAPs perform various functions such as wireless client connectivity and traffic flows, wired client connectivity and traffic flows, wireless security, network management, and location tracking. Like with any network element, an IAP can be subject to heavy loads. In such a scenario, it is important to prioritize the platform resources across different functions. Typically, the IAPs manage resources automatically in real-time. However, under special circumstances, if dynamic resource management needs to be enforced or disabled altogether, the dynamic CPU management feature settings can be modified.

Configuring for Dynamic CPU Management

You can configure the dynamic CPU management feature by using the Instant UI or CLI.

In the Instant UI

To enable or disable the management plane protection:

1. Click **System**> **Show Advanced Options**.
2. Select any of the following options from the **Dynamic CPU Management** drop-down.
   - **Automatic** – When selected, the CPU management is enabled or disabled automatically during run-time. This decision is based on real-time load calculations taking into account all different functions that the CPU needs to perform. This is the default and recommended option.
   - **Always disabled on all APs** – When selected, this setting manually disables CPU management on all APs, typically for small networks. This setting protects user experience.
   - **Always enabled on APs** – When selected, the client and network management functions are protected. This setting helps in large networks with high client density.
3. Click **OK**.

In the CLI

```
(Instant Access Point)(config)# dynamic-cpu-mgmt {auto| enable| disable}
```

Example

To enable the dynamic CPU management feature:

```
(Instant Access Point)(config)# dynamic-cpu-mgmt enable
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Chapter 30
Link Aggregation Control Protocol for IAP-220 Series

IAP-220 Series supports the IEEE 802.11ac standard for high-performance WLAN. To support maximum traffic, port aggregation is required as it increases throughput and enhances reliability. To support port aggregation, Instant supports Link Aggregation Control Protocol (LACP) based on the IEEE 802.3ad standard. 802.3ad standard for Ethernet aggregation uses LACP as a method to manage link configuration and balance traffic among aggregated ports.

LACP provides a standardized means for exchanging information with partner systems to form a dynamic link aggregation group. The LACP feature is automatically enabled during IAP boots and it dynamically detects the AP if connected to a partner system with LACP capability, by checking if there is any LACP Protocol Data Unit (PDU) received on either eth0 or eth1 port.

If the switch in the cluster has the LACP capability, you can combine eth0 and eth1 interfaces into the link aggregation group to form a single logical interface (port-channel). Port-channels can be used to provide additional bandwidth or link redundancy between two devices. IAP-220 Series supports link aggregation using either standard port-channel (configuration based) or Link Aggregation Control Protocol (protocol signaling based). IAP-220 Series can optionally be deployed with LACP configuration to benefit from the higher (greater than 1 Gbps) aggregate throughput capabilities of the two radios.

NOTE

LACP feature is supported only on IAP-220 Series.

To enable port-channel on a S3500 Mobility Access Switch:

1. Create a switching profile by running the following commands:

   ```
   interface-profile switching-profile <profile-name>
   switchport-mode {trunk}
   exit
   ```

2. Create a port-channel and associate the switching profile by running the following commands:

   ```
   interface port-channel <0-63>
   port-channel-members [<interface-list> | [add | delete] gigabitethernet <slot/modul
   e/port>]
   shutdown
   switching-profile <profile-name>
   ```

There is no configuration required on the AP for enabling LACP support. However, you can view the status of LACP on IAPs by using the following command:

```
(Instant Access Point)# show lacp status
AP LACP Status
--------------
Link Status  LACP Rate  Num Ports  Actor Key  Partner Key  Partner MAC
-----------  ---------  ---------  ---------  -----------  -----------
Up           slow       2          17         1            70:81:05:11:3e:80
Slave Interface Status
----------------------
Slave I/f Name  Permanent MAC Addr  Link Status  Member of LAG  Link Fail Count
--------------  ------------------  -----------  -------------  ---------------
eth0            6c:f3:7f:c6:76:6e   Up           Yes            0
eth1            6c:f3:7f:c6:76:6f   Up           Yes            0
Traffic Sent on Enet Ports
--------------------------
Radio Num  Enet 0 Tx Count  Enet 1 Tx Count
---------  ---------------  ---------------
```

```
0          0                 0
1          0                 0
non-wifi   2                 17
```

This section provides information on the following procedures:

- Configuring LED Display on page 321
- Backing up and Restoring IAP Configuration Data on page 321
- Converting an IAP to a Remote AP and Campus AP on page 322
- Resetting a Remote AP or Campus AP to an IAP on page 326
- Rebooting the IAP on page 326

Configuring LED Display

NOTE

The LED display is always in the **Enabled** mode during the an IAP reboot.

You can enable or disable LED Display for an IAP using either Instant UI or CLI.

In the Instant UI

To enable or disable LED display for all IAPs in an Instant network, perform the following steps:

1. In the Instant main window, click the **System** link. The **System** window appears.
2. In the **General** tab of **System** window, click **Show advanced options** to display the advanced options.
3. From the **LED Display** drop-down menu, select **Enabled** to enable LED display or **Disabled** to turn off the LED display.
4. Click **OK**.

In the CLI

To enable or disable LED display:

```
(Instant Access Point)(config)# led-off
(Instant Access Point)(config)# no led-off
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Backing up and Restoring IAP Configuration Data

You can back up the IAP configuration data and restore the configuration when required.

Viewing Current Configuration

To view the current configuration on the IAP:

- In the Instant UI, navigate to **Maintenance**>**Configuration**>**Current Configuration**.
- In the CLI, enter the following command at the command prompt:

  ```
  (Instant Access Point)# show running-config
  ```

Backing up Configuration Data

To back up the IAP configuration data:

1. Navigate to the **Maintenance > Configuration>** page.
2. Click **Backup Configuration**.
3. Click **Continue** to confirm the backup. The *instant.cfg* containing the IAP configuration data is saved in your local file system.
4. To view the configuration that is backed up by the IAP, enter the following command at the command prompt:

```
(Instant Access Point)# show backup-config
```

Restoring Configuration

To restore configuration:

1. Navigate to the **Maintenance > Configuration>**page.
2. Click **Restore Configuration**. Click **Browse** to browse your local system and select the configuration file .
3. Click **Restore Now**.
4. Click **Restore Configuration** to confirm restoration. The configuration is restored and the IAP reboots to load the new configuration.

Converting an IAP to a Remote AP and Campus AP

You can provision an IAP as a Campus AP or Remote AP in a controller-based network. Before converting an IAP, ensure that both the IAP and controller are configured to operate in the same regulatory domain.

This section describes the following procedures:

- Converting an IAP to Remote AP on page 322
- Converting an IAP to Campus AP on page 325
- Converting an IAP to Standalone Mode on page 325
- Converting an IAP using CLI on page 326

Converting an IAP to Remote AP

For Remote AP conversion, the Virtual Controller sends the Remote AP convert command to all the other IAPs. The Virtual Controller along with the other slave IAPs set up a VPN tunnel to the remote controller, and download the firmware through FTP. The Virtual Controller uses IPsec to communicate to the Mobility Controller over the Internet.

- If the IAP obtains AirWave information through DHCP (Option 43 and Option 60), it establishes an HTTPS connection to the AirWave server and downloads the configuration and operates in the IAP mode.
- If the IAP does not get AirWave information through DHCP provisioning, it tries provisioning through a firmware image server in the cloud by sending a serial number MAC address. If an entry for the IAP is present in the firmware image cloud server and is provisioned as an IAP > Remote AP, the firmware image cloud server responds with mobility controller IP address, AP group, and AP type. The IAP then contacts the controller, establishes certificate-based secure communication, and obtains configuration and image from the controller. The IAP reboots and comes up as a Remote AP. The IAP then establishes an IPSEC connection with the controller and begins operating in the Remote AP mode.
- If an IAP entry for the AP is present in the firmware image cloud server, the IAP obtains AirWave server information from the cloud server and downloads configuration from AirWave to operate in the IAP mode.
- If there is no response from the cloud server or AirGroup is received, the IAP comes up in Instant mode.
- For more information on firmware image cloud server, see Upgrading an IAP on page 72.

NOTE

A mesh point cannot be converted to Remote AP, because mesh access points do not support VPN connection.

An IAP can be converted to a Campus AP and Remote AP only if the controller is running ArubaOS 6.1.4 or later.

The following table describes the supported IAP platforms and minimal ArubaOS version required for the Campus AP or Remote AP conversion.

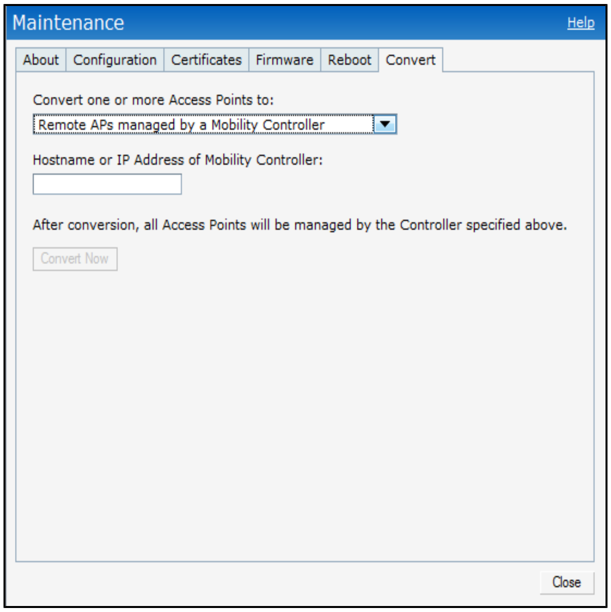
Table 60: *IAP Platforms and Minimal ArubaOS Versions for IAP to Remote AP Conversion*

IAP Platform	ArubaOS Version	Instant Version
IAP-92	6.1.4 or later	1.0 or later
IAP-93	6.1.4 or later	1.0 or later
IAP-104	6.1.4 or later	3.0 or later
IAP-105	6.1.4 or later	1.0 or later
IAP-134	6.1.4 or later	2.0 or later
IAP-135	6.1.4 or later	2.0 or later
IAP-175AC	6.1.4 or later	3.0 or later
IAP-175P	6.1.4 or later	3.0 or later
RAP-3WN	6.1.4 or later	3.0 or later
RAP-3WNP	6.1.4 or later	3.0 or later
RAP-108	6.2.0.0 or later	3.2 or later
RAP-109	6.2.0.0 or later	3.2 or later
RAP-155	6.2.1.0 or later	3.3 or later
RAP-155P	6.2.1.0 or later	3.3 or later

To convert an IAP to RAP, perform the following steps:

1. Click the **Maintenance** link in the Instant main window.
2. Click the **Convert** tab. The **Convert** tab is displayed.

Figure 108 *- Maintenance — Convert Tab*

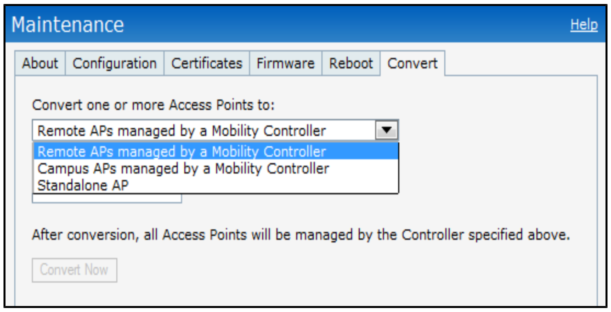


Convert one or more Access Points to:
Remote APs managed by a Mobility Controller

Hostname or IP Address of Mobility Controller:

After conversion, all Access Points will be managed by the Controller specified above.

Figure 109 *- Convert options*



Convert one or more Access Points to:
Remote APs managed by a Mobility Controller
Remote APs managed by a Mobility Controller
Campus APs managed by a Mobility Controller
Standalone AP

After conversion, all Access Points will be managed by the Controller specified above.

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

NOTE

Ensure that the mobility controller IP Address is reachable by the an IAPs.

5. Click **Convert Now** to complete the conversion. The IAP reboots and begins operating in the Remote AP mode.
6. After conversion, the IAP is managed by the mobility controller.

NOTE

For IAPs to function as Remote APs, configure the IAP in the Remote AP white-list and enable the FTP service on the controller.

NOTE

If the VPN setup fails and an error message is displayed, click **OK**, copy the error logs, and share them with your local administrator.

Converting an IAP using CLI

To an convert an IAP:

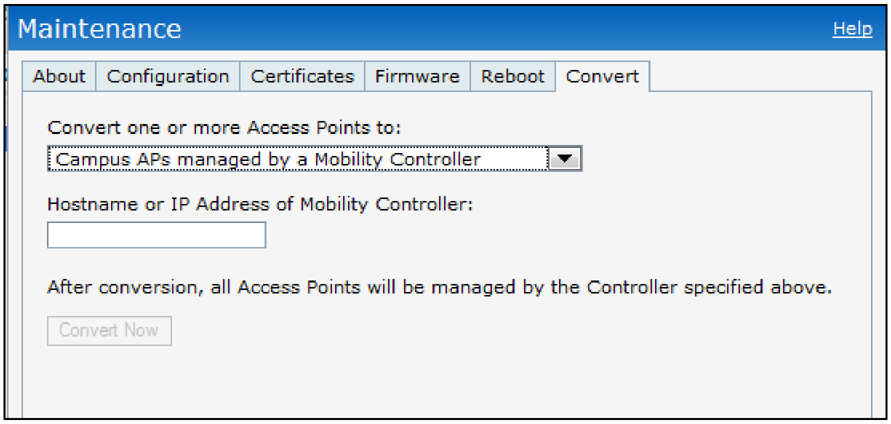
```
Instant Access Point# convert-aos-ap <mode> <controller-IP-address>
```

Converting an IAP to Campus AP

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

1. Click the **Maintenance** link in the Instant main window.
2. Click the **Convert** tab. The **Convert** tab is displayed.

Figure 110 - *Converting an IAP to Campus AP*



Convert one or more Access Points to: Campus APs managed by a Mobility Controller

Hostname or IP Address of Mobility Controller:

After conversion, all Access Points will be managed by the Controller specified above.

3. Select **Campus APs managed by a Mobility Controller** from the drop-down list.
4. Enter the hostname, Fully Qualified Domain Name (FQDN), or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. Contact your local administrator to obtain these details.
5. Ensure that the IAPs access the mobility controller IP Address.
6. Click **Convert Now** to complete the conversion.

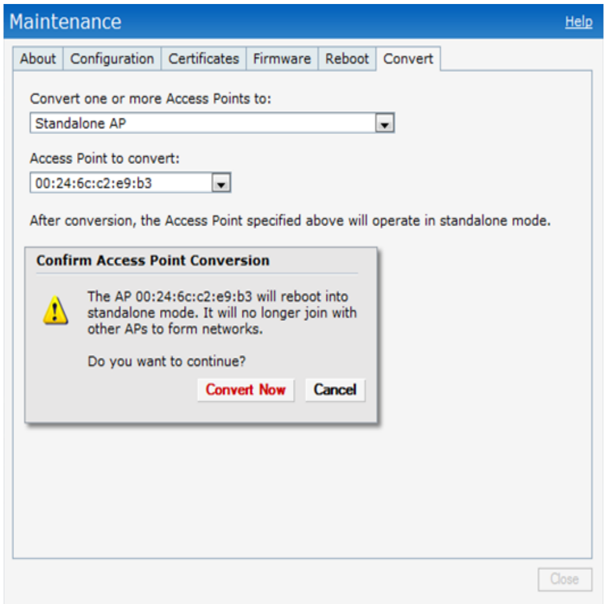
Converting an IAP to Standalone Mode

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

To convert an IAP to a standalone AP:

1. Click the **Maintenance** link in the Instant main window.
2. Click the **Convert** tab. The **Convert** tab is displayed.

Figure 111 - *Standalone AP Conversion*



Convert one or more Access Points to: Standalone AP

Access Point to convert: 00:24:6c:c2:e9:b3

After conversion, the Access Point specified above will operate in standalone mode.

Confirm Access Point Conversion

The AP 00:24:6c:c2:e9:b3 will reboot into standalone mode. It will no longer join with other APs to form networks.

Do you want to continue?

3. Select **Standalone AP** from the drop-down list.
4. Select the Access Point from the drop-down list.
5. Click **Convert Now** to complete the conversion. The an IAP now operates in the standalone mode.

Converting an IAP using CLI

To convert an IAP

```
(Instant Access Point)# convert-aos-ap <mode> <controller-IP-address>
```

Resetting a Remote AP or Campus AP to an IAP

The reset button located on the rear of an IAP can be used to reset the IAP to factory default settings.

To reset an IAP, perform the following steps:

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

NOTE

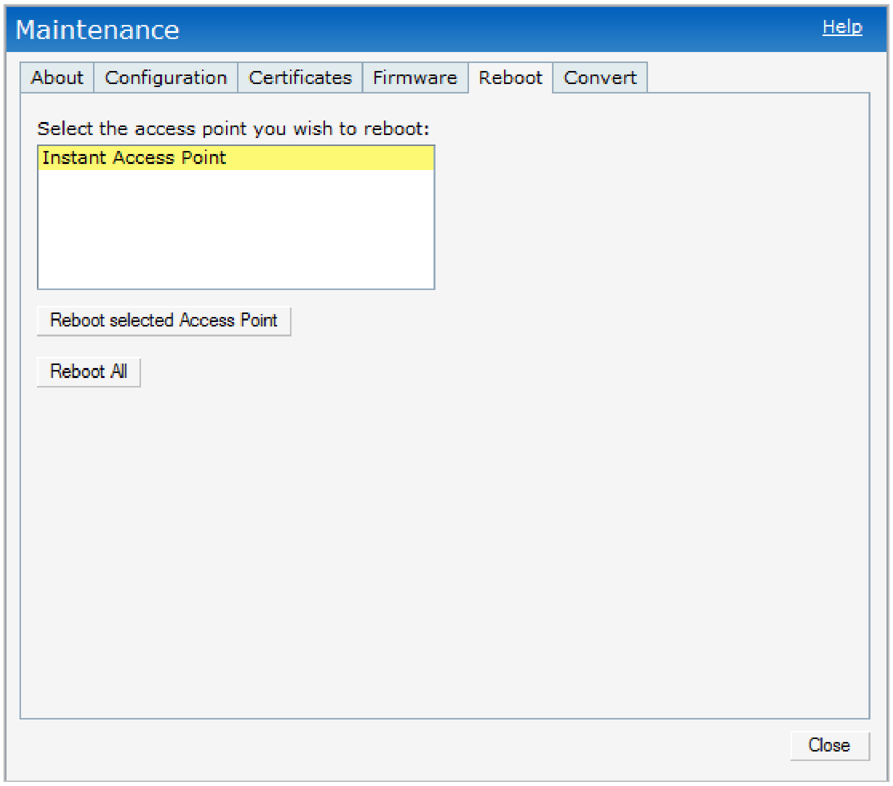
All APs have a reset button, except IAP-175P/175AC. Contact Aruba support for resetting these IAPs.

Rebooting the IAP

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

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

Figure 112 *- Rebooting the IAP*



Select the access point you wish to reboot:

Instant Access Point

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 AP** message is displayed. Click **Reboot Now** to proceed. The **Reboot in Progress** message appears indicating that the reboot is in progress. The **Reboot Successful** message is displayed after the process is complete. If the system fails to boot, the **Unable to contact Access Points after reboot was initiated message** is displayed.
5. Click **OK**.

This chapter provides the following information:

Configuring SNMP

This section provides the following information:

SNMP Parameters for IAP

Instant supports SNMPv1, SNMPv2c, and SNMPv3 for reporting purposes only. An IAP cannot use SNMP to set values in an Aruba system.

You can configure the following parameters for an IAP:

Table 61: *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 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.

Configuring SNMP

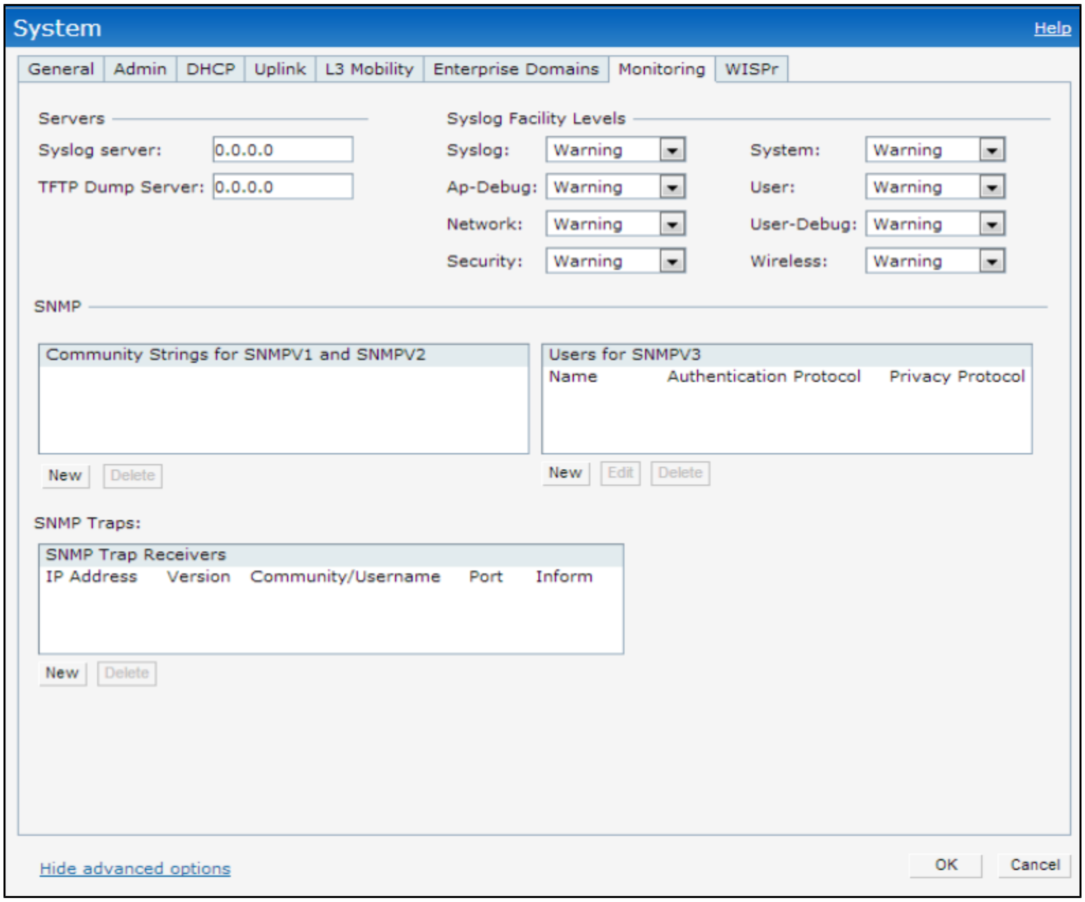
This section describes the procedure for configuring SNMPv1, SNMPv2, and SNMPv3 community strings using Instant UI or CLI.

Creating community strings for SNMPv1 and SNMPv2 Using Instant UI

To create community strings for SNMPv1 and SNMPv2:

1. Click **System** link at the top right corner of the Instant main window. The system window is displayed.
2. Click the **Monitoring** tab. The following figure shows the SNMP configuration parameters displayed in the **Monitoring** tab.

Figure 113 *Monitoring Tab: SNMP Configuration Parameters*



Syslog server: 0.0.0.0

TFTP Dump Server: 0.0.0.0

Syslog: Warning

Ap-Debug: Warning

Network: Warning

Security: Warning

System: Warning

User: Warning

User-Debug: Warning

Wireless: Warning

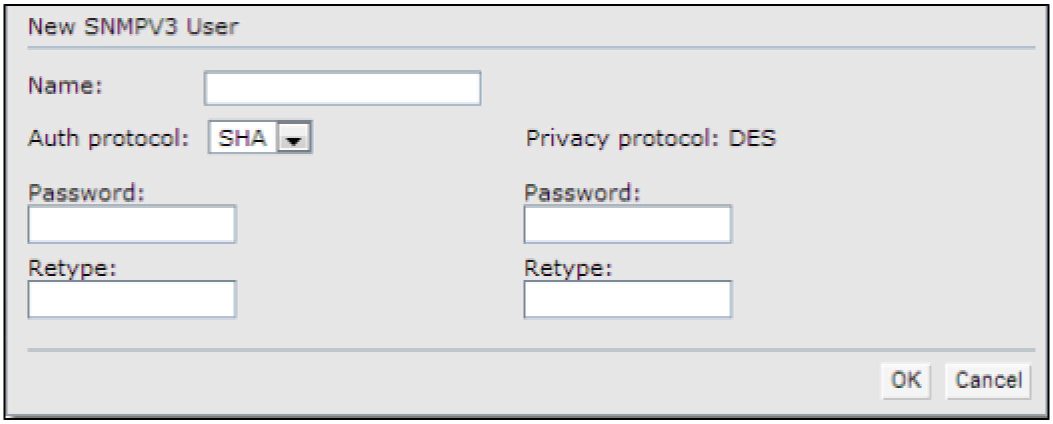
3. Click **New** in the Community Strings for SNMPV1 and SNMPV2 box.
4. Enter the string in the **New Community String** text box.
5. Click **OK**.
6. To delete a community string, select the string, and click **Delete**.

Creating community strings for SNMPv3 Using Instant UI

To create community strings for SNMPv3:

1. Click **System** link at the top right corner of the Instant main window. The system window is displayed.
2. Click the **Monitoring** tab. The SNMP configuration parameters displayed in the **Monitoring** tab.
3. Click **New** in the **Users for SNMPV3** box. A window for specifying SNMPv3 user information is displayed.

Figure 114 *SNMPv3 User*



New SNMPV3 User

Name:

Auth protocol: SHA

Privacy protocol: DES

Password:

Retype:

Password:

Retype:

4. Enter the name of the user in the **Name** text box.
5. Select the type of authentication protocol from the **Auth protocol** drop-down list.
6. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box.
7. Select the type of privacy protocol from the **Privacy protocol** drop-down list.
8. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box.
9. Click **OK**.
10. To edit the details for a particular user, select the user and click **Edit**.
11. To delete a particular user, select the user and click **Delete**.

Configuring SNMP Community Strings in the CLI

To configure an SNMP engine ID and host:

```
(Instant Access Point)(config)# snmp-server engine-id <engine-ID>
(Instant Access Point)(config)# host <ipaddr> version {1 <name> udp-port <port>}|{2c|3 <name>
[inform] [udp-port <port>]}
```

To configure SNMPv1 and SNMPv2 community strings:

```
(Instant Access Point)(config)# snmp-server community <password>
```

To configure SNMPv3 community strings:

```
(Instant Access Point)(config)# snmp-server user <name> <auth-protocol> <password> <privacy-pr
otocol> <password>
```

To view SNMP configuration:

```
(Instant Access Point)# show snmp-configuration

Engine ID:D8C7C8C44298
Community Strings
-----------------
Name
----
SNMPv3 Users
------------
Name  Authentication Type  Encryption Type
----  -------------------  ---------------
SNMP Trap Hosts
---------------
IP Address  Version  Name  Port  Inform
----------  -------  ----  ----  ------
```

Configuring SNMP Traps

Instant supports the configuration of external trap receivers. Only the IAP acting as the Virtual Controller generates traps. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

You can configure SNMP traps using Instant UI or CLI.

In the Instant UI

To configure an SNMP trap receiver:

1. Navigate to **System**>**Show advanced options**> **Monitoring**. The **Monitoring** window is displayed.
1. Under **SNMP Traps**, enter a name in the **SNMP Engine ID** text box. It indicates the name of the SNMP agent on the access point. The 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:
   - **IP Address–** Enter the **IP Address** of the new SNMP Trap receiver.
   - **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.
   - **Community/Username**– Specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps.
   - **Port**– Enter the port to which the traps are sent. The default value is 162.
   - **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.

In the CLI

To configure SNMP traps:

```
(Instant Access Point)(config)# snmp-server host <IP-address> {version 1 | version 2 | version
3} <name> udp-port <port> inform
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

NOTE

The current release of Instant supports SNMP management Information bases (MIBs) along with Aruba-MIBs. For information about Aruba MIBs, SNMP MIBs, and SNMP traps, see the Aruba Instant 6.3.1.1-4.0 *MIB Reference Guide*.

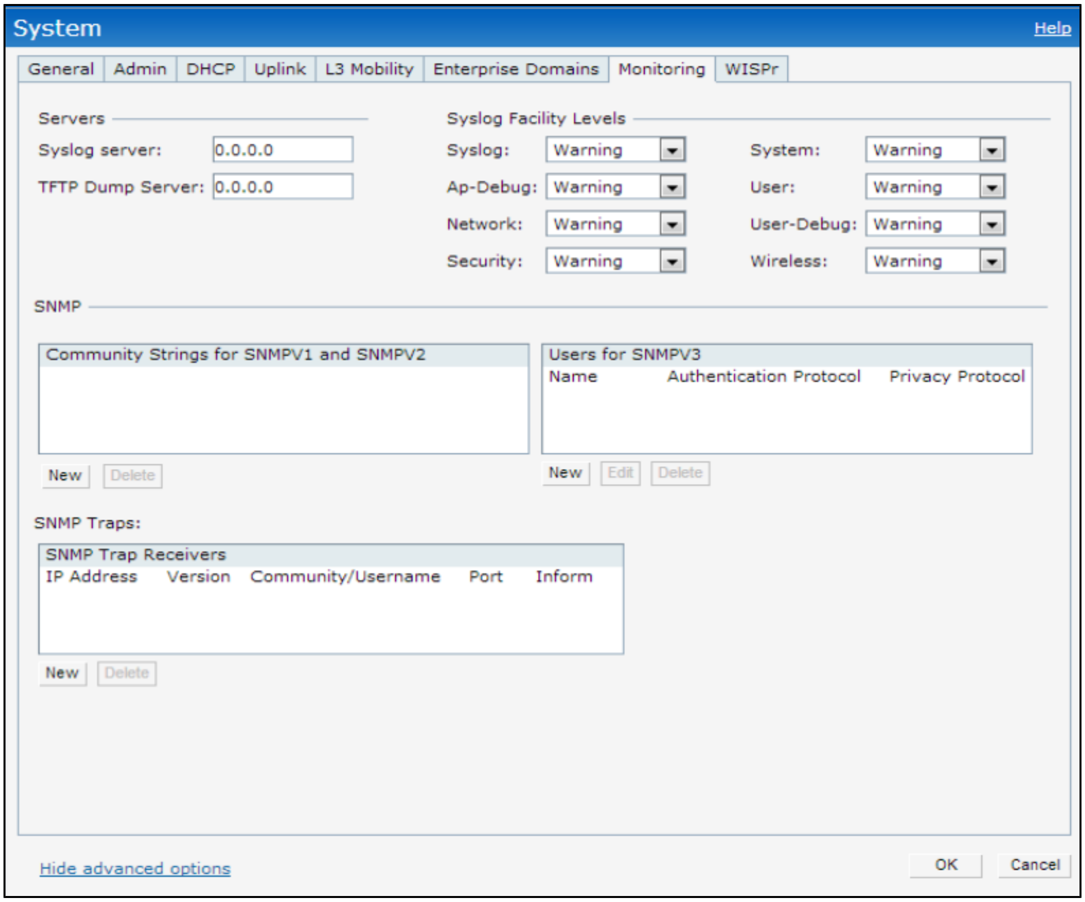
Configuring a Syslog Server

You can specify a syslog server for sending syslog messages to the external servers either by using Instant UI or CLI.

In the Instant UI

1. In the Instant main window, click the **System** link. The **System** window appears.
2. Click **Show advanced options** to display the advanced options.
3. Click the **Monitoring** tab. The **Monitoring** tab details are displayed.

Figure 115 *Syslog Server*



Syslog server: 0.0.0.0

TFTP Dump Server: 0.0.0.0

Syslog:	Warning	System:	Warning
Ap-Debug:	Warning	User:	Warning
Network:	Warning	User-Debug:	Warning
Security:	Warning	Wireless:	Warning

4. In the **Syslog server** text box, enter the IP address of the server to which you want to send system logs.
5. Select the required values to configure syslog facility 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 the 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.

The following table describes the logging levels in order of severity, from the most to the least severe.

Table 62: *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.

Logging Level	Description
Errors	Error conditions.
Warning	Warning messages.
Notice	Significant events of a non-critical and normal nature. The default value for all Syslog facilities.
Informational	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

6. Click **OK**.

In the CLI

To configure a syslog server:

```
(Instant Access Point)(config)# syslog-server <IP-address>
```

To configure syslog facility levels:

```
(Instant Access Point)(config)# syslog-level <logging-level> [ap-debug | network | security |
system | user | user-debug | wireless]
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

To view syslog logging levels:

```
Instant Access Point# show syslog-level

Logging Level
-------------
Facility    Level
--------    -----
ap-debug    warn
network     warn
security    warn
system      warn
user        warn
user-debug  warn
wireless    error
```

Configuring TFTP Dump Server

You can configure a TFTP server for storing core dump files by using the Instant UI or CLI.

In the Instant UI

1. In the Instant main window, click the **System** link. The **System** window appears.
2. Click **Show advanced options** to display the advanced options.
3. Click the **Monitoring** tab. The **Monitoring** tab details are displayed.
4. Enter the IP address of the TFTP server in the **TFTP Dump Server** text box.
5. Click **OK**.

In the CLI

To configure a TFTP server:

```
(Instant Access Point)(config)# tftp-dump-server <IP-address>
```

```
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Running Debug Commands from the Instant UI

To run the debugging commands from the Instant UI:

1. Navigate to **More**>**Support** at the top right corner of the Instant main window. The **Support** window is displayed.
2. Select the required option from the **Command** drop-down list.
3. Select **All Access Points** or **Instant Access Point(VC)** from the **Target** drop-down list.
4. Click **Run**.

Support Commands

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

- **AP 3G/4G Status–**Displays the cellular status of the IAP.
- **AP 802.1X Statistics–** Displays the 802.1X statistics of the IAP.
- **AP Access Rule Table–** Displays the list of ACL rules configured on the IAP.
- **AP Active–** Displays the list of active APs in Instant network.
- **AP Airgroup Cache–** Displays the Bonjour Multicast DNS (mDNS) records for the IAP.
- **AP Airgroup CPPM Entries –**Displays the AirGroup CPPM policies of the registered devices.
- **AP Airgroup CPPM Servers–** Displays the AirGroup CPPM server information.
- **AP Airgroup Debug Statistics–** Displays the debug statistics for the IAP.
- **AP Airgroup Servers–** Displays information about the Bonjour devices which supports AirPrint and AirPlay services for the IAP.
- **AP Airgroup User–** Displays the IP/MAC address, device name, VLAN, type of connection of the Bonjour devices for the IAP.
- **AP Allowed Channels–** Displays information of the allowed channels for the IAP.
- **AP Allowed MAX-EIRP–** Displays information on the maximum EIRP settings that can be configured on an IAP serving in a specific regulatory domain.
- **AP All Supported Timezones–** Displays all the supported time zones of Instant.
- **AP ARM Bandwidth Management–** Displays bandwidth management information for the IAP.
- **AP ARM Channels–** Displays ARM channel details for the IAP.
- **AP ARM Configuration–** Displays ARM configuration details for the IAP.
- **AP ARM History–** Displays the channel history and power changes due to Adaptive Radio Management (ARM) for the IAP.
- **AP ARM Neighbors–** Displays the ARM neighbors of the IAP.
- **AP ARM RF Summary–** Displays the status and statistics for all channels monitored by the IAP.
- **AP ARM Scan Times–** Displays channel scanning information for the IAP.
- **AP ARP Table–** Displays the ARP table of the IAP.
- **AP Association Table–** Displays information about the IAP association.
- **AP Authentication Frames–** Displays the authentication trace buffer information of the IAP.
- **AP BSSID Table–** Displays the Basic Service Set (BSS) table of the IAP.
- **AP Country Codes–** Displays country code details for the IAP.
- **AP CPU Details**–Displays detailed information about memory utilization and CPU load for system processes.
- **AP CPU Utilization–** Displays utilization of CPU for the IAP.

- **AP Crash Info–** Displays crash log information (if it exists) for the IAP. The stored information is cleared from the flash after the AP reboots.
- **AP Current Time–** Displays the current time configured on the IAP.
- **AP Current Timezone–** Displays the current time zone configured on the IAP.
- **AP Datapath ACL Table Allocation–** Displays ACL table allocation details for the IAP.
- **AP Datapath ACL Tables–** Displays the list of ACL rules configured for the SSID and Ethernet port profiles.
- **AP Datapath Bridge Table**– Displays bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for the IAP.
- **AP Datapath DMO Session**– Displays details of a DMO session.
- **AP Datapath Dns Id Map**–Displays the mapping details for the DNS ID.
- **AP Datapath Multicast Table–**Displays multicast table statistics for the IAP.
- **AP Datapath Nat Pool**–Displays NAT pool details configured in the datapath.
- **AP Datapath Route Table–** Displays route table statistics for the IAP.
- **AP Datapath Session Table–** Displays the datapath session table statistics for the IAP.
- **AP Datapath Statistics–** Displays the hardware packet statistics for the IAP.
- **AP Datapath User Table–** Displays datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length for the IAP.
- **AP Datapath VLAN Table–** Displays the VLAN table information such as VLAN memberships inside the datapath including L2 tunnels for the IAP.
- **AP Daylight Saving Time**–Displays the Daylight Saving Time configured on the IAP.
- **AP Driver Configuration–** Displays driver configuration details of the IAP.
- **AP Election** and **AP Election Statistics**–Display the master election statistics.
- **AP ESSID Table–** Displays the SSID profiles configured on the IAP.
- **AP Flash Configuration–** Displays statistics of the IAP configuration stored in flash memory.
- **AP IGMP Group Table**–Displays IGMP group information.
- **AP Interface Counters–** Displays information about the Ethernet interface packet counters for the IAP.
- **AP Interface Status–** Displays the Ethernet port status for the IAP.
- **AP Internal DHCP Status**–Displays details on DHCP allocation.
- **AP IP Interface**–Displays a summary of all IP-related information for Ethernet interfaces configured on the IAP.
- **AP IP Route Table–** Displays information about IP routes for the IAP.
- **AP L3 Mobility Datapath**–Display L3 mobility details.
- **AP L3 Mobility Events Log**–Displays a log with L3 client roaming details.
- **AP L3 Mobility Status**–Displays the status of L3 roaming clients.
- **AP Log All–** Displays all logs for the IAP.
- **AP Log AP-Debug–** Displays logs with debugging information for the IAP.
- **AP Log Conversion**–Displays image conversion details for the IAP.
- **AP Log Driver**–Displays the status of drivers configured on the IAP.
- **AP Log Kernel**–Displays logs for AP's kernel.
- **AP Log Network–** Displays network logs for the IAP.
- **AP Log PPPd**–Displays the Point-to-Point Protocol daemon (PPPd) network connection details.
- **AP Log Rapper**–Displays rapper information.
- **AP Log Sapd**– Displays SAPd logs.

- **AP Log Security–** Displays security logs of the IAP.
- **AP Log System–** Displays system logs of the IAP.
- **AP Log Tunnel Status Management**–Displays tunnel status.
- **AP Log Upgrade**–Displays image download and upgrade details for the IAP.
- **AP Log User-Debug–** Displays user-debug logs of the IAP.
- **AP Log User–** Displays user logs of the IAP.
- **AP Log VPN Tunnel Log–** Displays VPN tunnel status for the IAP.
- **AP Log Wireless–** Displays wireless logs of the IAP.
- **AP Management Frames–** Displays the traced 802.11 management frames for the IAP.
- **AP Memory Allocation State Dumps –** Displays the memory allocation details for the IAP.
- **AP Memory Utilization–** Displays memory utilization of the IAP.
- **AP Mesh Counters–** Displays the mesh counters of the IAP.
- **AP Mesh Link–** Displays the mesh link of the IAP.
- **AP Mesh Neighbors–** Displays the mesh link neighbors of the IAP.
- **AP Monitor Active Laser Beams**–Displays the active laser beam sources for the IAP.
- **AP Monitor AP Table–** Displays the list of APs monitored by the IAP.
- **AP Monitor ARP Cache**–Displays ARP cache details for the IAP.
- **AP Monitor Client Table–** Displays the list of clients monitored by the IAP.
- **AP Monitor Containment Information**– Displays containment details for the IAP.
- **AP Monitor Potential AP Table–** Displays the list of potential APs for the IAP.
- **AP Monitor Potential Client Table–** Displays the list of potential clients for the IAP.
- **AP Monitor Router**–Displays information about the potential wireless devices.
- **AP Monitor Scan Information**–Displays scanned information for the IAP
- **AP Monitor Status–** Displays the configuration and status of monitor information of the IAP.
- **AP Persistent Clients–** Displays the list persistent clients for the IAP.
- **AP PMK Cache**–Displays the PMK cache details for the clients associated with the IAP.
- **AP PPPoE uplink debug**–Displays PPPoE debug logs.
- **AP PPPoE uplink status**– Displays PPPoE uplink status.
- **AP Processes–** Displays the processes running on the IAP.
- **AP Radio 0 Stats–** Displays aggregate debug statistics of the IAP Radio 0.
- **AP Radio 1 Stats–** Displays aggregate debug statistics of the IAP Radio 1.
- **AP Radio 0 Client Match Status** – Displays information about the client match configuration status on IAP Radio 0.
- **AP Radio 1 Client Match Status** –Displays information about the client match configuration status on IAP Radio 1.
- **AP Radio 0 Client Probe Report**–Displays a report on the AP clients connected to IAP Radio 0.
- **AP Radio 1 Client Probe Report** –Displays a report on the AP clients connected to IAP Radio 1.
- **AP Client View** –Displays client details of an IAP.
- **AP Virtual Beacon Report**–Displays a report on virtual beacons for an IAP.
- **AP Client Match Live**– Displays the live details of the client match configuration on an IAP.
- **AP Client Match History**– Displays the historical details of the client match configuration on an IAP.
- **AP RADIUS Statistics–** Displays the RADIUS server statistics for the IAP.
- **AP Shaping Table–** Displays shaping information for clients associated with the IAP.

- **AP Sockets–** Displays information sockets of the IAP.
- **AP STM Configuration–** Displays STM configuration details for each SSID profile configured on the IAP.
- **AP System Status–** Displays detailed system status information for the IAP.
- **AP System Summary–** Displays the IAP configuration.
- **AP Swarm State**–Displays details of the IAP cluster to which the AP is connected.
- **AP Tech Support Dump–** Displays the logs with complete IAP configuration information required for technical support.
- **AP Uplink Status**–Displays uplink status for the IAP.
- **AP derivation-rules**–Displays derivation rules configured on the IAP.
- **AP User Table**–Displays the list of clients for the IAP.
- **AP Valid Channels–** Displays valid channels of the IAP.
- **AP Version–** Displays the version number of the IAP.
- **AP VPN Status**–Displays VPN status for the IAP.
- **AP Environment Variable**– Displays information about the type of antenna used by the IAP.
- **AP Wired Port Settings**– Displays wired port configuration details for the IAP.
- **AP Wired User Table**–Displays the list of clients associated with the wired network profile configured on the IAP.
- **VC 802.1x Certificate–** Displays the CA certificate and server certificate for the Virtual Controller.
- **VC About–** Displays information such as AP type, build time of image, and image version for the Virtual Controller.
- **VC Active Configuration–** Displays the active configuration of Virtual Controller.
- **VC Airgroup Service–** Displays the Bonjour services supported by the Virtual Controller.
- **VC Airgroup Status–** Displays the status of the AirGroup Air and CPPM server details configured on the Virtual Controller.
- **VC Allowed AP Table–** Displays the list of allowed APs.
- **VC AMP Current State Data**–Displays the current status of AirWave Management Platform.
- **VC AMP Current Stats Data**–Displays the current AirWave configuration details.
- **VC AMP Data Sent**–Displays information about the data exchange between AirWave Server and the Virtual Controller.
- **VC AMP Events Pending**–Displays information about the pending events on the AirWave server.
- **VC AMP Last Configuration Received**–Displays the last configuration details received from AirWave.
- **VC AMP Single Sign-on Key**–Displays single sign-on key details for AirWave.
- **VC Application Services–** Displays the details of application services, which includes protocol number, port number.
- **VC Auth-Survivability cache–** Displays the list of 802.1X cached user's information.
- **VC DHCP Option 43 Received**– Displays information about the current activities for the DHCP scope with Option 43.
- **VC Global Alerts–** Displays the list of alerts for all IAPs managed by the Virtual Controller.
- **VC Global Statistics–** Displays the flow information and signal strength of the Virtual Controller.
- **VC IDS AP List–** Displays the list of IAPs monitored by the Virtual Controller.
- **VC IDS Client List–** Displays the list of clients detected by IDS for the Virtual Controller.
- **VC Internal DHCP Server Configuration–** Displays the configuration details of the internal DHCP server.
- **VC Local User Database–** Displays the list of users configured for the IAP.
- **VC L2TPv3 config** –Displays the L2TPv3 configuration status.

- **VC L2TPv3 tunnel status**–Displays the L2TPv3 tunnel status.
- **VC L2TPv3 tunnel configuration**–Displays the L2TPv3 tunnel configuration status.
- **VC L2TPv3 session status**–Displays the L2TPv3 session configuration status.
- **VC L2TPv3 system wide global statistics** – Displays the L2TPv3 system statistics.
- **VC OpenDNS Configuration and Status–** Displays configuration details and status of the OpenDNS server.
- **VC Radius Attributes–** Displays information about the RADIUS attributes.
- **VC Radius Servers–** Displays the list of RADIUS servers configured on the IAP.
- **VC Saved Configuration–** Displays the configuration details of the Virtual Controller.
- **VC Scanning Statistics**–Displays the scanned information for the IAP.
- **VC SNMP Configuration–** Displays the SNMP configuration details of the IAP.
- **VC Uplink 3G/4G Configuration**–Displays the 3G/4G cellular configuration information for the IAPs managed by the Virtual Controller.
- **VC Uplink Management Configuration**–Displays uplink configuration details for the Virtual Controller.
- **VC WISPr Configuration –** Displays the WISPr configuration details.

NOTE

Use the support commands under the supervision of Aruba technical support.

This chapter provides the following information:

- Mobility Access Switch Overview on page 341
- Enabling MAS Integration on IAPs on page 341

Mobility Access Switch Overview

The Aruba Mobility Access Switch (MAS) enables secure, role-based network access for wired users and devices, independent of their location or application. Installed in wiring closets, the MAS delivers up to 384 wire-speed Gigabit Ethernet switch ports and operates as a wired access point when deployed with an Aruba Mobility Controller.

As a wired access point, users and their devices are authenticated and assigned a unique role by the Mobility Controller. These roles are applied irrespective of whether the user is a Wi-Fi client, or is connected to a port on the MAS. The use of MAS allows an enterprise workforce to have consistent and secure access to network resources based on the type of users, client devices, and connection method used.

Instant supports S3500 and S2500 Aruba Mobility Access Switch models.

For more information on MAS, see ArubaOS *7.2 User Guide*.

MAS Integration with an IAP

You can integrate an IAP with a MAS by connecting it directly to the MAS port. The following MAS integration features can be applied while integrating MAS with an IAP

- **Rogue AP containment**–When a rogue AP is detected by an IAP, it sends the MAC Address of the rogue AP to the MAS. The MAS blacklists the MAC address of the rogue AP and turns off the PoE on the port.
- **PoE prioritization**– When an IAP is connected directly into the MAS port, the MAS increases the PoE priority of the port. This is done only if the PoE priority is set by default in the MAS.

NOTE

The PoE Prioritization and Rogue AP Containment features is available for ArubaOS 7.2 release on Aruba Mobility Access Switches.

- **GVRP Integration**–Configuring GARP VLAN Registration Protocol (GVRP) in ArubaOS MAS enables the switch to dynamically register or de-register VLAN information received from a GVRP applicant such as an IAP. GVRP also enables the switch to propagate the registered VLAN information to the neighboring switches in the network.

NOTE

The associated static VLANs in used wired and wireless profiles are propagated to the upstream MAS using GVRP messages.

For information on steps to integrate MAS with an IAP, see Enabling MAS Integration on IAPs on page 341.

Enabling MAS Integration on IAPs

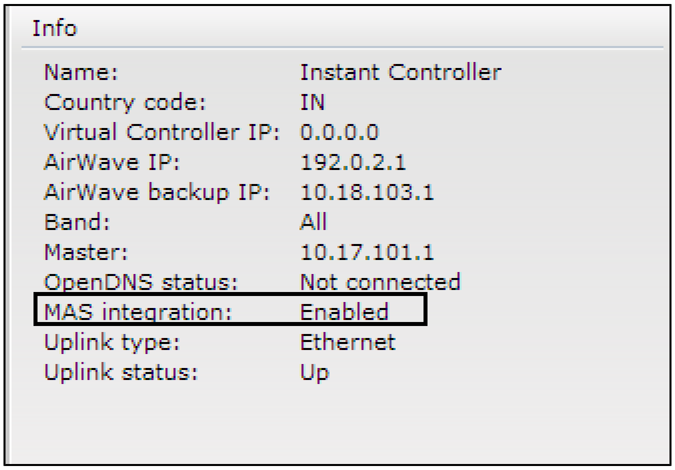
When an IAP is integrated with MAS, the Link Layer Discovery Protocol (LLDP) is enabled. Using this protocol, the IAPs instruct the MAS to turn off the ports where rogue APs are connected, perform actions such as increasing the PoE priority, and configure the VLANs on the ports to which the IAPs are connected.

You can enable MAS integration either using Instant UI or CLI.

In the Instant UI

1. Click **System** at the top right corner of the Instant Main window.
2. Navigate to **General** tab.
3. Select **Enabled** from the **MAS integration** drop-down list. The MAS integration status is displayed in the Info tab of Instant main window as shown in the following figure:

Figure 116 *- MAS Integration Status*



Info

Name:	Instant Controller
Country code:	IN
Virtual Controller IP:	0.0.0.0
AirWave IP:	192.0.2.1
AirWave backup IP:	10.18.103.1
Band:	All
Master:	10.17.101.1
OpenDNS status:	Not connected
MAS integration:	Enabled
Uplink type:	Ethernet
Uplink status:	Up

In the CLI

To enable MAS integration:

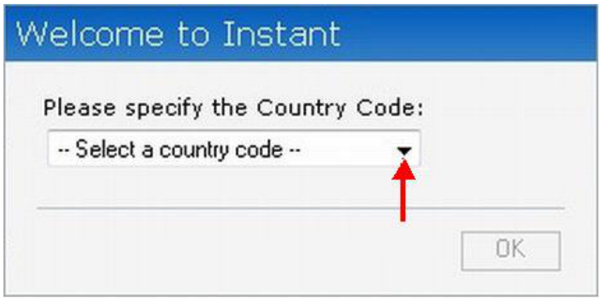
```
(Instant Access Point)(config)# mas-integration
(Instant Access Point)(config# end
(Instant Access Point)# commit apply
```

The IEEE 802.11/b/g/n Wi-Fi networks operate in the 2.4 GHz spectrum and IEEE 802.11a/n operate in the 5.0 GHz spectrum. The spectrum is 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 Instant operates. 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 for most of the IAP models. Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions on operators of wireless networks with devices set to improper country codes. Country Codes List on page 343 shows the list of country codes.

Figure 117 *- Specifying a Country Code*



Welcome to Instant

Please specify the Country Code:

Country Codes List

The following table provides a list of supported country codes:

Table 63: *Country Codes List*

Code	Country Name
AE	United Arab Emirates
AR	Argentina
AT	Austria
AU	Australia
BG	Bulgaria
BH	Bahrain
BM	Bermuda
BO	Bolivia
BR	Brazil

Code	Country Name
CA	Canada
CH	Switzerland
CL	Chile
CN	China
CO	Colombia
CR	Costa Rica
CS	Serbia and Montenegro
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
DO	Dominican Republic
DZ	Algeria
EC	Ecuador
EE	Estonia
EG	Egypt
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
GR	Greece
GT	Guatemala
HK	Hong Kong
HN	Honduras
ID	Indonesia
IE	Ireland
IL	Israel
IN	India

Code	Country Name
IS	Iceland
IT	Italy
JM	Jamaica
JO	Jordan
JP	Japan
KE	Kenya
KR	Republic of Korea (South Korea)
KW	Kuwait
KW	Kuwait
LB	Lebanon
LI	Liechtenstein
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania
LT	Lithuania
LU	Luxembourg
MA	Morocco
MA	Morocco
MU	Mauritius
MX	Mexico
MX	Mexico
NL	Netherlands
NO	Norway
NZ	New Zealand
NZ	New Zealand
OM	Oman
PA	Panama
PA	Panama

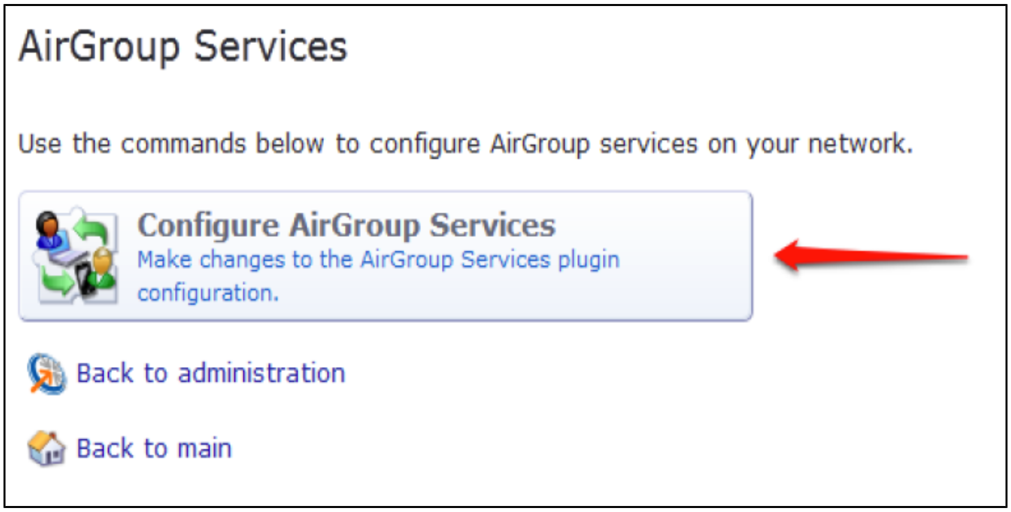
Code	Country Name
PE	Peru
PH	Philippines
PK	Islamic Republic of Pakistan
PL	Poland
PL	Poland
PR	Puerto Rico
PR	Puerto Rico
PT	Portugal
QA	Qatar
RO	Romania
RU	Russia
RU	Russia
SA	Saudi Arabia
SG	Singapore
SI	Slovenia
SI	Slovenia
SK	Slovak Republic
SK	Slovak Republic
SV	El Salvador
TH	Thailand
TH	Thailand
TN	Tunisia
TR	Turkey
TT	Trinidad and Tobago
TW	Taiwan
UA	Ukraine
US	United States
UY	Uruguay

Code	Country Name
UY	Uruguay
VE	Venezuela
VN	Vietnam
ZA	South Africa

To configure ClearPass Guest:

1. On ClearPass Guest, navigate to **Administration > AirGroup Services**.
2. Click **Configure AirGroup Services**.

Figure 118 *Configure AirGroup Services*



AirGroup Services

Use the commands below to configure AirGroup services on your network.

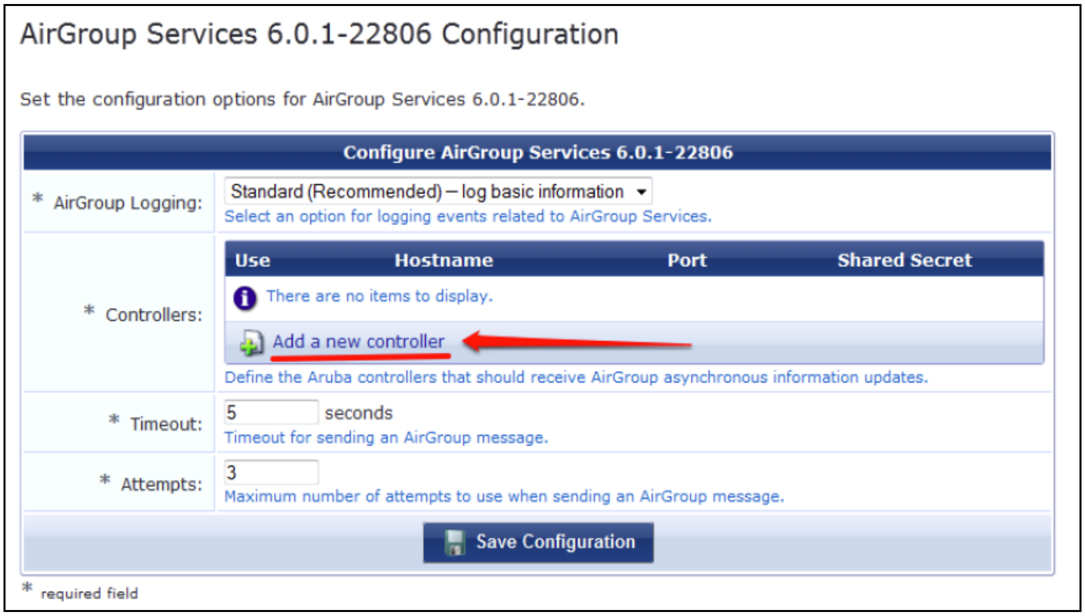
Configure AirGroup Services
Make changes to the AirGroup Services plugin configuration.

Back to administration

Back to main

3. Click **Add a new controller**.

Figure 119 *Add a New Controller for AirGroup Services*



AirGroup Services 6.0.1-22806 Configuration

Set the configuration options for AirGroup Services 6.0.1-22806.

Configure AirGroup Services 6.0.1-22806

* AirGroup Logging: Standard (Recommended) — log basic information
Select an option for logging events related to AirGroup Services.

* Controllers:

Use	Hostname	Port	Shared Secret
There are no items to display.			

Add a new controller
Define the Aruba controllers that should receive AirGroup asynchronous information updates.

* Timeout: 5 seconds
Timeout for sending an AirGroup message.

* Attempts: 3
Maximum number of attempts to use when sending an AirGroup message.

Save Configuration

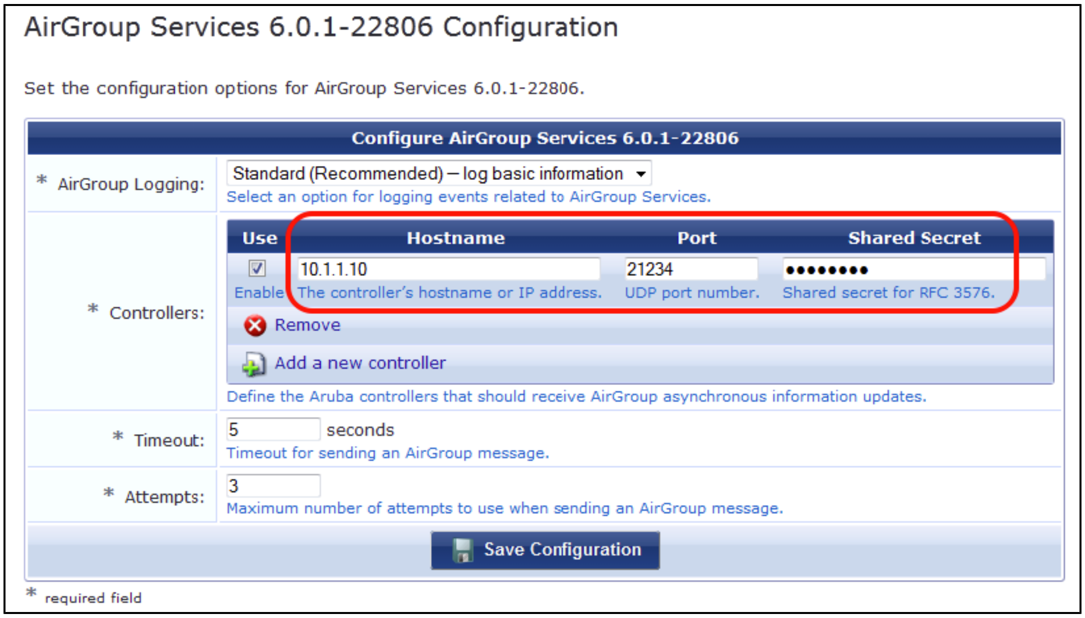
* required field

4. Update the fields with the appropriate information.

NOTE

Ensure that the port configured matches the CoA port (RFC 3576) set on the IAP configuration.

Figure 120 *Configure AirGroup Services Controller Settings*



AirGroup Services 6.0.1-22806 Configuration

Set the configuration options for AirGroup Services 6.0.1-22806.

Configure AirGroup Services 6.0.1-22806

* AirGroup Logging: Standard (Recommended) — log basic information ▾
Select an option for logging events related to AirGroup Services.

* Controllers:

Use	Hostname	Port	Shared Secret
☑ Enable	10.1.1.10 The controller's hostname or IP address.	21234 UDP port number.	●●●●●●●● Shared secret for RFC 3576.

Remove

Add a new controller

Define the Aruba controllers that should receive AirGroup asynchronous information updates.

* Timeout: 5 seconds
Timeout for sending an AirGroup message.

* Attempts: 3
Maximum number of attempts to use when sending an AirGroup message.

Save Configuration

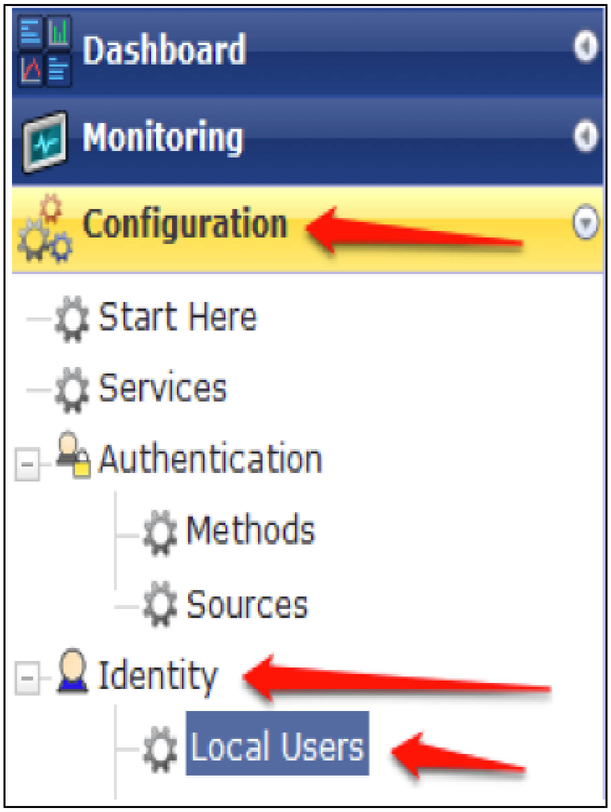
* required field

5. Click **Save Configuration**.

In order to demonstrate AirGroup, either an AirGroup Administrator or an AirGroup Operator account must be created.

1. Navigate to the ClearPass Policy Manager UI, and navigate to **Configuration > Identity > Local Users**.

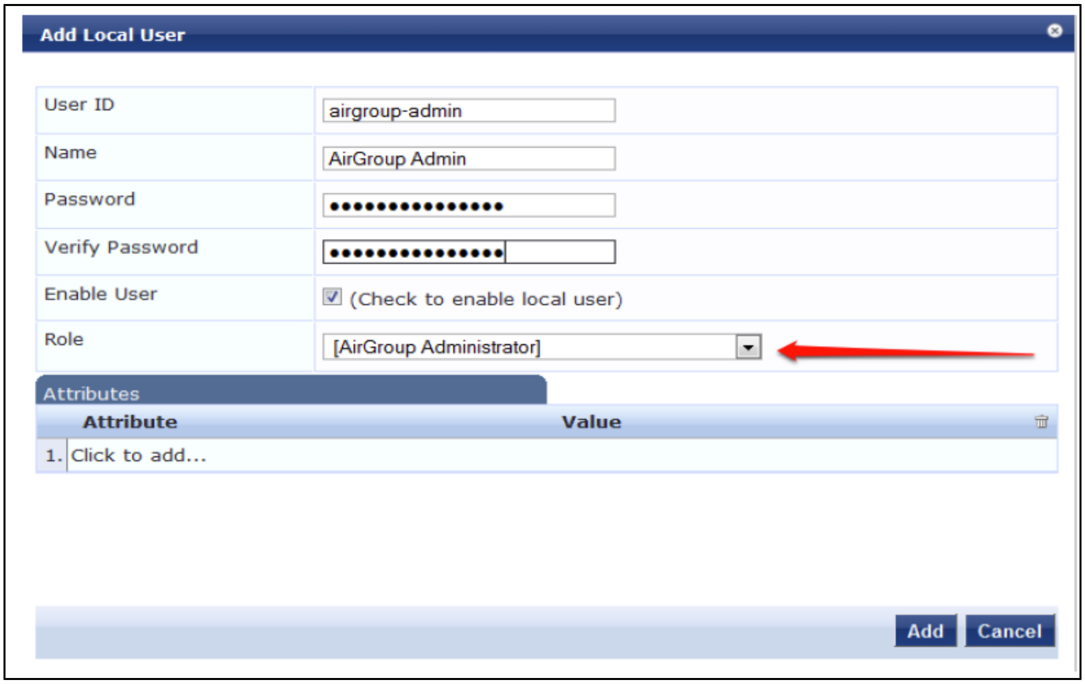
Figure 121 *Configuration > Identity > Local Users Selection*



2. Click **Add User**.

3. Create an **AirGroup Administrator**.

Figure 122 *Create an AirGroup Administrator*



Add Local User

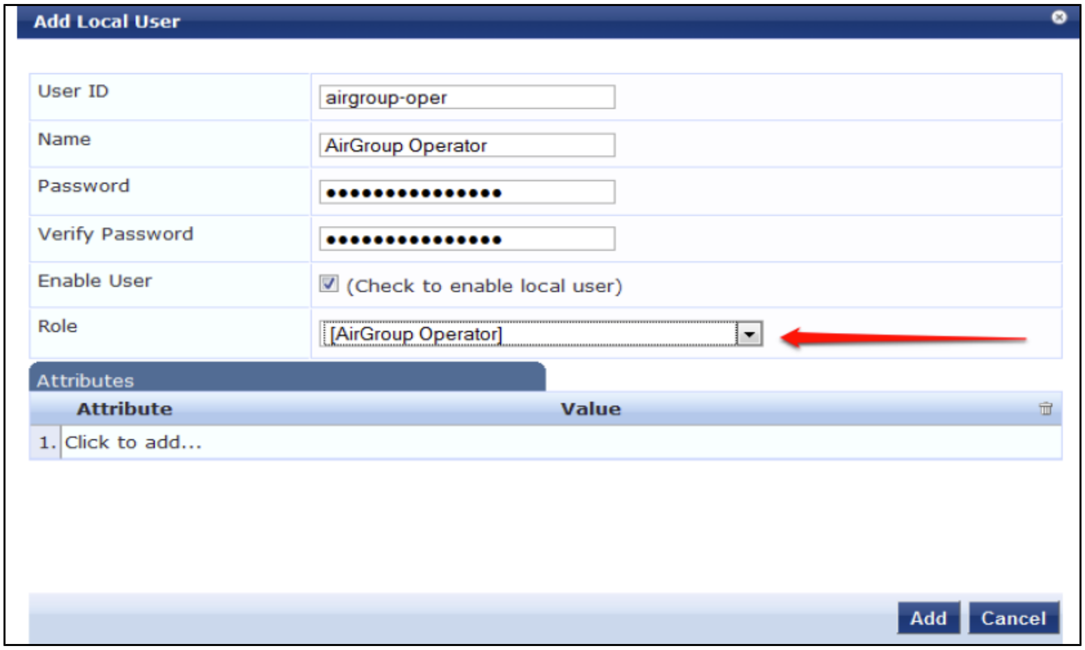
User ID	airgroup-admin
Name	AirGroup Admin
Password	●●●●●●●●●●●●●●●
Verify Password	●●●●●●●●●●●●●●●
Enable User	☑ (Check to enable local user)
Role	[AirGroup Administrator]

Attributes

Attribute	Value
1. Click to add...	

4. In this example, the password used is test123. Click **Add**.
5. Now click **Add User**, and create an **AirGroup Operator**.

Figure 123 *Create an AirGroup Operator*



Add Local User

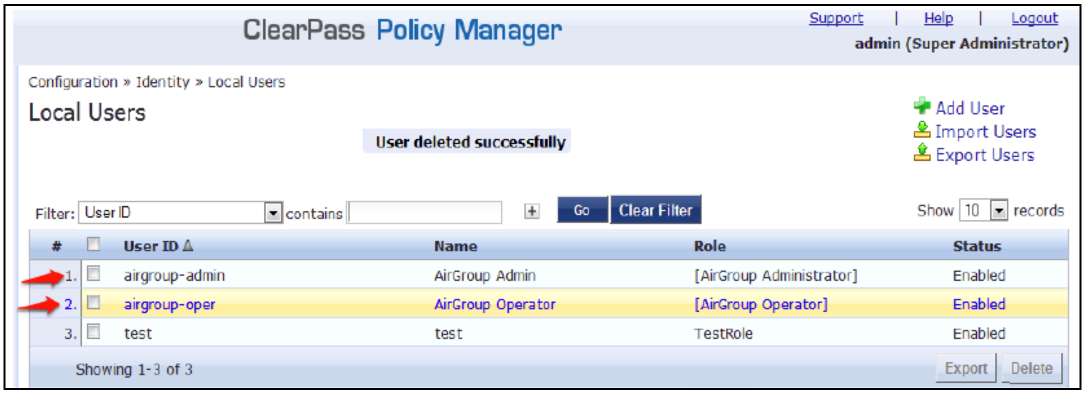
User ID	airgroup-oper
Name	AirGroup Operator
Password	●●●●●●●●●●●●●●●
Verify Password	●●●●●●●●●●●●●●●
Enable User	☑ (Check to enable local user)
Role	[AirGroup Operator]

Attributes

Attribute	Value
1. Click to add...	

6. Click **Add** to save the user with an **AirGroup Operator** role. The **AirGroup Administrator** and **AirGroup Operator IDs** will be displayed in the **Local Users UI** screen.

Figure 124 *Local Users UI Screen*



ClearPass Policy Manager

Support | Help | Logout

admin (Super Administrator)

Configuration » Identity » Local Users

Local Users

User deleted successfully

Add User
Import Users
Export Users

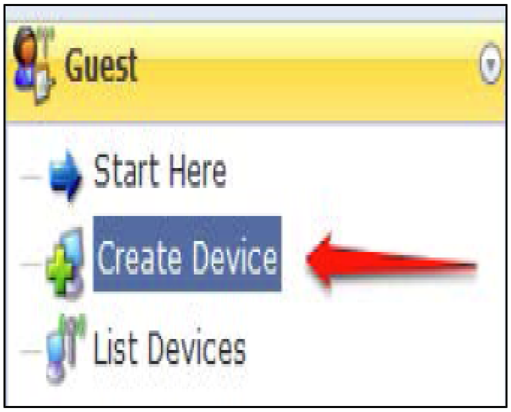
Filter: User ID contains | Go | Clear Filter | Show 10 records

#	□	User ID ▲	Name	Role	Status
1.	□	airgroup-admin	AirGroup Admin	[AirGroup Administrator]	Enabled
2.	□	airgroup-oper	AirGroup Operator	[AirGroup Operator]	Enabled
3.	□	test	test	TestRole	Enabled

Showing 1-3 of 3

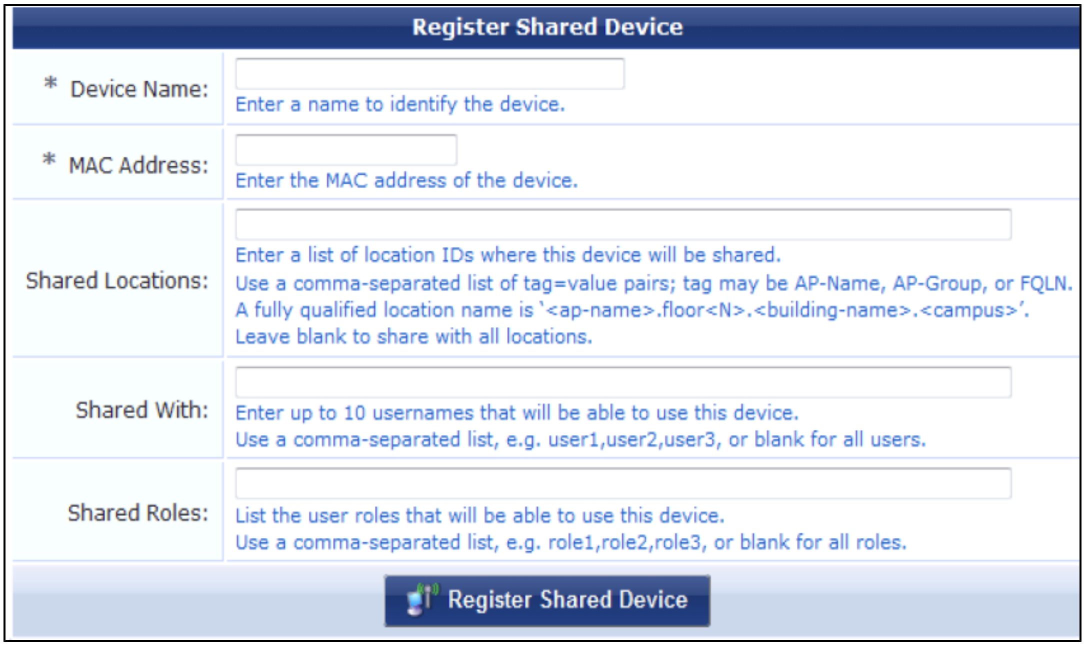
7. Navigate to the ClearPass Guest UI and click **Logout**. The **ClearPass Guest Login** page appears. Use the AirGroup admin credentials to log in.
8. After logging in, click **Create Device**.

Figure 125 *Create a Device*



The following page is displayed.

Figure 126 *- Register Shared Device*



Register Shared Device

* Device Name:	Enter a name to identify the device.
* MAC Address:	Enter the MAC address of the device.
Shared Locations:	Enter a list of location IDs where this device will be shared. Use a comma-separated list of tag=value pairs; tag may be AP-Name, AP-Group, or FQLN. A fully qualified location name is '<ap-name>.floor<N>.<building-name>.<campus>'. Leave blank to share with all locations.
Shared With:	Enter up to 10 usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.
Shared Roles:	List the user roles that will be able to use this device. Use a comma-separated list, e.g. role1,role2,role3, or blank for all roles.

For this test, add your AppleTV device name and MAC address but leave all other fields empty.

9. Click **Register Shared Device**.

Testing

To verify the setup:

1. Disconnect your AppleTV and OSX Mountain Lion/iOS 6 devices if they were previously connected to the wireless network. Remove their entries from the controller's user table using these commands:
   - Find the MAC address– `show user table`
   - Delete the address from the table– `aaa user delete mac 00:aa:22:bb:33:cc`
2. Reconnect both devices. To limit access to the AppleTV, access the ClearPass Guest UI using either the AirGroup admin or the AirGroup operator credentials. Next, navigate to **List Devices > Test Apple TV > Edit**. Add a username that is not used to log in to the Apple devices in the **Shared With field**.
3. Disconnect and remove the OSX Mountain Lion/iOS 6 device from the controller's user table. Reconnect the device by not using the username that you added to the **Shared With field**. The AppleTV should not be available to this device.
4. Disconnect the OSX Mountain Lion/iOS 6 device and delete it from the controller's user table. Reconnect using the username that was added to the **Shared With field**. The OSX Mountain Lion/iOS 6 device should once again have access to the AppleTV.

Troubleshooting

Table 64: *Troubleshooting*

Problem	Solution
Limiting devices has no effect.	Ensure IPv6 is disabled.
Apple Macintosh running Mountain Lion can use AirPlay but iOS devices cannot.	Ensure IPv6 is disabled.

Acronyms and Abbreviations

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

Table 65: *List of abbreviations*

Abbreviation	Expansion
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
BSS	Basic Server Set
BSSID	Basic Server Set Identifier
CA	Certification Authority
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
IAP	IAP
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

Table 65: *List of abbreviations*

Abbreviation	Expansion
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial In User Service
VC	Virtual Controller
VSA	Vendor-Specific Attributes
WLAN	Wireless Local Area Network

Glossary

The following table lists the terms and their definitions used in this guide.

Table 66: *List of Terms*

Term	Definition
802.11	An evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.
802.11a	Provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.
802.11b	WLAN standard often called Wi-Fi; backward compatible with 802.11. Instead of the phase-shift keying (PSK) modulation method historically used in 802.11 standards, 802.11b uses complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.
802.11g	Offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b. 802.11g operates in the 2.4 GHz band and employs orthogonal frequency division multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.
802.11n	Wireless networking standard to improve network throughput over the two previous standards 802.11a and 802.11g with a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz. 802.11n operates in the 2.4 and 5.0 bands.
AP	An access point (AP) connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. The number of access points a WLAN needs is determined by the number of users and the size of the network.
access point mapping	The act of locating and possibly exploiting connections to WLANs while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a WLAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.
ad-hoc network	A LAN or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.

Table 66: *List of Terms*

Term	Definition
band	A specified range of frequencies of electromagnetic radiation.
DHCP	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.
DNS Server	A Domain Name System (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.
DST	Daylight saving time (DST), also known as summer time, is the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.
EAP	Extensible authentication protocol (EAP) refers to the authentication protocol in wireless networks that expands on methods used by the point-to-point protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.
fixed wireless	Wireless devices or systems in fixed locations such as homes and offices. Fixed wireless devices usually derive their electrical power from the utility mains, unlike mobile wireless or portable wireless which tend to be battery-powered. Although mobile and portable systems can be used in fixed locations, efficiency and bandwidth are compromised compared with fixed systems.
frequency allocation	Use of radio frequency spectrum regulated by governments.
frequency spectrum	Part of the electromagnetic spectrum.
hotspot	A WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.
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.
POE	Power over Ethernet (PoE) is a method of delivering power on the same physical Ethernet wire used for data communication. Power for devices is provided in one of the following two ways:

Table 66: *List of Terms*

Term	Definition
	● Endspan– The switch that an AP is connected for power supply. ● Midspan– A device can sit between the switch and APs The choice of endspan or midspan depends on the capabilities of the switch to which the IAP is connected. Typically if a switch is in place and does not support PoE, midspan power injectors are used.
PPPoE	Point-to-Point Protocol over Ethernet (PPPoE) is a method of connecting to the Internet typically used with DSL services where the client connects to the DSL modem.
QoS	Quality of Service (QoS) refers to the capability of a network to provide better service to a specific network traffic over various technologies.
RF	Radio Frequency (RF) refers to the portion of electromagnetic spectrum in which electromagnetic waves are generated by feeding alternating current to an antenna.
VPN	A Virtual Private Network (VPN) network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN ensures privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). Data is encrypted at the sending end and decrypted at the receiving end.
W-CDMA	Officially known as IMT-2000 direct spread; ITU standard derived from Code-Division Multiple Access (CDMA). Wideband code-division multiple access (W-CDMA) is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices than commonly offered in today's market.
Wi-Fi	A term for certain types of WLANs. Wi-Fi can apply to products that use any 802.11 standard. Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks.
WEP	Wired equivalent privacy (WEP) is a security protocol specified in 802.11b, designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.
wireless	Describes telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.
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.

Table 66: *List of Terms*

Term	Definition
WISP	Wireless ISP (WISP) refers to an internet service provider (ISP) that allows subscribers to connect to a server at designated hot spots (access points) using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers, called stations, to access the Internet and the Web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.
wireless service provider	A company that offers transmission services to users of wireless devices through radio frequency (RF) signals rather than through end-to-end wire communication.
WLAN	Wireless local area network (WLAN) is a local area network (LAN) that the users access through a wireless connection.