Table of Contents

Figures

Tables

About this Guide

About Aruba Instant

Aruba Instant is a simple, easy to deploy turn-key WLAN solution consisting of one or more access points. An Ethernet port with routable connectivity to the Internet is the only network infrastructure required to deploy the Aruba Instant wireless network. Aruba Instant is specifically designed for easy deployment and proactive management of networks for small customers or remote locations without an on-site IT administrator.

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

Objective

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

Intended Audience

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

Conventions

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

Type Style	Description
Italics	This style is used to emphasize important terms and provide cross-references to other books.
`Screen input and output`	This style is used to illustrate: • Screen output • On screen system prompt • Filenames, software devices, and specific commands
Bold	This style is used to emphasize Instant UI elements. For example, name of a text box or the name of a drop-down list.

The following informational icons are used throughout this guide:

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

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

WARNING	Indicates a risk of personal injury or death.

Contacting Support

Web Site	
Main Site	http://www.arubanetworks.com
Support Site	https://support.arubanetworks.com
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
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

Telephone Numbers	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
United States	800-WI-FI-LAN (800-943-4526)
Universal Free Phone Service Number (UIFN): Australia, Canada, China, France, Germany, Hong Kong, Ireland, Israel, Japan, Korea, Singapore, South Africa, Taiwan, and UK	+800-4WIFI-LAN (+800-49434-526)
All other countries	+1 (408) 754-1200

Aruba Networks Instant User Guide

Chapter 1

IAP Mounting

This chapter provides information about mounting an Instant Access Point (IAP).

Mounting an IAP

You can mount an IAP on a wall or on the ceiling. Use the IAP placement map generated by the *Aruba's RF Plan software application* to determine the proper installation location(s). Each location should be as close as possible to the center of the intended coverage area and should be free from obstructions or obvious sources of interference. These RF absorbers/reflectors/interference sources can impact RF propagation. These sources should be accounted for during the planning phase and the RF plan should be appropriately adjusted.

NOTE	Do not mount an IAP on a desk, table, or a cube top with the antennas pointing up.

Using the Integrated Ceiling Tile Rail Slots

The snap-in tile rail slots on the rear of the IAPs can be used to securely attach the device directly to 15/16 inches wide standard ceiling tile rail.

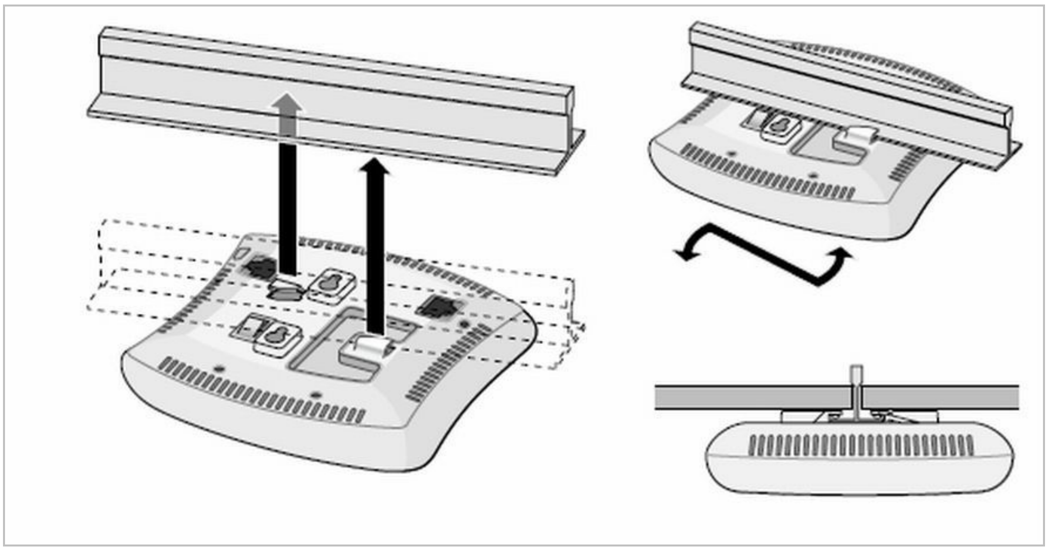
CAUTION	When hanging the IAP from the ceiling, make sure the IAP fits securely on the ceiling tile rail. Poor installation may cause the IAP to detach from the ceiling and fall on people or equipment.

To mount an IAP using the integrated ceiling tile rail slots, perform the following steps:

1. Pull the necessary cables through the prepared opening in the ceiling tile for placing the IAP.
2. If required connect the console cable to the console port on the rear of the IAP.

Hold the IAP next to the ceiling tile rail with the ceiling tile rail mounting slots at approximately 30-degree angle to the ceiling tile rail (see Figure 1). Make sure that any cable slack is above the ceiling tile.

Figure 1 *Orienting the Ceiling Tile Rail Mounting Slots*



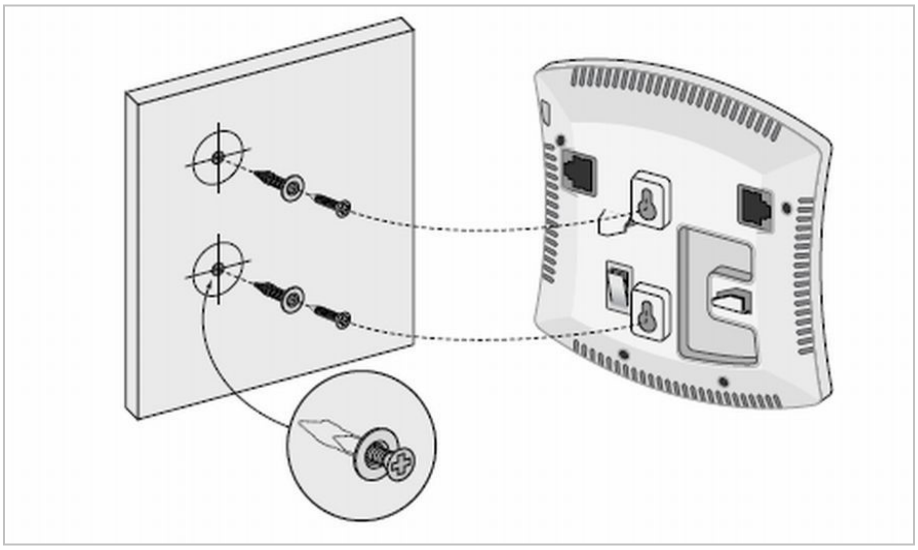
3. While pushing toward the ceiling tile, rotate the IAP clockwise until the device clicks into place on the ceiling tile rail.

Using the Integrated Wall-Mounting Slots

The keyhole-shaped slots on the rear of the IAPs can be used to attach the device upright to an indoor wall or shelf. When you choose the mounting location, allow additional space at the right of the unit for cables.

1. Since the ports are on the rear of the device, make sure that you mount the IAP in such a way that there is a clear path to the Ethernet port, such as a predrilled hole on the mounting surface.
2. At the mounting location, install two screws on the wall or shelf at 15/8 inches (4.7 cm) apart. If you are attaching the device to a drywall, Aruba recommends that you use appropriate wall anchors.
3. Align the mounting slots on the rear of the IAP over the screws and slide the unit into place (see Figure 2).

Figure 2 *Installing the IAP on a Wall*



IAP Internal Antenna Patterns

This section provides information about the internal antenna patterns in IAP-92, IAP-93, and IAP-105.

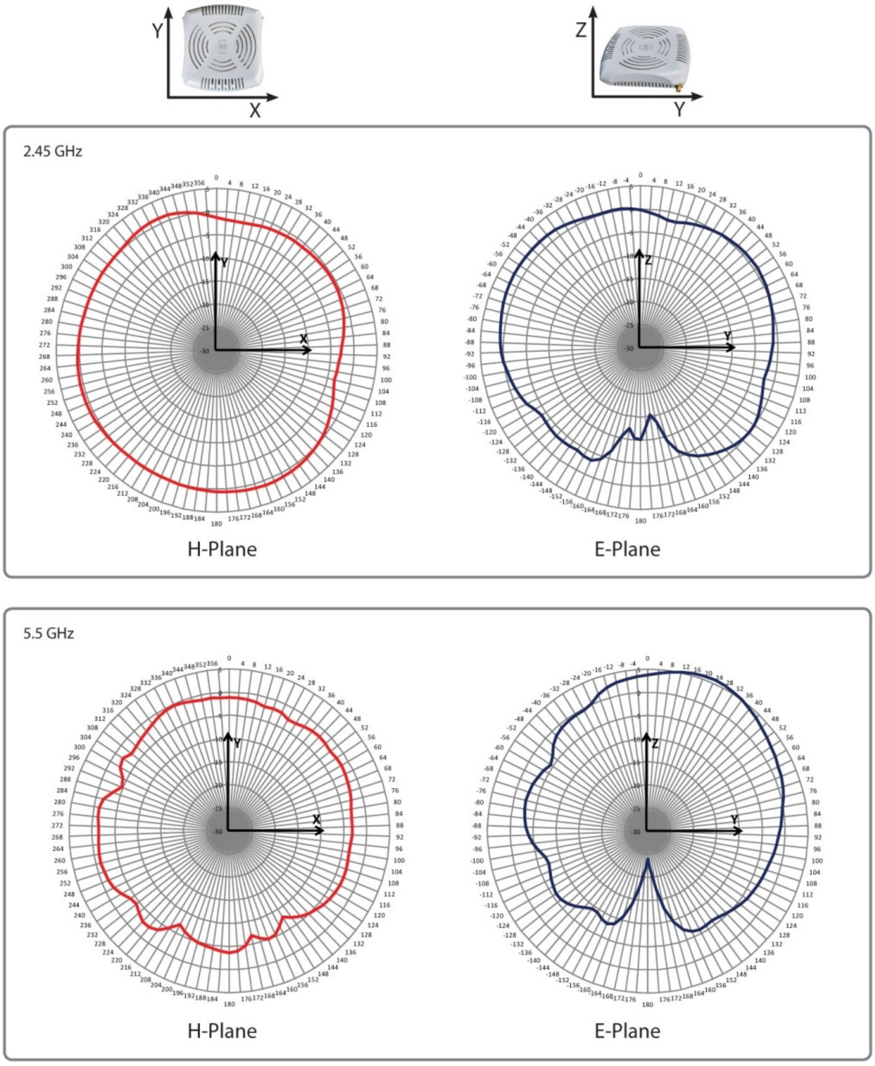
IAP-92 and IAP-93 Antenna Pattern

The antenna specifications of IAP-92 and IAP-93 are as follows:

- IAP-92: Dual, RP-SMA interfaces for external antenna support (supporting up to 2x2 MIMO with spatial diversity). For information to configure an external antenna, see Configuring an External Antenna.
- IAP-93: Integrated, omni-directional antenna elements (supporting up to 2x2 MIMO with spatial diversity)
- Maximum antenna gain for IAP-92 and IAP-93:
  - 2.4 GHz/2.5 dBi
  - 5 GHz/5.8 dBi

Figure 3 shows antenna patterns of IAP-93 for 2.45 GHz and 5.5 GHz.

Figure 3 *IAP-93 Antenna Pattern*



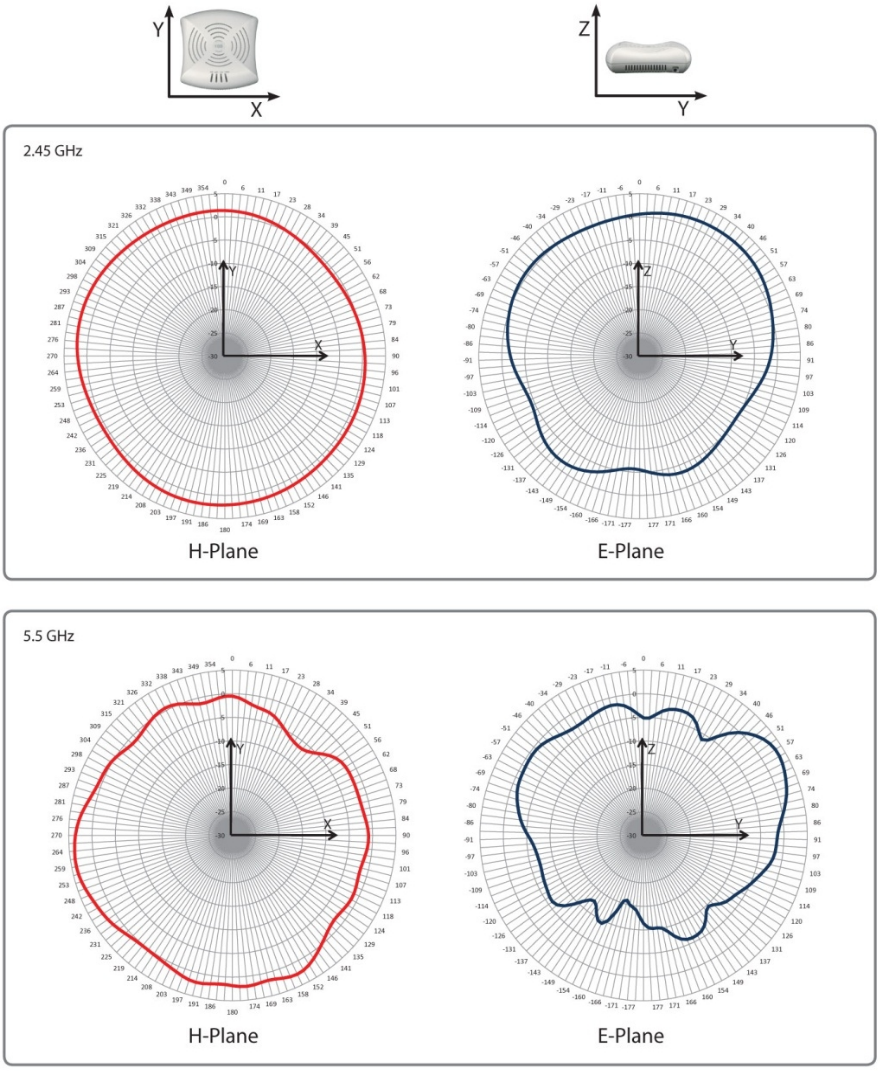
IAP-105 Antenna Pattern

The antenna specifications of IAP-105 are as follows:

- 4 x integrated, omni-directional antenna elements (supporting up to 2x2 MIMO with spatial diversity)
- Maximum antenna gain:
  - 2.4 GHz/2.5 dBi
  - 5.150 GHz to 5.875 GHz/4.0 dBi

Figure 4 shows antenna patterns of IAP-105 for 2.45 GHz and 5.5 GHz.

Figure 4 *IAP-105 Antenna Pattern*



Chapter 2
Initial Configuration

This chapter provides information that is required to set up Aruba Instant and access the Instant user interface.

Initial Setup

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

Pre-Installation Checklist

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

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

NOTE

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

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

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

- The following network services:
  - Dynamic Host Configuration Protocol (DHCP) server with internet service provider (ISP) specific options.
  - Domain Name System (DNS) server.

NOTE

- A DNS server functions as a phonebook for the Internet and Internet users. It converts human readable computer hostnames into IP addresses and vice-versa. A DNS server stores several records for a domain name, such as address 'A' record, name server (NS), and mail exchanger (MX) records. Address 'A' record is the most important record that is stored in a DNS server because it provides the required IP address for a network peripheral or element.
- The Dynamic Host Configuration Protocol (DHCP) is an auto-configuration protocol used on IP networks. Computers or any network peripherals that are connected to IP networks must be configured before they can communicate with other computers on the network. DHCP allows a computer to be configured automatically, thereby eliminating the need for a network administrator. DHCP also provides a central database to keep a track of computers connected to the network. This database helps in preventing any two computers from being configured with the same IP address.

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

1. Connecting the IAP to a power source.
2. Assigning an IP address to the IAP.
3. Connecting to the provisioning Wi-Fi network.
4. Login into the Instant user interface.

5. Specifying the country code. Skip this step, if you are installing the IAP in United States, Japan, or Israel.

Connecting the IAP to a Power Source

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

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

Assigning an IP Address to the IAP

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

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

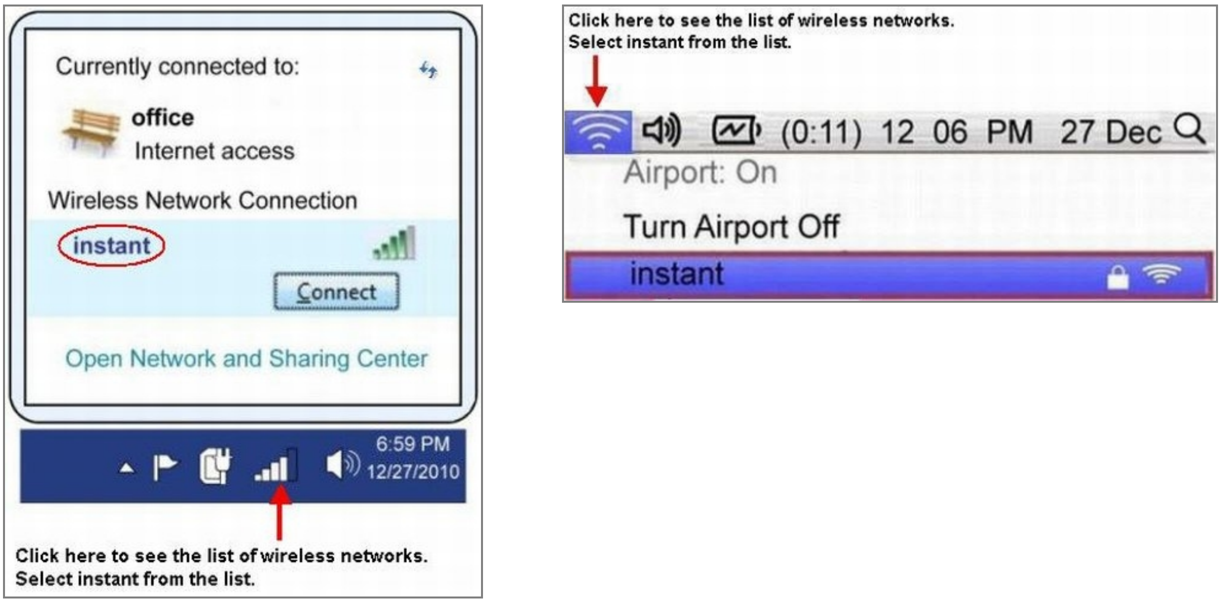
Connecting to the Provisioning Wi-Fi Network

Connect a wireless enabled client to the provisioning Wi-Fi network. By default, the provisioning Wi-Fi network is named **instant**.

- In the Microsoft Windows operating system, click the wireless network connection icon in the system tray. The **Wireless Network Connection** box appears. Click on the **instant** network and click **Connect**.
- In the MAC operating system, click the AirPort icon. A list of available Wi-Fi networks is displayed. Click on the **instant** network.

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

Figure 5 *Connecting to provisioning Wi-Fi network – Microsoft Windows and MAC OS*



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

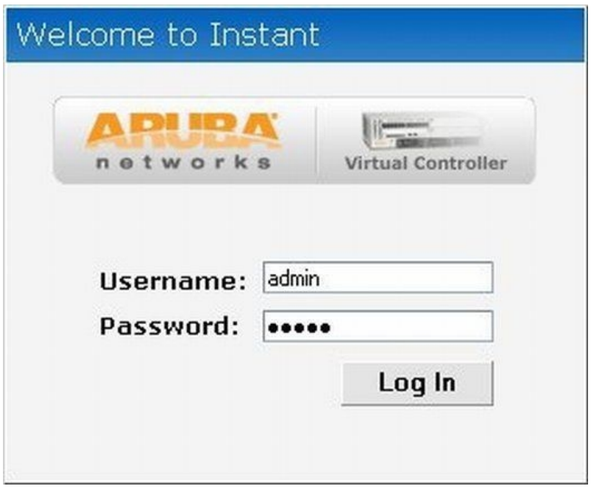
Click here to see the list of wireless networks.
Select instant from the list.

Login into Instant User Interface

Open a web browser and enter http://instant.arubanetworks.com/ (or any URL or web address) in the address field. In the login screen, enter the following credentials:

- Username – admin
- Password – admin

Figure 6 *Instant User Interface Login Screen*



Welcome to Instant

Username: admin

Password: •••••

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

Specifying the Country Code

NOTE

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

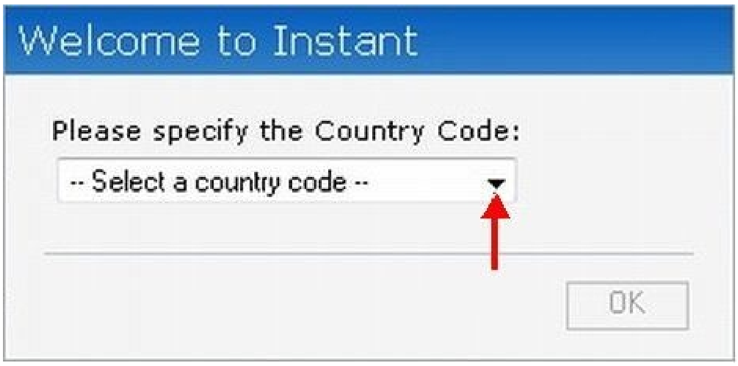
Aruba Instant Access Points are shipped in four variants:

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

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

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

Figure 7 *Specifying the Country Code*



Welcome to Instant

Please specify the Country Code:

Aruba Networks Instant User Guide

Chapter 3
Instant User Interface

This chapter describes the Instant user interface.

Instant User Interface Overview

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

Supported browsers are:

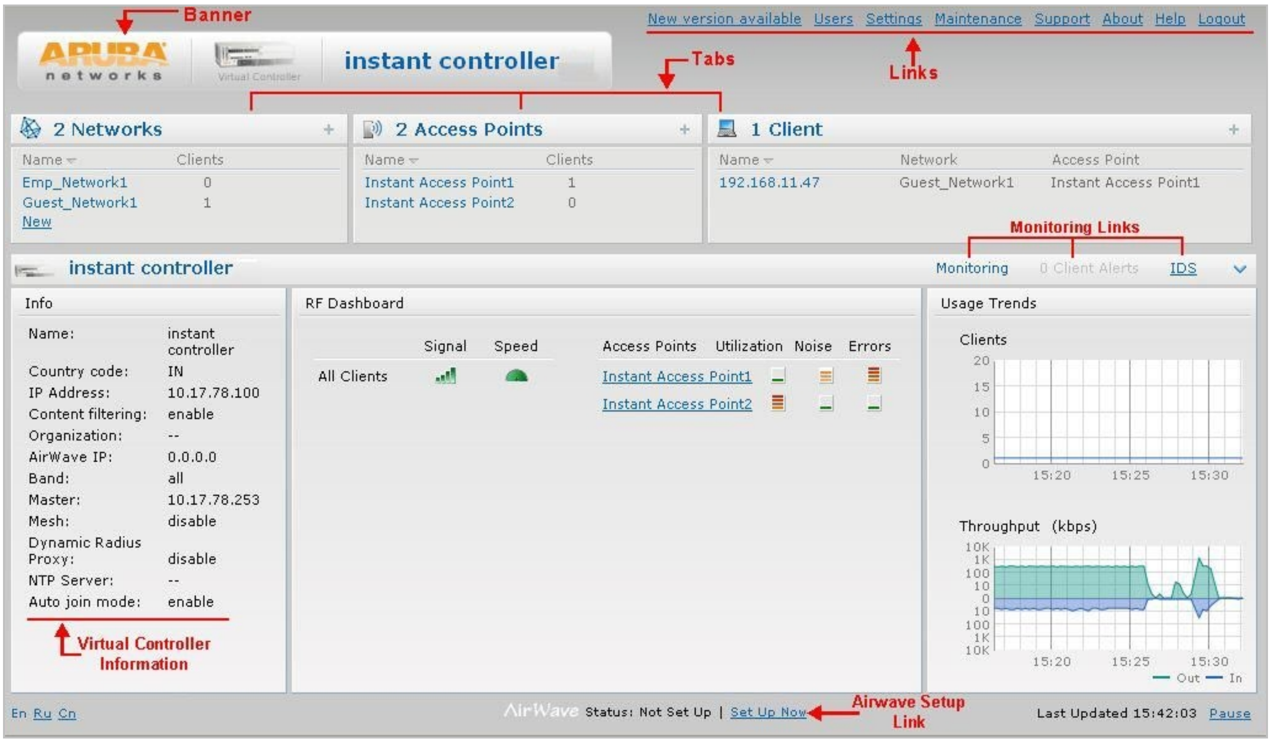
- Internet Explorer 7 or higher
- Safari
- Chrome
- Mozilla Firefox

Understanding the Instant UI Layout

The Instant UI consists of the following elements. These elements are explained in the following sections.

- Banner
- Tabs
- Links
- Views

Figure 8 *Basic Sections in the Instant UI*



2 Networks

Name	Clients
Emp_Network1	0
Guest_Network1	1
New	

2 Access Points

Name	Clients
Instant Access Point1	1
Instant Access Point2	0

1 Client

Name	Network	Access Point
192.168.11.47	Guest_Network1	Instant Access Point1

instant controller

Info

Name:	instant controller
Country code:	IN
IP Address:	10.17.78.100
Content filtering:	enable
Organization:	--
AirWave IP:	0.0.0.0
Band:	all
Master:	10.17.78.253
Mesh:	disable
Dynamic Radius Proxy:	disable
NTP Server:	--
Auto join mode:	enable

RF Dashboard

	Signal	Speed
All Clients		

Access Points	Utilization	Noise	Errors
Instant Access Point1			
Instant Access Point2			

Usage Trends

Status: Not Set Up | Set Up Now

Last Updated 15:42:03

Banner

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

Tabs

The Instant UI consists of the following tabs:

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

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

Each tab is explained in the following sections.

Networks Tab

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

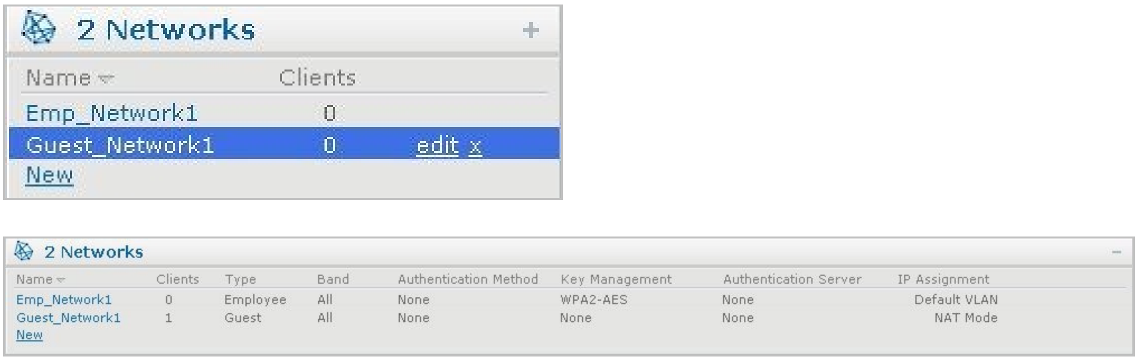
- **Name** - Name of the network.
- **Clients** - Number of clients that are connected to the network.
- **Type** - Network type: Employee, Guest, or Voice.
- **Band** - Band in which the network is broadcast: 2.4 GHz band, 5.4 GHz band, or both.
- **Authentication Method** - Authentication method required to connect to the network.
- **Key Management** - Authentication key type.
- **Authentication Server** - System's internal server or External RADIUS server.

- **IP Assignment** – Source of IP address for the client.

To add a Wi-Fi network, click the **New** link in the **Networks** tab. For more information about a wireless network and the procedure to add a wireless network, see Wireless Network.

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

Figure 9 *Networks Tab – Compressed View and Expanded View*



2 Networks

Name	Clients	
Emp_Network1	0	
Guest_Network1	0	edit x
New		

2 Networks

Name	Clients	Type	Band	Authentication Method	Key Management	Authentication Server	IP Assignment
Emp_Network1	0	Employee	All	None	WPA2-AES	None	Default VLAN
Guest_Network1	1	Guest	All	None	None	None	NAT Mode
New							

Access Points Tab

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

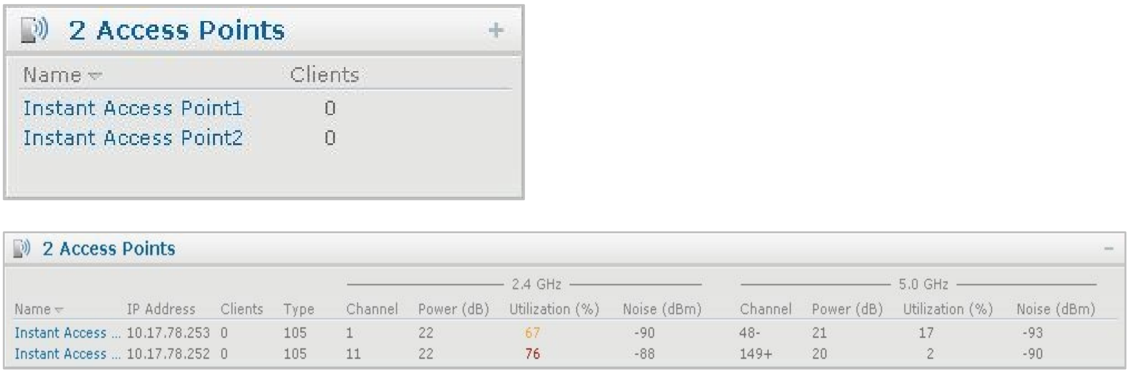
If Auto Join Mode is disabled, then a **New** link appears. Click this link to add a new IAP to the network. Also, if an IAP is configured and not active, its MAC Address is displayed in red.

The expanded view displays the following information about each IAP:

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

An **edit** link appears on clicking the IAP name. For information about editing IAP settings see, Editing IAP Settings.

Figure 10 *Access Points Tab – Compressed View and Expanded View*



2 Access Points

Name	Clients
Instant Access Point1	0
Instant Access Point2	0

2 Access Points

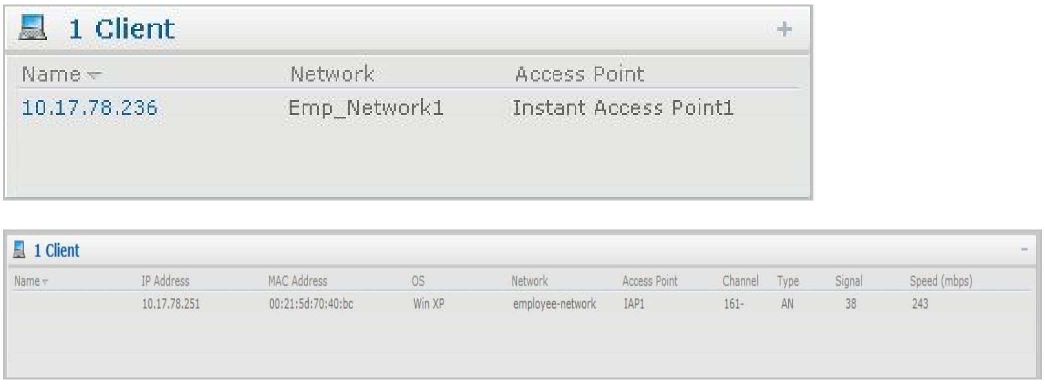
				2.4 GHz				5.0 GHz			
Name	IP Address	Clients	Type	Channel	Power (dB)	Utilization (%)	Noise (dBm)	Channel	Power (dB)	Utilization (%)	Noise (dBm)
Instant Access ...	10.17.78.253	0	105	1	22	67	-90	48-	21	17	-93
Instant Access ...	10.17.78.252	0	105	11	22	76	-88	149+	20	2	-90

Clients Tab

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

- **Name** - Name of the client.
- **IP Address** - IP address of the client.
- **MAC Address** - MAC address of the client.
- **OS** - Operating system that the client is running on.
- **Network** - Type of the network that the client is connected to: Employee, Voice, and Guest.
- **Access Point** - IAP to which the client is connected.
- **Channel** - Channel that the client is currently broadcasting on.
- **Type** - Wi-Fi type of the client: A, B, G, AN, or GN.
- **Signal** - Signal strength.
- **Speed (mbps)** - Data transfer speed.

Figure 11 *Client Tab – Compressed View and Expanded View*



1 Client

Name	Network	Access Point
10.17.78.236	Emp_Network1	Instant Access Point1

1 Client

Name	IP Address	MAC Address	OS	Network	Access Point	Channel	Type	Signal	Speed (mbps)
	10.17.78.251	00:21:5d:70:40:bc	Win XP	employee-network	IAP1	161-	AN	38	243

Links

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

- New version available
- Users
- Settings
- Maintenance
- Support
- About
- Help
- Logout
- Monitoring
- Client Alerts
- IDS
- Language
- AirWave setup
- Pause/Resume

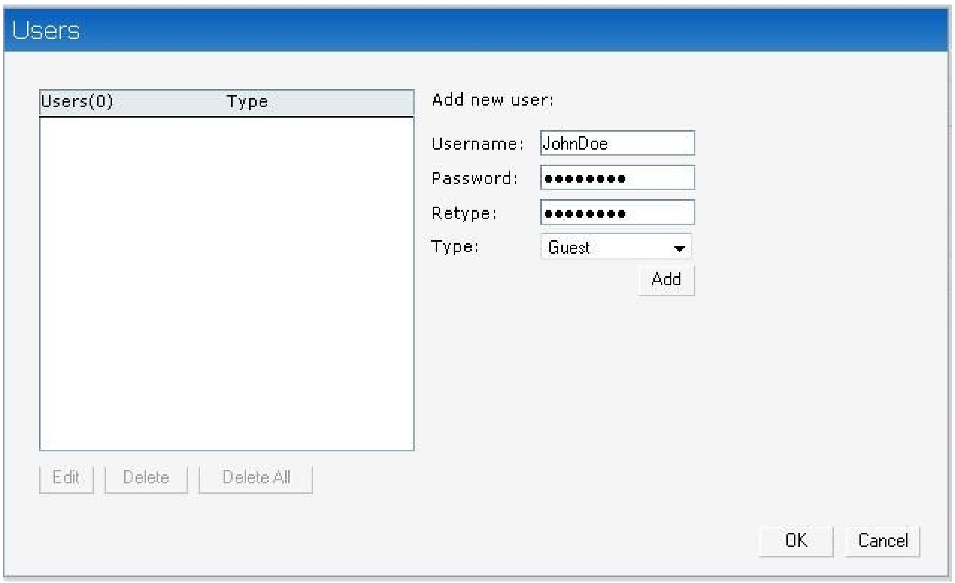
New version available

This link appears in the Instant UI only if a new image version is available on the image server and AirWave is not configured. For more information about the **New version available** link and its functions, see Firmware Image Server in Cloud Network.

Users

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

Figure 12 *Users Box*



Users

Users(0) Type

Add new user:

Username: JohnDoe

Password: ●●●●●●●●

Retype: ●●●●●●●●

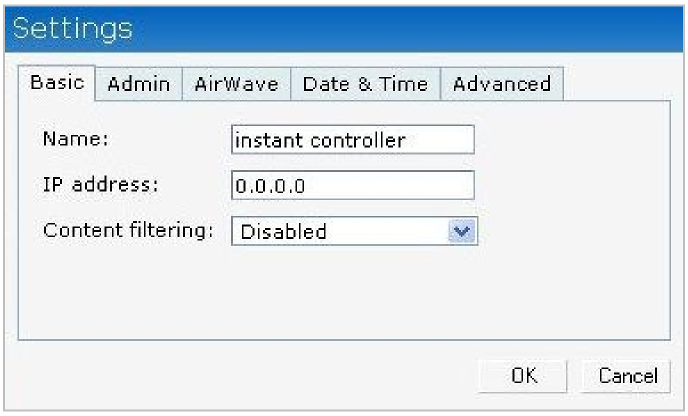
Type: Guest

Settings

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

- **Basic** - View or edit the virtual controller name, IP address, and Content filtering setting. For information about virtual controller settings and content filtering, see Virtual Controller and Content Filtering.
- **Admin** - View or edit the admin credentials.
- **AirWave** - View or edit the AirWave settings. For information about AirWave, see AirWave Integration and Management.
- **Date & Time** - View or edit the Network Time Protocol (NTP) server settings. For information about NTP server, see NTP Server.
- **Advanced** - View or edit the preferred band for the network, dynamic RADIUS Proxy, and Auto join mode settings. For information about dynamic RADIUS Proxy and Auto Join Mode, see External RADIUS Server and Auto Join Mode.

Figure 13 *Settings Link - Default View*



Name: instant controller

IP address: 0.0.0.0

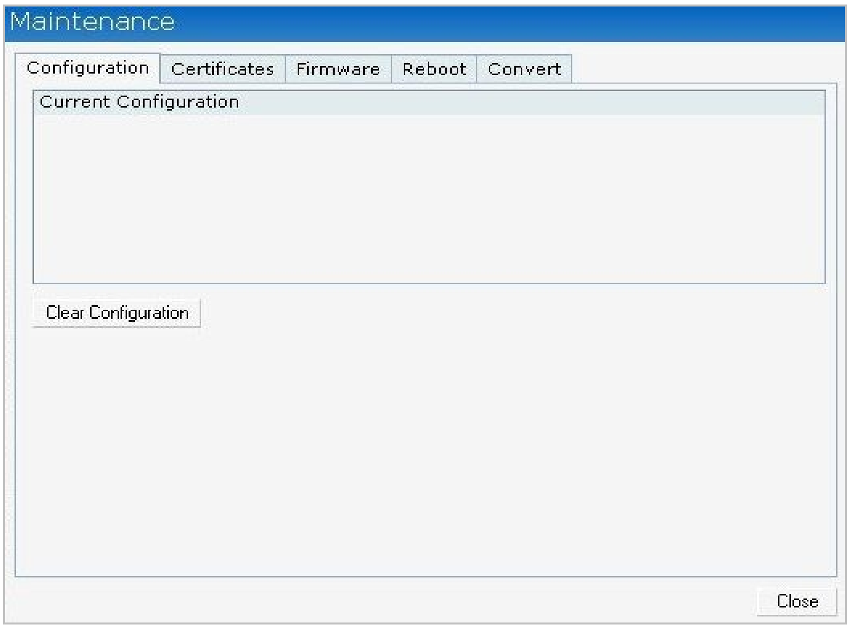
Content filtering: Disabled

Maintenance

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

- **Configuration** - Displays the current configuration of the network. The **Clear Configuration** button allows you to delete or clear the current configuration of the network and reset to provisioning configuration.
- **Certificates** - Displays information about current certificate installed in the network. Provides interface to upload new certificates and to set passphrase for the certificates. For more information, see Certificates.
- **Firmware** - Displays the current firmware version and provides options to upgrade to a new firmware version. For more information, see Manual Firmware Image Check and Upgrade.
- **Reboot** – Displays the lists of IAPs in the network and provides an option to reboot the required access point or all access points. For more information, see Rebooting the IAP.
- **Convert** - Provides an option to change the virtual controller managed network to an Aruba Mobility Controller managed network. For more information, see Migrating from a Virtual Controller Managed Network to Mobility Controller Managed Network.

Figure 14 *Maintenance Link - Default View*



Support

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

- **Command** drop-down list – Provides various options for which you can generate support logs.
- **Target** drop-down list – Provides a list of IAPs in the network.
- **Run** button – Click this button to generate the support log for the selected option and IAP.
- **Access point** tabs – Displays support log for the selected IAPs.

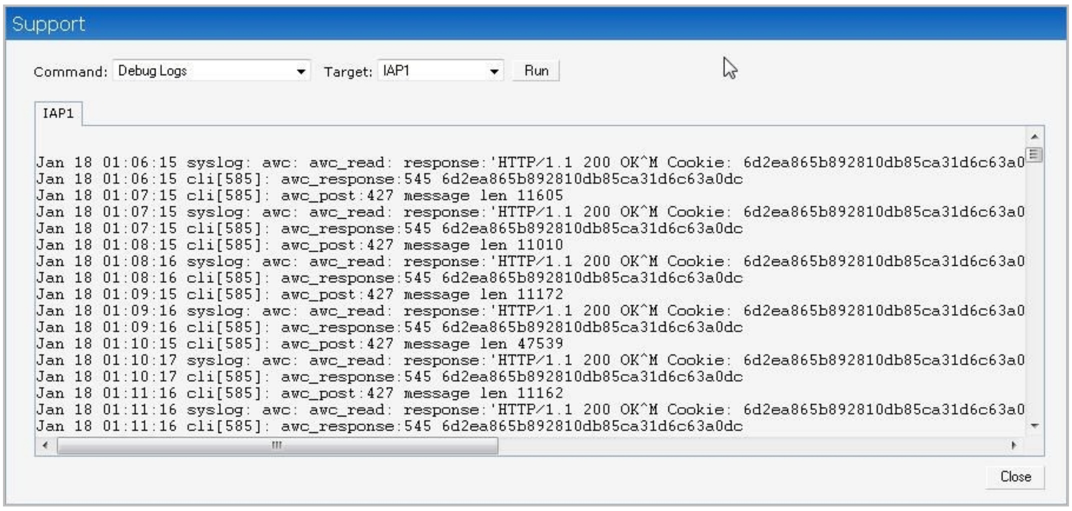
To view the logs and information, perform the following steps:

1. At the top right corner of Instant UI, click the **Support** link. The **Support** box appears.
2. Select the required option from the Command drop-down list. For example, Active Configuration.
3. From the **Target** drop-down list, select all IAPs or the required IAPs for which you want to view the Active Configuration.
4. Click **Run**.

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

- **Debug Logs** - Displays debug logs of the selected IAP.
- **Active Configuration** - Displays the active configuration of virtual controller.
- **Saved Configuration** - Displays the saved configuration of virtual controller.
- **AP Management Frames** - Displays the traced 802.11 management frames.
- **AP Authentication Frames** - Displays the authentication trace buffer information.
- **AP System Status** - Displays detailed system status information for the selected IAP.
- **AP Crash Info** - Displays crash log information (if it exists) for the selected IAP. The stored information is cleared from the flash after the AP reboots.
- **AP Client Table** - Displays information of the client connected to the selected IAP.
- **AP Radio 0 Stats** - Displays aggregate debug statistics of the selected IAP’s Radio 0.
- **AP Radio 1 Stats** - Displays aggregate debug statistics of the selected IAP’s Radio 1.
- **Bridge Table** - Displays bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for the selected IAP.
- **User Table** - Displays datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length for the selected IAP.
- **Session Table** - Displays the datapath session table statistics for the selected IAP.
- **Route Table** - Displays the datapath route table statistics for the selected IAP.
- **Datapath Statistics** - Displays the hardware packet statistics for the selected IAP.
- **VLAN Table** - Displays the VLAN table information such as VLAN memberships inside the datapath including L2 tunnels for the selected IAP.
- **BSSID Table** - Displays the Basic Service Set (BSS) table for the selected IAP.
- **IDS Status** - Displays WLAN Interface, Data Structures, WLAN Interface Switch Status and RTLS Configuration tables for the selected IAP.
- **IDS AP Table** - Displays the Monitored IAP Table, which lists all the IAPs monitored by the selected IAP.
- **ARM Bandwidth Management** - Displays bandwidth-management information for the selected IAP.
- **ARM History** - Displays the history of channel and power changes due to Adaptive Radio Management (ARM) for the selected IAP.
- **ARM Neighbors** - Displays the ARM settings for for the selected IAP's neighbors.
- **ARM RF Summary** - Displays the state and statistics for all channels being monitored by the selected IAP.
- **ARM Scan Times** - Displays AM channel scan times for the selected IAP.

Figure 15 *Support Box*



Command: Debug Logs Target: IAP1

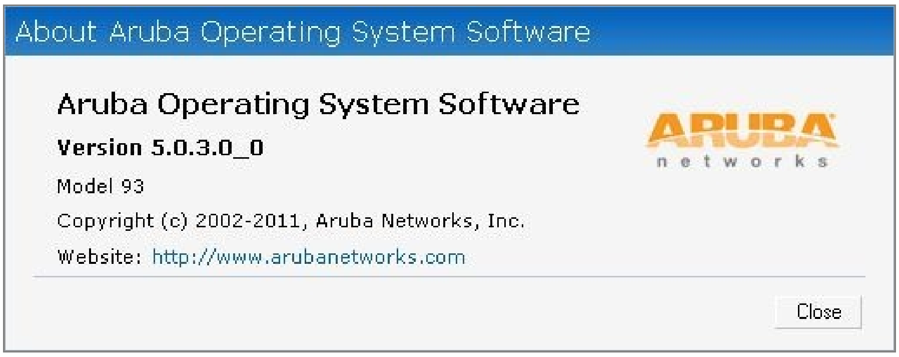
```
Jan 18 01:06:15 syslog: awc: awc_read: response:'HTTP/1.1 200 OK^M Cookie: 6d2ea865b892810db85ca31d6c63a0
Jan 18 01:06:15 cli[585]: awc_response:545 6d2ea865b892810db85ca31d6c63a0dc
Jan 18 01:07:15 cli[585]: awc_post:427 message len 11605
Jan 18 01:07:15 syslog: awc: awc_read: response:'HTTP/1.1 200 OK^M Cookie: 6d2ea865b892810db85ca31d6c63a0
Jan 18 01:07:15 cli[585]: awc_response:545 6d2ea865b892810db85ca31d6c63a0dc
Jan 18 01:08:15 cli[585]: awc_post:427 message len 11010
Jan 18 01:08:16 syslog: awc: awc_read: response:'HTTP/1.1 200 OK^M Cookie: 6d2ea865b892810db85ca31d6c63a0
Jan 18 01:08:16 cli[585]: awc_response:545 6d2ea865b892810db85ca31d6c63a0dc
Jan 18 01:09:15 cli[585]: awc_post:427 message len 11172
Jan 18 01:09:16 syslog: awc: awc_read: response:'HTTP/1.1 200 OK^M Cookie: 6d2ea865b892810db85ca31d6c63a0
Jan 18 01:09:16 cli[585]: awc_response:545 6d2ea865b892810db85ca31d6c63a0dc
Jan 18 01:10:15 cli[585]: awc_post:427 message len 47539
Jan 18 01:10:17 syslog: awc: awc_read: response:'HTTP/1.1 200 OK^M Cookie: 6d2ea865b892810db85ca31d6c63a0
Jan 18 01:10:17 cli[585]: awc_response:545 6d2ea865b892810db85ca31d6c63a0dc
Jan 18 01:11:16 cli[585]: awc_post:427 message len 11162
Jan 18 01:11:16 syslog: awc: awc_read: response:'HTTP/1.1 200 OK^M Cookie: 6d2ea865b892810db85ca31d6c63a0
Jan 18 01:11:16 cli[585]: awc_response:545 6d2ea865b892810db85ca31d6c63a0dc
```

About

This link provides the following information:

- Aruba operating system version
- IAP model name
- Copyright information
- Web address of Aruba Networks

Figure 16 *About Aruba Operating System*



About Aruba Operating System Software

Aruba Operating System Software

Version 5.0.3.0_0

Model 93

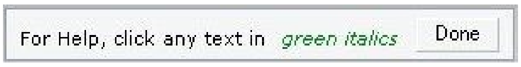
Copyright (c) 2002-2011, Aruba Networks, Inc.

Website: http://www.arubanetworks.com

Help

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

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



For Help, click any text in *green italics*

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

Logout

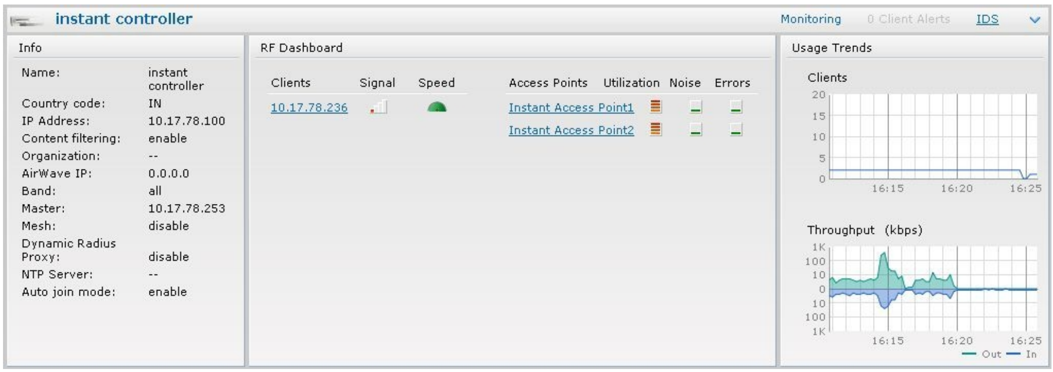
Use this link to logout of the Instant UI.

Monitoring

This link displays the monitoring pane. This pane can be used to monitor the Aruba Instant network. Use the down arrow ⌄ to compress or expand the monitoring pane. The monitoring pane consists of the following sections:

- Info
- RF Dashboard
- Usage Trends

Figure 17 *Monitoring Links on Instant UI*

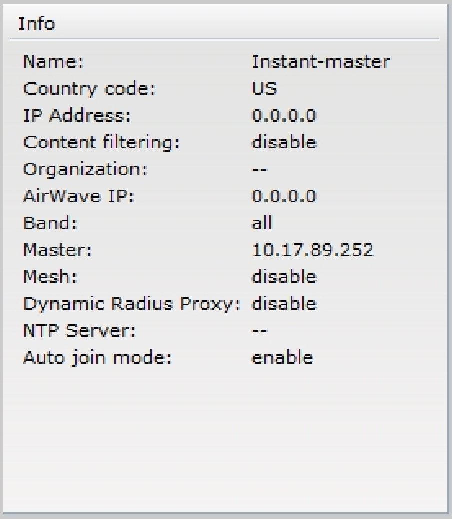


Name:	instant controller
Country code:	IN
IP Address:	10.17.78.100
Content filtering:	enable
Organization:	--
AirWave IP:	0.0.0.0
Band:	all
Master:	10.17.78.253
Mesh:	disable
Dynamic Radius Proxy:	disable
NTP Server:	--
Auto join mode:	enable

Clients	Signal	Speed	Access Points	Utilization	Noise	Errors
10.17.78.236			Instant Access Point1			
			Instant Access Point2			

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

Figure 18 *Info section in the Monitoring Pane*

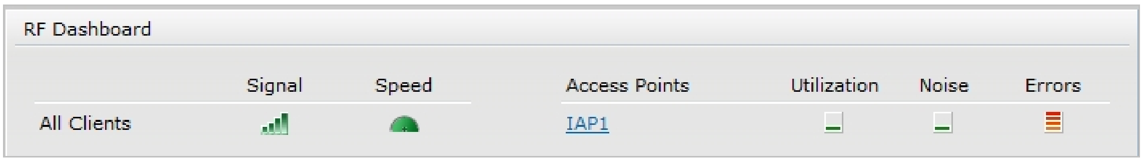


Info

Name:	Instant-master
Country code:	US
IP Address:	0.0.0.0
Content filtering:	disable
Organization:	--
AirWave IP:	0.0.0.0
Band:	all
Master:	10.17.89.252
Mesh:	disable
Dynamic Radius Proxy:	disable
NTP Server:	--
Auto join mode:	enable

- **RF Dashboard** - Allows you to view trouble spots in the network. It displays the following information:

Figure 19 *RF Dashboard section in the Monitoring Pane*



RF Dashboard

	Signal	Speed	Access Points	Utilization	Noise	Errors
All Clients			IAP1			

  - **Clients** - Lists the clients with low speed or signal strength in the network.
    - **Signal** - Displays the signal strength of the client. Depending on the signal strength of the client, the color of the lines on the signal bar changes from Green > Orange > Red.
      - Green - Signal strength is more than 20 decibels.
      - Orange - Signal strength is between 15 - 20 decibels.

    - Red - Signal strength is less than 15 decibels.

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

  - **Speed** - Displays the data transfer speed of the client. Depending on the data transfer speed of the client, the color of semicircle icon ◓ 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 semicircle icon ◓ against the client in the **Speed** column.

- **Access Points** – Lists the IAPs whose utilization, noise, or errors are not within the specified threshold. The IAP names appear as links. When the IAP is clicked, the IAP configuration information is displayed in the **Info** section. The **RF Dashboard** section is pushed to the bottom left corner of the Instant UI. The **RF Trends** section appears in its place. This section consists of the Utilization, Band frames, Noise Floor, and Errors graphs. For more information on the graphs, refer to Monitoring.
  - **Utilization** - Displays the radio utilization rate of the IAPs. Depending on the percentage of utilization, the color of the lines on the rectangle icon ▤ in the **Utilization** column changes from Green > Orange > Red.
    - Green - Utilization is less than 50 percent.
    - Orange - Utilization is between 50 - 75 percent.
    - Red - Utilization is more than 75 percent.

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

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

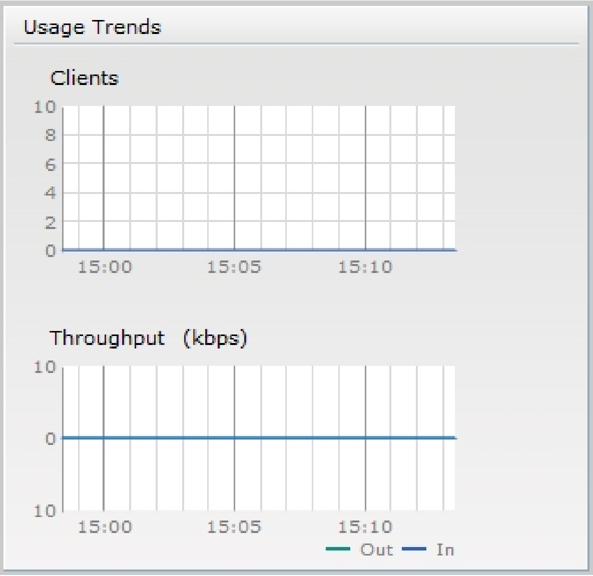
  To view the noise floor graph of an IAP, click on the rectangle icon ▤ against the IAP in the **Noise** column.

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

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

- **Usage Trends** - Displays the Clients and Throughput graphs.

Figure 20 *Usage Trends section in the Monitoring Pane*



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

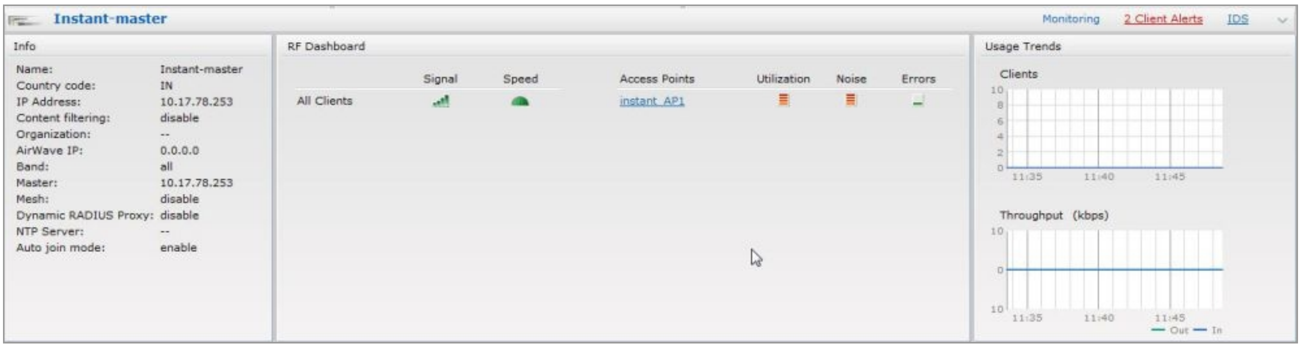
For more information about the graphs and monitoring procedures, see Monitoring.

Client Alerts

If there are any client alerts, this link appears in red. Click this link to see the related client alerts. Each alert consists of the following fields:

- **Timestamp** - Displays the time at which the client alert was recorded.
- **MAC address** - Displays the MAC address of the client.
- **Description** - Provides a short description of the error or alert.
- **Details** - Provides a detailed description of the error or alert.

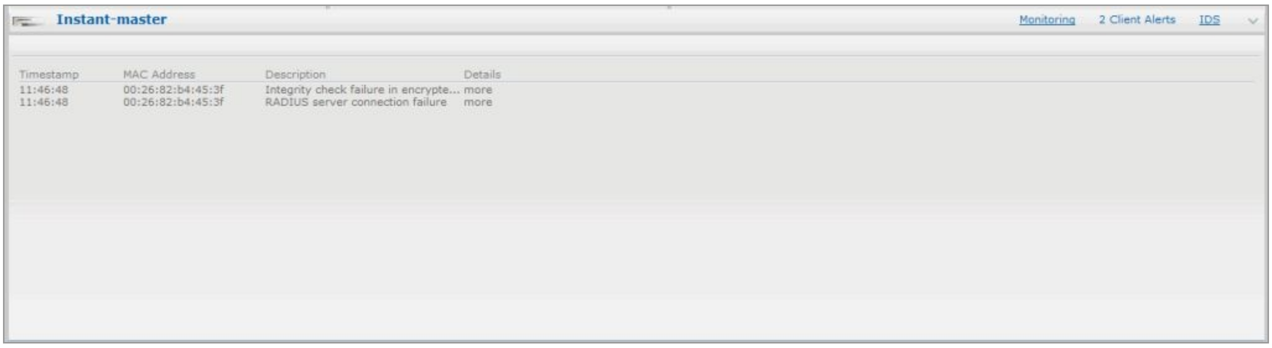
Figure 21 *Client Alerts link on Instant UI*



Name:	Instant-master
Country code:	IN
IP Address:	10.17.78.253
Content filtering:	disable
Organization:	--
AirWave IP:	0.0.0.0
Band:	all
Master:	10.17.78.253
Mesh:	disable
Dynamic RADIUS Proxy:	disable
NTP Server:	--
Auto join mode:	enable

	Signal	Speed	Access Points	Utilization	Noise	Errors
All Clients			instant_AP1			

Figure 22 *Client Alerts Link*



Timestamp	MAC Address	Description	Details
11:46:48	00:26:82:b4:45:3f	Integrity check failure in encrypte...	more
11:46:48	00:26:82:b4:45:3f	RADIUS server connection failure	more

For more information about alerts, see Alert Types and Management.

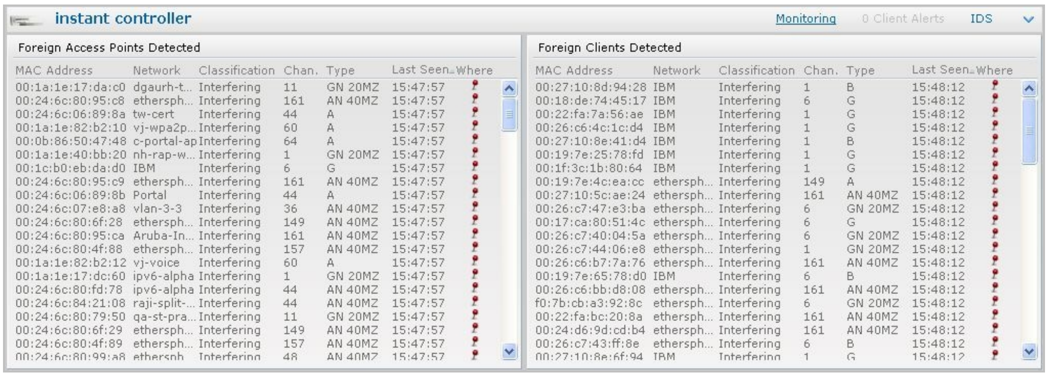
IDS

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

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

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

Figure 23 *Intrusion Detection on Instant UI*



Foreign Access Points Detected

MAC Address	Network	Classification	Chan.	Type	Last Seen	Where
00:1a:1e:17:da:c0	dgaurh-t...	Interfering	11	GN 20MZ	15:47:57	📍
00:24:6c:80:95:c8	ethersph...	Interfering	161	AN 40MZ	15:47:57	📍
00:24:6c:06:89:8a	tw-cert	Interfering	44	A	15:47:57	📍
00:1a:1e:82:b2:10	vj-wpa2p...	Interfering	60	A	15:47:57	📍
00:0b:86:50:47:48	c-portal-ap	Interfering	64	A	15:47:57	📍
00:1a:1e:40:bb:20	nh-rap-w...	Interfering	1	GN 20MZ	15:47:57	📍
00:1c:b0:eb:da:d0	IBM	Interfering	6	G	15:47:57	📍
00:24:6c:80:95:c9	ethersph...	Interfering	161	AN 40MZ	15:47:57	📍
00:24:6c:06:89:8b	Portal	Interfering	44	A	15:47:57	📍
00:24:6c:07:e8:a8	vlan-3-3	Interfering	36	AN 40MZ	15:47:57	📍
00:24:6c:80:6f:28	ethersph...	Interfering	149	AN 40MZ	15:47:57	📍
00:24:6c:80:95:ca	Aruba-In...	Interfering	161	AN 40MZ	15:47:57	📍
00:24:6c:80:4f:88	ethersph...	Interfering	157	AN 40MZ	15:47:57	📍
00:1a:1e:82:b2:12	vj-voice	Interfering	60	A	15:47:57	📍
00:1a:1e:17:dc:60	ipv6-alpha	Interfering	1	GN 20MZ	15:47:57	📍
00:24:6c:80:fd:78	ipv6-alpha	Interfering	44	AN 40MZ	15:47:57	📍
00:24:6c:84:21:08	raji-split-...	Interfering	44	AN 40MZ	15:47:57	📍
00:24:6c:80:79:50	qa-st-pra...	Interfering	11	GN 20MZ	15:47:57	📍
00:24:6c:80:6f:29	ethersph...	Interfering	149	AN 40MZ	15:47:57	📍
00:24:6c:80:4f:89	ethersph...	Interfering	157	AN 40MZ	15:47:57	📍
00:24:6c:80:99:a8	ethersph	Interfering	48	AN 40MZ	15:47:57	📍

Foreign Clients Detected

MAC Address	Network	Classification	Chan.	Type	Last Seen	Where
00:27:10:8d:94:28	IBM	Interfering	1	B	15:48:12	📍
00:18:de:74:45:17	IBM	Interfering	6	G	15:48:12	📍
00:22:fa:7a:56:ae	IBM	Interfering	1	G	15:48:12	📍
00:26:c6:4c:1c:d4	IBM	Interfering	1	G	15:48:12	📍
00:27:10:8e:41:d4	IBM	Interfering	1	B	15:48:12	📍
00:19:7e:25:78:fd	IBM	Interfering	1	G	15:48:12	📍
00:1f:3c:1b:80:64	IBM	Interfering	1	G	15:48:12	📍
00:19:7e:4c:ea:cc	ethersph...	Interfering	149	A	15:48:12	📍
00:27:10:5c:ae:24	ethersph...	Interfering	161	AN 40MZ	15:48:12	📍
00:26:c7:47:e3:ba	ethersph...	Interfering	6	GN 20MZ	15:48:12	📍
00:17:ca:80:51:4c	ethersph...	Interfering	6	G	15:48:12	📍
00:26:c7:40:04:5a	ethersph...	Interfering	6	GN 20MZ	15:48:12	📍
00:26:c7:44:06:e8	ethersph...	Interfering	1	GN 20MZ	15:48:12	📍
00:26:c6:b7:7a:76	ethersph...	Interfering	161	AN 40MZ	15:48:12	📍
00:19:7e:65:78:d0	IBM	Interfering	6	B	15:48:12	📍
00:26:c6:bb:d8:08	ethersph...	Interfering	161	AN 40MZ	15:48:12	📍
f0:7b:cb:a3:92:8c	ethersph...	Interfering	6	GN 20MZ	15:48:12	📍
00:22:fa:bc:20:8a	ethersph...	Interfering	161	AN 40MZ	15:48:12	📍
00:24:d6:9d:cd:b4	ethersph...	Interfering	161	AN 40MZ	15:48:12	📍
00:26:c7:43:ff:8e	ethersph...	Interfering	6	B	15:48:12	📍
00:27:10:8e:6f:94	IBM	Interfering	1	G	15:48:12	📍

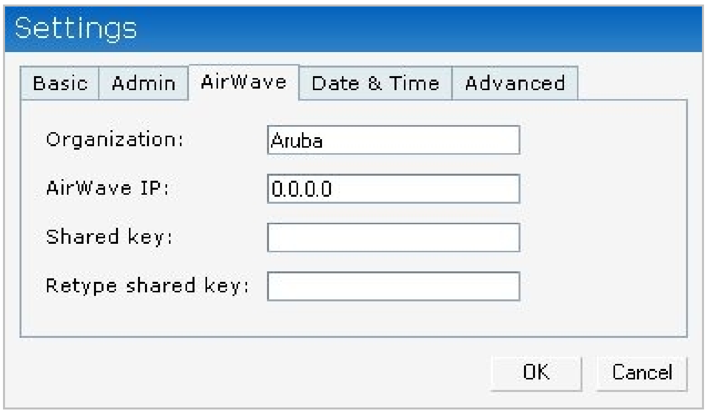
Language

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

AirWave Setup

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

Figure 24 *AirWave Setup Link – AirWave Configuration*



Organization: Aruba

AirWave IP: 0.0.0.0

Shared key:

Retype shared key:

Pause/Resume

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

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

The **Pause** link is useful when you want to analyze or monitor the network or a network element and therefore do not want the user interface to refresh.

Automatic refreshing allows you to get the latest information about the network and network elements.

View Types

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

- Virtual Controller view – The Virtual Controller view is the default view. This view allows you to monitor the Aruba Instant network.
- Network view – The Network view provides information that is necessary to monitor a selected wireless network. All Wi-Fi networks in the Aruba Instant network are listed in the **Networks** tab. Click the network that you want to monitor. Network View for the selected network appears.
- Access Point view – The Access Point view provides information that is necessary to monitor a selected IAP. All IAPs in the Aruba Instant network are listed in the **Access Points** tab. Click the IAP that you want to monitor. Access Point view for that IAP appears.
- Client view – The Client view provides information that is necessary to monitor a selected client. In the Virtual Controller view, all clients in the Aruba 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 detailed information on these views, see Monitoring.

Chapter 4
Wireless Network

Wi-Fi Network Overview

In a wireless LAN (WLAN), laptops, desktops, PDAs, and other computer peripherals are connected to each other without any network cables. These network elements or clients use radio signals to communicate with each other. Wireless networks are set up based on the IEEE 802.11 standards. The IEEE 802.11 is a set of standards that are categorized based on the radio wave frequency and the data transfer rate. For more information about the IEEE 802.11 standards, see Table 1.

Table 1 *IEEE 802.11 Standards*

IEEE Network Standard	Frequency Used (in GHz)	Maximum Data Transfer Rate (in Mbps)
802.11a	5.0	54
802.11b	2.4	11
802.11g	2.4	54
802.11n	2.4 or 5	300

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

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

Network Types

Aruba Instant wireless networks are categorized as:

- Employee Network
- Voice Network
- Guest Network

Employee Network

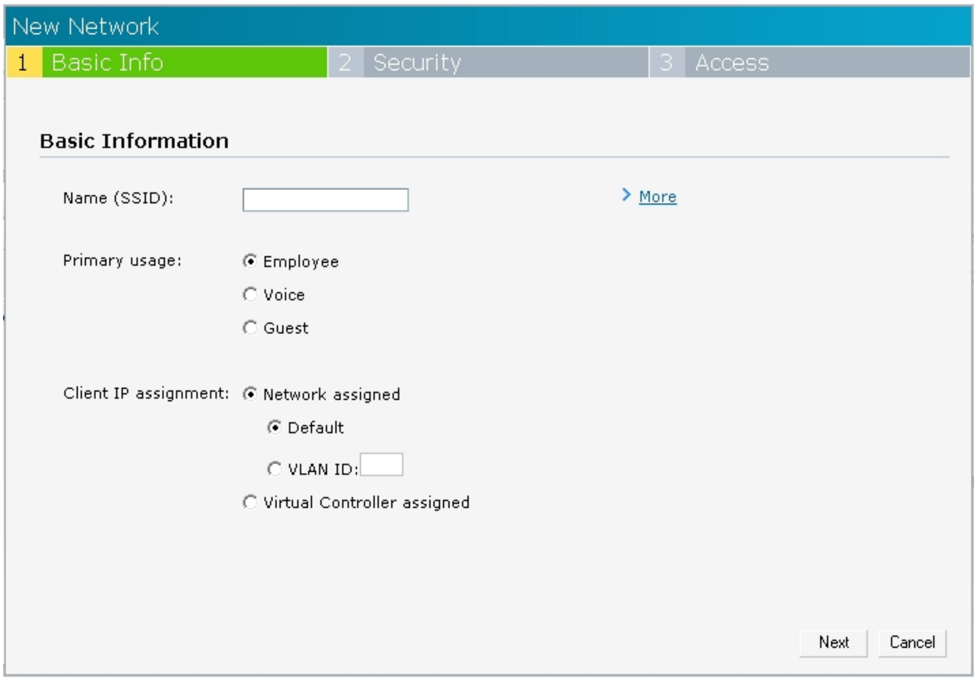
An Employee network is a classic Wi-Fi network. This network type is supported with full customization on Aruba Instant. It will be used by the employees in the organization. Passphrase based or 802.1X based authentication methods are supported for this network type. Employees can access the protected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

Adding an Employee Network

This section describes the procedure to add an employee network.

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

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



New Network

1 Basic Info | 2 Security | 3 Access

Basic Information

Name (SSID):

Primary usage: ● Employee ○ Voice ○ Guest

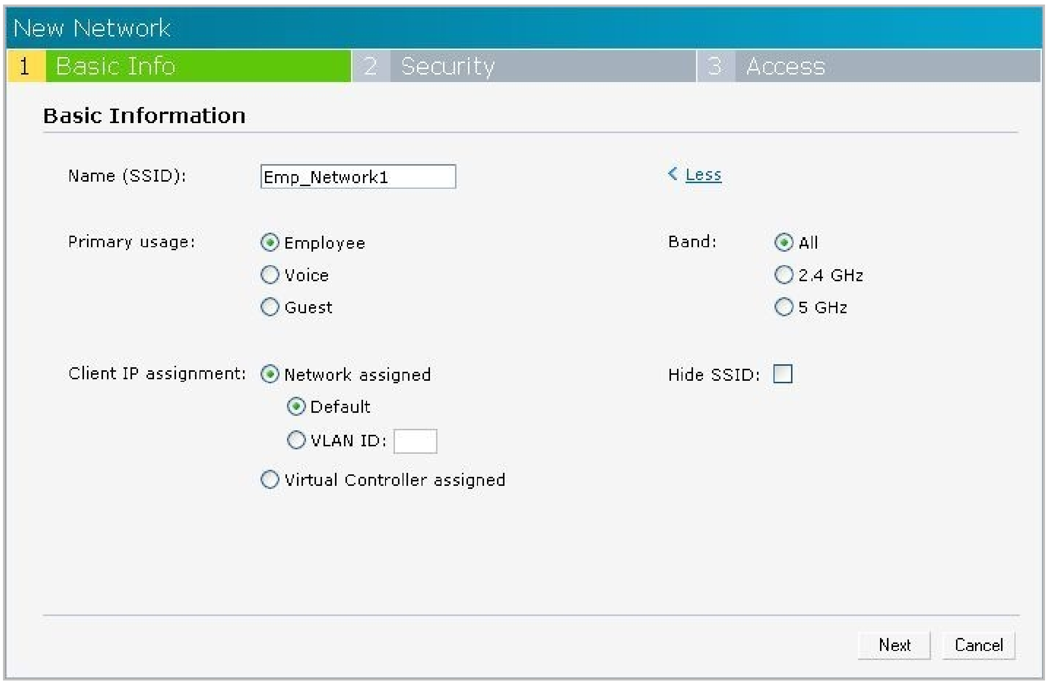
Client IP assignment: ● Network assigned
● Default
○ VLAN ID:
○ Virtual Controller assigned

2. In the **Basic Info** tab, perform the following steps:
   a. Type a name for the network in the **Name** (SSID) text box.
   b. Select the **Employee** radio button (this is selected by default) from the Primary usage options. This selection determines the primary usage of the network being added.
   c. Select the required **Client IP assignment** option. Available options for an Employee network are **Network assigned - Default**, **Network assigned - VLAN ID**, and **Virtual Controller assigned**.

If	then,
You select the **Network assigned – Default** option	The default enterprise network assigns the IP address. This option requires a DHCP server to be configured in the network.
You select the **Network assigned – VLAN ID** option	The client gets the IP address from the specified VLAN. Enter the ID of the VLAN in the **VLAN ID** text box.
You select **Virtual Controller assigned** option	The client gets the IP address from the virtual controller. The virtual controller creates a private subnet and VLAN for the IAPs and the wireless clients. The virtual controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network.

3. Click the **More** link and perform the following steps (These steps are optional).
   a. **Band** - Set the band at which the wireless network will transmit radio signals. Available options are All, 2.4 GHz, and 5 GHz. The All option is selected by default. It is also the recommended option.
   b. **Hide SSID** - Select this check box if you want to hide the **SSID** (network name) from users.

Figure 26 *Band and Hide SSID Settings*



New Network

1 Basic Info | 2 Security | 3 Access

Basic Information

Name (SSID): Emp_Network1

Primary usage: ● Employee ○ Voice ○ Guest

Band: ● All ○ 2.4 GHz ○ 5 GHz

Client IP assignment: ● Network assigned
- ● Default
- ○ VLAN ID:
- ○ Virtual Controller assigned

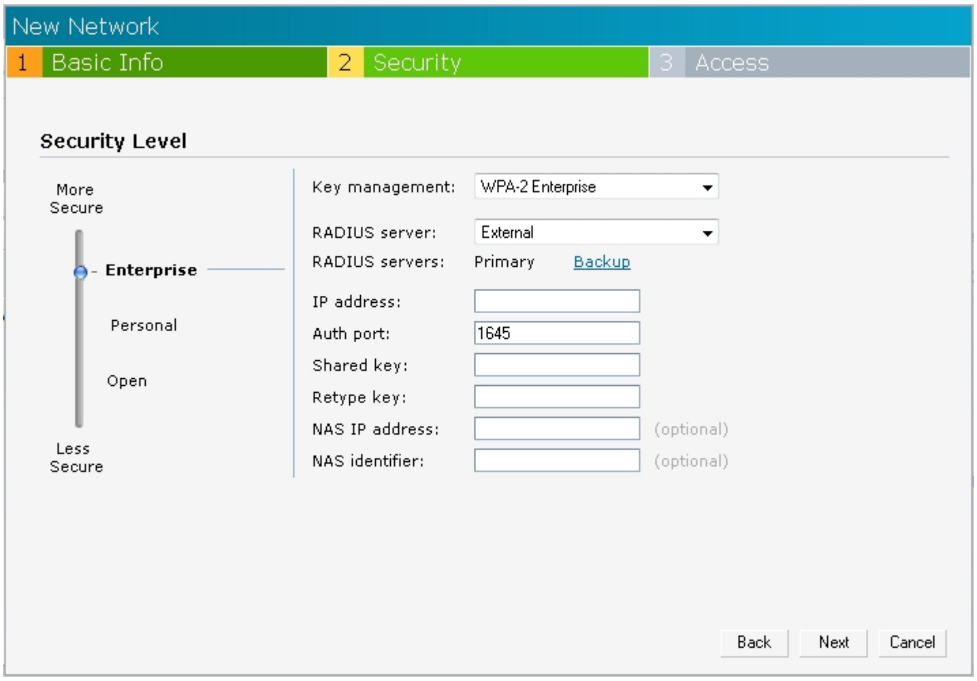
Hide SSID: □

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

If	then,
You select the **Enterprise** security level	Perform the following steps: 1. Select the required key options from **the Key management** drop-down list. Available options are: - WPA-2 Enterprise - WPA Enterprise - Both (WPA-2 & WPA) - Dynamic WEP with 802.1x For more information on encryption and recommended encryption type, see Encryption. 2. Select the required RADIUS server option from the **RADIUS Server** drop-down list. Available options are: - **External** – If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Configuring an External RADIUS Server. - **Internal** – If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the **Users** link to add the users. For information on adding a user, see Adding a User.
You want to use the default security level, **Personal**,	Perform the following steps: 1. Select the required key options from the **Key management** drop-down list. Available options are: - WPA-2 Personal - WPA Personal - Both (WPA-2 & WPA) - Static WEP If you selected **Static WEP**, then do the following: a. Select appropriate WEP key size from the **WEP key size** drop-down list. Available options are **64-bit** and **128-bit**. b. Select appropriate Tx key from the **Tx Key** drop-down list. Available options are **1, 2, 3, and 4**. c. Enter an appropriate WEP key in the **WEP Key** text box and reconfirm. For more information on encryption and recommended encryption type, see Encryption. 1. Enter a passphrase in the **Passphrase** text box and reconfirm. 2. Select the required option from the **MAC authentication** drop-down list. Available options are - **None** - This option provides open authentication. Any client that requests association is allowed to connect to the network. Open authentication is not recommended unless you want users to gain quick access to the network.

If	then,
	▪ **External RADIUS Server** - If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring external RADIUS server, see Configuring an External RADIUS Server.
You select the **Open** security level	Select the required MAC authentication from the **MAC authentication** drop-down list. Available options are: • **None** – This option provides open authentication. Any client that requests association is allowed to connect to the network. Open authentication is not recommended unless you want users to gain quick access to the network. • **External RADIUS Server** - If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Configuring an External RADIUS Server.

Figure 27 *Security Tab - Enterprise*



Key management: WPA-2 Enterprise

RADIUS server: External

RADIUS servers: Primary Backup

IP address:

Auth port: 1645

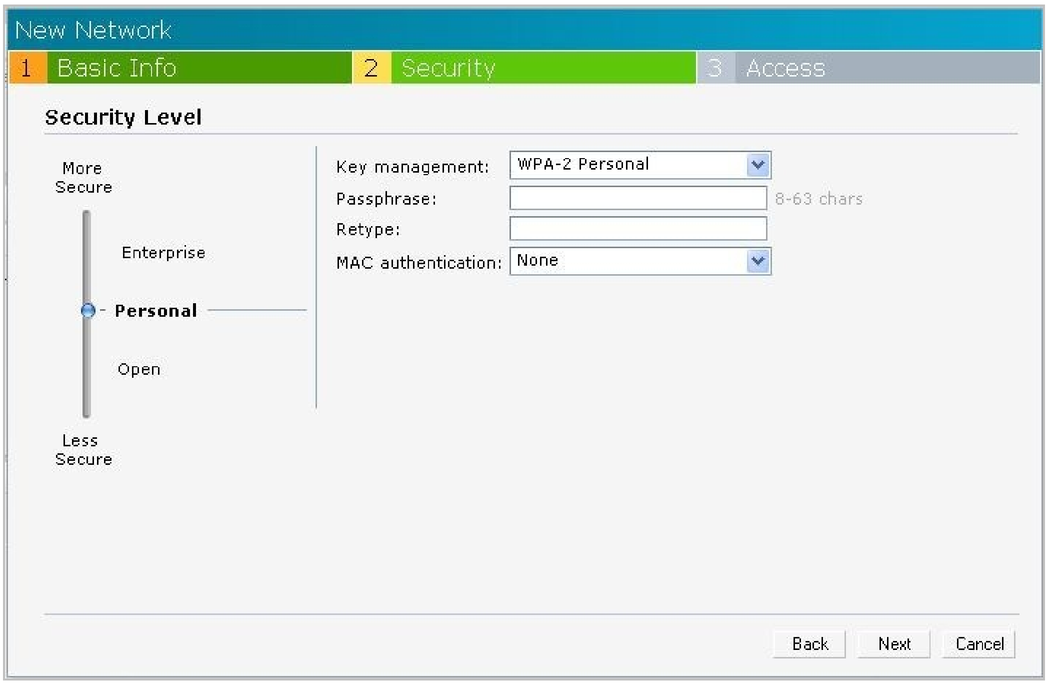
Shared key:

Retype key:

NAS IP address: (optional)

NAS identifier: (optional)

Figure 28 *Security Tab - Personal*



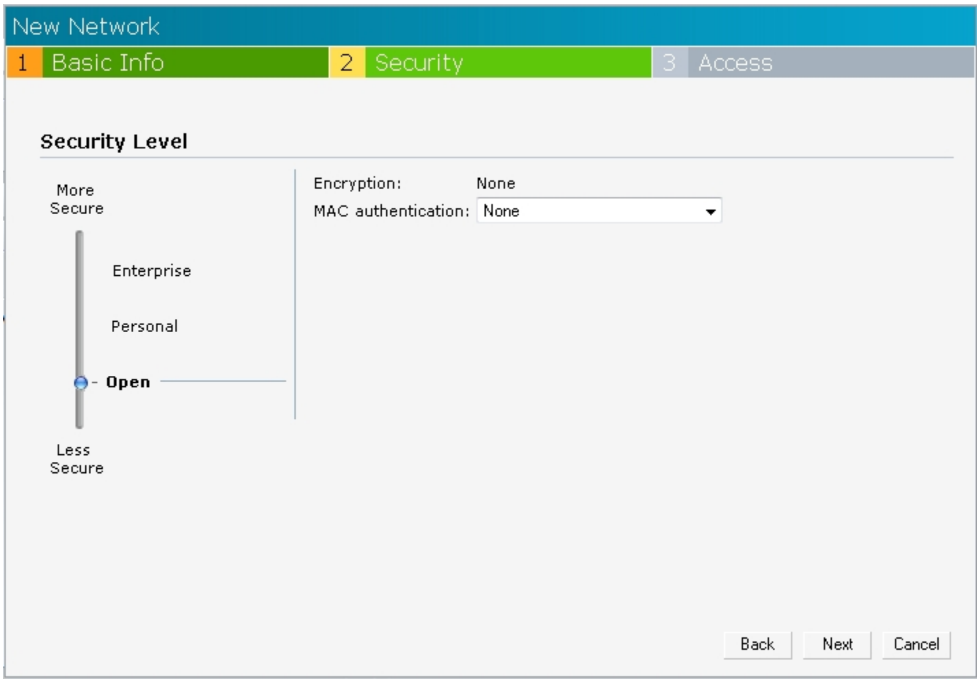
Key management: WPA-2 Personal

Passphrase: 8-63 chars

Retype:

MAC authentication: None

Figure 29 *Security Tab - Open*



Encryption: None

MAC authentication: None

5. Click **Next.** The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. InstantFirewall treats packets based on the first rule matched. For more information, see InstantFirewall.

To edit the default rule, perform the following steps:

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

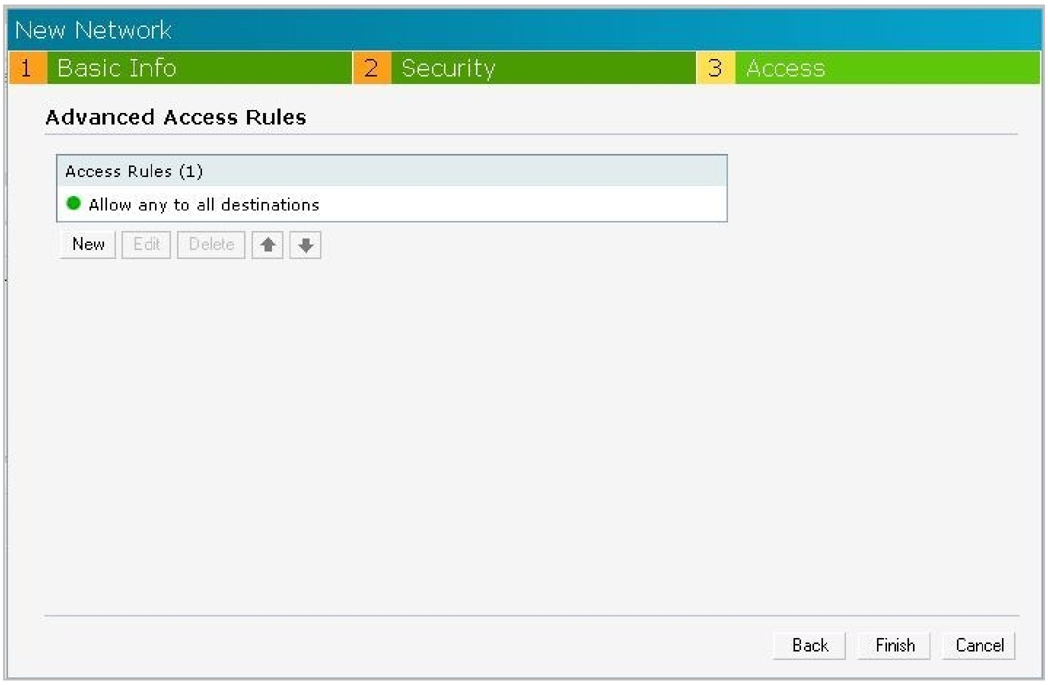
b. Select appropriate options in the **Edit Rule** box and click **OK**.

To define an access rule, perform the following steps:

a. Click the **New** button,

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

Figure 30 *Adding an Employee Network – Access Rules Tab*



Advanced Access Rules

Access Rules (1)

● Allow any to all destinations

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

Voice Network

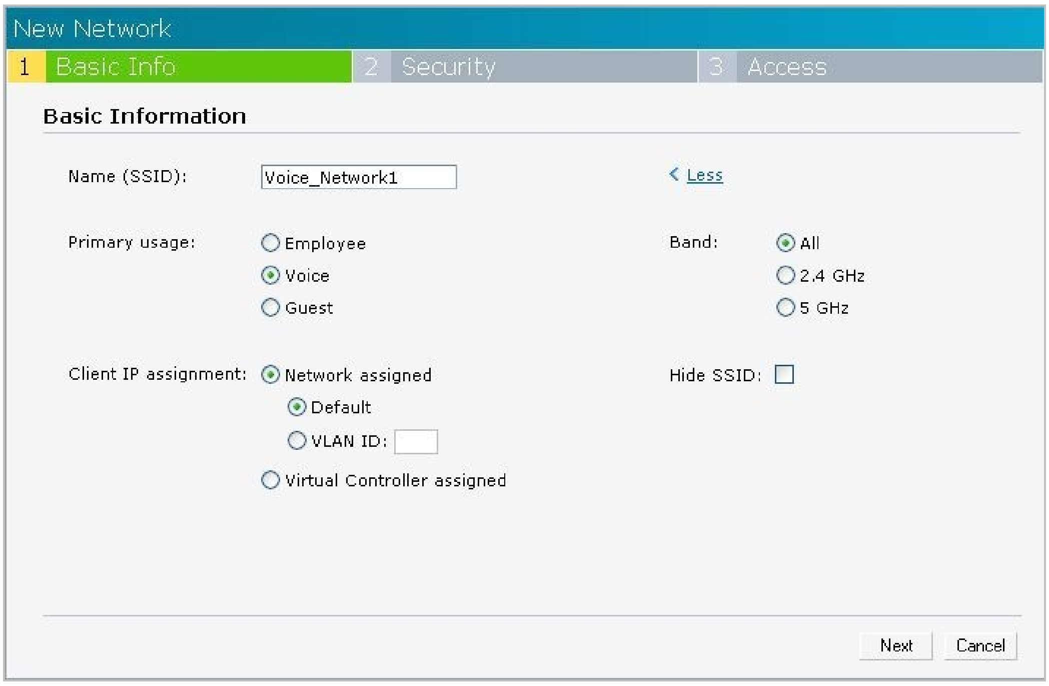
Use the Voice network type when you want devices that provide only voice services like handsets or only applications that require voice-like prioritization need connectivity.

Adding a Voice Network

This section provides the procedure to add a voice network.

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

Figure 31 *Adding a Voice Network – Basic Info Tab*



New Network

1 Basic Info | 2 Security | 3 Access

Basic Information

Name (SSID): Voice_Network1

Primary usage: ○ Employee ● Voice ○ Guest

Band: ● All ○ 2.4 GHz ○ 5 GHz

Client IP assignment: ● Network assigned (● Default ○ VLAN ID:) ○ Virtual Controller assigned

Hide SSID: □

2. In the **Basic Info** tab, perform the following steps:
   a. Type a name for the network in the **Name (SSID)** text box.
   b. Select the **Voice** radio button from the **Primary usage** options. This selection determines the primary usage of the network being added.
   c. Select the required client IP assignment option. Available options for a Voice network are **Network assigned - Default**, **Network assigned - VLAN ID**, and **Virtual Controller assigned**.

If	then,
You select the **Network assigned – Default** option	The default enterprise network assigns the IP address. This option requires a DHCP server to be configured in the network.
You select the **Network assigned – VLAN ID** option	The client gets the IP address from the specified VLAN. Enter the ID of the VLAN in the **VLAN ID** text box.
You select **Virtual Controller assigned** option	The client gets the IP address from the virtual controller. The virtual controller creates a private subnet and VLAN for the IAPs and the wireless clients. The virtual controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network.

3. Click the **More** link and perform the following steps (These steps are optional).
    a. **Band** - Set the band at which the network will transmit radio signals. Available options are **All, 2.4 GHz, and 5 GHz**. The **All** option is selected by default. It is also the recommended option.
    b. **Hide SSID** - Select this check box if you want to hide the SSID (network name) from the users.
4. Click **Next** and set appropriate security levels using the slider button in the **Security** tab. Default selection is **Personal**. Available options are **Enterprise, Personal**, and **Open**.

If	then,
You select the **Enterprise** security level	Perform the following steps: 1. Select the required key options from the **Key management** drop-down list. Available options are: ▪ WPA-2 Enterprise ▪ WPA Enterprise ▪ Both (WPA-2 & WPA) ▪ Dynamic WEP with 802.1x For more information on encryption and recommended encryption type, see Encryption. 2. Select the required RADIUS server option from the **RADIUS Server** drop-down list. Available options are: ▪ **External** - If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Configuring an External RADIUS Server. ▪ **Internal** - If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the **Users** link to add the users. For information about adding a user, see Adding a User.
You want to use the default security level, **Personal**,	Perform the following steps: 1. Select the required key options from the **Key management** drop-down list. Available options are: ▪ WPA-2 Personal ▪ WPA Personal ▪ Both (WPA-2 & WPA) ▪ Static WEP If you selected **Static WEP**, then do the following: i. Select appropriate **WEP key size** from the **WEP key size** drop-down list. Available options are 64-bit and 128-bit. ii. Select appropriate **Tx key** from the **Tx Key** drop-down list. Available options are 1, 2, 3, and 4. iii. Enter an appropriate **WEP key** in the **WEP Key** text box and reconfirm. For more information on encryption and recommended encryption type, see Encryption. 2. Enter a passphrase in the **Passphrase** text box and reconfirm.

If	then,
	3. Select the required option from the **MAC authentication** drop-down list. Available options are: ▪ **None** - This option provides open authentication. Any client that requests association is allowed to connect to the network. Open authentication is not recommended unless you want users to gain quick access to the network. ▪ **External RADIUS Server** - For information on configuring an external RADIUS server, see Configuring an External RADIUS Server.
You select the **Open** security level	Select the required MAC authentication from the **MAC authentication** drop-down list. Available options are: • **None** - This option provides open authentication. Any client that requests association is allowed to connect to the network. Open authentication is not recommended unless you want users to gain quick access to the network. • **External RADIUS Server** - For information on configuring an external RADIUS server, see Configuring an External RADIUS Server.

5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. InstantFirewall treats packets based on the first rule matched. For more information, see InstantFirewall.

   To edit the default rule, perform the following steps:

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

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

   To define an access rule, perform the following steps:

   a. Click the **New** button,

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

   c. Click **OK**.

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

Guest Network

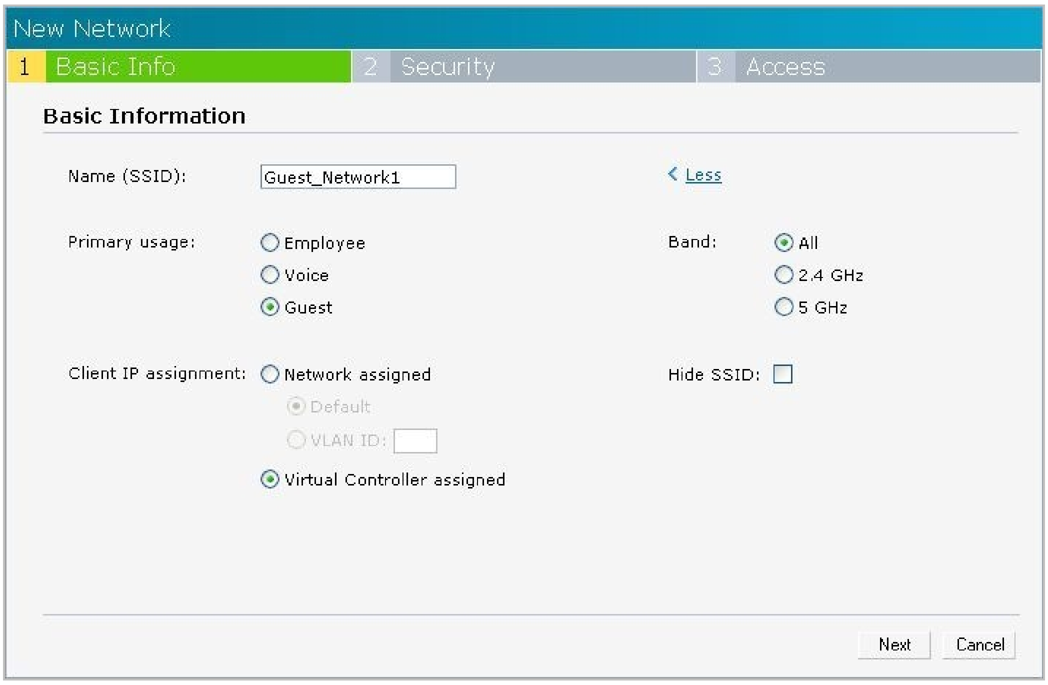
The Guest wireless network is created for guests, visitors, contractors, and any non-employee users who will use the enterprise Wi-Fi network. The virtual controller assigns the IP address for the guest clients. Captive portal or passphrase based authentication methods can be set for this wireless network. Typically, a guest network is an unencrypted network. However, you can specify encryption settings in the **Security** tab (see step 5 of the following procedure).

Adding a Guest Network

This section provides the procedure to add a guest network.

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

Figure 32 *Adding a Guest Network – Basic Info Tab*



Basic Information

Name (SSID): Guest_Network1

Primary usage: ○ Employee ○ Voice ● Guest

Band: ● All ○ 2.4 GHz ○ 5 GHz

Client IP assignment: ○ Network assigned (● Default ○ VLAN ID:) ● Virtual Controller assigned

Hide SSID: □

2. In the **Basic Info** tab, perform the following steps:
   a. Type a name for the network in the **Name (SSID)** text box.
   b. Select the Guest radio button from the **Primary usage** options. This selection determines the primary usage of the network being added.

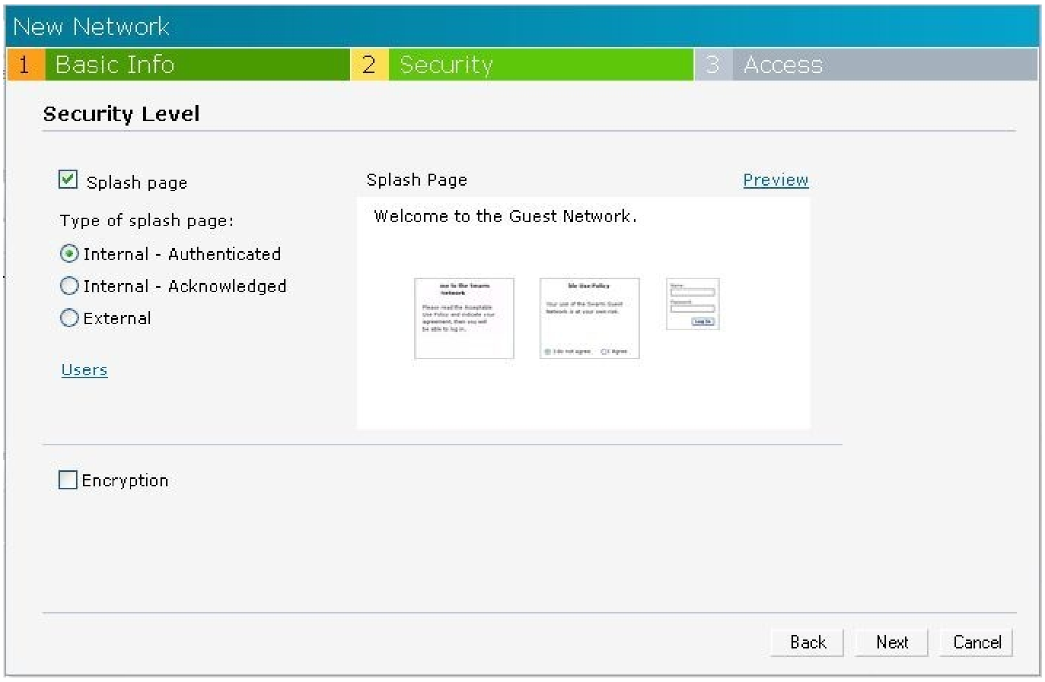
   The **Client IP assignment** selection automatically changes to **Virtual Controller assigned**. The virtual controller creates a private subnet and VLAN for the IAPs and the wireless clients. The virtual controller NATs all traffic out of this interface. For more information, see Guest DMZ.

3. Click the **More** link and perform the following steps (These steps are optional).
   a. **Band** - Set the band at which the network will transmit radio signals. Available options are **All, 2.4 GHz, and 5 GHz**. The **All** option is selected by default. It is also the recommended option.
   b. **Hide SSID** - Select this check box if you want to hide the SSID (network name) from the users.
4. Click **Next**. The **Security** tab appears. This tab allows you to configure the captive portal page for the Guest network. Select one of the following splash page type:

Splash Page Type	Description and steps to set up
Internal - Authenticated	A user has to accept the terms and conditions and enter a username and password on the captive portal page. If this option is selected, then add the users who are required to use the captive portal authentication to the user database. Click the **Users** link to add the users. For information about adding a user, see Adding a User. For information on customizing the splash page, see Customizing a Splash Page.
Internal - Acknowledged	A user has to accept the terms and conditions for this splash page type. For information on customizing the splash page, see Customizing a Splash Page.
External	An external server will be used to display the splash page to the user. If this option is selected, then do the following: 1. Enter the IP or hostname of the external server in the **IP or hostname** text box. 2. Enter the URL of the captive portal page in the **URL** text box. 3. Enter the number of the port to be used for communicating with the external server in the **Port** text box. 4. In the **Authentication** text box, enter the unique signature that the external server will return in the response after a successful user authentication.

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

Figure 33 *Adding a Guest Network – Splash Page Settings*



Security Level

☑ Splash page

Type of splash page:

● Internal - Authenticated

○ Internal - Acknowledged

○ External

Users

Splash Page

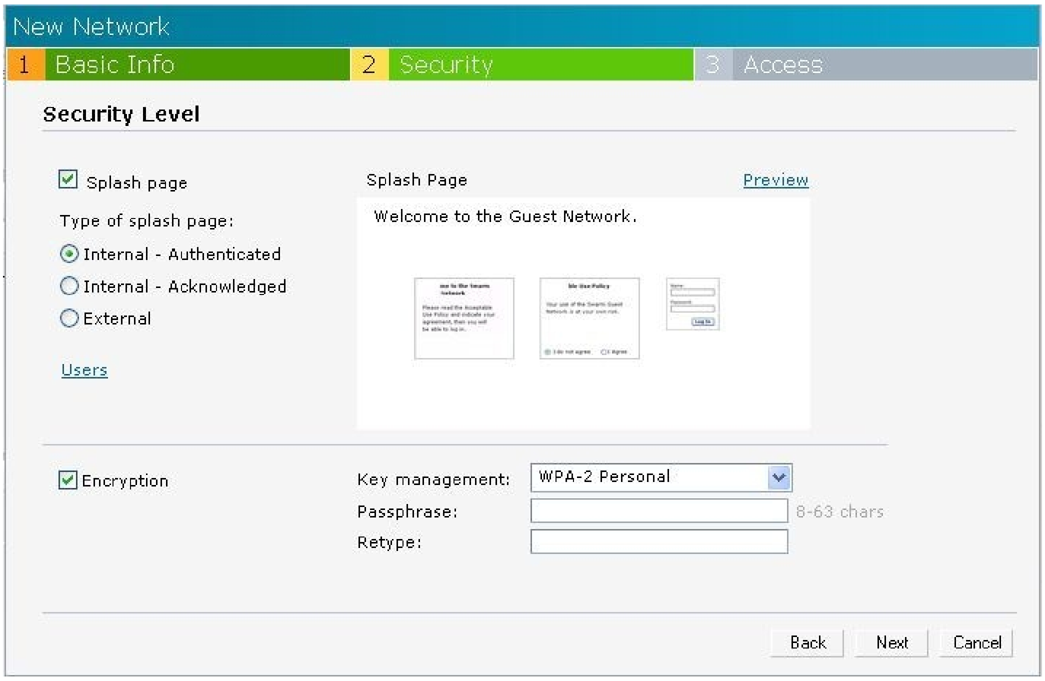
Welcome to the Guest Network.

□ Encryption

5. Select the **Encryption** check box and perform the following steps (This step is optional):
   a. Select the required key management option from the **Key management** drop-down list. Available options are:
      - WPA-2 Personal
      - WPA Personal
      - Both (WPA-2 & WPA)
      - Static WEP. If you selected Static WEP, then do the following:
        i. Select the appropriate WEP key size from the **WEP key size** drop-down list. Available options are 64-bit and 128-bit.
        ii. Select the appropriate Tx key from the **Tx Key** drop-down list. Available options are 1,2,3, and 4.
        iii. Enter an appropriate WEP key in the **WEP Key** text box and reconfirm.

iv. Enter a passphrase in the **Passphrase** text box and reconfirm.

Figure 34 *Configuring a Splash Page – Encryption Settings*



Security Level

☑ Splash page

Type of splash page:

● Internal - Authenticated

○ Internal - Acknowledged

○ External

Users

Splash Page Preview

Welcome to the Guest Network.

☑ Encryption

Key management: WPA-2 Personal

Passphrase: 8-63 chars

Retype:

6. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. InstantFirewall treats packets based on the first rule matched. For more information, see InstantFirewall.

   To edit the default rule, perform the following steps:

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

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

   To define an access rule, perform the following steps:

   a. Click the **New** button,

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

   c. Click **OK**.

7. Click **Finish**.

Editing a Network

To edit a network, perform the following steps:

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

Deleting a Network

To delete a network, perform the following steps:

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

Chapter 5
Managing IAPs

The Aruba Instant network supports up to 16 IAPs. This chapter describes the auto join mode feature in Aruba Instant, provides procedures for adding and removing IAPs, editing the IAP settings, and upgrading the firmware on the IAP using the Instant UI.

Auto Join Mode

The Auto Join Mode feature allows the IAPs to automatically,

1. Discover the virtual controller.
2. Join the network.
3. Begin functioning.

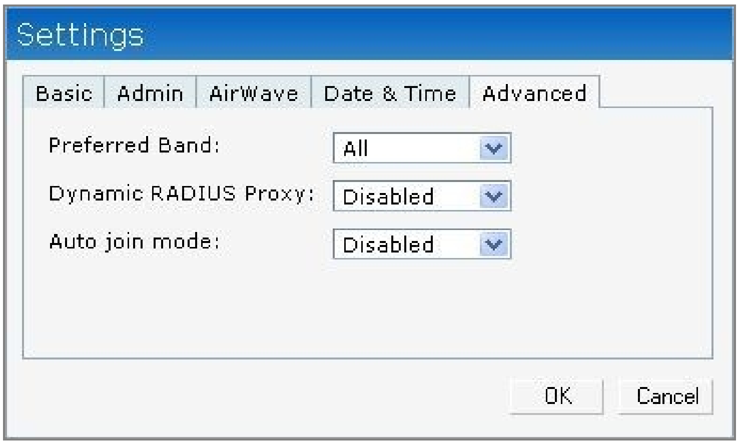
The Auto Join Mode feature is enabled by default. When the Auto Join Mode feature is disabled, a **New** link appears in the **Access Points** tab. Click this link to add IAPs to the network. For more information, see Adding an IAP to the Network. Also, when this feature is disabled, IAPs that are configured but not active appear in red.

Disabling Auto Join Mode

To disable Auto Join Mode, perform the following steps:

1. At the top right corner of Instant UI, click the **Settings** link. The **Settings** box appears.
2. In the **Settings** box, click the **Advanced** tab.
3. Select **Disabled** from the **Auto join mode** drop-down list.

Figure 35 *Disabling Auto Join Mode*



Preferred Band: All

Dynamic RADIUS Proxy: Disabled

Auto join mode: Disabled

4. Click **OK**.

Adding an IAP to the Network

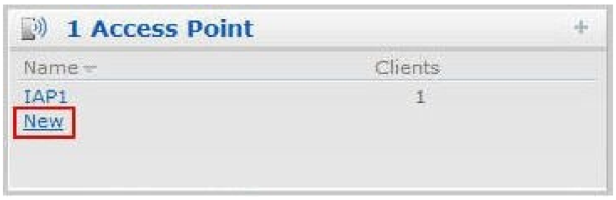
To add an IAP to the Aruba Instant network, assign an IP address. For more information, see Assigning an IP address to the IAP.

After an IAP is connected to the network, if the Auto Join Mode feature is enabled, it is listed in the **Access Points** tab in the Instant UI. The IAP inherits the configuration and image from the virtual controller.

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

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

Figure 36 *Adding an IAP to the Instant Network*

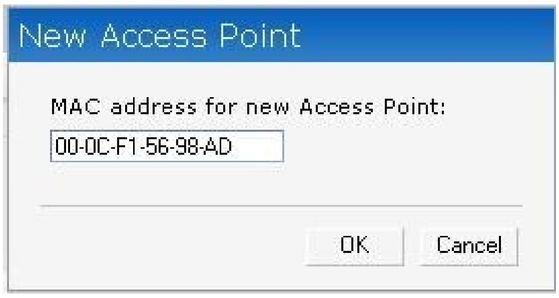


1 Access Point

Name	Clients
IAP1	1
New	

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

Figure 37 *Entering MAC Address for the New IAP*



New Access Point

MAC address for new Access Point: 00-0C-F1-56-98-AD

3. Click **OK.**

Removing an IAP from the Network

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

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

Editing IAP Settings

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

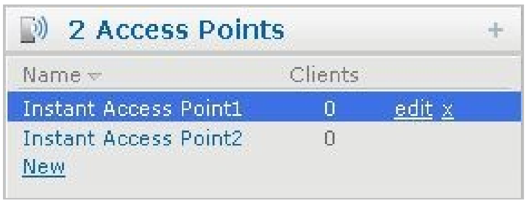
- Name
- IP Address
- Adaptive Radio Configuration (ARM)
- External Antenna Configuration
- Migrating from a Virtual Controller Managed to Mobility Controller Managed

Changing IAP Name

To change the IAP name, perform the following steps:

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

Figure 38 *Editing IAP Settings*

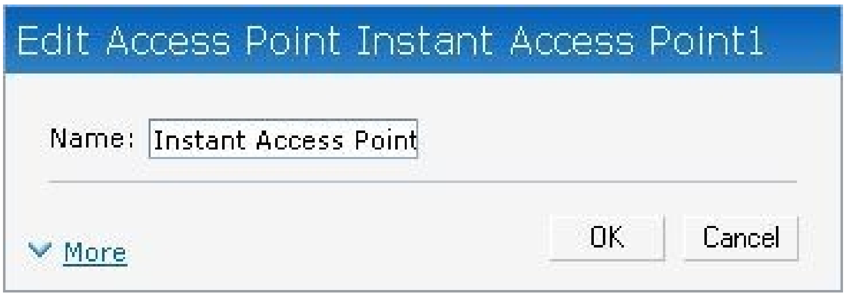


2 Access Points

Name	Clients	
Instant Access Point1	0	edit x
Instant Access Point2	0	
New		

2. Click the **edit** link.

Figure 39 *Changing IAP Name*



Edit Access Point Instant Access Point1

Name: Instant Access Point

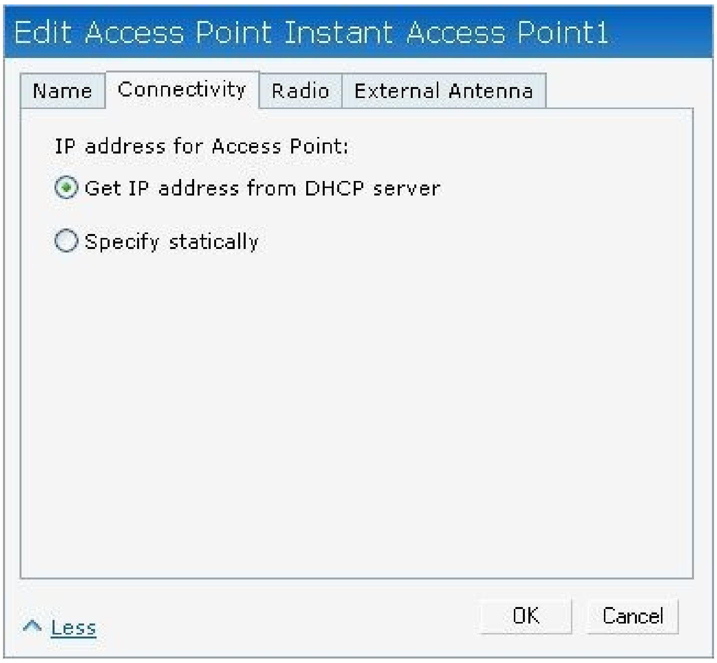
3. Edit the IAP name in the **Name** text box.
4. Click **OK**.

Changing IP Address of the IAP

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

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

Figure 40 *Configuring IAP Settings – Connectivity Tab*



IP address for Access Point:

● Get IP address from DHCP server

○ Specify statically

5. Select the **Get IP address from DHCP server** or **Specify statically** option. If you selected the **Specify statically** option, perform the following steps:

   a. Enter the new IP address for the IAP in the **IP address** text box.

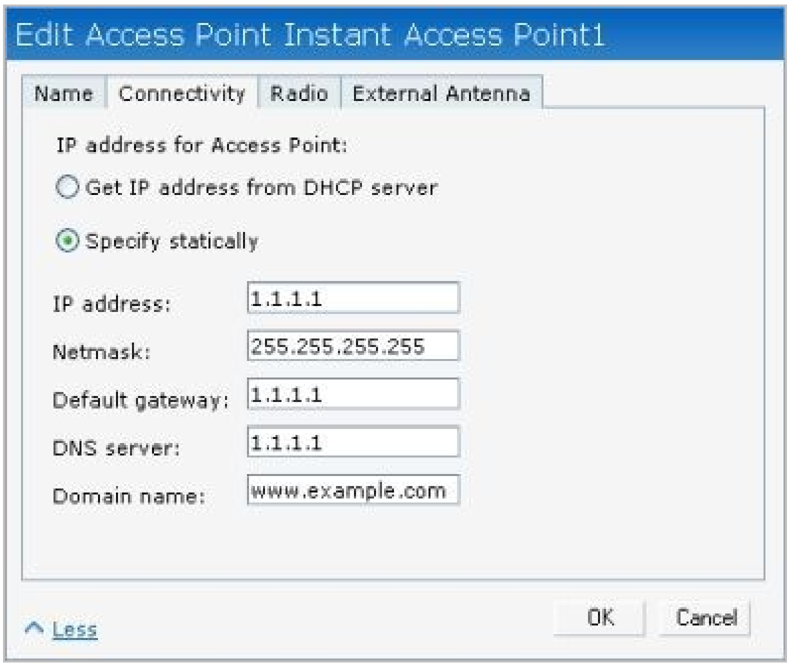
   b. Enter the netmask of the network in the **Netmask** text box.

   c. Enter the IP address of the default gateway in the **Default gateway** text box.

   d. Enter the IP address of the DNS server in the **DNS server** text box.

   e. Enter the domain name in the **Domain name** text box.

Figure 41 *Configuring IAP Connectivity Settings – Specifying Static Settings*



IP address for Access Point:

○ Get IP address from DHCP server

● Specify statically

IP address: 1.1.1.1

Netmask: 255.255.255.255

Default gateway: 1.1.1.1

DNS server: 1.1.1.1

Domain name: www.example.com

6. Click **OK.**

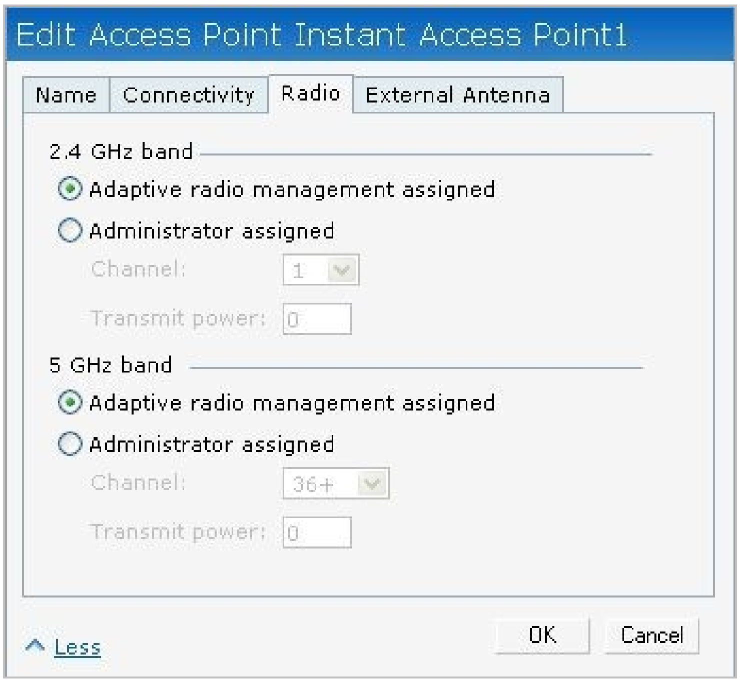
Configuring Adaptive Radio Management

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

To configure ARM, perform the following steps:

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

Figure 42 *Configuring IAP Radio Settings*



2.4 GHz band

● Adaptive radio management assigned

○ Administrator assigned

Channel: 1

Transmit power: 0

5 GHz band

● Adaptive radio management assigned

○ Administrator assigned

Channel: 36+

Transmit power: 0

6. Click **OK.**

Configuring an External Antenna

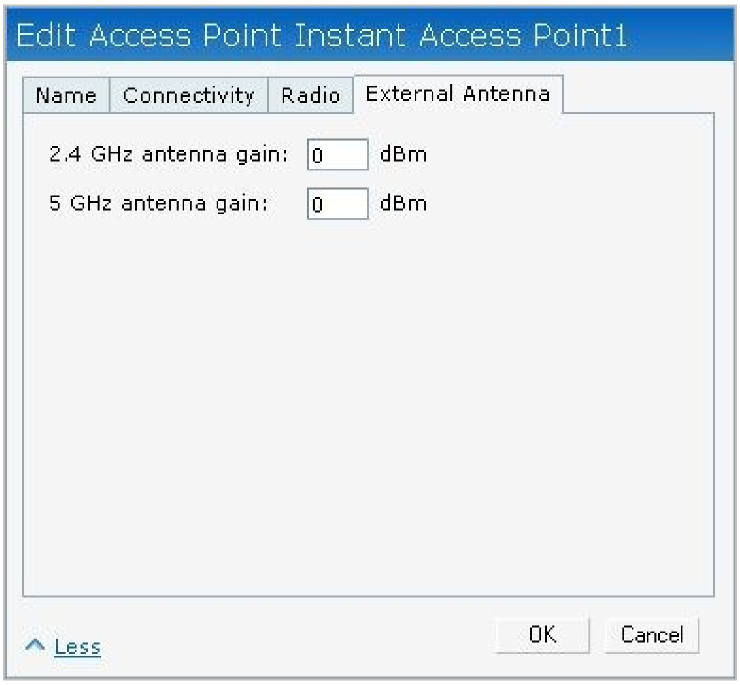
To configure an external antenna for an IAP, perform the following steps:

NOTE

Only IAP 92 supports external antenna configuration. Skip this section, if you are using IAP 93 or IAP 105. For appropriate configuration values, see the relevant *IAP documentation.*

1. In the **Access Points** tab, click the IAP for which you want to configure an external antenna. The **edit** link appears.
2. Click the **edit** link. The **Edit AP** box appears.
3. In the **Edit AP** box, click the **More** link.
4. Click the **External Antenna** tab and specify appropriate values.

Figure 43 *Configuring IAP External Antenna Settings*



2.4 GHz antenna gain: 0 dBm

5 GHz antenna gain: 0 dBm

5. Click **OK**.

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

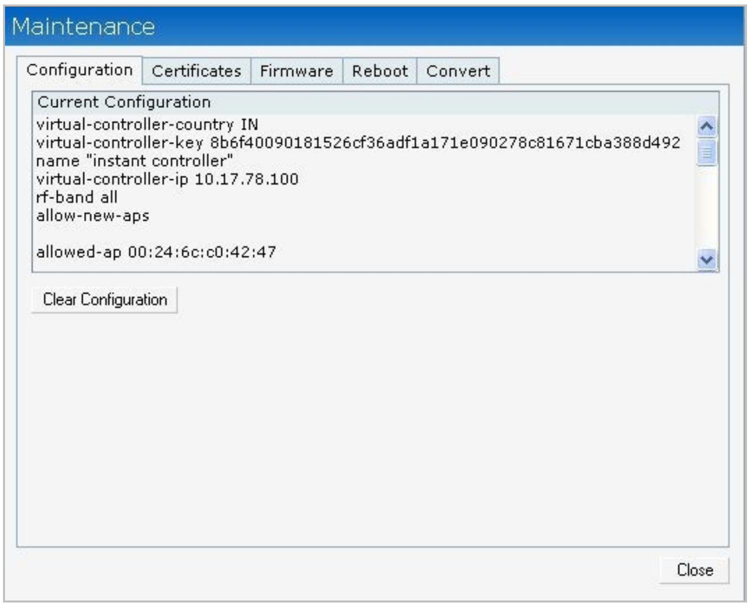
An IAP can be converted to an ArubaOS Campus AP. You have to configure the IP address of the controller in the Instant UI. Before converting the IAP, ensure that both the IAP and controller are configured to operate in the same regulatory domain. After conversion the IAP acts as an ArubaOS Campus AP.

CAUTION

Migrating from a virtual controller managed network to mobility controller managed network is a one way transition. An ArubaOS Campus AP cannot be converted to an IAP.

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

Figure 44 *Maintenance Box*



Maintenance

Configuration | Certificates | Firmware | Reboot | Convert

Current Configuration

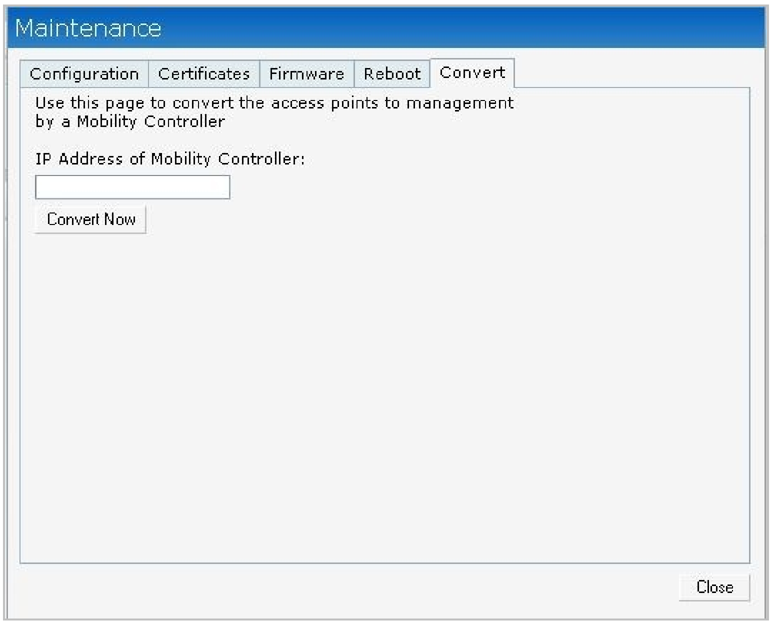
```
virtual-controller-country IN
virtual-controller-key 8b6f40090181526cf36adf1a171e090278c81671cba388d492
name "instant controller"
virtual-controller-ip 10.17.78.100
rf-band all
allow-new-aps

allowed-ap 00:24:6c:c0:42:47
```

Clear Configuration

Close

2. Click the **Convert** tab.

Figure 45 *Maintenance – Convert Tab*



Maintenance

Configuration | Certificates | Firmware | Reboot | Convert

Use this page to convert the access points to management by a Mobility Controller

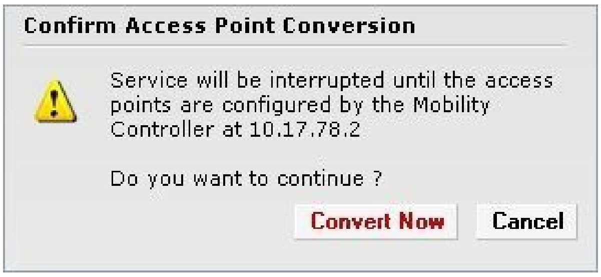
IP Address of Mobility Controller:

Convert Now

Close

3. Enter the IP address of mobility controller in the **IP Address of Mobility Controller** text box.
4. Click **Convert Now**. Confirm the conversion in the **Confirm Access Point Conversion** box.

Figure 46 *Confirm Access Point Conversion Box*



Confirm Access Point Conversion

Service will be interrupted until the access points are configured by the Mobility Controller at 10.17.78.2

Do you want to continue ?

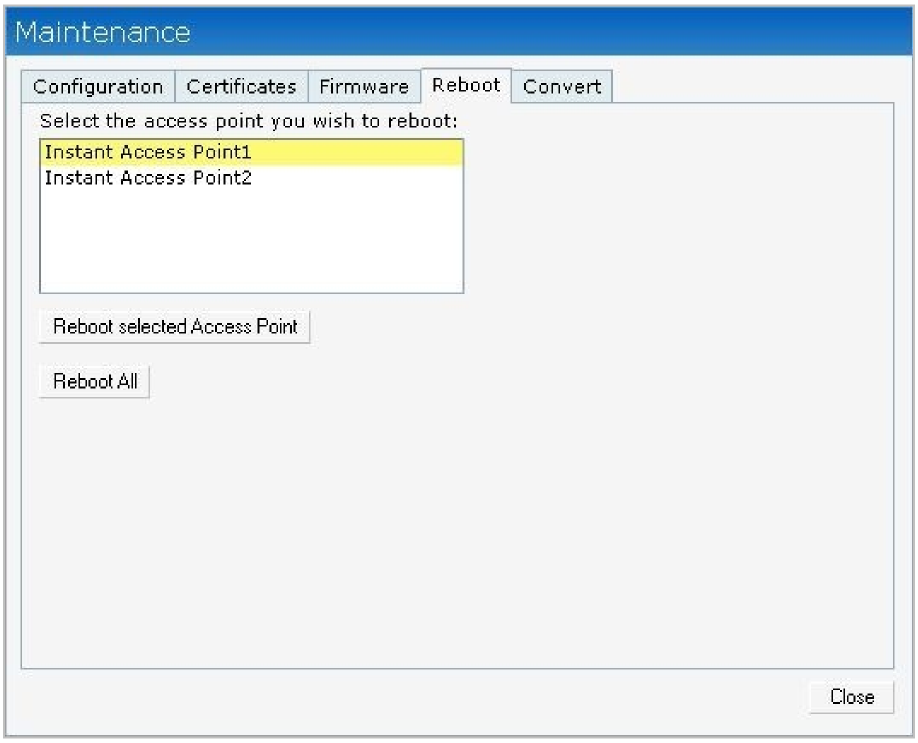
5. Click **Close**.

Rebooting the IAP

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

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

Figure 47 *Rebooting the IAP*



Select the access point you wish to reboot:

Instant Access Point1
Instant Access Point2

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. Click **Close**.

Firmware Image Server in Cloud Network

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

Automatic Firmware Image Check and Upgrade

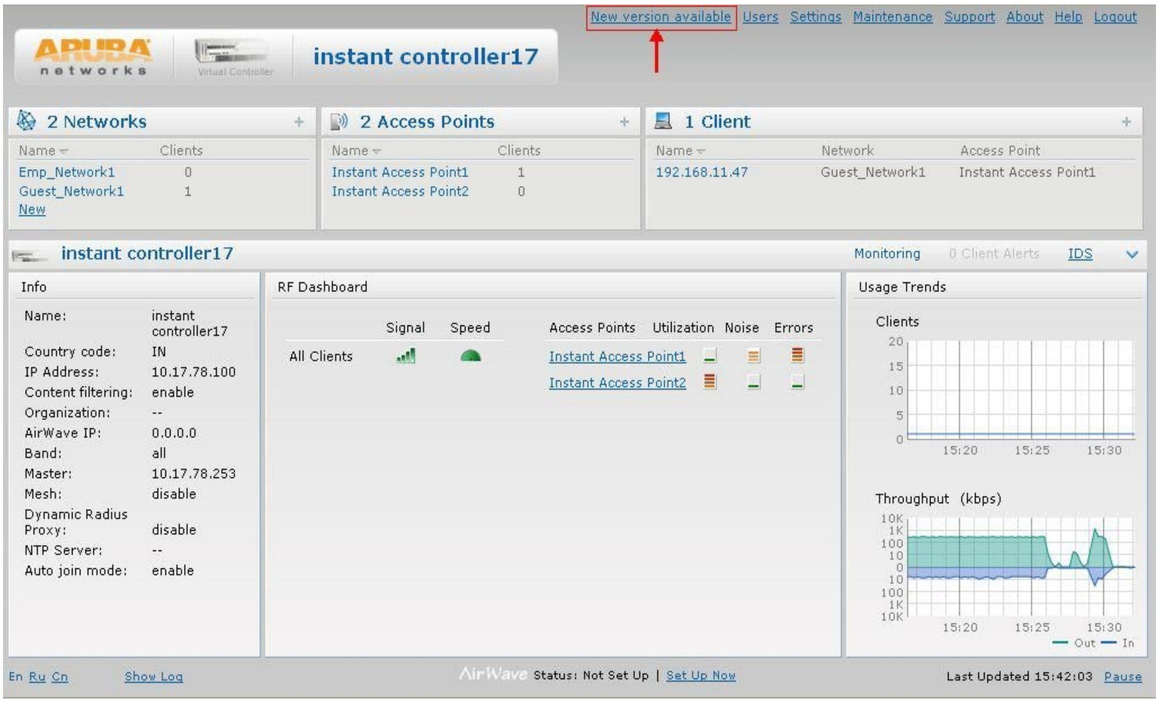
Automatic image check is enabled by default. If AirWave is configured, then the automatic image check is automatically disabled. You have to use the manual image check option. For more information, see Manual Firmware Image Check and Upgrade.

If Automatic image check is enabled, then it is performed:

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

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

Figure 48 *Automatic Image Check – New Version Available Link*



Name	Clients
Emp_Network1	0
Guest_Network1	1
New	

Name	Clients
Instant Access Point1	1
Instant Access Point2	0

Name	Network	Access Point
192.168.11.47	Guest_Network1	Instant Access Point1

Info

Name:	instant controller17
Country code:	IN
IP Address:	10.17.78.100
Content filtering:	enable
Organization:	--
AirWave IP:	0.0.0.0
Band:	all
Master:	10.17.78.253
Mesh:	disable
Dynamic Radius Proxy:	disable
NTP Server:	--
Auto join mode:	enable

RF Dashboard

	Signal	Speed
All Clients		

Access Points	Utilization	Noise	Errors
Instant Access Point1			
Instant Access Point2			

Status: Not Set Up | Set Up Now

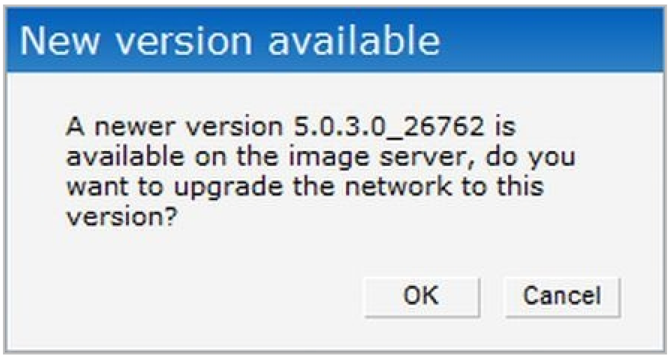
Last Updated 15:42:03

Upgrading to the new OS version

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

1. Click the **New version available** link.
2. Click **OK** in the confirmation box.

Figure 49 *New Version Available Box*



New version available

A newer version 5.0.3.0_26762 is available on the image server, do you want to upgrade the network to this version?

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

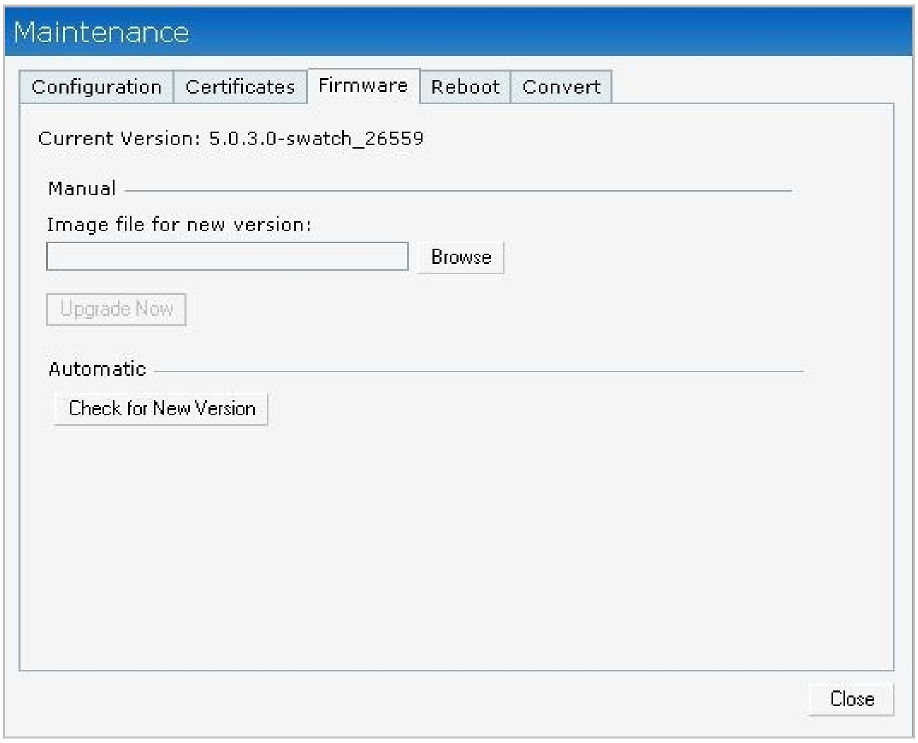
- Upgrading – While image upgrading is in progress.
- Upgrade successful – When the upgrading is successful.
- Upgrade fail – When the upgrading fails.

Manual Firmware Image Check and Upgrade

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

1. Click the **Maintenance** link at the top right of the Instant UI.
2. In the **Maintenance** box, click the **Firmware** tab.

Figure 50 *Manual Image Check*



Current Version: 5.0.3.0-swatch_26559

3. In the **Firmware** tab, click the **Check for New Version** button.

   After the image check is completed, one of the following messages will appear:

   - No new version available – If there is no new version available.
   - Image server timed out – Connection or session between the image server and the IAP is timed out.
   - Image server failure – If the image server does not respond.
   - A new image version found – If a new image version is found.
4. If a new version is found, the **Upgrade Now** button appears and the **New version available** message and the version number are displayed.
5. Click the **Upgrade Now** button.

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

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

Chapter 6
NTP Server

This chapter provides information about the Network Time Protocol Server.

NTP Server Overview

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

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

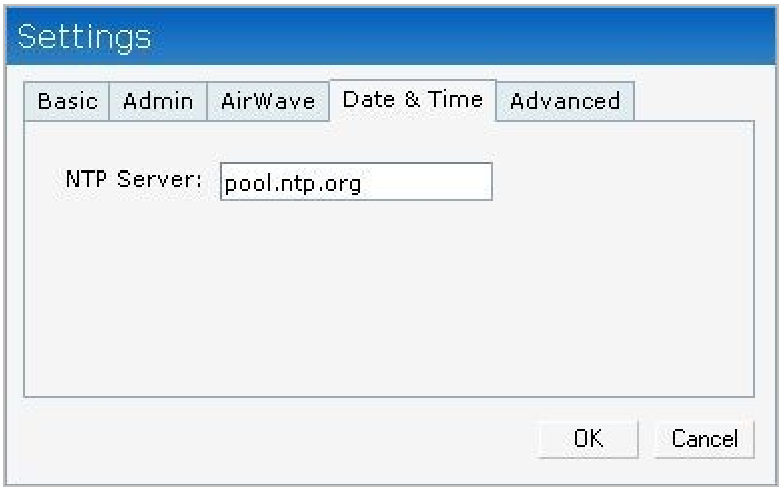
Network Time Protocol (NTP) is required to obtain the precise time from a server and to regulate the local time in each network element. If NTP server is not configured in the Aruba Instant network, an IAP reboot may lead to variation in time and data.

Configuring an NTP Server

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

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

Figure 51 *Configuring NTP Server*



NTP Server: pool.ntp.org

Chapter 7
Virtual Controller

This chapter provides information about the virtual controller in the Aruba Instant network.

Virtual Controller Overview

Aruba Instant does not require an external controller to regulate and manage the Wi-Fi network. Any IAP in the Aruba Instant network dynamically takes up the role of a Virtual Controller (VC) without impacting the network. It coordinates, stores, and distributes all the settings required to provide a centralized functionality to regulate and manage the Wi-Fi network. The virtual controller also functions like any other AP with full RF scalability. It also acts as a node, coordinating DHCP address allocation for network address translated clients ensuring mobility of the clients when they roam between different IAPs.

Master Election Protocol

The Aruba Instant network supports 16 IAPs without any external controller. However, there is a need to manage the network. The Master Election Protocol enables the Aruba Instant network to dynamically elect an IAP to take on a VC role, allow graceful failover to a new virtual controller when the existing VC is down, and avoid race conditions. This protocol ensures stability of the network during initial startup or when the VC goes down by allowing only one IAP to self-elect as a VC.

Virtual Controller IP Address

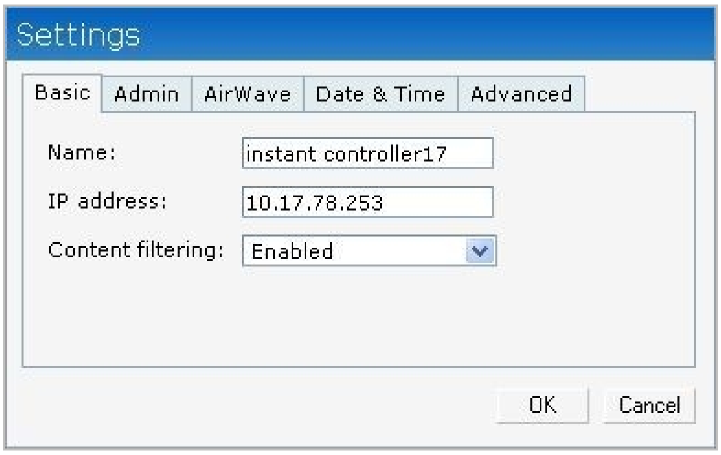
You can specify a single static IP address that can be used to manage a multi-AP Aruba Instant network. This IP address is automatically provisioned on a shadow interface on the IAP that takes the role of a virtual controller. When an IAP becomes a virtual controller, it sends three Address Resolution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

Specifying Name and IP Address for the Virtual Controller

To change name and IP address of virtual controller, perform the following steps:

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

Figure 52 *Specifying Virtual Controller Name and IP Address*



Settings

Name: instant controller17

IP address: 10.17.78.253

Content filtering: Enabled

2. Enter a name for virtual controller in the **Name** text box.
3. Enter the appropriate IP address in the **IP address** text box.
4. Click **OK**.

Aruba Networks Instant User Guide

Chapter 8
Authentication

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

Authentication Methods in Aruba Instant

The following authentication methods are supported in Aruba Instant:

- 802.1X Authentication
- Captive Portal
- MAC Authentication

802.1X Authentication

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

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

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

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

NOTE

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

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

Internal RADIUS Server

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

- EAP-TTLS (MSCHAPv2) - The EAP-TTLS (Tunneled Transport Layer Security) method uses server-side certificates to set up authentication between clients and servers. However, the actual authentication is performed using passwords.

- EAP-PEAP (MSCHAPv2) - Protected 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 mutual authentication between the client and authentication server.

CAUTION

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

External RADIUS Server

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

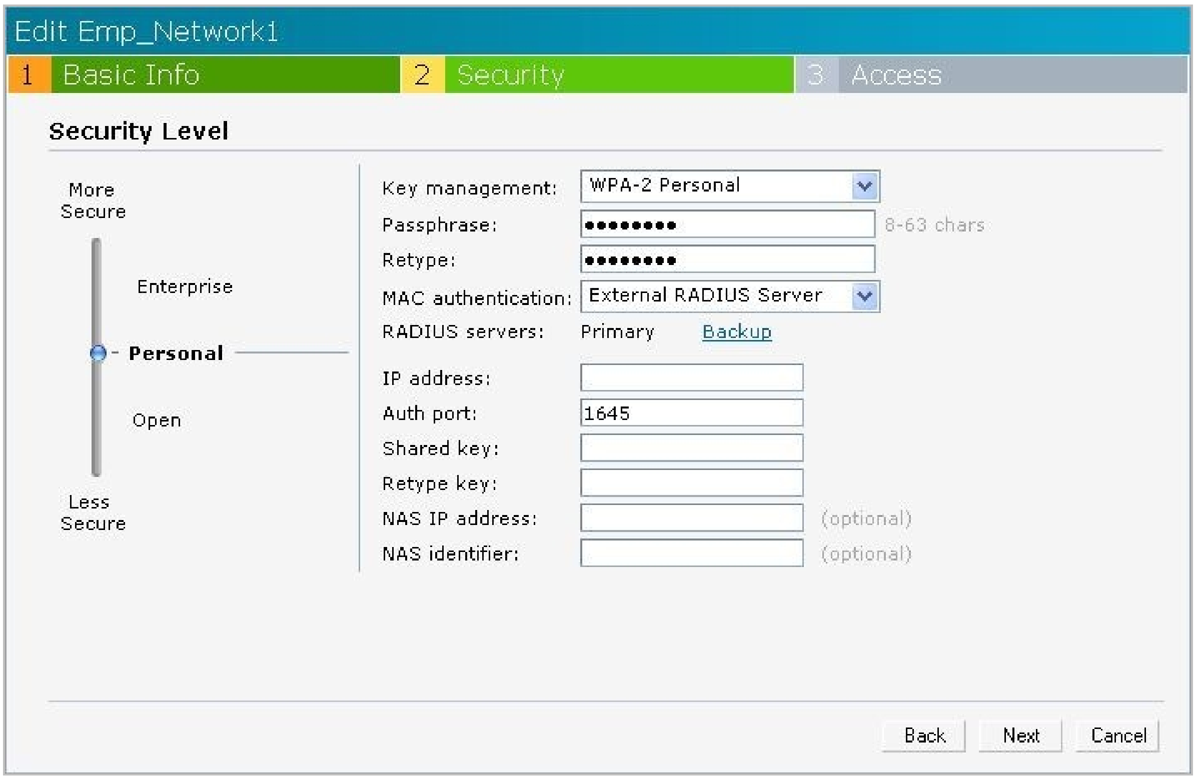
InstantRADIUS dynamically forwards authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an Access-Accept or Access-Reject message. Users are allowed or denied access to the network depending on the response from the RADIUS server.

Configuring an External RADIUS Server

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

1. In the **Network** tab, click the network for which you want to configure the external RADIUS Server. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** box appears.
3. Click **Next** and perform the following tasks in the **Security** tab:
   a. For a network with **Personal** or **Open** security level, select **External Radius Server** from the **MAC Authentication** drop-down list.
   b. Click the **Primary** link and perform the following steps:
      i. Enter the IP address of the external RADIUS server in the **IP address** text box.
      ii. Enter the authorization port number of the external RADIUS server in the **Auth Port** text box. The port number is set to 1645 by default.
      iii. Enter a shared key for communicating with the external RADIUS server in the **Shared key** text box.
      iv. Enter the virtual controller IP address in the **NAS IP address** text box. The NAS IP address is the virtual controller IP address that is sent in the data packets.
   c. Click the **Backup** link and set appropriate values for the backup RADIUS server.

Figure 53 *Configuring External Radius Server*



Edit Emp_Network1

Security Level

Key management: WPA-2 Personal

Passphrase: •••••••• 8-63 chars

Retype: ••••••••

MAC authentication: External RADIUS Server

RADIUS servers: Primary Backup

IP address:

Auth port: 1645

Shared key:

Retype key:

NAS IP address: (optional)

NAS identifier: (optional)

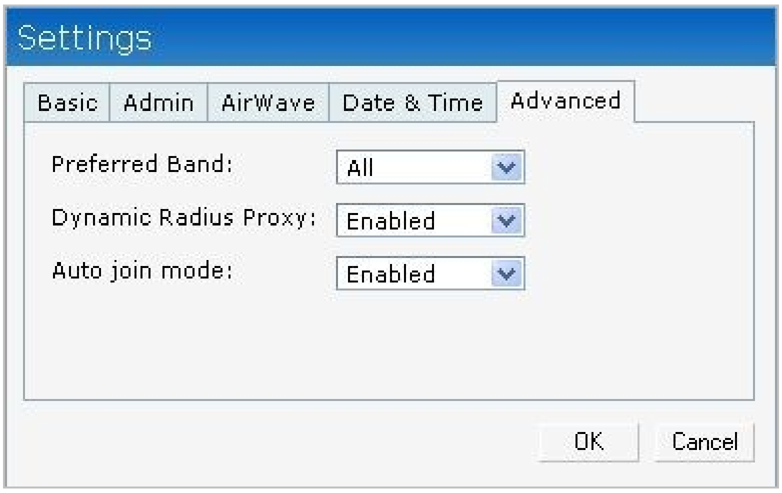
4. Click **Next** and click **Finish**.

Enabling InstantRADIUS

To enable InstantRADIUS, perform the following steps:

1. At the top right corner of the Instant UI, click the **Settings** link.
2. In the **Settings** box, click the **Advanced** tab.
3. Select **Enabled** from the **Dynamic RADIUS Proxy** drop-down list.

Figure 54 *Enabling Instant RADIUS*



Settings

Preferred Band: All

Dynamic Radius Proxy: Enabled

Auto join mode: Enabled

4. Click **OK**.

Captive Portal

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

- Internal Captive Portal
- External Captive Portal

Internal Captive Portal

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

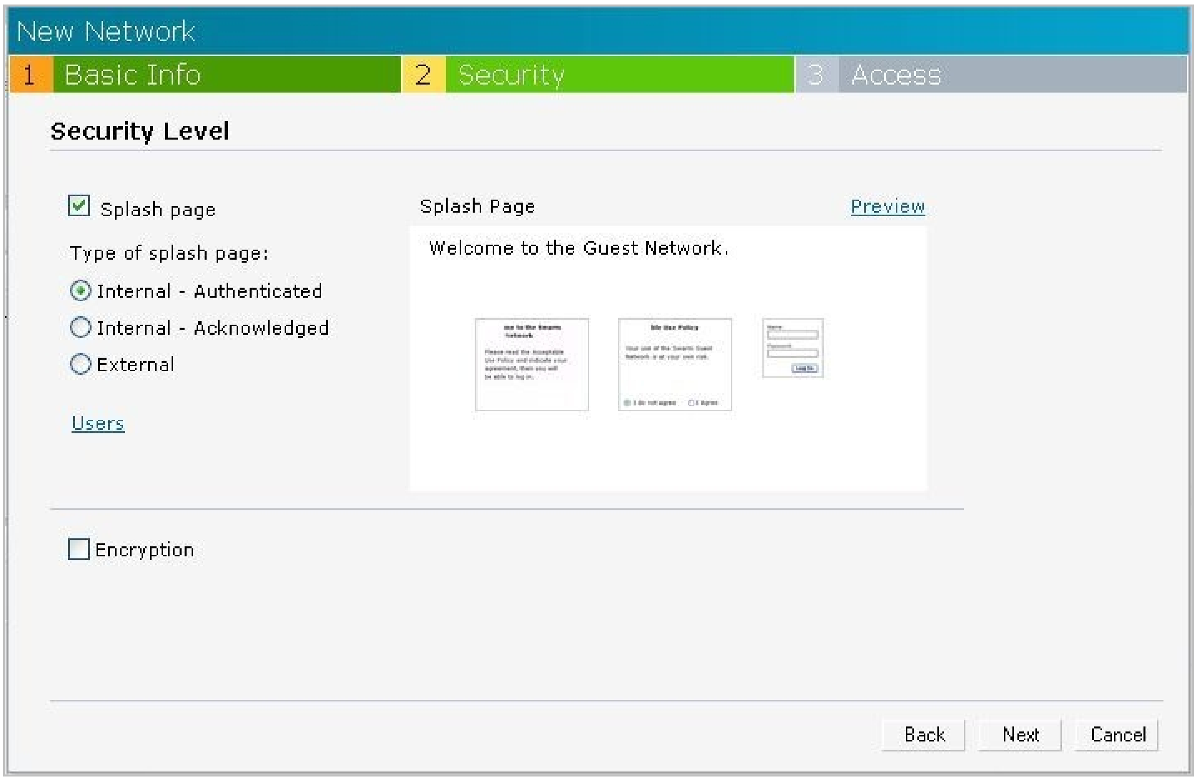
- Internal Authenticated - To gain access to the wireless network, a user must authenticate in the captive portal page. If this option is selected, then users who are required to authenticate have to be added to the user database. Click the **Users** link to add the users. For information about adding users, see Adding a User. Internal Authenticated is the recommended option.
- Internal Acknowledged - To gain access to the wireless network, a user must accept the terms and conditions.

Configuring Internal Captive Portal Authentication when Adding a Guest Network

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

1. In the **Network** tab, click the **New** link. The **New Network** box appears.
2. In the **Basic Info** tab, perform the following:
   a. Enter a name for the network in the **Name (SSID)** text box.
   b. Click the **Guest** radio button and click **Next**.
3. In the **Security** tab, select one of the following options for the splash page type:
   - **Internal - Authenticated**
   - **Internal - Acknowledged**

Figure 55 *Configuring Captive Portal when Adding a Guest Network*



New Network

1 Basic Info | 2 Security | 3 Access

Security Level

☑ Splash page

Type of splash page:

● Internal - Authenticated

○ Internal - Acknowledged

○ External

Users

Splash Page — Preview

Welcome to the Guest Network.

□ Encryption

The appearance of a splash page can be customized as required. For information on customizing a splash page, see Customizing a Splash Page.

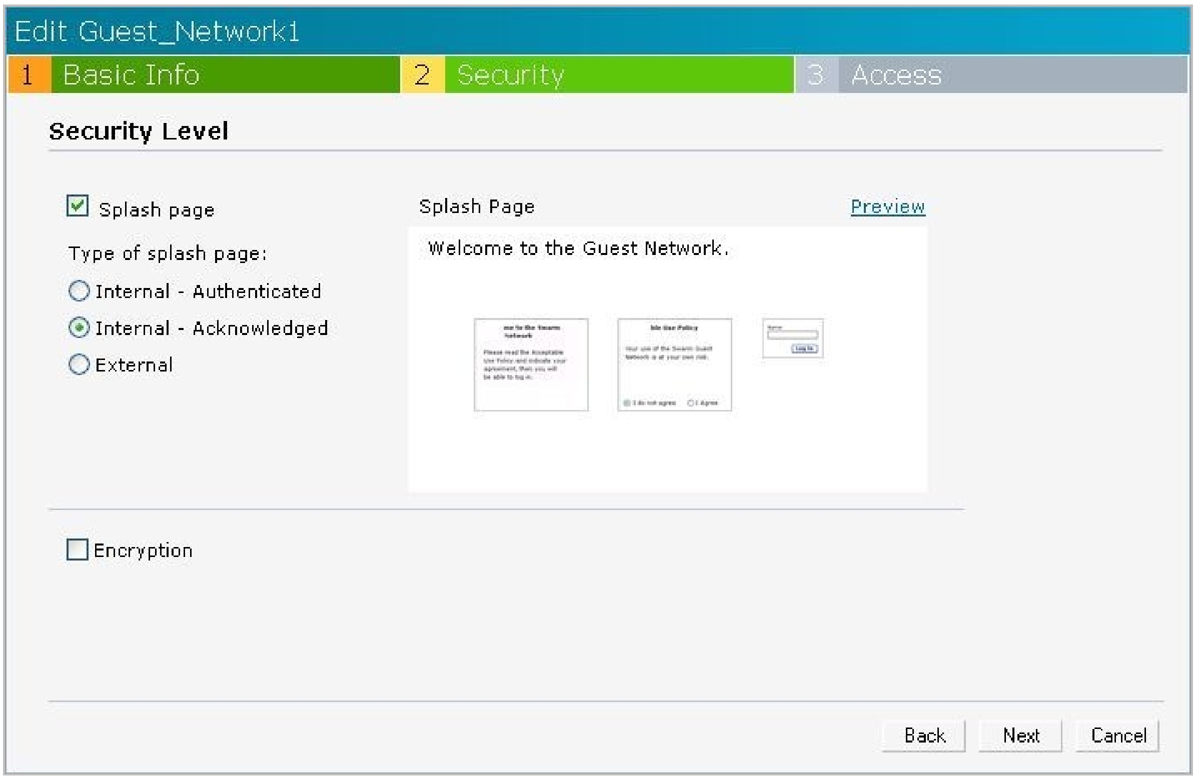
4. Click **Next** and click **Finish.**

Configuring Internal Captive Portal Authentication when Editing a Guest Network

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

1. In the **Network** tab, click the network for which you want to configure internal captive portal authentication. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** box for the network appears.
3. Click **Next** and select one of the following options for the splash page type in the **Security** tab:
   - **Internal - Authenticated**
   - **Internal - Acknowledged**

Figure 56 *Configuring Captive Portal when Editing a Guest Network*



Security Level

☑ Splash page

Type of splash page:

○ Internal - Authenticated

● Internal - Acknowledged

○ External

Splash Page

Welcome to the Guest Network.

□ Encryption

Depending on the requirement, splash pages can be customized. For information on customizing a splash page, see Customizing a Splash Page.

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

Customizing a Splash Page

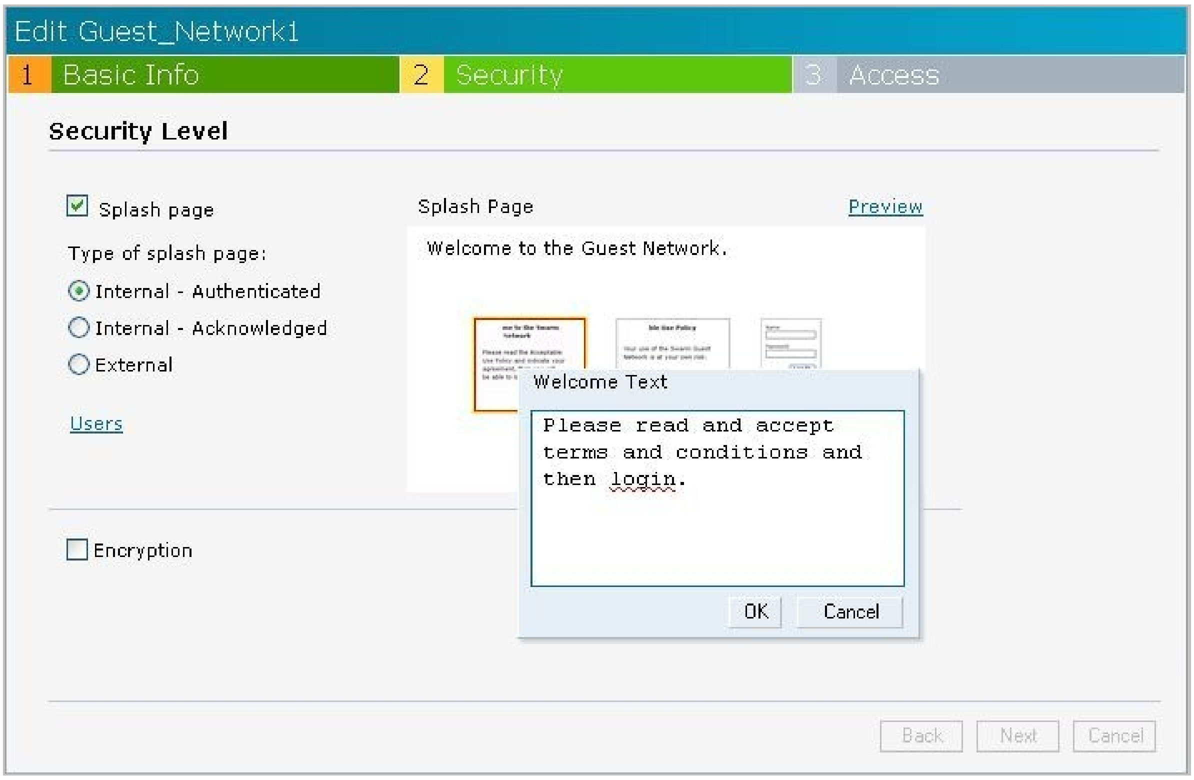
A splash page is a web page that is displayed to a guest user when they are trying to access the internet. The appearance of a splash page can be customized as required. To customize a splash page, perform the following steps:

1. In the **Network** tab, click the network for which you want to customize the splash page. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** box for the network appears.
3. Click **Next** and perform the following tasks in the **Security** tab:
    a. To change the color of the splash page, click the Splash page rectangle and select the required color from the Background Color palette.

    b. To change the welcome text, click the first square in the splash page, type the required text in the **Welcome** text box, and click **OK**. The welcome text should not exceed 127 characters.

    c. To change the policy text, click the second square in the splash page, type the required text in the **Policy** text box, and click **OK.** The policy text should not exceed 255 characters.

Figure 57 *Customizing a Splash Page*



Edit Guest_Network1

Security Level

☑ Splash page

Type of splash page:

● Internal - Authenticated

○ Internal - Acknowledged

○ External

☐ Encryption

Splash Page

Welcome to the Guest Network.

Welcome Text

Please read and accept terms and conditions and then login.

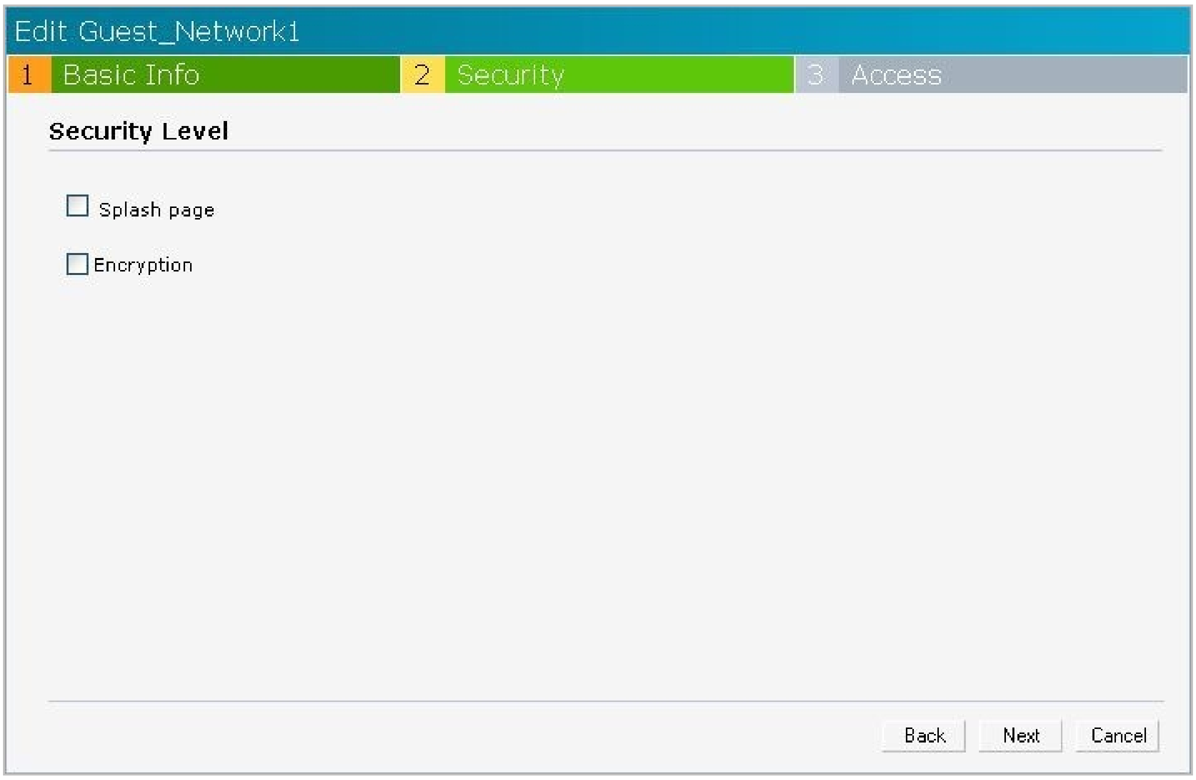
4. Click **Next** and click **Finish.**

Disabling Captive Portal authentication

To disable captive portal authentication, perform the following steps:

1. In the **Network** tab, click the network for which you want to disable captive portal authentication. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** box for the network appears.
3. Click **Next** and clear the **Splash page** check box in the **Security** tab.

Figure 58 *Disabling Captive Portal Authentication*



□ Splash page

□ Encryption

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

External Captive Portal

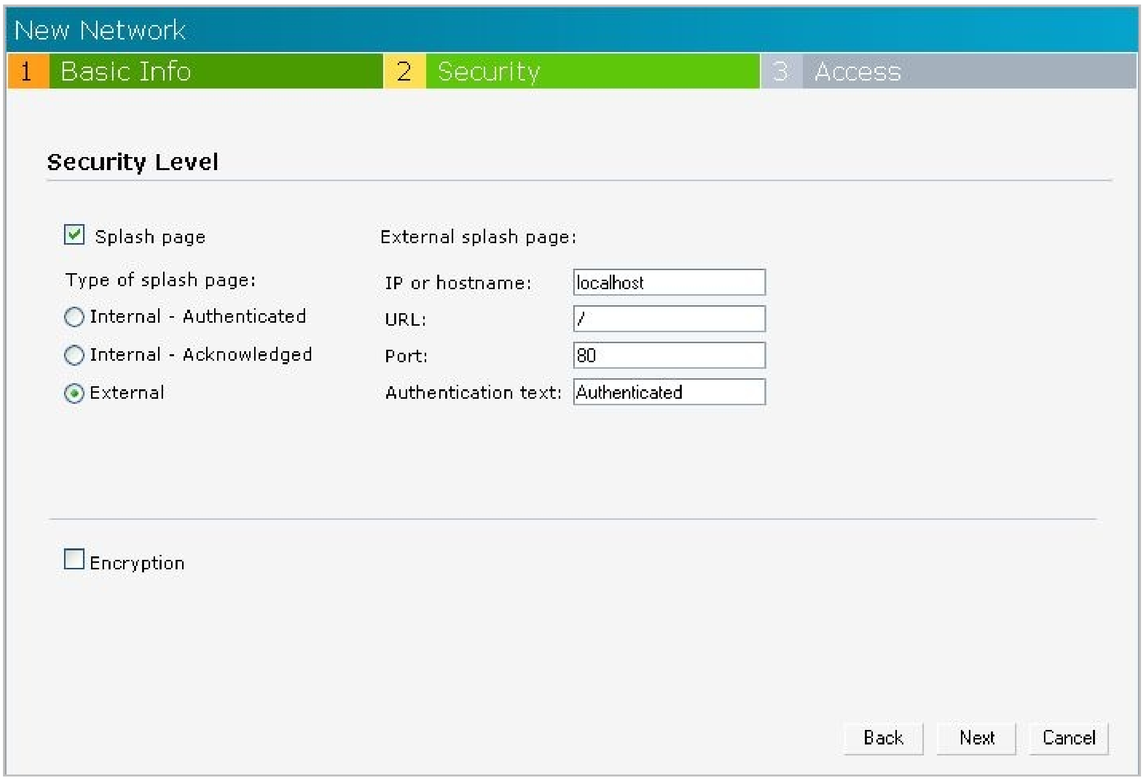
Aruba Instant supports external captive portal authentication. The external portal can be in a cloud or on a server outside the enterprise network.

Configuring External Captive Portal Authentication when Adding a Guest Network

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

1. In the **Network** tab, click the **New** link. The **New Network** box appears.
2. In the **Basic Info** tab, perform the following:
    a. Enter a name for the network in the **Name (SSID)** text box.
    b. Select the **Guest** radio button and click **Next.**
3. In the **Security** tab, click the **External** button and perform the following steps:
    a. Enter the IP address or the hostname in the **IP or hostname** text box.
    b. Enter the URL for the splash page in the **URL** text box.
    c. Enter the number of the port to be used for communicating with the external server in the **Port** text box.
    d. In the **Authentication** text box, enter the unique signature that the external server will return in the response after a successful authentication.

Figure 59 *Configuring External Captive Portal when Adding a Guest Network*



Security Level

☑ Splash page

Type of splash page:

○ Internal - Authenticated

○ Internal - Acknowledged

● External

External splash page:

IP or hostname:	localhost
URL:	/
Port:	80
Authentication text:	Authenticated

□ Encryption

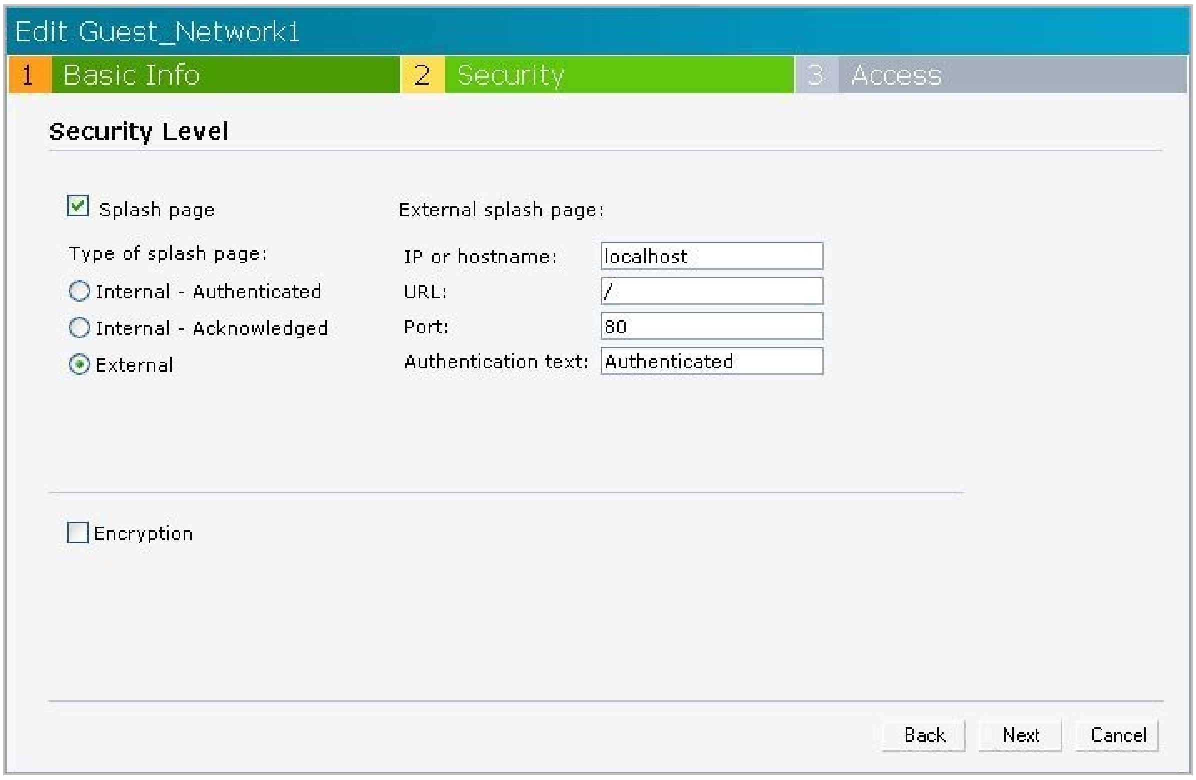
4. Click **Next** and click **Finish**.

Configuring External Captive Portal Authentication when Editing a Guest Network

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

1. In the **Network** tab, click the network for which you want to configure the external captive portal authentication. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** box for the network appears.
3. Click **Next** and click the **External** button. In the **Security** tab, perform the following steps:
    a. Enter the IP address or the hostname in the **IP or hostname** text box.
    b. Enter the URL for the splash page in the **URL** text box.
    c. Enter the number of the port to be used for communicating with the external server in the **Port** text box.
    d. In the **Authentication** text box, enter the unique signature that the external server will return in the response after a successful authentication.

Figure 60 Configuring External Captive Portal Authentication



Edit Guest_Network1

1 Basic Info | 2 Security | 3 Access

Security Level

☑ Splash page

Type of splash page:

○ Internal - Authenticated

○ Internal - Acknowledged

● External

External splash page:

IP or hostname: localhost

URL: /

Port: 80

Authentication text: Authenticated

□ Encryption

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

MAC Authentication

Media Access Control (MAC) authentication is used to authenticate devices based on their physical MAC addresses. It is an early form of filtering. MAC authentication requires that the MAC address of a machine must match a manually defined list of addresses. This form of authentication does not scale past a handful of devices, because it is difficult to maintain the list of MAC addresses. Additionally, it is easy to change the MAC address of a station to match one on the accepted list. This spoofing is trivial to perform with built-in driver tools, and it should not be relied upon to provide security.

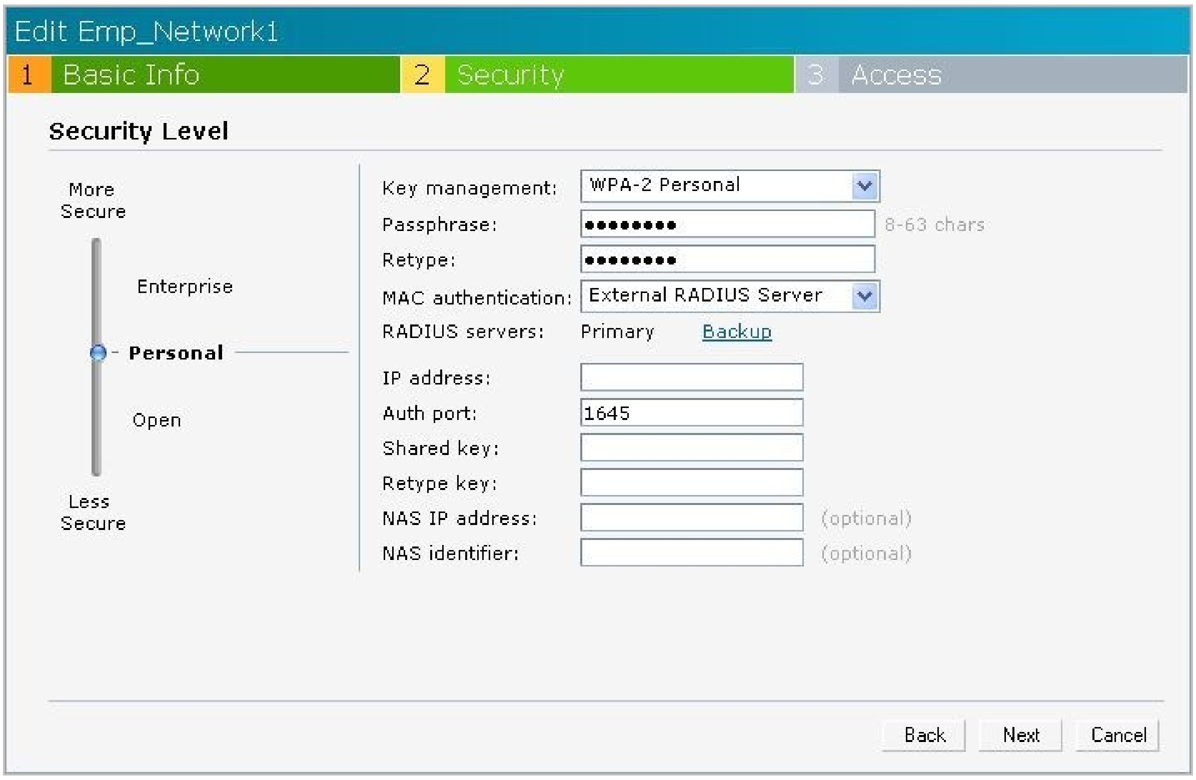
MAC authentication can be used alone, but typically it is combined with other forms of authentication, such as WEP authentication. Because MAC addresses are easily observed during transmission and easily changed on the client, this form of authentication should be considered nothing more than a minor hurdle that will not deter the determined intruder. Aruba recommends against the use of MAC based authentication.

Configuring MAC Authentication

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

1. In the **Network** tab, click the network for which you want to enable MAC authentication. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** box appears.
3. Click **Next**. In the **Security** tab, perform the following steps:
   a. For a network with **Personal** or **Open** security level, select **External Radius Server** from the **MAC Authentication** drop-down list.
   b. Click the **Primary** link and perform the following steps:
      - Enter the IP address of the external RADIUS server in the **IP address** text box.
      - Enter the authorization port number of the external RADIUS server in the **Auth Port** text box. The port number is set to 1645 by default.
      - Enter a shared key for communicating with the external RADIUS server in the **Shared key** text box.
      - Enter the virtual controller IP address in the **NAS IP address** text box. The NAS IP is the virtual controller IP address that is sent in the data packets.
   c. Click the **Backup** link and set appropriate values for the backup RADIUS server.

Figure 61 *Configuring MAC Authentication*



Key management: WPA-2 Personal

Passphrase: ●●●●●●●●● 8-63 chars

Retype: ●●●●●●●●●

MAC authentication: External RADIUS Server

RADIUS servers: Primary Backup

IP address:

Auth port: 1645

Shared key:

Retype key:

NAS IP address: (optional)

NAS identifier: (optional)

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

Certificates

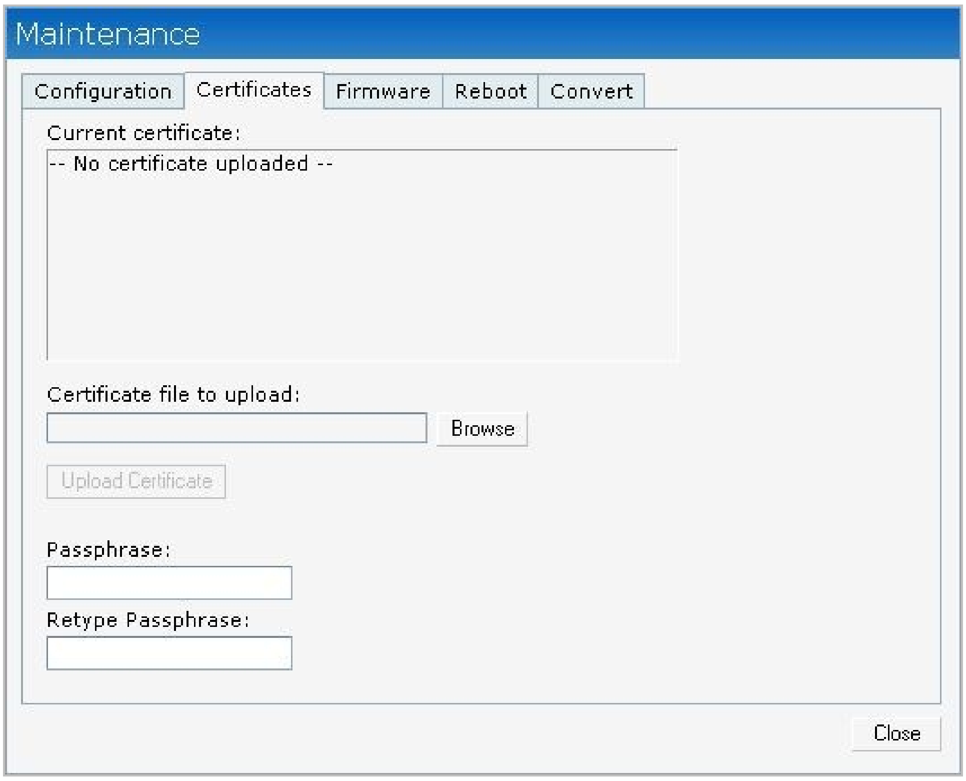
A certificate is a digital file that certifies the identity of the organization or products of the organization. It is also used to establish your credentials for any web transactions. It contains the organization name, a serial number, expiration date, a copy of the certificate-holder's public key,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

Loading Certificates

To load a certificate, perform the following steps:

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

Figure 62 *Loading Certificates*



Current certificate:
-- No certificate uploaded --

Certificate file to upload:

Passphrase:

Retype Passphrase:

3. Click the **Browse** button. Browse and select the appropriate certificate file, and click the **Upload Certificate** button.
4. Enter passphrase in the **Passphrase** text box and reconfirm.
5. Click **Close**.

Chapter 9 Encryption

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

Encryption Types Supported in Aruba Instant

The following encryption types are supported in Aruba Instant:

WEP

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

TKIP

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

AES

The Advanced Encryption Standard (AES) encryption algorithm is now widely supported and is the recommended encryption type for all wireless networks that contain any confidential data. AES in Wi-Fi leverages 802.1X or PSKs to generate per station keys for all devices. AES provides a high level of security, similar to what is used by IP Security (IPsec) clients. Aruba recommends that all devices be upgraded or replaced so that they are capable of AES encryption.

Encryption Recommendations

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

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

Understanding WPA and WPA2

The Wi-Fi Alliance created the Wi-Fi Protected Access (WPA) and WPA2 certifications to describe the 802.11i standard. The standard was written to replace WEP, which was found to have numerous security flaws. It was taking longer than expected to complete the standard, so WPA was created based on a draft of 802.11i, which allowed people to move forward quickly to create more secure WLANs. WPA2 encompasses the full implementation of the 802.11i standard. Table 2 summarizes the differences between the two certifications. WPA2 is a superset that encompasses the full WPA feature set. WPA and WPA2 can be further classified as follows:

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

Table 2 *WPA and WPA2 Features*

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

Recommended Authentication and Encryption Combinations

Table 3 summarizes the recommendations for authentication and encryption combinations that should be used in Wi-Fi networks.

Table 3 *Recommended Authentication and Encryption Combinations*

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

Chapter 10
Guest DMZ

This chapter provides information about the Guest DMZ feature in Aruba Instant.

Guest DMZ Overview

A De-Militarized Zone (DMZ) is a sub-network created between an internal network and an external network, for example, the Internet. The DMZ adds an extra layer of security to the network of an enterprise or organization. You can specify or select whether you want to segregate the guests from accessing your internal network or the external network, that is, the Internet. To apply the Guest DMZ feature for the networks that you create, select the **Virtual Controller assigned** option in the **Client IP Assignment** section while creating a network. When this option is selected, the virtual controller creates a private subnet and VLAN for the IAPs and wireless clients. The virtual controller NATs all traffic that passes out of this interface. This eliminates the need for complex VLAN and IP address management for a multi-site wireless network. Layer 2 multicast applications are not supported in the Guest DMZ (virtual controller assigned) networks. In Aruba Instant, Guest DMZ performs the following functions:

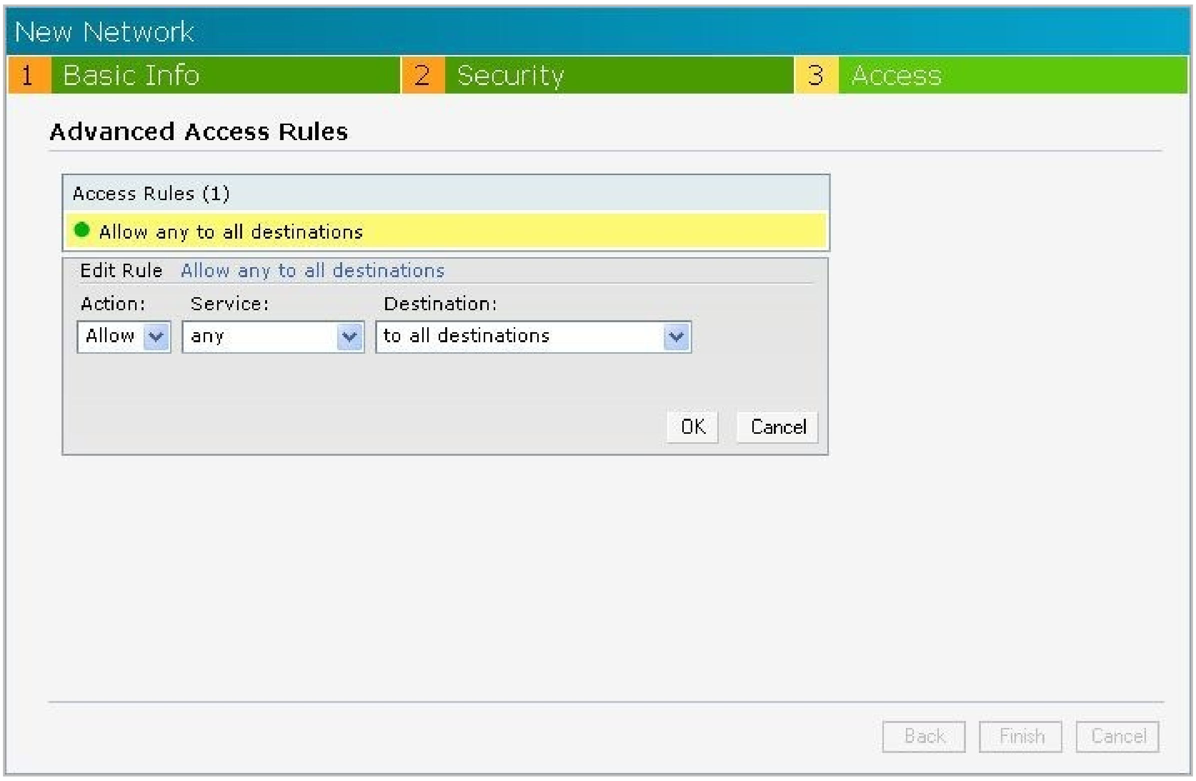
- Automatically segregates guest network users and employee or voice network users.
- Stops guest users from accessing internal network.
- Auto-NATs guest traffic as it passes from the enterprise network to the Internet.

Chapter 11
InstantFirewall

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

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

Figure 63 *Access Tab – InstantFirewall Settings*



Advanced Access Rules

Access Rules (1)

● Allow any to all destinations

Edit Rule Allow any to all destinations

Action: Allow
Service: any
Destination: to all destinations

Service Options

Table 4 lists a sample set of service options available on the Instant UI. You can allow or deny access to any or all of these services depending on your requirements.

Table 4 *Network Service Options*

Service	Description
any	Access is allowed or denied to all services.
custom	Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If you select the Other option, enter the appropriate ID.

Service	Description
adp	Application Distribution Protocol
bootp	Bootstrap Protocol
dhcp dns	Dynamic Host Configuration Protocol Domain Name Server
esp	Encapsulating Security Payload
ftp gre	File Transfer Protocol Generic Routing Encapsulation
h323-tcp	H.323-Transmission Control Protocol
h323-udp	H.323-User Datagram Protocol
http-proxy2	Hypertext Transfer Protocolproxy2
http-proxy3	Hypertext Transfer Protocolproxy3
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
netbio-sns	Network Basic Input/Output System-Name Service
netbios-ssn	Network Basic Input/Output System-Session Service
ntp	Network Time Protocol
papi	Point of Access for Providers of Information
pop3	Post Office Protocol 3
pptp	Point-to-Point Tunneling Protocol
rtsp	Real Time Streaming Protocol
sccp	Skinny Call Control Protocol
sips	Session Initiation Protocol Secure
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

Service	Description
smtp	Simple mail transfer protocol
snmp	Simple network management protocol
snmp-trap	Simple network management protocol-trap
svp	Software Validation Protocol
tftp	Trivial File Transfer Protocol

Destination Options

Table 5 lists the destination options available on the Aruba Instant UI. You can allow or deny access to any or all of these destinations depending on your requirements.

Table 5 *Destination Options*

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

Example Access Rules

This section provides procedures to create the following access rules.

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

Allow TCP service to a particular network

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

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

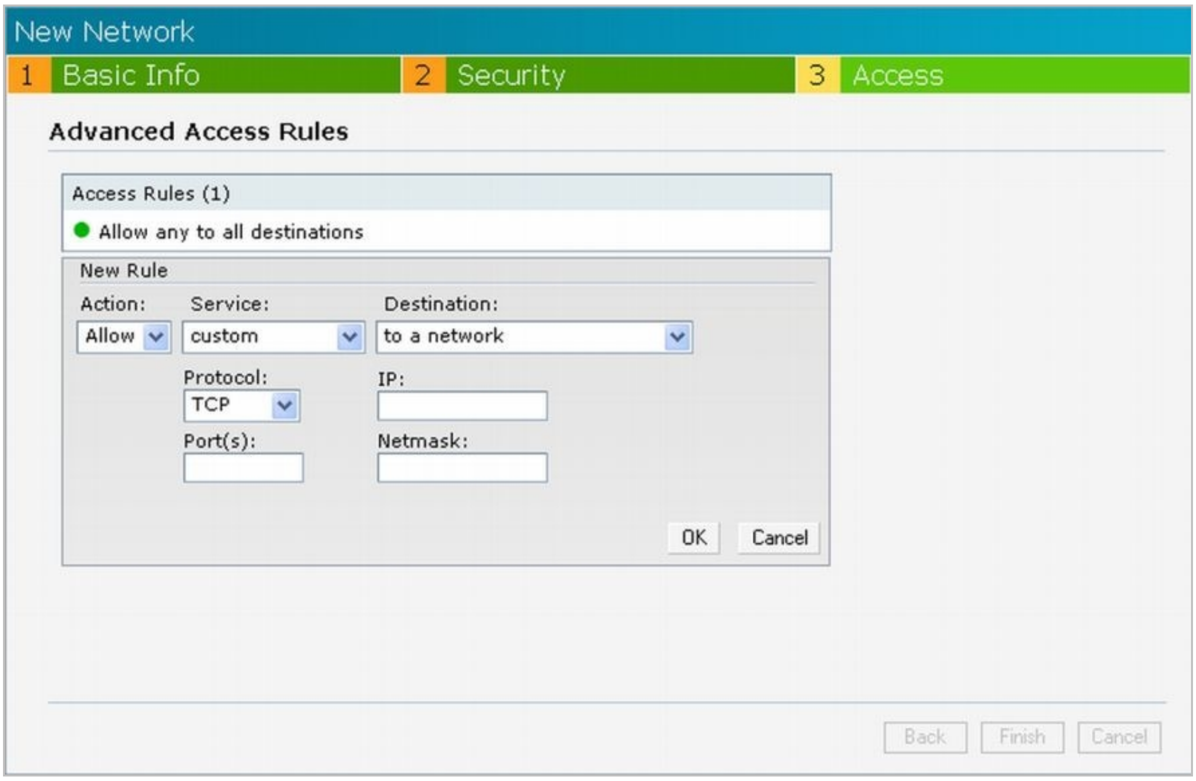
2. In the **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate values in the **Security** tab.
4. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is available by default. This rule allows traffic to all destinations. To define allow TCP service access rule to a particular network, perform the following steps:
   a. Click the **New** button. The **New Rule** box appears.
   b. Select **Allow** from the **Action** drop-down list.
   c. Select **custom** from the **Service** drop-down list.
      i. Select **TCP** from the **Protocol** drop-down list.
      ii. Enter appropriate port number in the **Port(s)** text box.

d. Select **to a network** from the **Destination** drop-down list.

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

   ii. Enter appropriate netmask in the **Netmask** text box.

Figure 64 *Defining Rule - Allow TCP Service to a Particular Network*



New Network

Advanced Access Rules

Access Rules (1)

● Allow any to all destinations

New Rule

Action: Allow

Service: custom

Destination: to a network

Protocol: TCP

IP:

Port(s):

Netmask:

e. Click **OK.**

5. Click **Finish**.

Allow PoP3 service to a particular server

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

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

2. In the **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate security levels using the slider button in the **Security** tab.
4. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is available by default. This rule allows traffic to all destinations. To define allow POP3 service access rule to a particular server, perform the following steps:

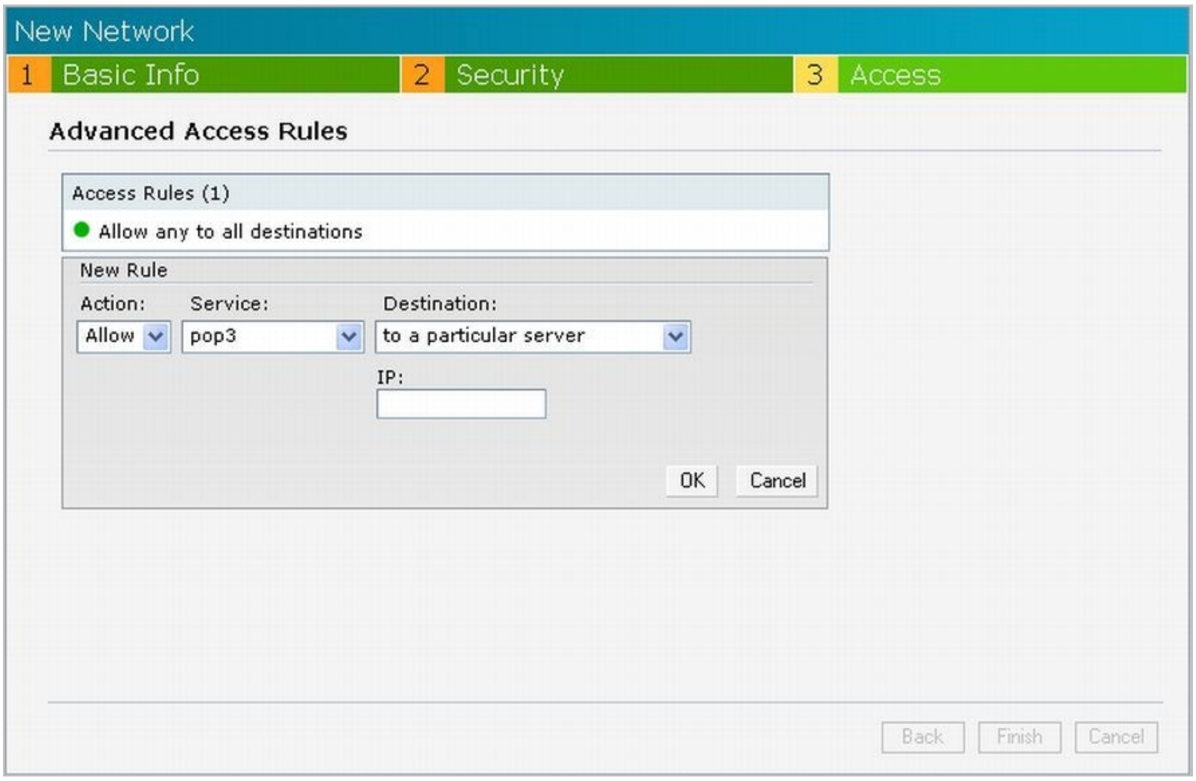
   a. Click the **New** button. The **New Rule** box appears.

   b. Select **Allow from the Action** drop-down list.

   c. Select **pop3** from the **Service** drop-down list.

   d. Select **to a particular server** from the **Destination** drop-down list and enter appropriate IP address in the **IP** text box.

Figure 65 *Defining Rule – Allow PoP3 service to a particular server*



New Network

1 Basic Info 2 Security 3 Access

Advanced Access Rules

Access Rules (1)

● Allow any to all destinations

New Rule

Action: Allow

Service: pop3

Destination: to a particular server

IP:

e. Click **OK**.

5. Click **Finish**.

Deny FTP service except to a particular server

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

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

2. In the **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate security levels using the slider button in the **Security** tab.
4. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is available by default. This rule allows traffic to all destinations. To define the deny FTP service access rule except to a particular server rule, perform the following steps.

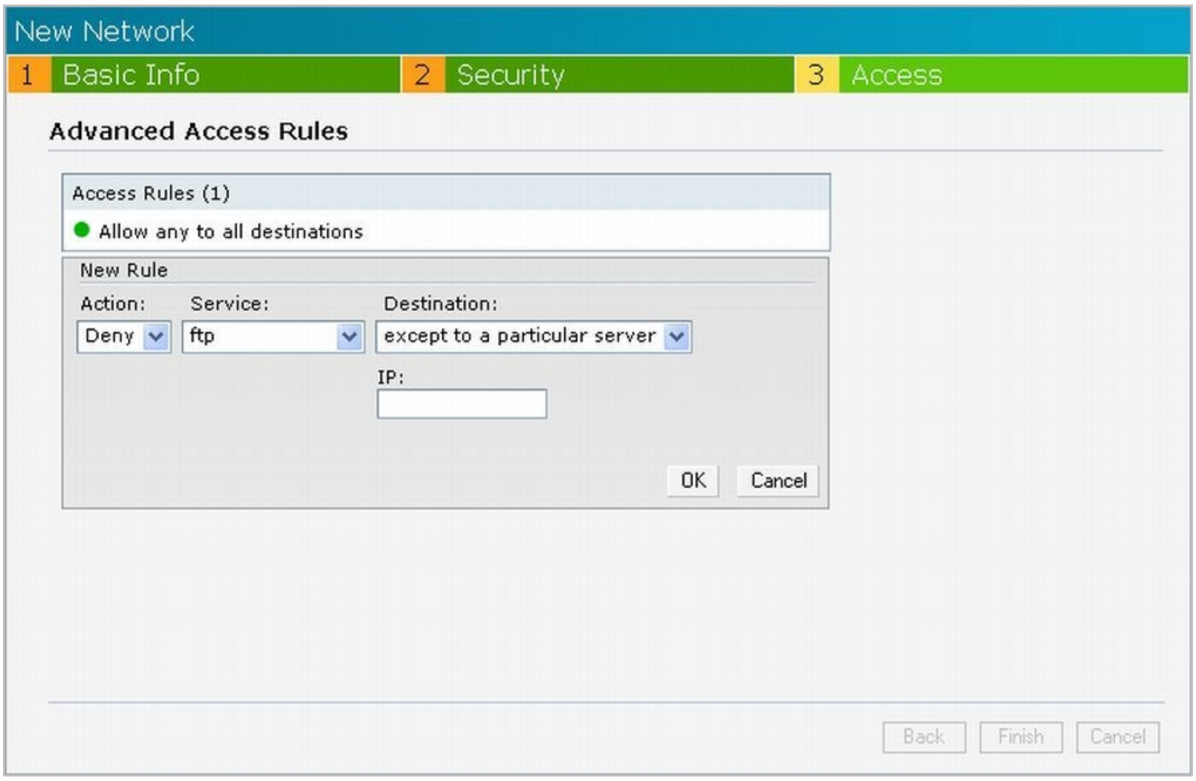
   a. Click the **New** button. The **New Rule** box appears.

   b. Select **Deny** from the **Action** drop-down list.

   c. Select **ftp** from the **Service** drop-down list.

   d. Select **except to a particular server** from the **Destination** drop-down list and enter appropriate IP address in the **IP** text box.

Figure 66 *Defining Rule – Deny FTP Service except to a Particular Server*



New Network

1 Basic Info | 2 Security | 3 Access

Advanced Access Rules

Access Rules (1)

● Allow any to all destinations

New Rule

Action: Deny

Service: ftp

Destination: except to a particular server

IP:

e. Click **OK**.

5. Click **Finish**.

Deny bootp service except to a particular network

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

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

2. In the **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate security levels using the slider button in the **Security** tab.
4. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is available by default. This rule allows traffic to all destinations. To define the deny bootp service access rule except to a network, perform the following steps:

   a. Click the **New** button. The **New Rule** box appears.

   b. Select **Deny** from the **Action** drop-down list.

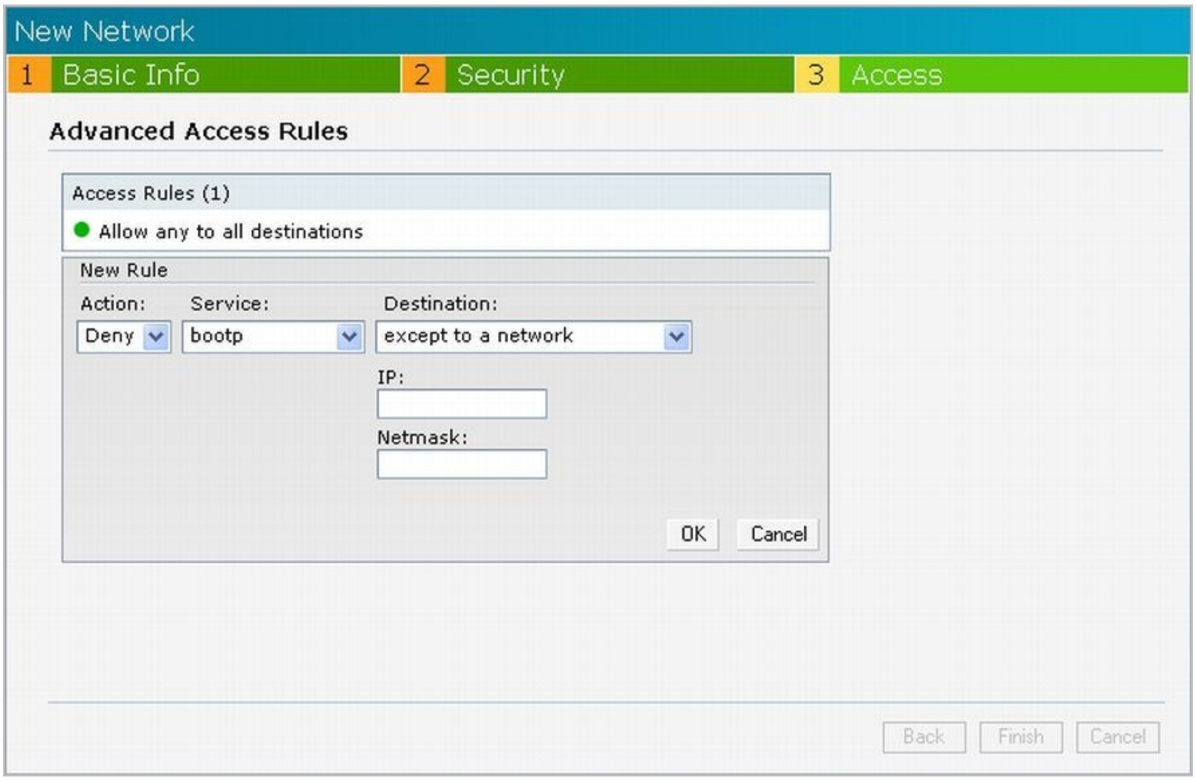
   c. Select **bootp** from the **Service** drop-down list.

   d. Select **except to a network** from the **Destination** drop-down list.

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

      ii. Enter appropriate netmask in the **Netmask** text box.

Figure 67 *Defining Rule - Deny bootp Service Except to a Particular Network*



Action: Deny

Service: bootp

Destination: except to a network

IP:

Netmask:

e. Click **OK**.

5. Click **Finish**.

Chapter 12
Content Filtering

This chapter provides information about the Content Filtering feature in Aruba Instant.

Content Filtering Overview

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

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

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

When this feature is enabled on Aruba Instant, all Domain Name Server (DNS) requests are forwarded to OpenDNS servers. If this feature is disabled, the DNS requests are forwarded to the configured DNS server of the IAP. A user is allowed or denied access to a website depending on the blacklist and whitelist entries in these servers.

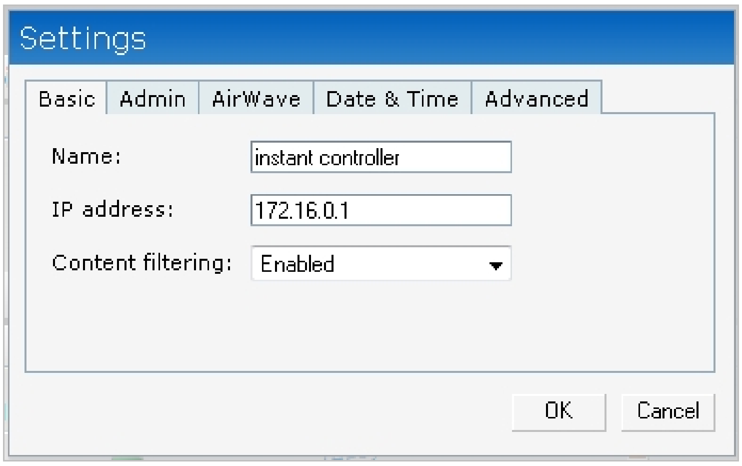
This feature also enables the IAP to store or cache the responses from the OpenDNS servers. When the IAP receives an access request, it searches the cache memory. If a suitable record is found, the IAP responds accordingly instead of contacting the DNS server again.

Enabling Content Filtering

To enable content filtering using the Aruba Instant UI, perform the following steps:

1. At the top right corner of the Instant UI, click the **Settings** link.
2. Select **Enabled** from the **Content Filtering** drop-down list and click **OK**.

Figure 68 *Enabling Content Filtering*



Settings

Name: instant controller

IP address: 172.16.0.1

Content filtering: Enabled

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

Chapter 13
OS Fingerprinting

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

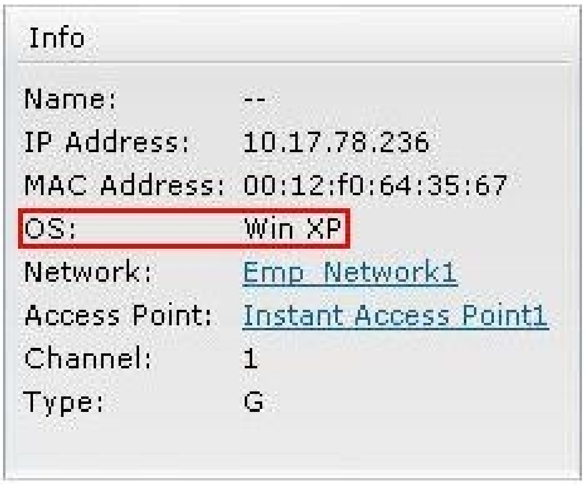
- Identifying rogue clients – Helps to identify clients that are running on forbidden operating systems.
- Identifying outdated operating systems - Helps to locate outdated and unexpected OS in the company network.
- Locating and patching vulnerable operating systems - Assists in locating and patching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

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

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

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

Figure 69 *OS Fingerprinting*



Info

Name:	--
IP Address:	10.17.78.236
MAC Address:	00:12:f0:64:35:67
OS:	Win XP
Network:	Emp_Network1
Access Point:	Instant Access Point1
Channel:	1
Type:	G

Chapter 14
Adaptive Radio Management

This chapter provides information about the Adaptive Radio Management feature in Aruba Instant.

Adaptive Radio Management 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, and n client types to inter-operate at the highest performance levels.

ARM Features

This section describes the ARM features that are available in Aruba Instant.

Channel or Power Assignment

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

Voice Aware Scanning

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

Load Aware Scanning

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

Band Steering

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

Air Time Fairness

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

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 reports data regarding network (WLAN) coverage, interference, and intrusion detection, to a virtual controller.

ARM Metrics

ARM computes coverage and interference metrics for each valid channel and chooses the best performing channel and transmit power settings for each IAP’s RF environment. Each IAP gathers other metrics on their ARM-assigned channel to provide a snapshot of the current RF health state.

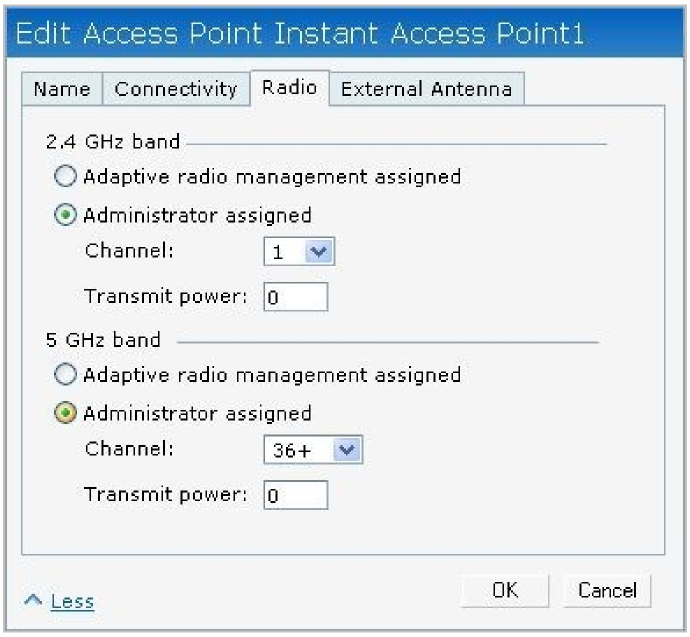
Configuring Administrator Assigned Radio Settings for IAP

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

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

1. In the **Access Points** tab, click the AP for which you want to enable ARM. The **edit** link appears.
2. Click the **edit** link. The **Edit AP** box appears.
3. Click the **More** link. More options appear in the **Edit AP** box.
4. Click the **Radio** tab.

Figure 70 *Configuring Administrator Assigned Radio Settings for IAP*



2.4 GHz band

○ Adaptive radio management assigned

● Administrator assigned

Channel: 1

Transmit power: 0

5 GHz band

○ Adaptive radio management assigned

● Administrator assigned

Channel: 36+

Transmit power: 0

5. Select the **Administrator assigned** radio button 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**.

Chapter 15
Intrusion Detection System

This chapter provides information about the Intrusion Detection System feature in Aruba Instant.

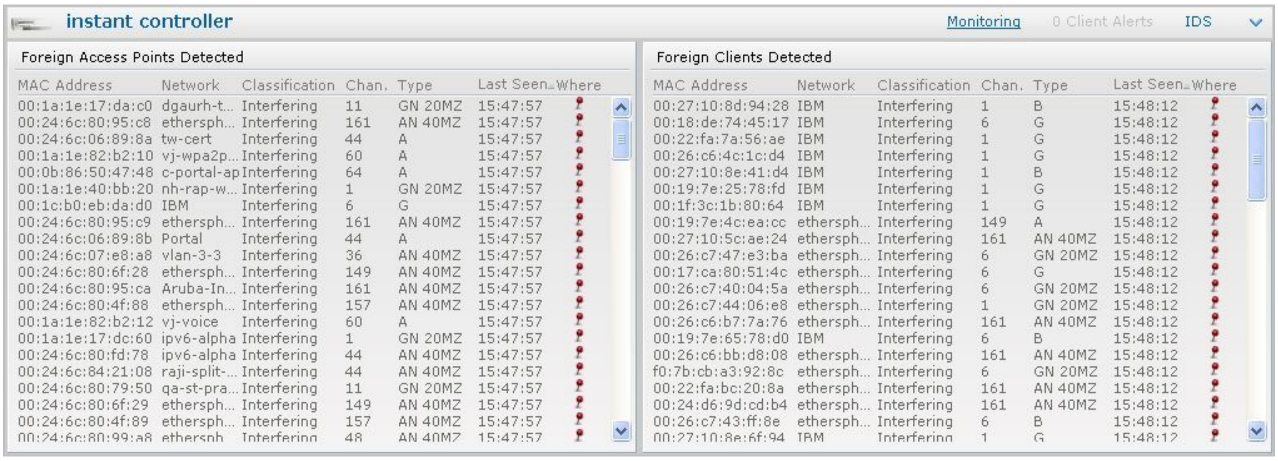
Intrusion Detection System Overview

Intrusion detection system (IDS) is a feature that monitors the network for the presence of unauthorized IAPs and clients. It also logs information about the unauthorized IAPs and clients, and generates reports based on the logged information.

Rogue AP Detection and Classification

The most important IDS functionality offered in the Aruba Instant network is the ability to detect rogue APs, interfering APs, and other devices that can potentially disrupt network operations. An AP is considered to be a rogue AP if it is both unauthorized and plugged into the wired side of the network. An AP is considered to be an interfering AP if it is seen in the RF environment but is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat since it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

Figure 71 *Intrusion Detection*



Foreign Access Points Detected

MAC Address	Network	Classification	Chan.	Type	Last Seen	Where
00:1a:1e:17:da:c0	dgaurh-t...	Interfering	11	GN 20MZ	15:47:57	📍
00:24:6c:80:95:c8	ethersph...	Interfering	161	AN 40MZ	15:47:57	📍
00:24:6c:06:89:8a	tw-cert	Interfering	44	A	15:47:57	📍
00:1a:1e:82:b2:10	vj-wpa2p...	Interfering	60	A	15:47:57	📍
00:0b:86:50:47:48	c-portal-ap	Interfering	64	A	15:47:57	📍
00:1a:1e:40:bb:20	nh-rap-w...	Interfering	1	GN 20MZ	15:47:57	📍
00:1c:b0:eb:da:d0	IBM	Interfering	6	G	15:47:57	📍
00:24:6c:80:95:c9	ethersph...	Interfering	161	AN 40MZ	15:47:57	📍
00:24:6c:06:89:8b	Portal	Interfering	44	A	15:47:57	📍
00:24:6c:07:e8:a8	vlan-3-3	Interfering	36	AN 40MZ	15:47:57	📍
00:24:6c:80:6f:28	ethersph...	Interfering	149	AN 40MZ	15:47:57	📍
00:24:6c:80:95:ca	Aruba-In...	Interfering	161	AN 40MZ	15:47:57	📍
00:24:6c:80:4f:88	ethersph...	Interfering	157	AN 40MZ	15:47:57	📍
00:1a:1e:82:b2:12	vj-voice	Interfering	60	A	15:47:57	📍
00:1a:1e:17:dc:60	ipv6-alpha	Interfering	1	GN 20MZ	15:47:57	📍
00:24:6c:80:fd:78	ipv6-alpha	Interfering	44	AN 40MZ	15:47:57	📍
00:24:6c:84:21:08	raji-split-...	Interfering	44	AN 40MZ	15:47:57	📍
00:24:6c:80:79:50	qa-st-pra...	Interfering	11	GN 20MZ	15:47:57	📍
00:24:6c:80:6f:29	ethersph...	Interfering	149	AN 40MZ	15:47:57	📍
00:24:6c:80:4f:89	ethersph...	Interfering	157	AN 40MZ	15:47:57	📍
00:24:6c:80:99:a8	ethersph	Interfering	48	AN 40MZ	15:47:57	📍

Foreign Clients Detected

MAC Address	Network	Classification	Chan.	Type	Last Seen	Where
00:27:10:8d:94:28	IBM	Interfering	1	B	15:48:12	📍
00:18:de:74:45:17	IBM	Interfering	6	G	15:48:12	📍
00:22:fa:7a:56:ae	IBM	Interfering	1	G	15:48:12	📍
00:26:c6:4c:1c:d4	IBM	Interfering	1	G	15:48:12	📍
00:27:10:8e:41:d4	IBM	Interfering	1	B	15:48:12	📍
00:19:7e:25:78:fd	IBM	Interfering	1	G	15:48:12	📍
00:1f:3c:1b:80:64	IBM	Interfering	1	G	15:48:12	📍
00:19:7e:4c:ea:cc	ethersph...	Interfering	149	A	15:48:12	📍
00:27:10:5c:ae:24	ethersph...	Interfering	161	AN 40MZ	15:48:12	📍
00:26:c7:47:e3:ba	ethersph...	Interfering	6	GN 20MZ	15:48:12	📍
00:17:ca:80:51:4c	ethersph...	Interfering	6	G	15:48:12	📍
00:26:c7:40:04:5a	ethersph...	Interfering	6	GN 20MZ	15:48:12	📍
00:26:c7:44:06:e8	ethersph...	Interfering	1	GN 20MZ	15:48:12	📍
00:26:c6:b7:7a:76	ethersph...	Interfering	161	AN 40MZ	15:48:12	📍
00:19:7e:65:78:d0	IBM	Interfering	6	B	15:48:12	📍
00:26:c6:bb:d8:08	ethersph...	Interfering	161	AN 40MZ	15:48:12	📍
f0:7b:cb:a3:92:8c	ethersph...	Interfering	6	GN 20MZ	15:48:12	📍
00:22:fa:bc:20:8a	ethersph...	Interfering	161	AN 40MZ	15:48:12	📍
00:24:d6:9d:cd:b4	ethersph...	Interfering	161	AN 40MZ	15:48:12	📍
00:26:c7:43:ff:8e	ethersph...	Interfering	6	B	15:48:12	📍
00:27:10:8e:6f:94	IBM	Interfering	1	G	15:48:12	📍

Chapter 16
AirWave Integration and Management

AirWave Overview

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

AirWave Features

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

Image Management

AirWave allows updating the firmware on WLAN devices by defining a minimum acceptable firmware version for each make and model of a device. It remotely distributes the firmware image to the WLAN devices that require updates, and also schedules the firmware updates such that updating is completed without the necessity to manually monitor the devices.

The following models can be used to upgrade the firmware:

- Directed: In this model, the user initiates a new image upgrade by giving a command to the virtual controller with an URL that provides the new image location.
- Automatic: In this model, the virtual controller periodically checks for newer updates from a configured URL, and automatically initiates upgrade of the network.

IAP and Client Monitoring

AirWave allows you to find any IAP or client on the wireless network and to see real-time monitoring views. These monitoring views can be used to aggregate critical information and high-end monitoring information.

Template Based Configuration

AirWave automatically creates a configuration template based on any of the existing IAPs, and it applies that template across the network. 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 mis-configured device.

Trending Reports

AirWave saves up to two years of actionable information, including network performance data and user roaming patterns so you can analyze how network usage and performance trends have changed over time. It also provides the detailed capacity reports with which you can plan the capacity and plan right strategies for your organization.

Intrusion Detection System

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

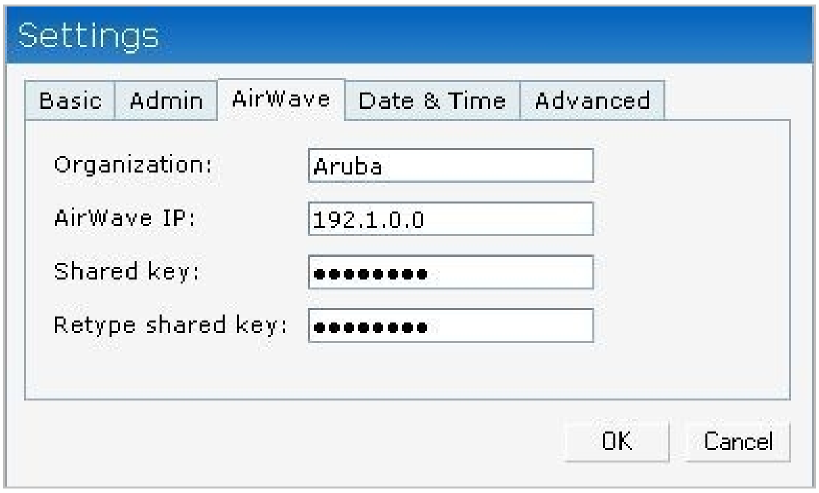
Configuring AirWave

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

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

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

Figure 72 *Configuring AirWave*



Organization: Aruba

AirWave IP: 192.1.0.0

Shared key: ●●●●●●●●

Retype shared key: ●●●●●●●●

2. Enter the name of your organization in the **Organization** name text box.
3. Enter the IP address of the AirWave server in the **AirWave IP** text box.
4. Enter the shared key in the **Shared key** text box, and reconfirm. This shared key is used for configuring the first AP in the Aruba Instant network.
5. Click **OK**.

Chapter 17
Monitoring

You can monitor the Aruba Instant network, IAPs, Wi-Fi networks, and clients in the network for various parameters using one or all of the following views:

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

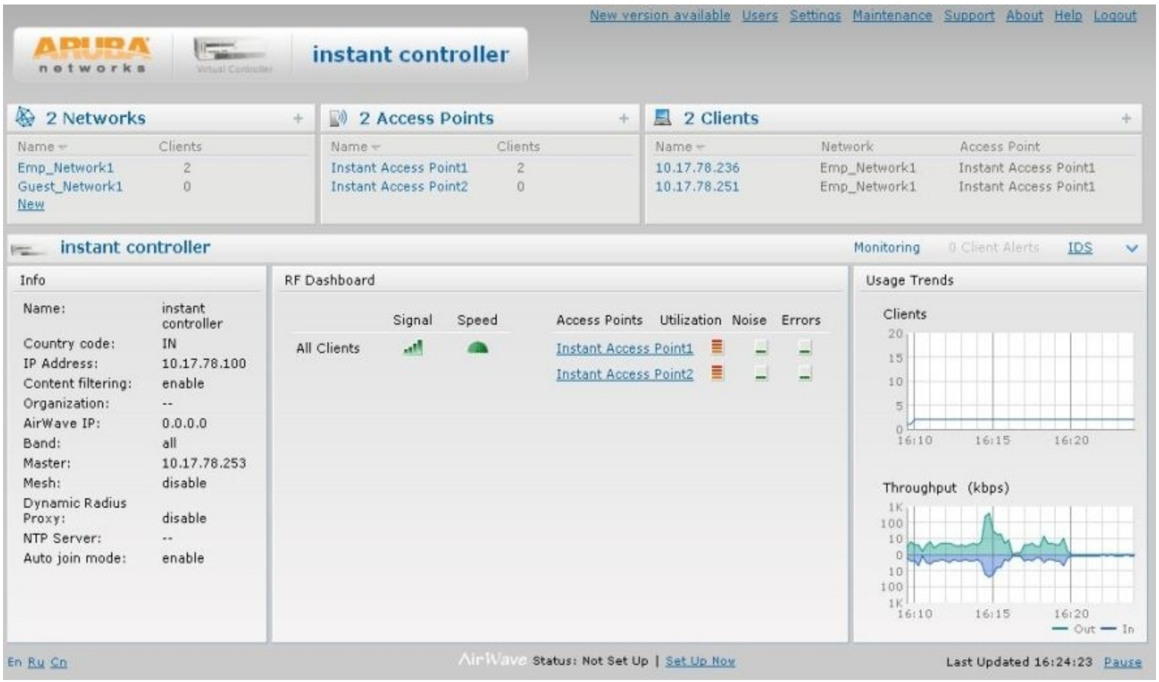
This chapter provides information about the parameters that can be monitored using these views. It also provides procedures to monitor these parameters.

Virtual Controller View

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

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

Figure 73 *Virtual Controller View*



Name	Clients
Emp_Network1	2
Guest_Network1	0
New	

Name	Clients
Instant Access Point1	2
Instant Access Point2	0

Name	Network	Access Point
10.17.78.236	Emp_Network1	Instant Access Point1
10.17.78.251	Emp_Network1	Instant Access Point1

Name:	instant controller
Country code:	IN
IP Address:	10.17.78.100
Content filtering:	enable
Organization:	--
AirWave IP:	0.0.0.0
Band:	all
Master:	10.17.78.253
Mesh:	disable
Dynamic Radius Proxy:	disable
NTP Server:	--
Auto join mode:	enable

	Signal	Speed
All Clients		

Access Points	Utilization	Noise	Errors
Instant Access Point1			
Instant Access Point2			

Status: Not Set Up | Set Up Now

Last Updated 16:24:23

Monitoring Link

This link is clicked by default and the following sections are displayed. These sections provide information about the virtual controller and allow you to monitor the network.

- Info
- RF Dashboard
- Usage Trends

Info

The **Info** section displays the following information about the virtual controller:

- **Name** - Virtual controller name.
- **Country Code** - Country in which the virtual controller is operating.
- **IP address** - IP address of the virtual controller.
- **Content filtering** - Status of the Content Filtering feature: Enabled or Disabled.
- **Organization** - Name of the organization.
- **AirWave IP** - IP address of the AirWave server.
- **Band** - Band in which the virtual controller is operating: 2.4 GHz band, 5.4 GHz band, or both.
- **Master** - IP address of the master IAP.
- **Mesh** - Status of Mesh: Enabled or Disabled.
- **Dynamic Radius Proxy** - Status of InstantRADIUS: Enabled or Disabled.
- **NTP server** - IP address of the NTP server.
- **Auto Join mode** - Status of the Auto Join mode feature: Enabled or Disabled.

RF Dashboard

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

- IP address, Signal, and Speed information about the clients in the Aruba Instant network. If the speed or signal strength of a client is low, IP address of the client appears as a link. Click the link to monitor the client. For more information, see Client View.
- Instant Access Points, Utilization, Noise, and Errors information about the IAPs in the Aruba Instant network. If the utilization, noise, and errors of an IAP is low, the IAP name appears as a link. Click the link to monitor the selected IAP. For more information, see Instant Access Point View.

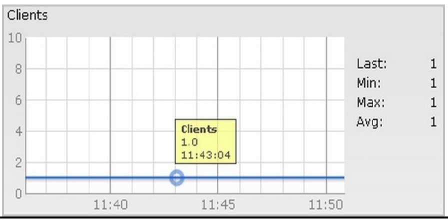
Usage Trends

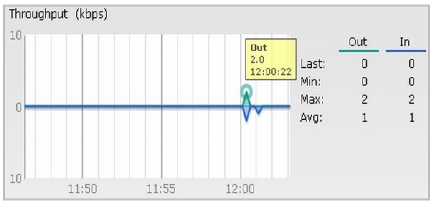
The **Usage Trends** section displays the following graphs for the virtual controller:

- Clients Graph
- Throughput Graph

For more information about graphs in the virtual controller view and for monitoring procedures, see Table 6.

Table 6 *Virtual Controller View – Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients Graph	The Clients Graph shows the number of clients associated with the virtual controller for the last 15 minutes.  	To check the number of clients associated with the virtual controller for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. Study the Clients graph in the **Usage Trends** pane. For example, the graph on the left shows that one client is associated with the virtual controller at 11:43 hours.

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 virtual controller for the last 15 minutes. To see the exact number of clients in the Aruba Instant network at a particular time, hover the cursor over the graph line.	
Throughput Graph	The Throughput Graph shows the throughput of all networks and IAPs associated with the virtual controller for the last 15 minutes.  Outgoing traffic - Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. Incoming traffic - Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the virtual controller for the last 15 minutes. To see the exact throughput of the Aruba Instant network at a particular time, hover the cursor over the graph line.	To check the throughput of the networks and IAPs associated with the virtual controller for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. Study the Throughput graph in the **Usage Trends** pane. For example, the graph on the left shows 2.0 kbps outgoing traffic throughput at 12:00 hours. It also shows some incoming traffic throughput at the same time.

Client Alerts Link

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

IDS Link

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

Network View

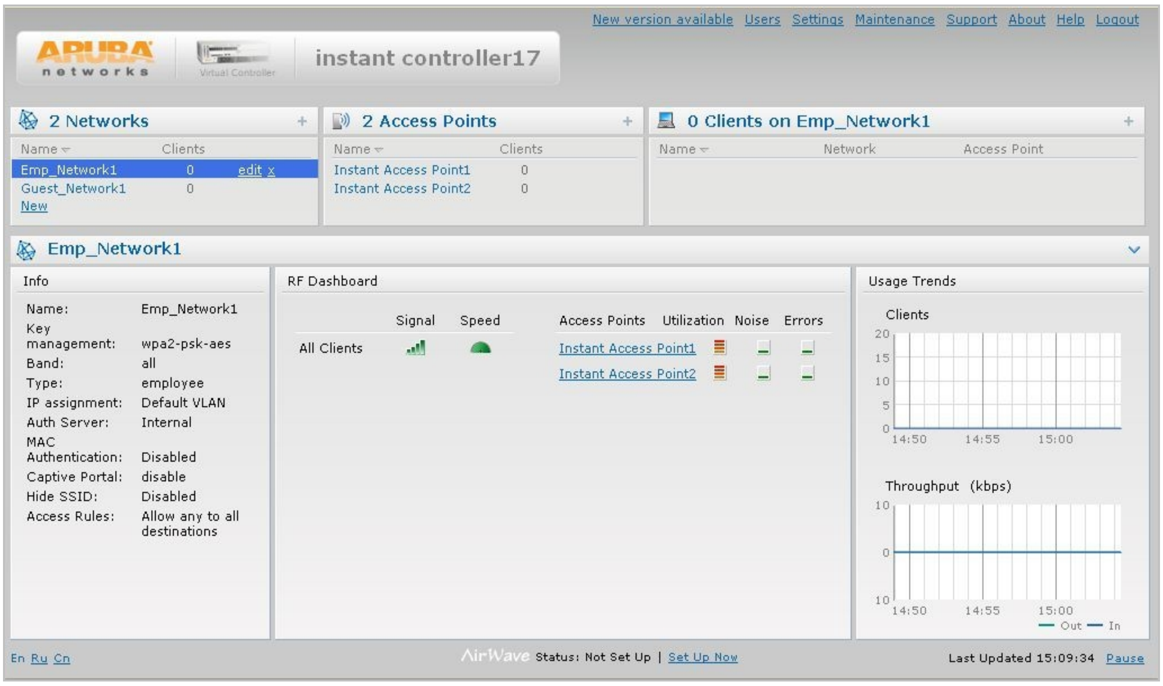
All Wi-Fi networks in the Aruba Instant network are listed in the **Networks** tab. Click the network that you want to monitor. Network View for the selected network appears.

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

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

- Info
- Usage Trends

Figure 74 *Network View*



New version available Users Settings Maintenance Support About Help Logout

instant controller17

2 Networks

Name	Clients	
Emp_Network1	0	edit x
Guest_Network1	0	
New		

2 Access Points

Name	Clients
Instant Access Point1	0
Instant Access Point2	0

0 Clients on Emp_Network1

Name	Network	Access Point

Emp_Network1

Info

Name:	Emp_Network1
Key management:	wpa2-psk-aes
Band:	all
Type:	employee
IP assignment:	Default VLAN
Auth Server:	Internal
MAC Authentication:	Disabled
Captive Portal:	disable
Hide SSID:	Disabled
Access Rules:	Allow any to all destinations

RF Dashboard

	Signal	Speed
All Clients		

Access Points	Utilization	Noise	Errors
Instant Access Point1			
Instant Access Point2			

Usage Trends

En Ru Cn AirWave Status: Not Set Up | Set Up Now Last Updated 15:09:34 Pause

Info

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

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

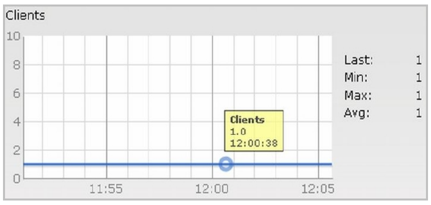
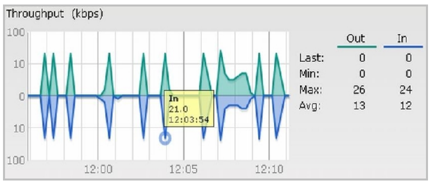
Usage Trends

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

- Clients Graph
- Throughput Graph

For more information about graphs in the network view and for monitoring procedures, see Table 7.

Table 7 *Network View – Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients Graph	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 network for the last 15 minutes. To see the exact number of clients in the selected network at a particular time, hover the cursor over the graph line.	To check the number of clients associated with the network for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Networks** tab, click the network for which you want to check the client association. The Network view appears. 3. Study the Clients graph in the **Usage Trends** pane. For example, the graph on the left shows that one client is associated with the selected network at 12:00 hours.
Throughput Graph	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 network for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Networks** tab, click the network for which you want to check the client association. The Network view appears. 3. Study the Throughput graph in the **Usage Trends** pane. For example, the graph on the left shows 22.0 kbps incoming traffic throughput for the selected network at 12:03 hours.

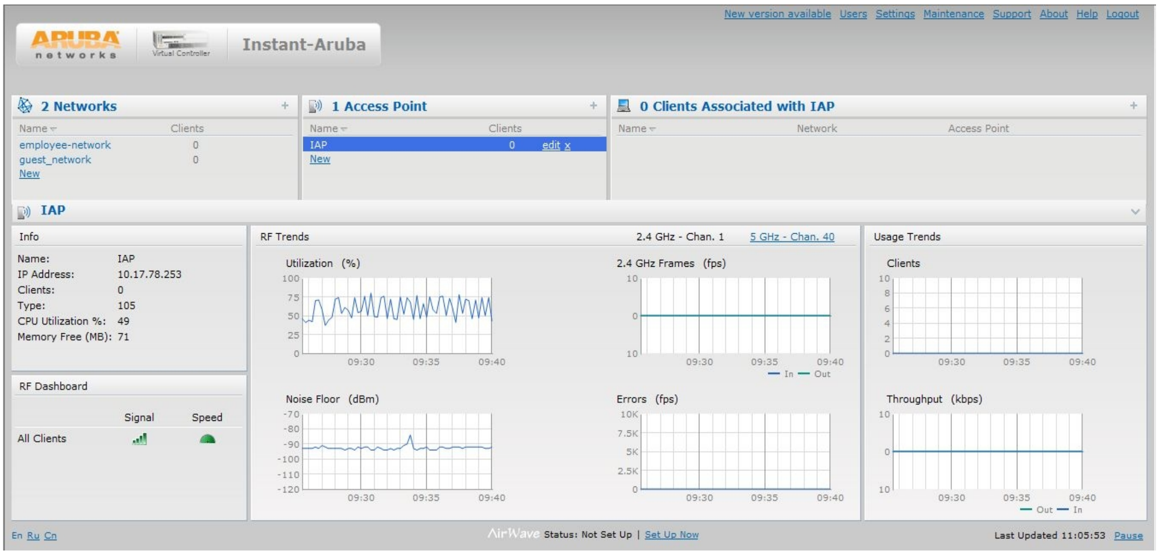
Instant Access Point View

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

Similar to the Virtual Controller view, the Access Point view also has three tabs: Networks, Access Points, and Clients. The following sections in the Instant UI provide information about the selected IAP:

- Info
- RF Dashboard
- RF Trends
- Usage Trends

Figure 75 *Instant Access Point View*



2 Networks

Name	Clients
employee-network	0
guest_network	0
New	

1 Access Point

Name	Clients	
IAP	0	edit x
New		

0 Clients Associated with IAP

Name	Network	Access Point

IAP

Info

Name: IAP
IP Address: 10.17.78.253
Clients: 0
Type: 105
CPU Utilization %: 49
Memory Free (MB): 71

RF Dashboard

	Signal	Speed
All Clients	📶	●

Status: Not Set Up | Set Up Now

Last Updated 11:05:53 Pause

Info

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

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

RF Dashboard

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

RF Trends

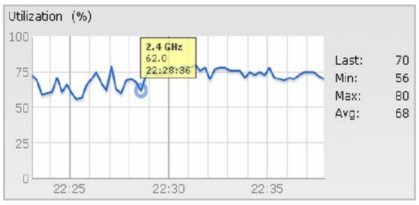
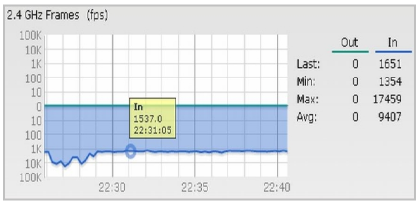
The **RF Trends** section has two links - **2.4 GHz** and **5 GHz**. The **2.4 GHz** link is clicked by default and the following graphs are displayed for that band:

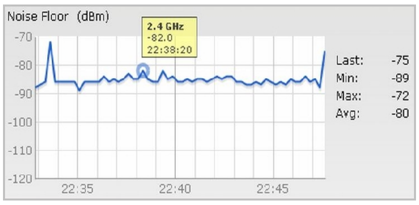
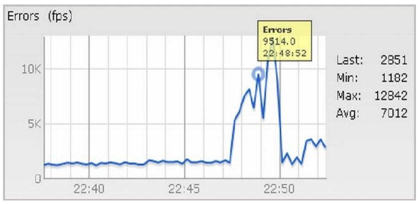
- Utilization
- 2.4 GHz Frames
- Noise Floor
- Errors

To see the graphs for the 5 GHz band, click the **5 GHz** link.

For more information about the graphs in the instant access point view and for monitoring procedures, see Table 8.

Table 8 *Instant Access Point View – RF Trends Graphs and Monitoring Procedures*

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

Graph Name	Description	Monitoring Procedure
	particular time, hover the cursor over the graph line.	
Noise Floor	The Noise Floor graph shows the signals created by all the noise sources and unwanted signals in the network. Noise floor is measured in decibels per metre. Too many unwanted signals hamper the performance of the IAP. Monitor the noise floor regularly for optimal performance of the IAP.  To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In and Out frames. To see the exact utilization percent at a particular time, hover the cursor over the graph line.	To monitor the noise floor for the IAP for the last 15 minutes, 1. Log in to the 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 noise floor. The IAP view appears. 3. Study the Noise Floor graph in the **RF Trends** pane. For example, the graph on the left shows that the noise floor for the IAP at 22:38 hours is -82.0 dBm. NOTE You can also click the rectangle icon ▤ under the Noise column in the **RF Dashboard** pane to see the Noise graph for the selected IAP.
Errors	The Errors graph shows the errors that occurred while receiving the frames for the last 15 minutes. The errors are measured in frames/second.  To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In and Out frames. To see the exact utilization percent at a particular time, hover the cursor over the graph line.	To monitor the errors for the IAP for the last 15 minutes, 1. Log in to the 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 errors. The IAP view appears. 3. Study the Errors graph in the **RF Trends** pane. For example, the graph on the left shows that the noise floor for the IAP at 22:48 hours is 9514.0 frames per second. NOTE You can also click the rectangle icon ▤ under the Errors column in the **RF Dashboard** pane to see the Errors graph for the selected IAP.

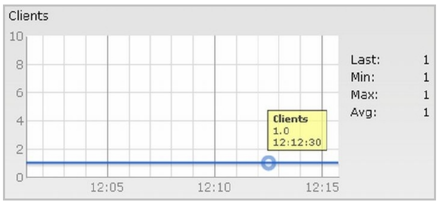
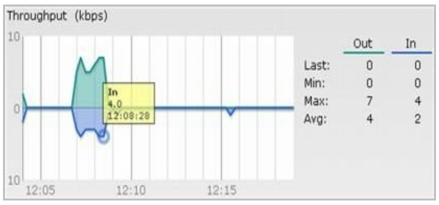
Usage Trends

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

- Clients Graph
- Throughput Graph

For more information about the usage trends graphs in the instant access point view and for monitoring procedures, see Table 9.

Table 9 *Instant Access Point View – Usage Trends Graphs and Monitoring Procedures*

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

Client View

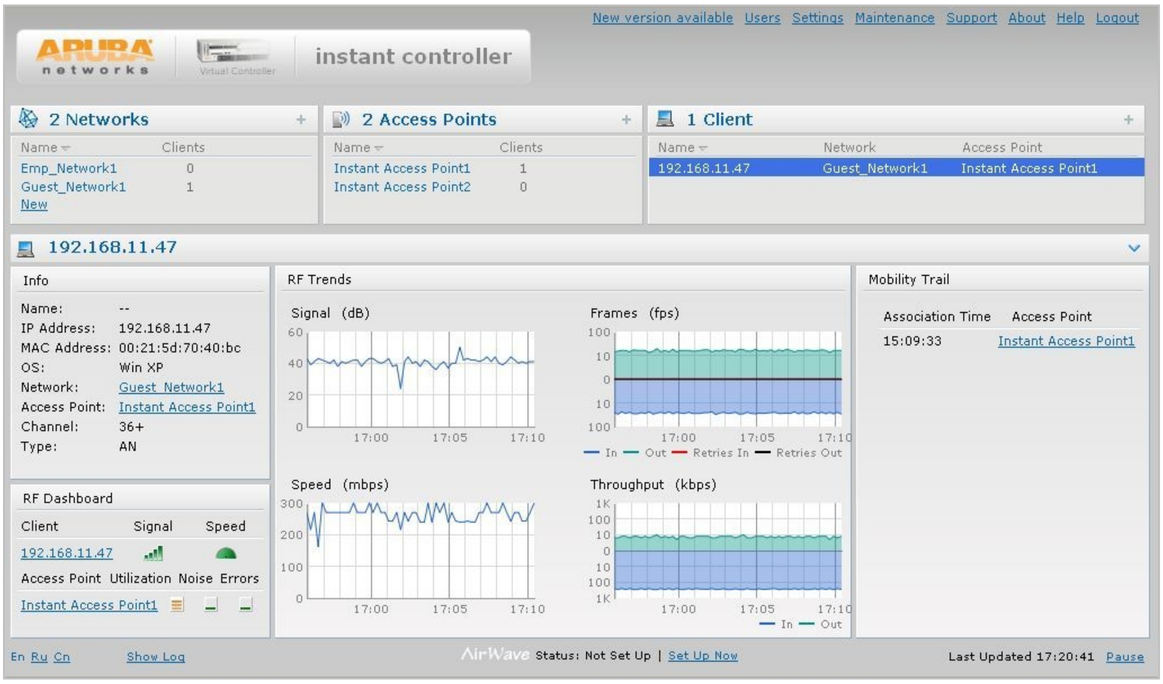
In the Virtual Controller view, all clients in the Aruba Instant network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor. Client view for that client appears.

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

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

- Info
- RF Dashboard
- RF Trends
- Usage Trends

Figure 76 *Client View*



New version available Users Settings Maintenance Support About Help Logout

instant controller

2 Networks

Name	Clients
Emp_Network1	0
Guest_Network1	1
New	

2 Access Points

Name	Clients
Instant Access Point1	1
Instant Access Point2	0

1 Client

Name	Network	Access Point
192.168.11.47	Guest_Network1	Instant Access Point1

192.168.11.47

Info

Name:	--
IP Address:	192.168.11.47
MAC Address:	00:21:5d:70:40:bc
OS:	Win XP
Network:	Guest_Network1
Access Point:	Instant Access Point1
Channel:	36+
Type:	AN

RF Dashboard

Client	Signal	Speed
192.168.11.47		

Access Point	Utilization	Noise	Errors
Instant Access Point1			

RF Trends

Mobility Trail

Association Time	Access Point
15:09:33	Instant Access Point1

En Ru Cn Show Log AirWave Status: Not Set Up | Set Up Now Last Updated 17:20:41 Pause

Info

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

- **Name** - Name of the selected client.
- **IP Address** - IP address of the client.
- **MAC Address** - MAC Address of the client.
- **OS** - Operating System that is running on the client.
- **Network** - Network to which the client is connected to.
- **Access Point** - IAP to which the client is connected to.
- **Channel** - Channel that the client is using.
- **Type** - Channel type that the client is broadcasting on.

RF Dashboard

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

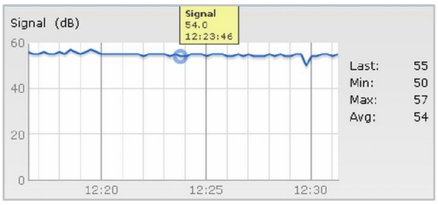
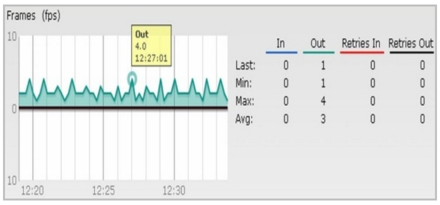
RF Trends

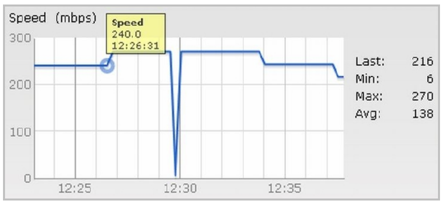
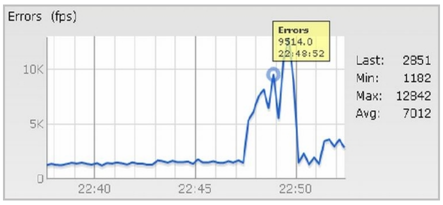
The **RF Trends** section displays the following graphs for the selected client:

- Signal
- Frames
- Speed
- Throughput

For more information about RF trends graphs in the client view and for monitoring procedures, see Table 10.

Table 10 *Client View – RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Signal	The Signal Graph shows the signal strength of the client for the last 15 minutes. It is measured in decibels.  To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average signal statistics for the client for the last 15 minutes. To see the exact strength at a particular time, hover the cursor over the graph line.	To monitor the signal strength of the selected client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the signal strength. The client view appears. 3. Study the Signal graph in the **RF Trends** pane. For example, the graph on the left shows that signal strength for the client is 54.0 dB at 12:23 hours.
Frames	The Frames Graph shows the In and Out frame rate per second for the client for the last 15 minutes. It also shows data for the Retry In and Retry Out frames.  Outgoing frames – Outgoing frame traffic is displayed in green. It is shown above the median line. Incoming frames – Incoming frame traffic is displayed in blue. It is shown below the median line. Retry Out - Retries for the outgoing frames is displayed in black and is show above the median line. Retry In - Retries for the incoming frames is displayed in red and is shown below the median line. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In, Out, Retries In, and Retries Out frames. To see the exact frames at a particular time, hover the cursor over the graph line.	To monitor the In and Out frame rate per second and retry frames for the In and Out traffic, for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Clients** tab, click the IP address link of the client for which you want to monitor the frames. The client view appears. 3. Study the Frames graph in the **RF Trends** pane. For example, the graph on the left shows 4.0 frames per second for the client at 12:27 hours.
Speed	The Speed graph shows the data transfer speed for the client. Data transfer is measured in Mega bits per second (mbps).	To monitor the speed for the client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the speed. The client view appears. 3. Study the Speed graph in the **RF Trends** pane. For example, the graph on the left shows that

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 client for the last 15 minutes. To see the exact speed at a particular time, hover the cursor over the graph line.	the data transfer speed at 12:26 hours is 240 mbps.
Throughput	The Throughput Graph shows the throughput for the selected client for the last 15 minutes.  Outgoing traffic - Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. Incoming traffic - Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the client for the last 15 minutes. To see the exact throughput at a particular time, hover the cursor over the graph line.	To monitor the errors for the client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the throughput. The client view appears. 3. Study the Throughput graph in the **RF Trends** pane. For example, the graph on the left shows 1.0 kbps outgoing traffic throughput for the client at 12:30 hours.

Mobility Trail

The **Mobility Trail** section displays the following mobility trail information for the selected client:

- **Association Time** - The time at which the selected client was associated with a particular IAP. It shows the client-IAP association for the last 15 minutes.
- **Access Point** - IAP name with which the client was associated.

NOTE

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

Chapter 18
Alert Types and Management

Alert Types

Alerts are generated when a user encounters problems while accessing or connecting to the Wi-Fi network. These alerts enable you to troubleshoot the problems. The alerts that are generated on Aruba Instant can be categorized as follows:

- 802.11 related association and authentication failure alerts.
- 802.1X related mode and key mismatch, server, and client timeout failure alerts.
- IP address related failure -Static IP address or DHCP related alerts.

Table 11 displays a list of alerts that are generated on the Aruba Instant network.

Table 11 *Alerts List*

Type code	Description	Details	Corrective Actions
100101	Internal error	The IAP has encountered an internal error for this client.	Contact the Aruba Networks 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 wifi driver and manager software.
100103	Mismatched authentication/ encryption setting	The IAP cannot allow this client to associate because its authentication or encryption settings do not match IAP's configuration.	Ascertain the correct authentication or encryption settings and try to associate again.
100104	Unsupported 802.11 rate	The IAP cannot allow this client to associate because it does not support the 802.11 rate requested by this client.	Check the configuration on the IAP to see if the desired rate can be supported; if not, consider replacing the IAP with another model that can support the rate.
100105	Maximum capacity reached on IAP	The IAP has reached maximum capacity and cannot accommodate any more clients.	Consider expanding capacity by installing additional IAPs or balance load by relocating IAPs.
100206	Invalid MAC Address	The IAP cannot authenticate this client because client’s MAC address is not valid.	This condition may be indicative of a misbehaving client. Try to locate the client device and check its hardware and software.
100307	Client blocked due to repeated authentication failures	The IAP is temporarily blocking the 802.1X authentication request from this client because the credentials provided have been rejected by the RADIUS server too many times.	Identify the client and check its 802.1X credentials.

Type code	Description	Details	Corrective Actions
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, etc) provided by the client.	Ascertain the correct authentication credentials and log in again.
100410	Integrity check failure in encrypted message	The IAP cannot receive data from this client because the integrity check of the received message (MIC) has failed.	Check the encryption setting on the client and on the IAP.

Aruba Networks Instant User Guide

Chapter 19 User Database

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

A guest user can be a visitor who will be temporarily using the enterprise network to access the internet. However, you wouldn’t want to share the internal network and the intranet with them. To segregate the guest traffic from the enterprise traffic, you can create a Guest WLAN, specify the required authentication, encryption, and access rules and allow the guest user to use the enterprise network.

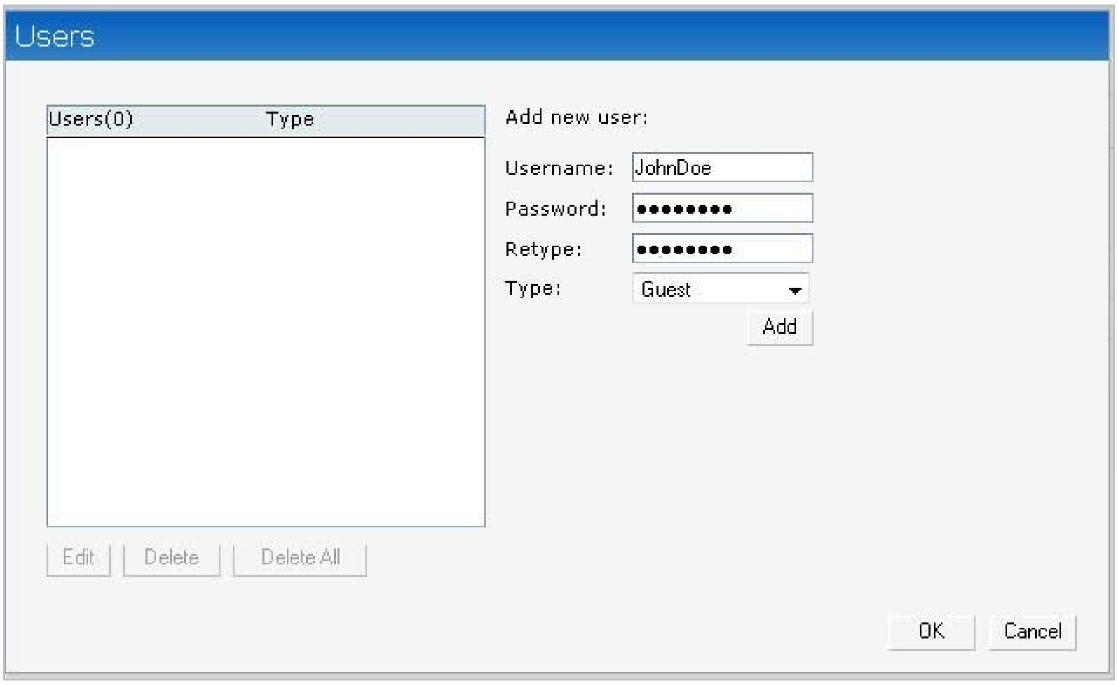
An employee user is the employee who will be using the enterprise network for various official tasks. You can create Employee WLANs, specify the required authentication, encryption and access rules and allow the employees to use the enterprise network.

Adding a User

To add a user, perform the following steps:

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

Figure 77 *Adding a User*



Users

Users(0) Type

Add new user:

Username: JohnDoe

Password: ●●●●●●●●

Retype: ●●●●●●●●

Type: Guest

2. Enter the username in the **Username** text box.
3. Enter the password in the **Password** text box and reconfirm.
4. Select appropriate network type from the **Type** drop-down list.
5. Click **Add** and click **OK**. The users are listed in the **Users** list.

Editing User Settings

To edit user settings, perform the following steps:

1. In the top right corner of the Instant UI, click the **Users** link. The **Users** box appears.
2. In the **Users** section, select the username for which you want to edit the settings and click **Edit**. The user's details appear on the right side.
3. Edit as required and click **OK.**

Deleting a User

To delete a user, perform the following steps:

1. In the top right corner of the Instant UI, click the **Users** link. The **Users** box appears.
2. In the **Users** section, select the username that you want to delete and click **Delete.**

To delete all the users or multiple users at a time, select the usernames to be deleted, and click **Delete All.**

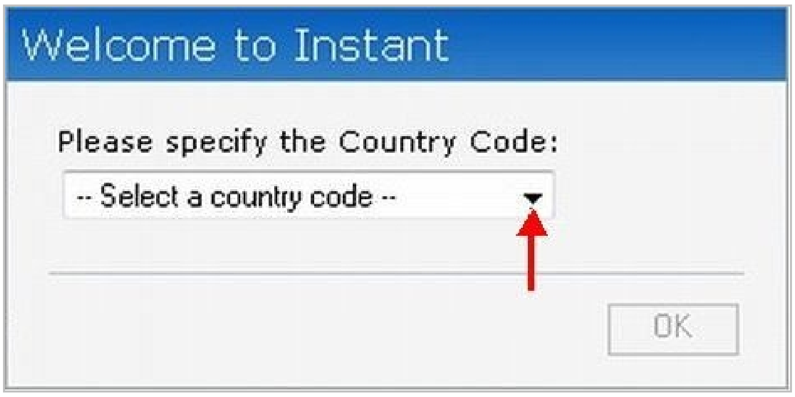
Chapter 20 Regulatory Domain

The IEEE 802.11/b/g/n Wi-Fi networks operate in 2.4 GHz and IEEE 802.11a/n operate in 5.0 GHz spectrum. These spectrums are divided into channels. The 2.4 GHz spectrum is divided into 14 overlapping, staggered 20 MHz wireless carrier channels. These channels are spaced 5 MHz apart. The 5 GHz spectrum is divided into more channels. The channels that can be used in a particular country differ based on the regulations of that country.

The initial Wi-Fi setup requires you to specify the country code for the country in which the Aruba Instant will operate. This setup 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 configuration. The available 20 MHz and 40 MHz channels are dependent on the specified country code.

You cannot change the country code for the IAPs designated for US, Japan, and Israel. Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions on operators of wireless networks with devices set to improper country codes.

Figure 78 *Specifying a Country Code*



Welcome to Instant

Please specify the Country Code:

Country Codes List

Table 12 *Country Codes List*

Code	Country Name
US	United States
CA	Canada
JP3	Japan
DE	Germany
NL	Netherlands
IT	Italy
PT	Portugal
LU	Luxembourg
NO	Norway

Code	Country Name
FI	Finland
DK	Denmark
CH	Switzerland
CZ	Czech Republic
ES	Spain
GB	United Kingdom
KR	Republic of Korea (South Korea)
CN	China
FR	France
HK	Hong Kong
SG	Singapore
TW	Taiwan
BR	Brazil
IL	Israel
SA	Saudi Arabia
LB	Lebanon
AE	United Arab Emirates
ZA	South Africa
AR	Argentina
AU	Australia
AT	Austria
BO	Bolivia
CL	Chile
GR	Greece
IS	Iceland
IN	India
KW	Kuwait
LI	Liechtenstein
LT	Lithuania
MX	Mexico
MA	Morocco
NZ	New Zealand
PL	Poland
PR	Puerto Rico
SK	Slovak Republic

Code	Country Name
SI	Slovenia
TH	Thailand
UY	Uruguay
PA	Panama
RU	Russia
EG	Egypt
TT	Trinidad and Tobago
TR	Turkey
CR	Costa Rica
EC	Ecuador
HN	Honduras
KE	Kenya
UA	Ukraine
VN	Vietnam
BG	Bulgaria
CY	Cyprus
EE	Estonia
MU	Mauritius
RO	Romania
CS	Serbia and Montenegro
ID	Indonesia
PE	Peru
VE	Venezuela
JM	Jamaica
BH	Bahrain
OM	Oman
JO	Jordan
BM	Bermuda
CO	Colombia
DO	Dominican Republic
GT	Guatemala
PH	Philippines
LK	Sri Lanka
SV	El Salvador
TN	Tunisia
PK	Islamic Republic of Pakistan

Code	Country Name
QA	Qatar
DZ	Algeria

Appendix A
Abbreviations

The following table describes abbreviations used in this user guide.

Abbreviations	Expansion
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
BSS	Basic Server Set
BSSID	Basic Server Set Identifier
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
IAP	Instant Access Point
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
Instant UI	Instant User Interface
LEAP	Lightweight Extensible Authentication Protocol
MX	Mail Exchanger
MAC	Media Access Control
NAS	Network Access Server
NAT	Network Address Translation
NS	Name Server
NTP	Network Time Protocol
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial In User Service
VC	Virtual Controller
WLAN	Wireless Local Area Network