Instant Access Point 6.1.3.4-3.1.0.0

ARUBA®
networks

User Guide

Copyright

Open Source Code

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

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

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

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

ARUBA®
networks

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Figures

Tables

About this Guide

Aruba Instant Overview

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

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 or a self-enclosed network, is used to deploy an Instant Wireless Network. An Instant Access Point (IAP) can be installed at a single site or deployed across multiple geographically-dispersed locations. Designed specifically for easy deployment, and proactive management of networks, Instant is ideal for small customers or remote locations without any on-site IT administrator.

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

Supported Devices

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

- IAP-92
- IAP-93
- IAP-104
- IAP-105
- IAP-134
- IAP-135
- IAP-175P/175AC
- RAP-3WN/3WN-US/3WNP/3WNP-US

NOTE

IAP-104, IAP-105, IAP-134, IAP-135, and IAP-175 support an unlimited number of IAPs on Layer 2 networks. IAP -92/93 supports 16 IAPs.

Objective

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

Intended Audience

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

Conventions

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

Table 1 *Conventions*

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

The following informational icons are used throughout this guide:

NOTE

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

CAUTION

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

WARNING

Indicates a risk of personal injury or death.

Contacting Support

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

Chapter 2

Initial Configuration

This chapter provides information required to setup 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) switch or a midspan PSE device.
  - Aruba power adapter kit (this kit is sold separately).

NOTE

PoE is a method of delivering power on the same physical Ethernet wire that is used for data communication. Power for devices is provided in one of the following two ways:
Endspan— The switch that the IAP is connected to can provide power.
Midspan— A device can sit between the switch and the IAP.
The choice of endspan or midspan depends on the capabilities of the switch to which the IAP is connected. Typically if a switch is in place and does not support PoE, midspan power injectors are used.

NOTE

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

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

1. “Connecting the IAP to a Power Source” on page 24
2. “Assigning an IP Address to the IAP” on page 24
3. “Connecting to a Provisioning Wi-Fi Network” on page 24
4. “Log in to the Instant User Interface” on page 26

5. "Specifying the Country Code" on page 26 — Skip this step if you are installing the IAP in United States, Japan or Israel.

Connecting the IAP to a Power Source

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

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

Assigning an IP Address to the IAP

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

To get an IP address for an IAP:

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 receives an IP address provided by the switch or router.

NOTE

After the IAP starts up, the IAP tries to connect to the DHCP server if the static IP configuration is not available. If DHCP times out, a default IP within 169.254.x.y/16 subnet is configured on the IAP. The DHCP client still continues to run so that when the DHCP service recovers, the IAP gets a valid IP address and reboots. In addition, you can manually assign a static IP without the support of DHCP, after the IAP comes up with the 169.254.x.y/16 subnet.

Connecting to a Provisioning Wi-Fi Network

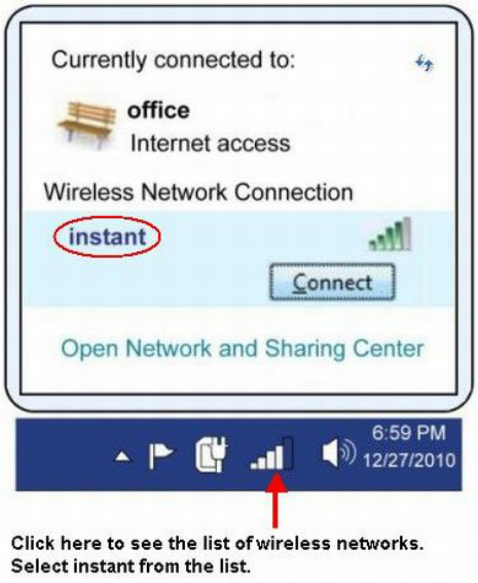
To connect to a provisioning Wi-Fi network:

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

NOTE

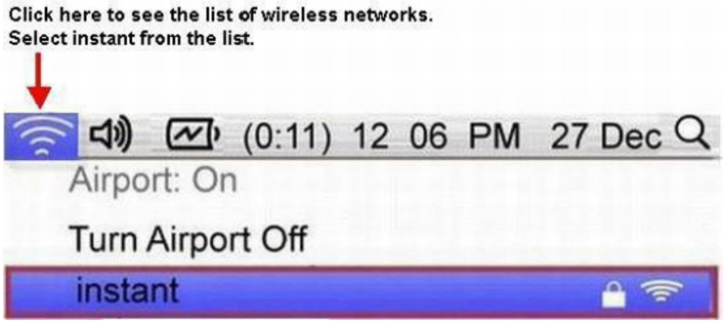
While connecting to the provisioning Wi-Fi network, ensure that the client is not connected to any wired network.

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



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

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


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

Disabling the Provisioning Wi-Fi Network

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

To disable the provisioning network:

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

Table 2 *Terminal Communication Settings*

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

5. In the apboot mode, use the following commands to disable the provisioning network:

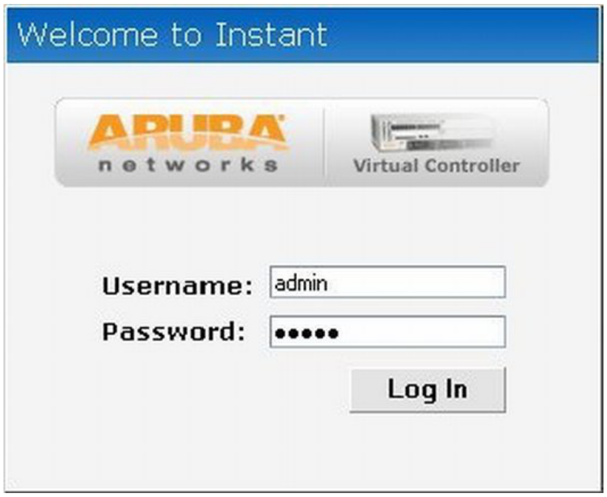
- `apboot> factory_reset`
- `apboot> setenv disable_prov_ssid 1`
- `apboot> saveenv`
- `apboot> reset`

Log in to the Instant User Interface

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

- Username— admin
- Password— admin

Figure 3 *Instant User Interface Login Screen*



Welcome to Instant

Username: admin

Password: ●●●●●

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

Specifying the Country Code

NOTE

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

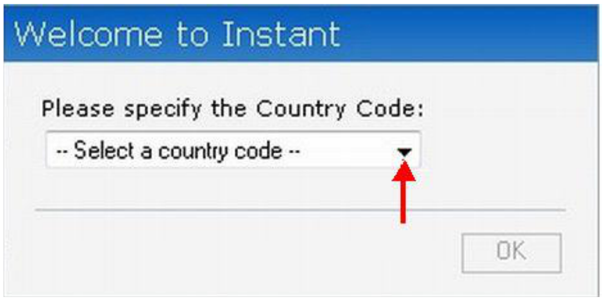
Aruba Instant Access Points are shipped in four variants:

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

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

For the complete list of the countries that are supported in the IAP-ROW variant type, see “Regulatory Domain” on page 253.

Figure 4 *Specifying the Country Code*



Welcome to Instant

Please specify the Country Code:

-- Select a country code --

IAP Cluster

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

NOTE

Moving an IAP from one cluster to another requires a factory reset of the IAP that is being moved. See Chapter 6, "Managing IAPs" on page 85 for more information.

Chapter 3

Instant User Interface

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

Supported browsers are:

- Internet Explorer 8 or higher
- Safari
- Google Chrome
- Mozilla Firefox

NOTE

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

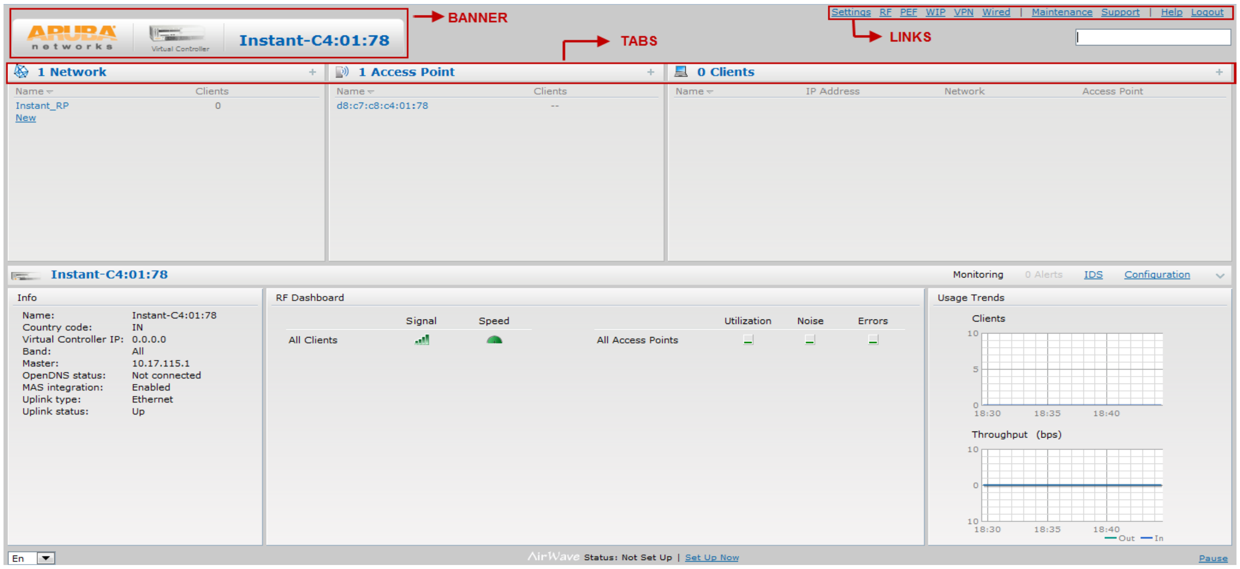
Understanding the Instant UI Layout

The Instant UI consists of the following elements:

- Banner
- Search
- Tabs
- Links
- Views

These elements are explained in the following sections.

Figure 5 *Instant UI Interface*



Name	Clients
Instant_RP	0
New	

Name	Clients
d8:c7:c8:c4:01:78	--

Name	IP Address	Network	Access Point

Instant-C4:01:78

Info

Name:	Instant-C4:01:78
Country code:	IN
Virtual Controller IP:	0.0.0.0
Band:	All
Master:	10.17.115.1
OpenDNS status:	Not connected
MAS integration:	Enabled
Uplink type:	Ethernet
Uplink status:	Up

RF Dashboard

	Signal	Speed
All Clients		

	Utilization	Noise	Errors
All Access Points			

Status: Not Set Up | Set Up Now

Banner

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

Search

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

Tabs

The 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 Instant network.
- **Clients**— Provides information about the clients in the Instant network.

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

Networks Tab

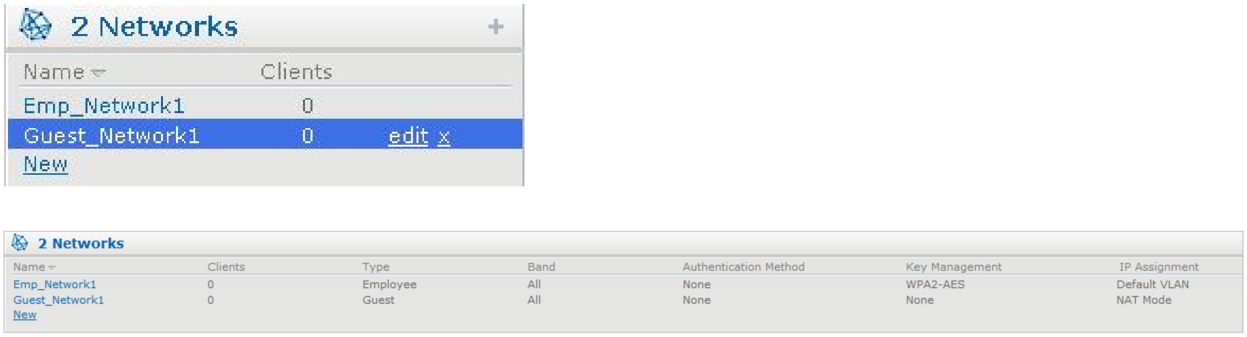
This tab displays a list of Wi-Fi networks that are configured in the Aruba Instant network. The network names appear as links. The expanded view displays the following information about each Wi-Fi network:

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

To add a Wi-Fi network, click the **New** link in the **Networks** tab. For more information about a wireless network and the procedure to add a wireless network, see Chapter 4, “Wireless Network” on page 53.

An **edit** link appears on clicking the network name in the **Networks** tab. For information about editing a wireless network, see “Editing a Network” on page 78. To delete a network, click on the link **x** located next to the **edit** link.

Figure 6 *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	IP Assignment
Emp_Network1	0	Employee	All	None	WPA2-AES	Default VLAN
Guest_Network1	0	Guest	All	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 is displayed in the **Access Points** tab. The IAP names are displayed as links.

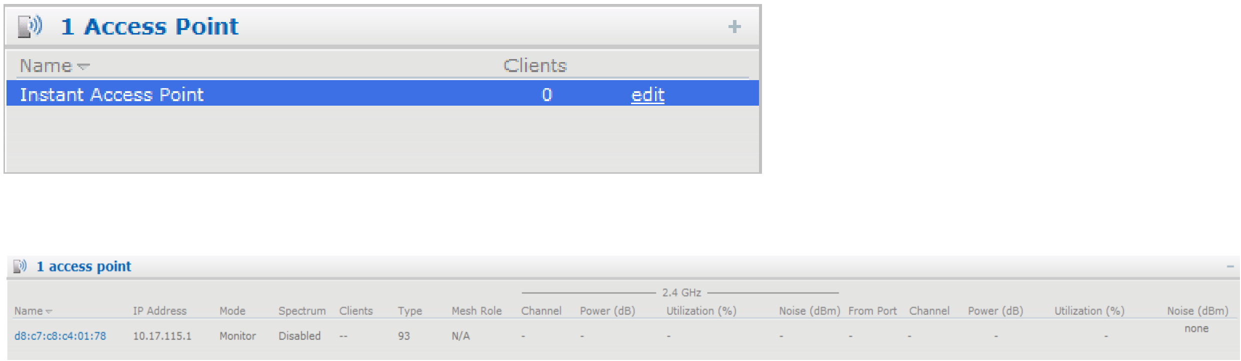
If the Auto Join Mode feature is disabled, a **New** link appears. Click on this link to add a new IAP to the network. If an IAP is configured and not active, its MAC Address is displayed in red.

The expanded view displays the following information about each IAP:

- **Name**— Name of the access point.
- **IP Address**— IP address of the IAP.
- **Mode—** Mode of the IAP.
- **Spectrum—** Enabled, if the IAP is configured as dedicated full-spectrum RF monitor.
- **Clients**— Number of clients that are connected to the IAP.
- **Type**— Model number of the IAP.
- **Mesh Role—** Role of the mesh IAP
- **Channel**— Channel the IAP is currently broadcasting on.
- **Power (dB)**— Maximum transmit EIRP of the radio.
- **Utilization (%)**— Utilization percentage of the IAP radios.
- **Noise (dBm)**— Noise floor of the IAP.

An **edit** link appears on clicking the IAP name. For details about editing IAP settings see, "Editing IAP Settings" on page 91.

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



1 Access Point

Name	Clients	
Instant Access Point	0	edit

1 access point

							2.4 GHz								
Name	IP Address	Mode	Spectrum	Clients	Type	Mesh Role	Channel	Power (dB)	Utilization (%)	Noise (dBm)	From Port	Channel	Power (dB)	Utilization (%)	Noise (dBm)
d8:c7:c8:c4:01:78	10.17.115.1	Monitor	Disabled	--	93	N/A	-	-	-	-	-	-	-	-	none

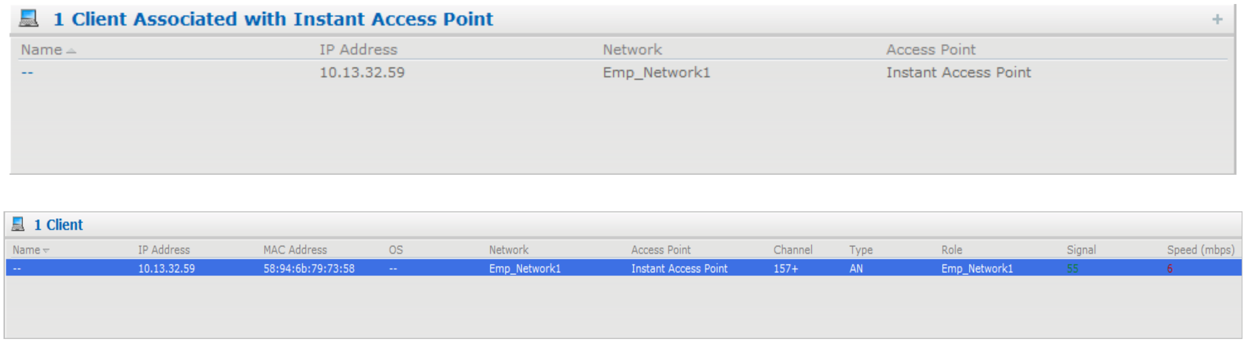
Clients Tab

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**— Network that the client is connected to.
- **Access Point**— IAP to which the client is connected.
- **Channel** — Channel that the client is currently broadcasting on.
- **Type**— Wi-Fi type of the client: A, G, AN, or GN.
- **Role—** Role assigned to the client.
- **Signal—** Indicates Signal strength**.**

- **Speed (mbps)**— Data transfer speed.

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



1 Client Associated with Instant Access Point

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

1 Client

Name	IP Address	MAC Address	OS	Network	Access Point	Channel	Type	Role	Signal	Speed (mbps)
--	10.13.32.59	58:94:6b:79:73:58	--	Emp_Network1	Instant Access Point	157+	AN	Emp_Network1	55	6

Links

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

- New Version Available
- Settings
- RF
- PEF
- Wired
- WIP
- VPN
- Maintenance
- Support
- Help
- Logout
- Monitoring
- Spectrum
- Alerts
- IDS
- Configuration
- Language
- AirWave Setup
- Pause/Resume

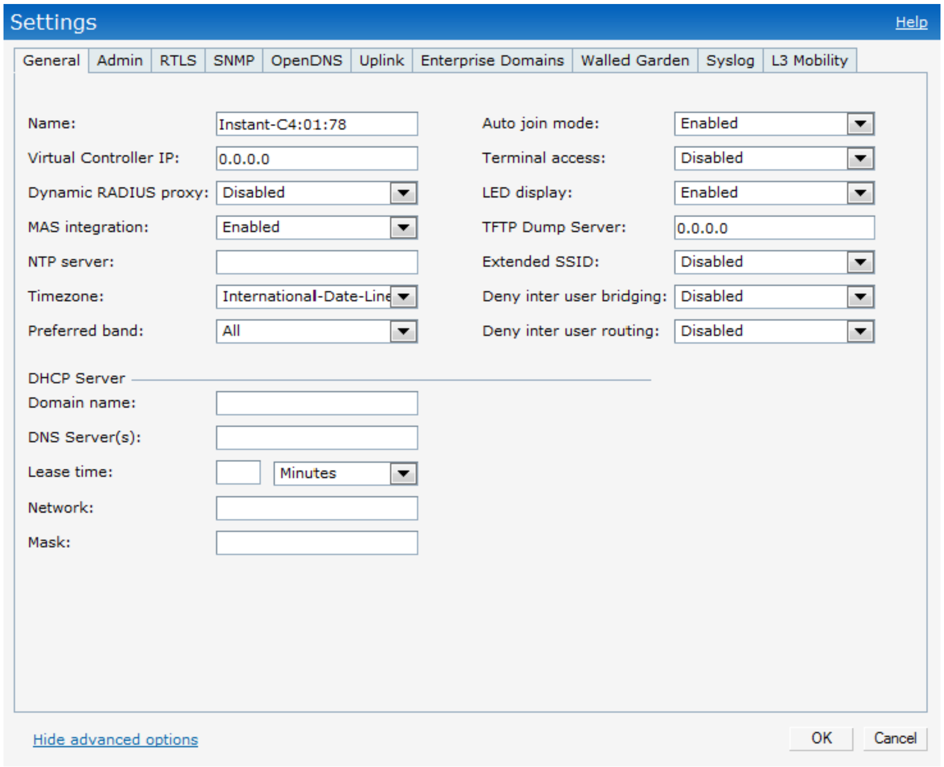
New Version Available

This link appears in the top right corner of Instant UI only if a new image version is available on the image server and AirWave is not configured. For more information about the **New version available** link and its functions, see "Firmware Image Server in Cloud Network" on page 101.

Settings

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

Figure 9 *Settings Link*



Name:	Instant-C4:01:78	Auto join mode:	Enabled
Virtual Controller IP:	0.0.0.0	Terminal access:	Disabled
Dynamic RADIUS proxy:	Disabled	LED display:	Enabled
MAS integration:	Enabled	TFTP Dump Server:	0.0.0.0
NTP server:		Extended SSID:	Disabled
Timezone:	International-Date-Line	Deny inter user bridging:	Disabled
Preferred band:	All	Deny inter user routing:	Disabled

DHCP Server

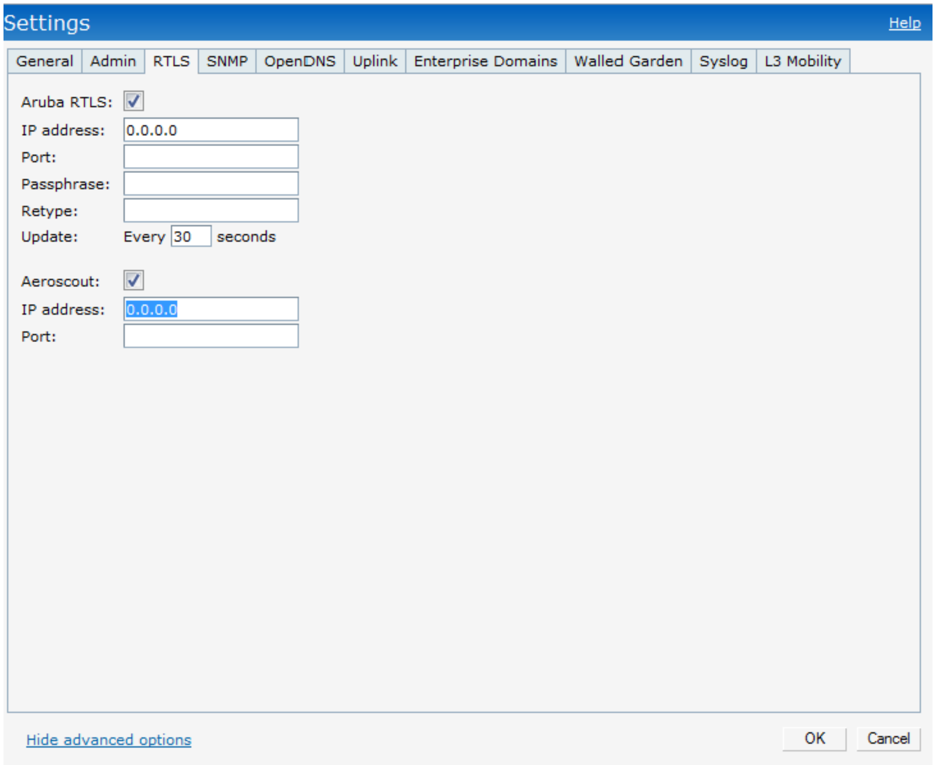
Domain name:	
DNS Server(s):	
Lease time:	Minutes
Network:	
Mask:	

NOTE

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

- **General**— View or edit the Name, IP address, NTP Server, and DHCP server settings of the Virtual Controller. For information about Virtual Controller settings and NTP Server, see Chapter 11, “Virtual Controller” and Chapter 10, “NTP Server” . For information about Auto join mode, Terminal Access, LED display, TFTP Dump Server, and Deny inter user bridging see Chapter 6, “Managing IAPs” . For information on MAS integration, see Chapter 7, “Mobility Access Switch Integration” .
- **Admin**— View or edit the admin credentials for access to the Virtual Controller Management User Interface. See “Management Authentication Settings” on page 130 for more information. You can also configure AirWave in this tab. See “Configuring AirWave” on page 207 for more information.
- **RTLS**— View or edit the RTLS server settings.
  - **Aruba RTLS—** Enable this to integrate with AirWave Management platform, Ekahau Real Time Location Server and Nearbuy Real Time Location Server. Specify the IP address and port number of the server to which location reports are sent, a shared secret key, and the frequency at which packets are sent to the server. **Update** indicates how frequently the Virtual Controller updates the RTLS server.
  - **Aeroscout—** Enables the AP to send RFID tag information to an AeroScout real-time asset location (RTLS) server. Specify the IP address and port number of the AeroScout server to which location reports should be sent.

Figure 10 *RTLS*



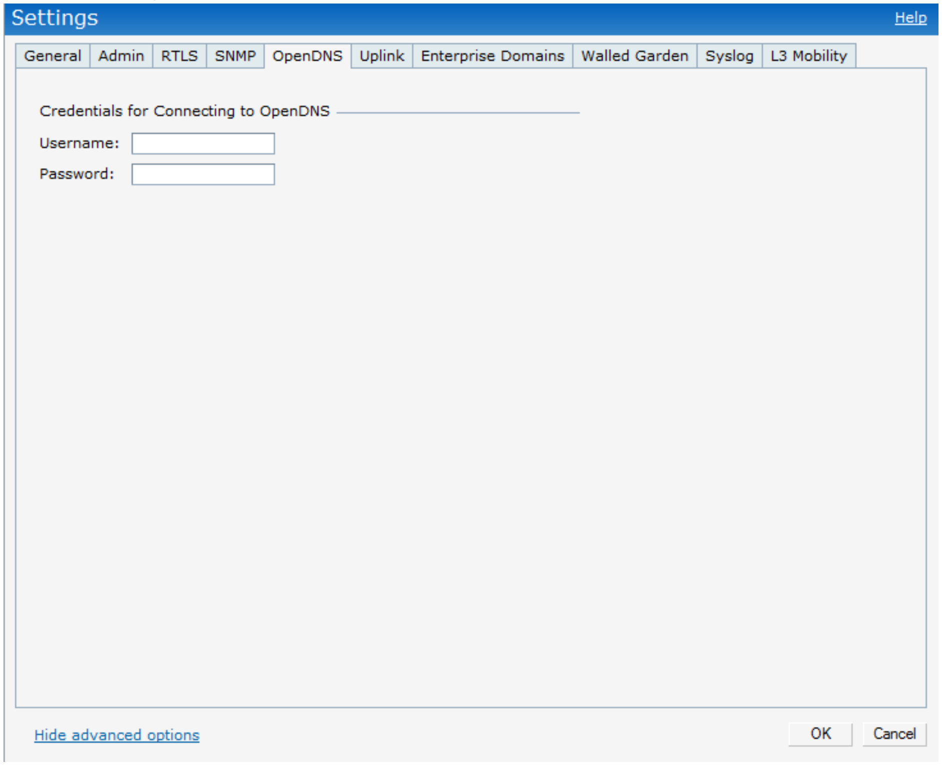
Settings

Aruba RTLS: ☑
IP address: 0.0.0.0
Port:
Passphrase:
Retype:
Update: Every 30 seconds

Aeroscout: ☑
IP address: 0.0.0.0
Port:

- **SNMP—** View or specify SNMP agent settings. See Chapter 21, “SNMP” for more information.
- **OpenDNS—** Instant supports OpenDNS business solutions which requires an OpenDNS (http://www.opendns.com) account comprising a username and a password**.** These credentials are used by Instant to access OpenDNS to provide enterprise-level content filtering.

Figure 11 *OpenDNS*



Credentials for Connecting to OpenDNS

Username:

Password:

NOTE

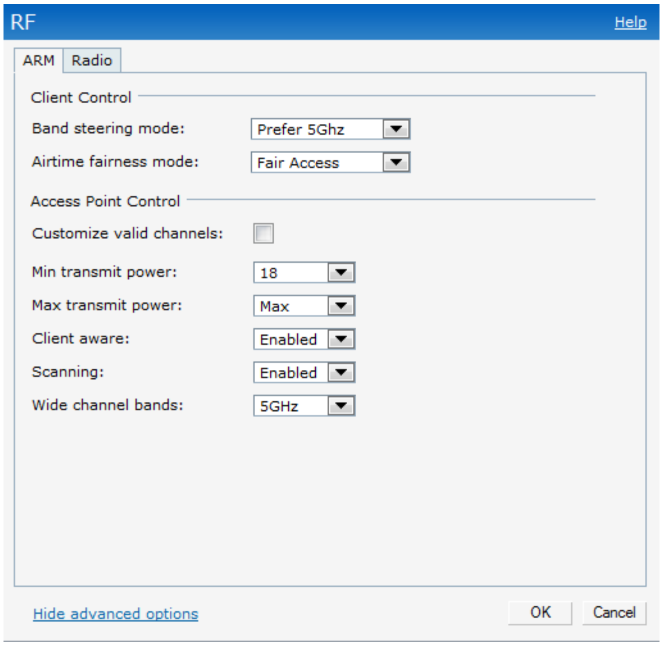
For OpenDNS to work, enable **Content Filtering** feature while creating a new network. Click **New** in the **Networks** tab and then select **Enabled** from the **Content filtering** drop-down list.

- **Uplink—** View or configure uplink settings. See Chapter 24, "Uplink Configuration" for more information.
- **Enterprise Domains—** This tab indicates all the DNS domain names valid on the enterprise network which is used to determine how client DNS requests should be routed. When **Content Filtering** is enabled for the wireless network, the names that do not match this list are sent to OpenDNS server.
- **Walled Garden—** The Walled Garden directs the user's navigation within particular areas to allow access to a selection of websites and/or prevent access to other websites. For more information, see "Walled Garden Access" on page 142.
- **Syslog—** View or specify a Syslog Server for sending syslog messages to the external servers. See "Syslog Server" on page 89 for more information.
- **L3 Mobility—** View or configure the Layer-3 mobility settings. See "Layer-3 Mobility" on page 107 for more information.

RF

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

Figure 12 *RF*



RF

Help

Client Control

Band steering mode: Prefer 5Ghz

Airtime fairness mode: Fair Access

Access Point Control

Customize valid channels: □

Min transmit power: 18

Max transmit power: Max

Client aware: Enabled

Scanning: Enabled

Wide channel bands: 5GHz

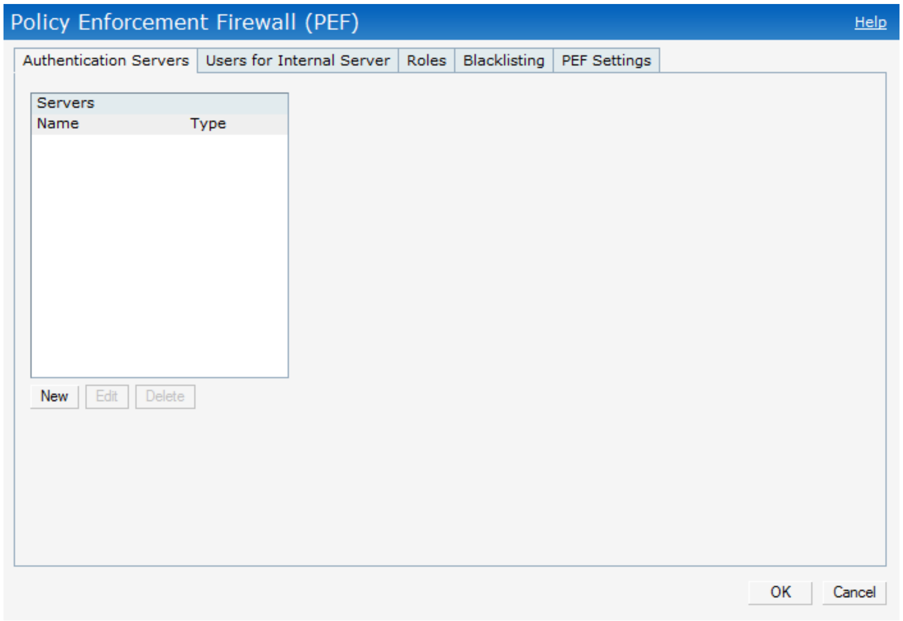
ARM — View or assign channel and power settings for all the IAPs in the network. For information about ARM (Adaptive Radio Management), see "ARM Features" on page 173.

Radio — View or configure radio settings for 2.4 GHz and the 5 GHz radio profiles. For information about Radio, see "Configuring Radio Profiles in Instant" on page 177.

PEF

This link displays the following features.

Figure 13 *PEF*



Policy Enforcement Firewall (PEF)

Help

Servers

Name	Type

Authentication Servers— Use this window to configure an external RADIUS server for a wireless network. See "Configuring an External RADIUS Server" on page 125 for more information.

Users for Internal Server— Use this window to populate the system's internal authentication server with users. This list is used by networks for which per-user authorization is specified using the Virtual

Controller's internal authentication server. For more information about users, see Chapter 30, "User Database" .

Roles— This window displays all the roles defined for all the Networks and the **Access Rules** lists the permissions for each role. For more information, see "User Roles" on page 151.

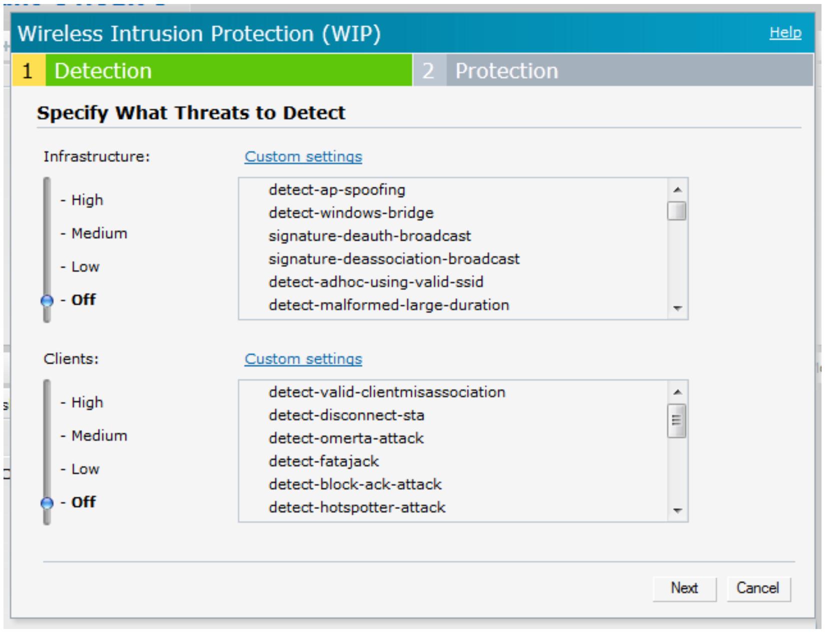
Blacklisting— Use this window to manually blacklist clients. See "Client Blacklisting" on page 239 for more information.

PEF Settings— Use this window to enable/disable gateway filters supporting address and port translation for various protocols. See Chapter 28, "Policy Enforcement Firewall" on page 235 for more information.

WIP

WIP offers a wide selection of intrusion detection and protection features to protect the network against wireless threats. Use this window to specify desired levels of threat detection. See "Wireless Intrusion Protection (WIP)" on page 181 for more information.

Figure 14 *WIP*



Wireless Intrusion Protection (WIP)

1 Detection

2 Protection

Specify What Threats to Detect

Infrastructure: Custom settings

- High
- Medium
- Low
- **Off**

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

Clients: Custom settings

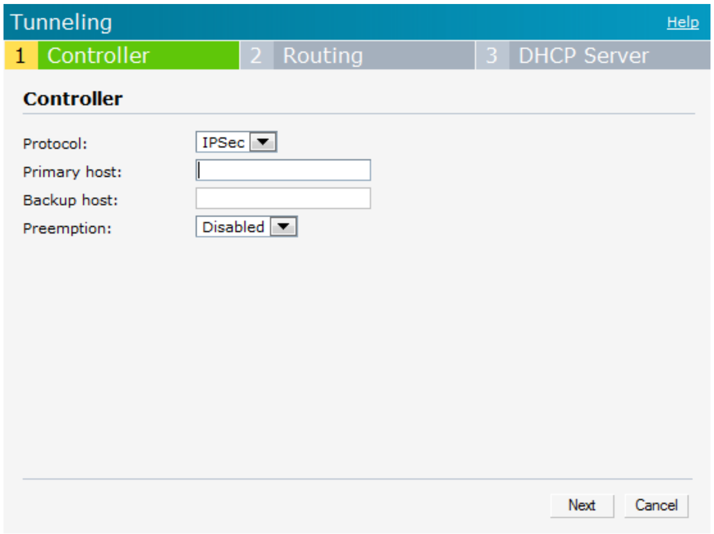
- High
- Medium
- Low
- **Off**

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

VPN

Use this window to define how the IAP communicates with the remote controller. See Chapter 29, "VPN Configuration" on page 243 for more information.

Figure 15 *VPN*



Controller

Protocol: IPSec

Primary host:

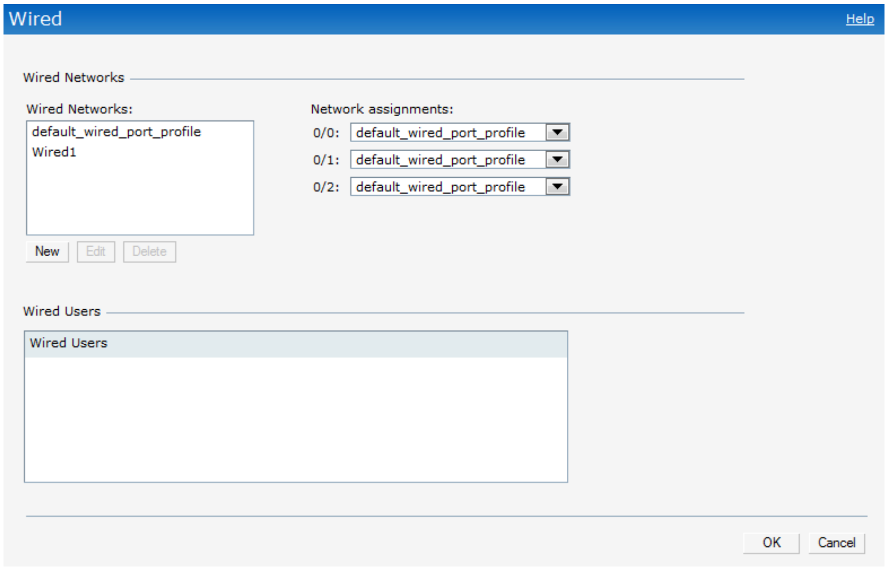
Backup host:

Preemption: Disabled

Wired

Specify the desired profile for each port of the IAP. See Chapter 23, “Ethernet Downlink” for more information.

Figure 16 *Wired*



Wired Networks

Wired Networks:
default_wired_port_profile
Wired1

Network assignments:

0/0: default_wired_port_profile

0/1: default_wired_port_profile

0/2: default_wired_port_profile

Wired Users

Wired Users

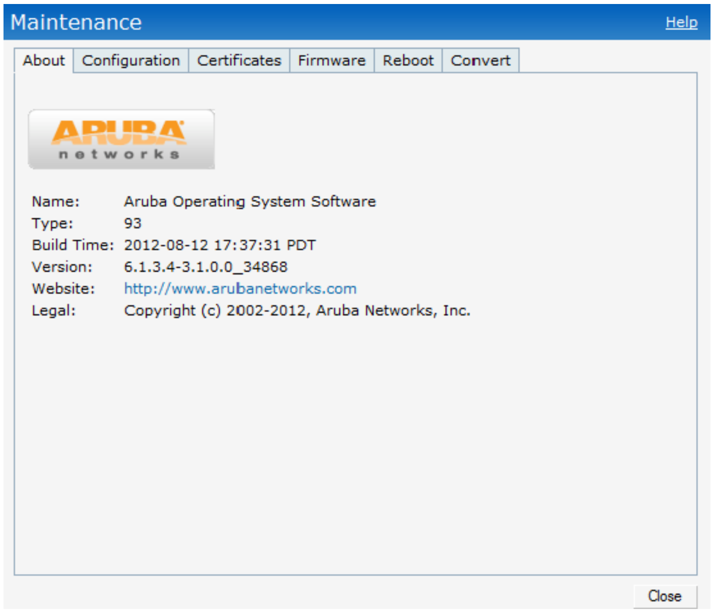
Maintenance

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

- **About**— Displays the Build Time, IAP model name, Aruba OS version, Web address of Aruba Networks, and Copyright information.
- **Configuration**— Displays the current configuration of the network.
  - **Clear Configuration—** Click to delete or clear the current configuration of the network and reset to provisioning configuration.
  - **Backup Configuration—** Use this feature to create local Instant configuration backup. Click **Backup Configuration** to save the configuration file named **instant.cfg**.

  - **Restore Configuration—** Click **Restore Configuration** to browse and locate the backup file to restore. Reboot the IAP for the changes to take effect.
- **Certificates** — Displays information about the current certificate installed in the network. Provides an interface to upload new certificates and to set a passphrase for the certificates. For more information, see "Certificates" on page 143.
- **Firmware** — Displays the current firmware version and provides options to upgrade to a new firmware version. For more information, see"Upgrading to New Version" on page 102.
- **Reboot** — Displays the IAPs in the network and provides an option to reboot the required access point or all access points. For more information, see "Rebooting the IAP" on page 99.
- **Convert** — Provides an option to change the network from a Virtual Controller managed network to an Aruba Mobility Controller managed network. For more information, see "Migrating to a Mobility Controller Managed Network" on page 95.

Figure 17 *Maintenance Link — Default View*



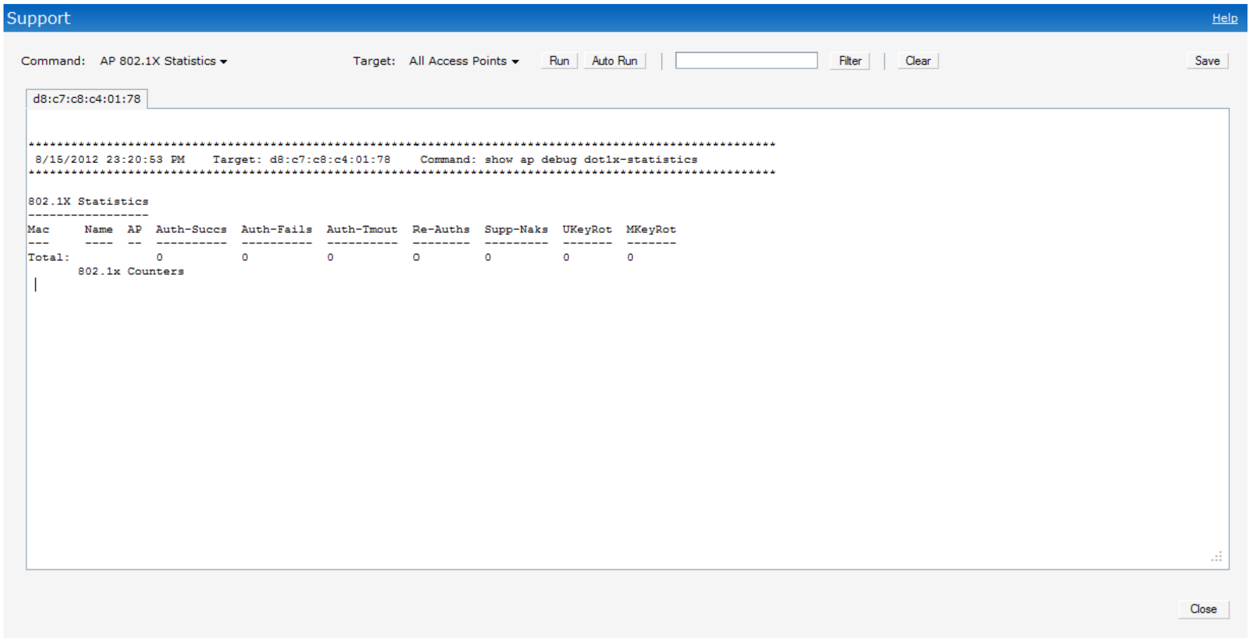
Name: Aruba Operating System Software
Type: 93
Build Time: 2012-08-12 17:37:31 PDT
Version: 6.1.3.4-3.1.0.0_34868
Website: http://www.arubanetworks.com
Legal: Copyright (c) 2002-2012, Aruba Networks, Inc.

Support

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

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

Figure 18 *Support Window*



Command: AP 802.1X Statistics

Target: All Access Points

d8:c7:c8:c4:01:78

```
*********************************************************************************************************
 8/15/2012 23:20:53 PM    Target: d8:c7:c8:c4:01:78    Command: show ap debug dot1x-statistics
*********************************************************************************************************

802.1X Statistics
-----------------
Mac     Name  AP  Auth-Succs  Auth-Fails  Auth-Tmout  Re-Auths  Supp-Naks  UKeyRot  MKeyRot
---     ----  --  ----------  ----------  ----------  --------  ---------  -------  -------
Total:            0           0           0           0         0          0        0
       802.1x Counters
```

To view the log information:

1. At the top right corner of Instant UI, click **Support**. The **Support** window appears.
2. Select the required option from the **Command** drop-down list. For example, **AP ARM Configuration**.
3. Select **All Access Points** or a specific IAP from the **Target** drop-down list for which you want to view the **AP ARM Configuration**.
4. Click **Run**.

NOTE

Use the support commands under the supervision of Aruba technical support.

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

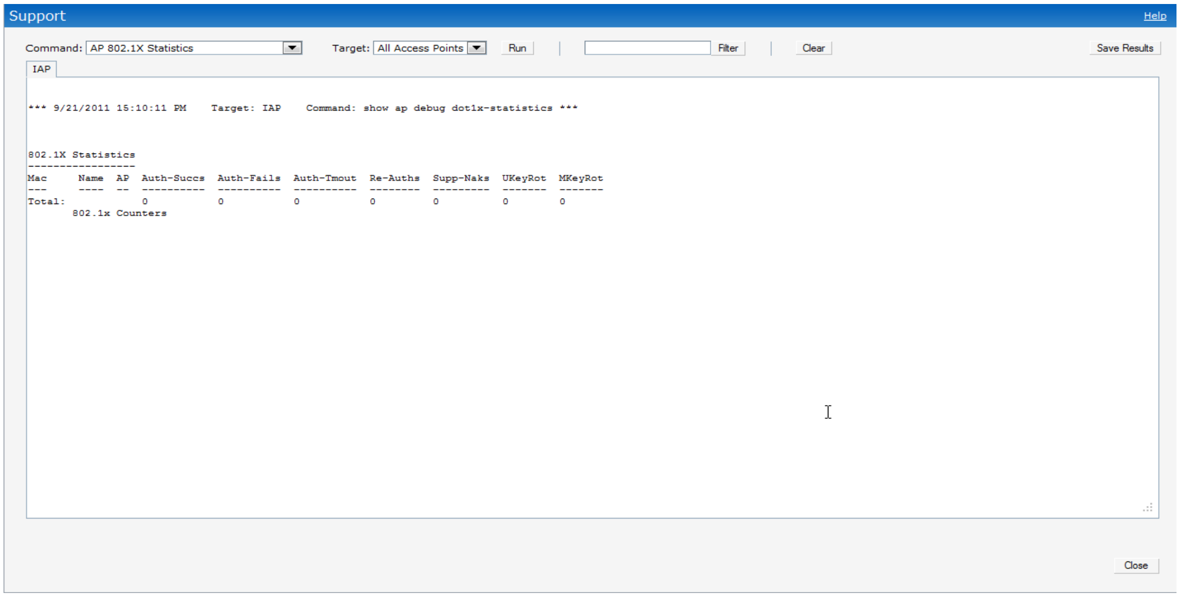
- **AP Access Rule Table—** Displays all the ACL rules of the selected IAP**.**
- **AP Active—** Displays all the APs of Instant**.**
- **AP All Supported Timezones—** Displays all the supported time zones of Instant**.**
- **AP ARM Channels—** Displays channels of ARM in the selected IAP**.**
- **AP ARM Configuration—** Displays configuration of ARM in the selected IAP**.**
- **AP Country Codes—** Displays country code for the selected IAP**.**

- **AP CPU Utilization—** Displays utilization of CPU for the selected IAP.
- **AP Current Time—** Displays current time of the selected IAP.
- **AP Current Timezone—** Displays current time zone of the selected IAP.
- **AP Log All—** Displays all logs of the selected IAP.
- **AP Log Debug—** Displays logs about the selected IAP.
- **AP Log Network—** Displays network logs of the selected IAP.
- **AP Log Security—** Displays security logs of the selected IAP.
- **AP Log System—** Displays system logs of the selected IAP.
- **AP Log User-Debug—** Displays user-debug logs of the selected IAP.
- **AP Log User—** Displays user logs of the selected IAP.
- **AP Log Wireless—** Displays wireless logs of the selected IAP.
- **AP Driver Configuration—** Displays driver configuration details of the selected IAP.
- **AP Essid Table—** Displays networks of the selected IAP.
- **AP Flash Configuration—** Displays statistics of the selected IAP in flash.
- **AP Memory Utilization—** Displays memory utilization of the selected IAP.
- **AP Mesh Counters—** Displays the mesh counters of the selected IAP.
- **AP Mesh Link—** Displays the mesh link of the selected IAP.
- **AP Mesh Neighbors—** Displays the mesh link neighbors of the selected IAP.
- **AP Monitor AP Table—** Displays the list of monitored APs of the selected IAP.
- **AP Monitor Client Table—** Displays the list of monitored clients of the selected IAP.
- **AP Monitor Potential AP Table—** Displays the list of potential AP of the selected IAP.
- **AP Monitor Potential Client Table—** Displays the list of potential AP of the selected IAP.
- **AP Monitor Status—** Displays the configuration and status of monitor information of the selected IAP.
- **AP Persistent Clients—** Displays the persistent clients of the selected IAP.
- **AP Process—** Displays the processes of the selected IAP.
- **AP Shaping Table—** Displays the VAP statistics of the selected IAP.
- **AP Sockets—** Displays the using sockets of the selected IAP.
- **AP STM Configuration—** Displays the SSID configuration in STM of the selected IAP.
- **AP Valid Channels—** Displays valid channels of the selected IAP.
- **AP Version—** Displays the version number of the selected IAP.
- **IDS Client List—** Displays the IDS detected client list of the selected IAP.
- **Interface Counters—** Displays the package counters of bond0 of the selected IAP.
- **Interface Port Status—** Displays the status of br0 of the selected IAP.
- **IP ARP Table—** Displays the ARP table of the selected IAP.
- **IP DHCP Database—** Displays the configuration of internal DHCP server of the selected IAP.
- **IP Route Table—** Displays the route table of the selected IAP.
- **VC 802.1X Certificate—** Displays the CA certificate and server certificate of the selected IAP.
- **VC About—** Displays some info of the selected IAP, including AP type, build time of image, image version.
- **VC Allowed AP Table—** Displays allowed AP enable/disable status and allowed AP list of the selected IAP.

- **VC Application Services—** Displays the details of application services of the selected IAP, which includes protocol number, port number**.**
- **VC Global Alerts—** Displays all the alerts about client of the selected IAP**.**
- **VC Global Statistics—** Displays the flow information and signal strength of the selected **IAP.**
- **VC Local User Database—** Displays the user configuration of the selected **IAP.**
- **VC Radius Attributes—** Displays the RADIUS attributes of the selected **IAP.**
- **VC Radius Servers—** Displays the RADIUS servers' configuration of the selected **IAP.**
- **VC Saved Configuration—** Displays the saved configuration information of the selected **IAP.**
- **VC SNMP Configuration—** Displays the SNMP configuration of the selected **IAP.**
- **AP Summary**— Displays the IAP configuration.
- **Debug Logs**— Displays debug logs of the selected IAP.
- **Driver Logs**— Displays the driver logs of the selected IAP.
- **Tech Support Dump**— Displays the technical support dump logs of the selected IAP.
- **Active Configuration**— Displays the active configuration of Virtual Controller.
- **Saved Configuration**— Displays the saved configuration of Virtual Controller.
- **AP Management Frames**— Displays the traced 802.11 management frames for the selected IAP.
- **AP Authentication Frames**— Displays the authentication trace buffer information of the selected IAP.
- **AP System Status**— Displays detailed system status information for the selected IAP.
- **AP Crash Info**— Displays crash log information (if it exists) for the selected IAP. The stored information is cleared from the flash after the AP reboots.
- **AP 802.1X Statistics**— Displays the 802.1X statistics of the selected IAP.
- **AP RADIUS Statistics**— Displays the RADIUS statistics of the selected IAP.
- **AP System Status**— Displays the system status of the selected IAP.
- **AP Client Table**— Displays information of the client connected to the selected IAP.
- **AP Association Table**— Displays information of the selected IAP association.
- **AP Allowed Channels**— Displays information of the allowed channels for the selected IAP.
- **AP Radio 0 Stats**— Displays aggregate debug statistics of the selected IAP Radio 0.
- **AP Radio 1 Stats**— Displays aggregate debug statistics of the selected IAP Radio 1.
- **Bridge Table**— Displays bridge table entry statistics including Mac address, VLAN, assigned VLAN, Destination and flag information for the selected IAP.
- **User Table**— Displays datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length for the selected IAP.
- **Session Table**— Displays the datapath session table statistics for the selected IAP.
- **Route Table**— Displays datapath route table statistics for the selected IAP.
- **Datapath Statistics**— Displays the hardware packet statistics for the selected IAP.
- **VLAN Table**— Displays the VLAN table information such as VLAN memberships inside the datapath including L2 tunnels for the selected IAP.
- **BSSID Table**— Displays the Basic Service Set (BSS) table of the selected IAP.
- **IDS Status**— Displays WLAN Interface, Data Structures, WLAN Interface Switch Status and RTLS Configuration tables for the selected IAP.
- **IDS AP Table**— Displays the Monitored IAP Table, which lists all the IAPs monitored by the selected IAP.

- **ARM Bandwidth Management**— Displays bandwidth management information for the selected IAP.
- **ARM History**— Displays the channel history and power changes due to Adaptive Radio Management (ARM) for the selected IAP.
- **ARM Neighbors**— Displays the ARM settings for the selected IAP's neighbors.
- **ARM RF Summary**— Displays the state and statistics for all channels being monitored by the selected IAP.
- **ARM Scan Times**— Displays AM channel scan times for the selected IAP.
- **OpenDNS Configuration and Status**— Displays configuration and status about open dns server.

Figure 19 *Support commands*



```
*** 9/21/2011 15:10:11 PM    Target: IAP    Command: show ap debug dot1x-statistics ***


802.1X Statistics
-----------------
Mac     Name  AP  Auth-Succs  Auth-Fails  Auth-Tmout  Re-Auths  Supp-Naks  UKeyRot  MKeyRot
---     ----  --  ----------  ----------  ----------  --------  ---------  -------  -------
Total:            0           0           0           0         0          0        0
       802.1x Counters
```

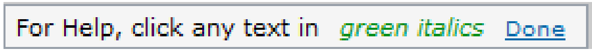
Help

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:

1. At the top right corner of Instant UI, click the **Help** link.

Figure 20 *Help Link*



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

Logout

Use this link to logout of the Instant UI.

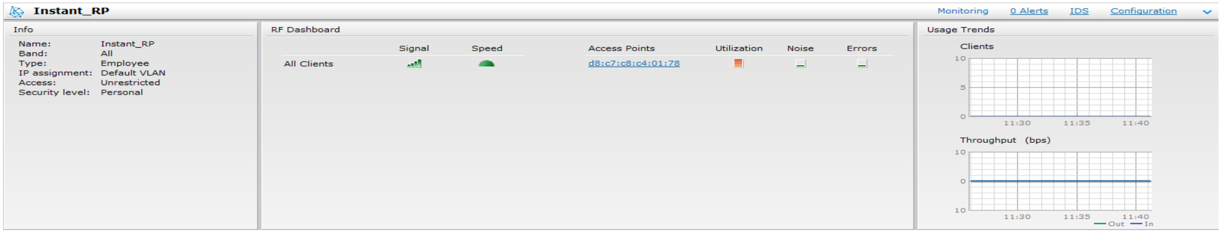
Monitoring

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

- Info
- RF Dashboard

- Usage Trends

Figure 21 *Monitoring on Instant UI*



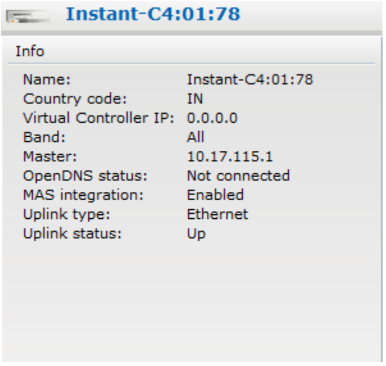
Name: Instant_RP
Band: All
Type: Employee
IP assignment: Default VLAN
Access: Unrestricted
Security level: Personal

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

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 22 *Info Section in the Monitoring Pane*

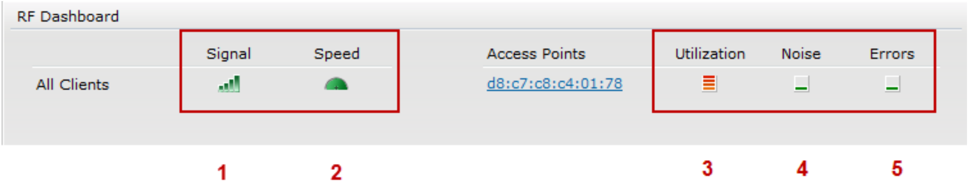


Name: Instant-C4:01:78
Country code: IN
Virtual Controller IP: 0.0.0.0
Band: All
Master: 10.17.115.1
OpenDNS status: Not connected
MAS integration: Enabled
Uplink type: Ethernet
Uplink status: Up

RF Dashboard

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

Figure 23 *RF Dashboard in the Monitoring Pane*



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

The following table lists the icons in the RF Dashboard.

Table 3 *RF Dashboard icons*

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

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

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

  - Speed— Displays the data transfer speed of the client. Depending on the data transfer speed of the client, the color of the Signal bar changes from Green > Orange > Red.
    - Green— Data transfer speed is more than 50 percent of the maximum speed supported by the client.
    - Orange— Data transfer speed is between 25-50 percent of the maximum speed supported by the client.
    - Red— Data transfer speed is less than 25 percent of the maximum speed supported by the client.

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

- Access Points— Lists the IAPs whose utilization, noise, or errors are not within the specified threshold. The IAP names appear as links. When the IAP is clicked, the IAP configuration information is displayed in the Info section. The RF Dashboard section is pushed to the bottom left corner of the Instant UI. The RF Trends section appears in its place. This section consists of the Utilization, Band frames, Noise Floor, and Errors graphs. For more information on the graphs, see Chapter 26, “Monitoring” .
  - Utilization— Displays the radio utilization rate of the IAPs. Depending on the percentage of utilization, the color of the lines on the Utilization icon changes from Green > Orange > Red.
    - Green— Utilization is less than 50 percent.
    - Orange— Utilization is between 50-75 percent.
    - Red— Utilization is more than 75 percent.

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

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

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

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

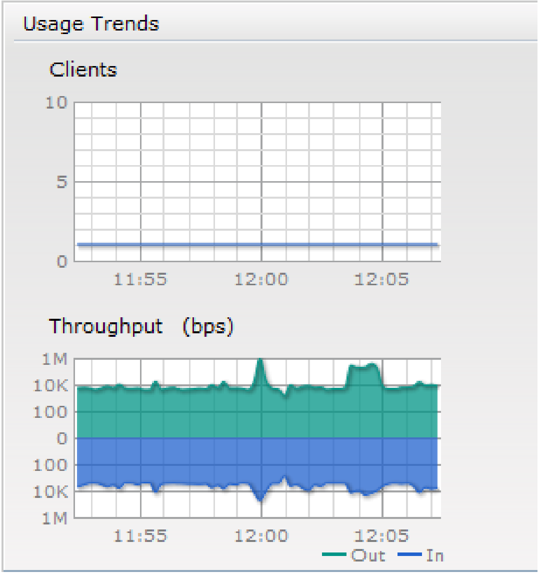
To view the errors graph of an IAP, click on the Errors icon against the IAP in the Errors column.

Usage Trends

Displays the following graphs:

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

Figure 24 *Usage Trends Section in the Monitoring Pane*



For more information about the graphs and monitoring procedures, see Chapter 26, “Monitoring” .

Spectrum

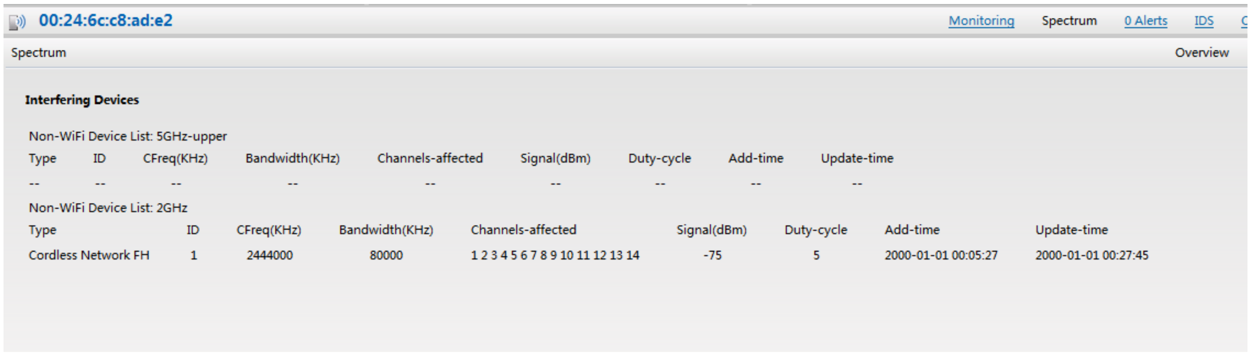
The spectrum link (in the Access Point view) displays the spectrum data that is collected by a hybrid AP or by an IAP that has enabled spectrum monitor. The spectrum data is not reported to the VC.

The spectrum link displays the following:

Overview (Device list)

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

Figure 25 *Device List*



Interfering Devices

Non-WiFi Device List: 5GHz-upper

Type	ID	CFreq(KHz)	Bandwidth(KHz)	Channels-affected	Signal(dBm)	Duty-cycle	Add-time	Update-time
--	--	--	--	--	--	--	--	--

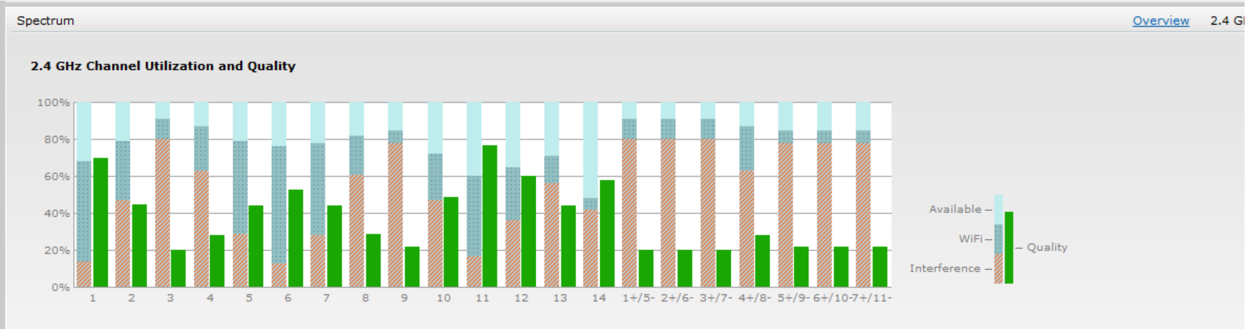
Non-WiFi Device List: 2GHz

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

2.4 GHz

This graph shows channel utilization information such as, channel quality, availability and utilization metrics as seen by a spectrum monitor for the 2.4 GHz radio band. The data displayed includes percentage of Quality, Availability, Wi-Fi utilization, and Interference utilization.

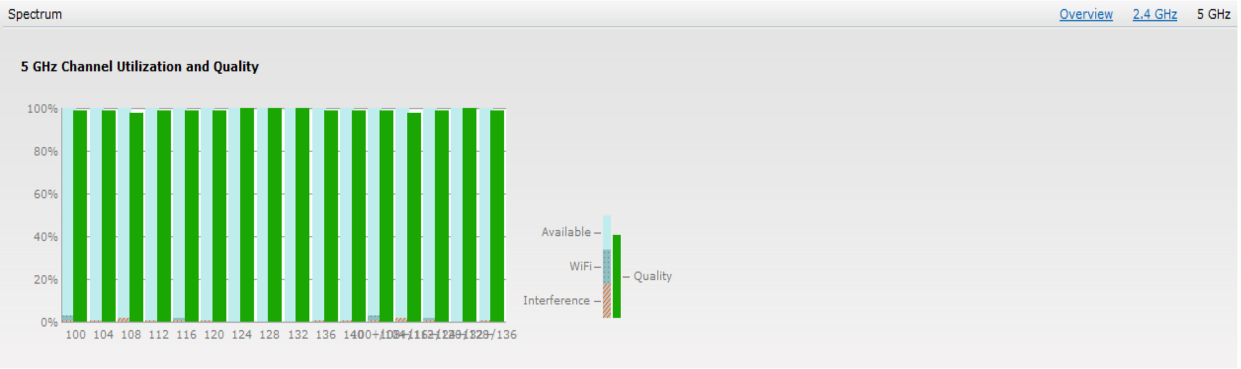
Figure 26 *Channel Metrics for the 2.4 GHz Radio Channel*



5 GHz

This graph shows channel utilization information such as, channel quality, availability and utilization metrics as seen by a spectrum monitor for the 5 GHz radio band. The data displayed includes percentage of Quality, Availability, Wi-Fi utilization, and Interference utilization.

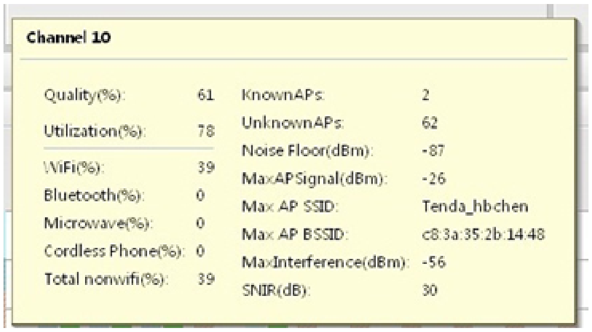
Figure 27 *Channel Metrics for the 5 GHz Radio Channel*



Channel Details

When you hover your mouse over a channel, the channel details or the summary of the 802.11a or 802.11g channels seen by a spectrum monitor is displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference and the signal-to-noise-and-interference Ratio (SNIR). Spectrum monitors display spectrum analysis data seen on all channels in the selected band, and hybrid IAPs display data from the one channel they are monitoring.

Figure 28 *Channel Details Information*



Channel 10

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

For more information on spectrum monitoring, see “Spectrum Monitor” on page 111.

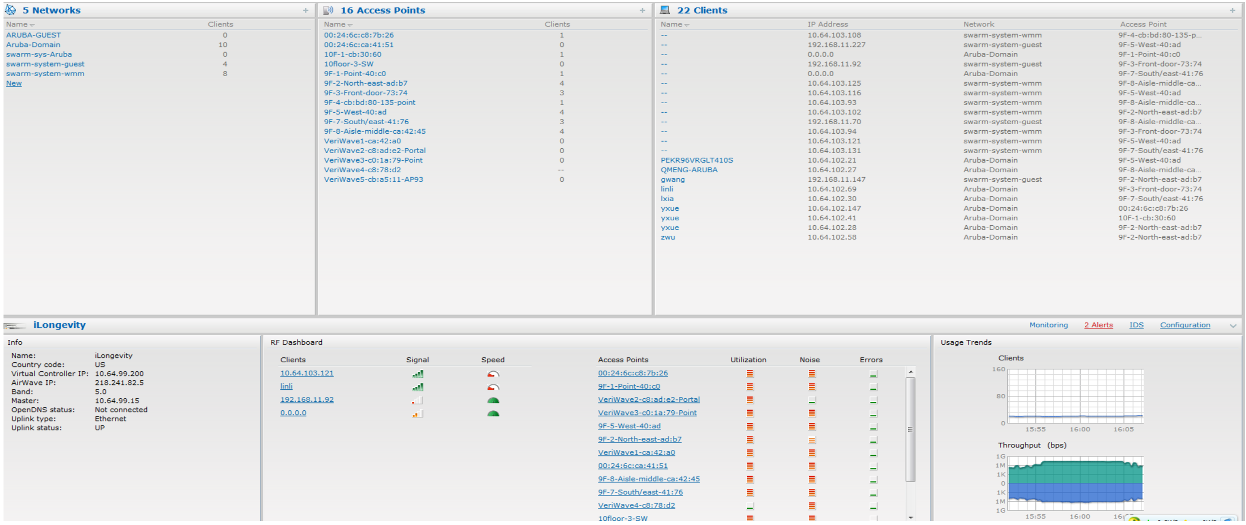
Alerts

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

NOTE

New alerts are generated for an incomplete DHCP transaction of a client.

Figure 29 *Alerts Link*



5 Networks

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

16 Access Points

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

22 Clients

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

iLongevity

Info

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

RF Dashboard

Clients
10.64.103.121
linli
192.168.11.92
0.0.0.0

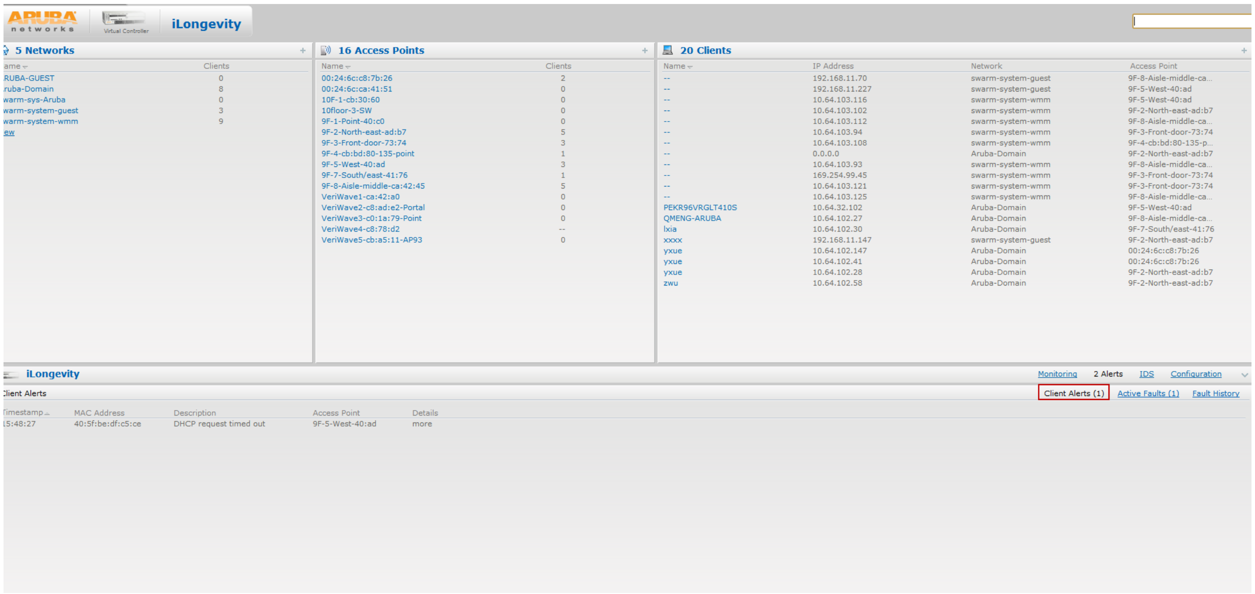
Access Points
00:24:6c:c8:7b:26
9F-1-Point-40:c0
VeriWave2-c8:ad:e2-Portal
VeriWave3-c0:1a:79-Point
9F-5-West-40:ad
9F-2-North-east-ad:b7
VeriWave1-ca:42:a0
00:24:6c:ca:41:51
9F-8-Aisle-middle-ca:42:45
9F-7-South/east-41:76
VeriWave4-c8:78:d2
10floor-3-SW

Client Alerts

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

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

Figure 30 *Client Alerts*



5 Networks

ame	Clients
RUBA-GUEST	0
ruba-Domain	8
warm-sys-Aruba	0
warm-system-guest	3
warm-system-wmm	9
ew	

16 Access Points

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

20 Clients

Name	IP Address	Network	Access Point
--	192.168.11.70	swarm-system-guest	9F-8-Aisle-middle-ca...
--	192.168.11.227	swarm-system-guest	9F-5-West-40:ad
--	10.64.103.116	swarm-system-wmm	9F-5-West-40:ad
--	10.64.103.102	swarm-system-wmm	9F-2-North-east-ad:b7
--	10.64.103.112	swarm-system-wmm	9F-8-Aisle-middle-ca...
--	10.64.103.94	swarm-system-wmm	9F-3-Front-door-73:74
--	10.64.103.108	swarm-system-wmm	9F-4-cb:bd:80-135-p...
--	0.0.0.0	Aruba-Domain	9F-2-North-east-ad:b7
--	10.64.103.93	swarm-system-wmm	9F-8-Aisle-middle-ca...
--	169.254.99.45	swarm-system-wmm	9F-3-Front-door-73:74
--	10.64.103.121	swarm-system-wmm	9F-3-Front-door-73:74
--	10.64.103.125	swarm-system-wmm	9F-8-Aisle-middle-ca...
PEKR96VRGLT410S	10.64.32.102	Aruba-Domain	9F-5-West-40:ad
QMENG-ARUBA	10.64.102.27	Aruba-Domain	9F-8-Aisle-middle-ca...
lxia	10.64.102.30	Aruba-Domain	9F-7-South/east-41:76
xxxx	192.168.11.147	swarm-system-guest	9F-2-North-east-ad:b7
yxue	10.64.102.147	Aruba-Domain	00:24:6c:c8:7b:26
yxue	10.64.102.41	Aruba-Domain	00:24:6c:c8:7b:26
yxue	10.64.102.28	Aruba-Domain	9F-2-North-east-ad:b7
zwu	10.64.102.58	Aruba-Domain	9F-2-North-east-ad:b7

lient Alerts

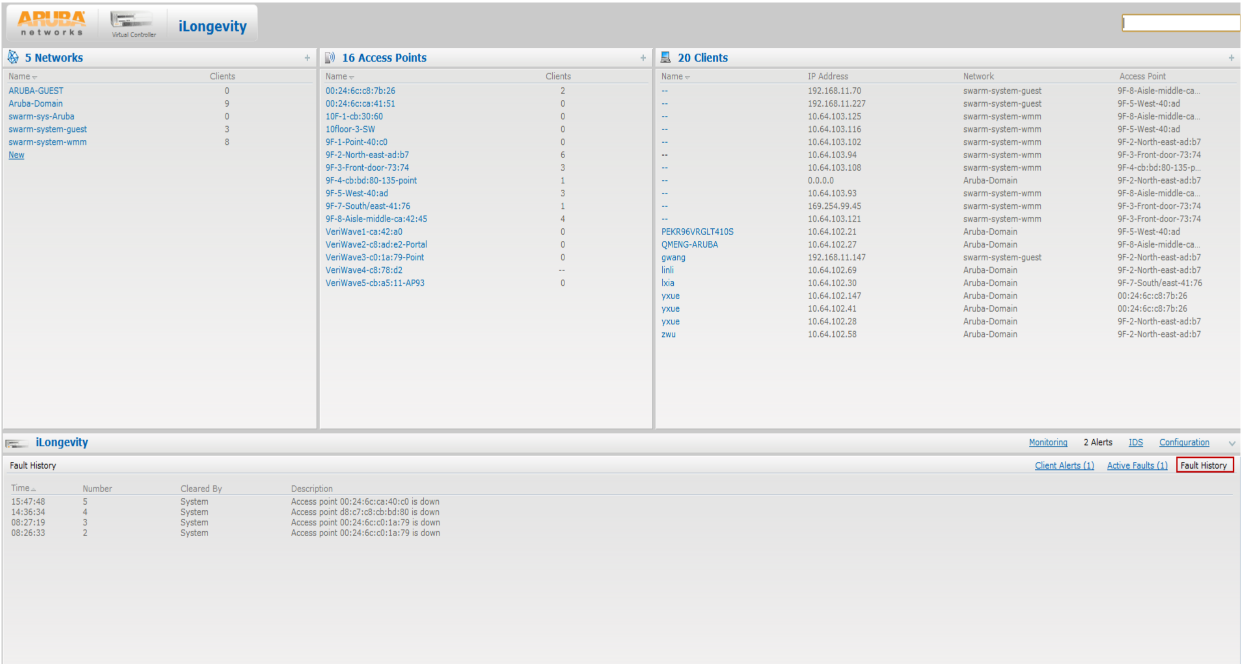
imestamp	MAC Address	Description	Access Point	Details
5:48:27	40:5f:be:df:c5:ce	DHCP request timed out	9F-5-West-40:ad	more

Fault History

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

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

Figure 31 *Fault History*



5 Networks

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

16 Access Points

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

20 Clients

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

Fault History

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

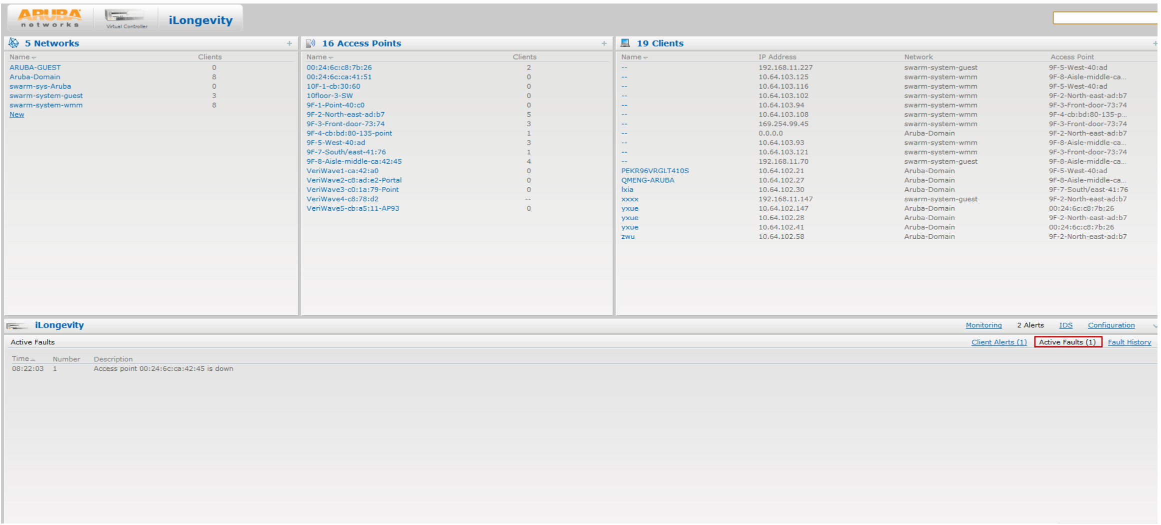
Active Faults

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

- Time— Displays the system time when an event occurs.

- Number— Indicates the number of sequence.
- Description— Displays the event details.

Figure 32 *Active Faults*



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

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

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

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

For more information about alerts, see Chapter 27, “Alert Types and Management” .

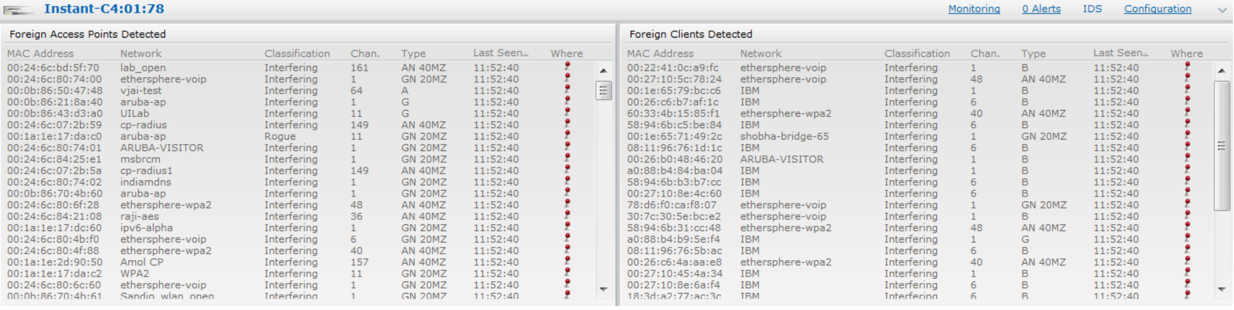
IDS

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

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

For more information on the intrusion detection feature, see Chapter 20, “Intrusion Detection System” .

Figure 33 *Intrusion Detection on Instant UI*



Foreign Access Points Detected

MAC Address	Network	Classification	Chan.	Type	Last Seen	Where
00:24:6c:bd:5f:70	lab_open	Interfering	161	AN 40MZ	11:52:40	📍
00:24:6c:80:74:00	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40	📍
00:0b:86:50:47:48	vjai-test	Interfering	64	A	11:52:40	📍
00:0b:86:21:8a:40	aruba-ap	Interfering	1	G	11:52:40	📍
00:0b:86:43:d3:a0	UILab	Interfering	11	G	11:52:40	📍
00:24:6c:07:2b:59	cp-radius	Interfering	149	AN 40MZ	11:52:40	📍
00:1a:1e:17:da:c0	aruba-ap	Rogue	11	GN 20MZ	11:52:40	📍
00:24:6c:80:74:01	ARUBA-VISITOR	Interfering	1	GN 20MZ	11:52:40	📍
00:24:6c:84:25:e1	msbrcm	Interfering	1	GN 20MZ	11:52:40	📍
00:24:6c:07:2b:5a	cp-radius1	Interfering	149	AN 40MZ	11:52:40	📍
00:24:6c:80:74:02	indiamdns	Interfering	1	GN 20MZ	11:52:40	📍
00:0b:86:70:4b:60	aruba-ap	Interfering	1	GN 20MZ	11:52:40	📍
00:24:6c:80:6f:28	ethersphere-wpa2	Interfering	48	AN 40MZ	11:52:40	📍
00:24:6c:84:21:08	raji-aes	Interfering	36	AN 40MZ	11:52:40	📍
00:1a:1e:17:dc:60	ipv6-alpha	Interfering	1	GN 20MZ	11:52:40	📍
00:24:6c:80:4b:f0	ethersphere-voip	Interfering	6	GN 20MZ	11:52:40	📍
00:24:6c:80:4f:88	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40	📍
00:1a:1e:2d:90:50	Amol CP	Interfering	157	AN 40MZ	11:52:40	📍
00:1a:1e:17:da:c2	WPA2	Interfering	11	GN 20MZ	11:52:40	📍
00:24:6c:80:6c:60	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40	📍
00:0b:86:70:4b:61	Sandin_wlan_open	Interfering	1	GN 20MZ	11:52:40	📍

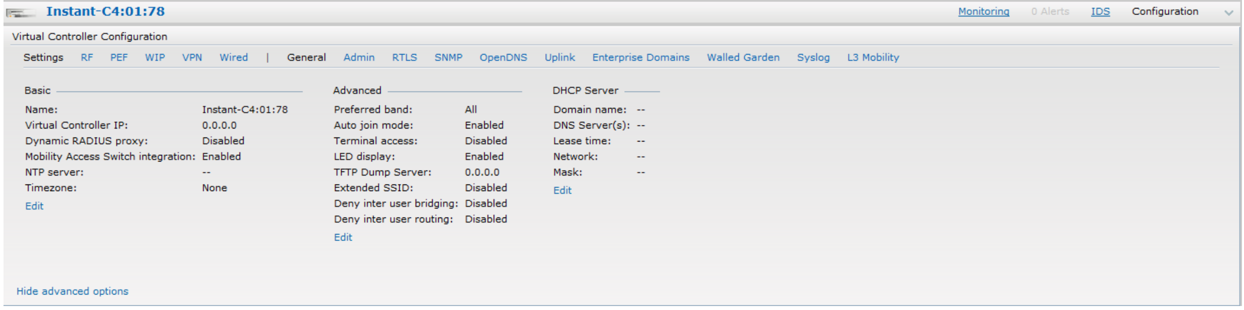
Foreign Clients Detected

MAC Address	Network	Classification	Chan.	Type	Last Seen	Where
00:22:41:0c:a9:fc	ethersphere-voip	Interfering	1	B	11:52:40	📍
00:27:10:5c:78:24	ethersphere-voip	Interfering	48	AN 40MZ	11:52:40	📍
00:1e:65:79:bc:c6	IBM	Interfering	1	B	11:52:40	📍
00:26:c6:b7:af:1c	IBM	Interfering	6	B	11:52:40	📍
60:33:4b:15:85:f1	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40	📍
58:94:6b:c5:be:84	IBM	Interfering	6	B	11:52:40	📍
00:1e:65:71:49:2c	shobha-bridge-65	Interfering	1	GN 20MZ	11:52:40	📍
08:11:96:76:1d:1c	IBM	Interfering	6	B	11:52:40	📍
00:26:b0:48:46:20	ARUBA-VISITOR	Interfering	1	B	11:52:40	📍
a0:88:b4:84:ba:04	IBM	Interfering	1	B	11:52:40	📍
58:94:6b:b3:b7:cc	IBM	Interfering	6	B	11:52:40	📍
00:27:10:8e:4c:60	IBM	Interfering	6	B	11:52:40	📍
78:d6:f0:ca:f8:07	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40	📍
30:7c:30:5e:bc:e2	ethersphere-voip	Interfering	1	B	11:52:40	📍
58:94:6b:31:cc:48	ethersphere-wpa2	Interfering	48	AN 40MZ	11:52:40	📍
a0:88:b4:b9:5e:f4	IBM	Interfering	1	G	11:52:40	📍
08:11:96:76:5b:ac	IBM	Interfering	6	B	11:52:40	📍
00:26:c6:4a:aa:e8	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40	📍
00:27:10:45:4a:34	IBM	Interfering	1	B	11:52:40	📍
00:27:10:8e:6a:f4	IBM	Interfering	6	B	11:52:40	📍
18:3d:a2:77:ac:3c	IBM	Interfering	6	B	11:52:40	📍

Configuration

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

Figure 34 *Configuration*



Virtual Controller Configuration

Basic

Name: Instant-C4:01:78
Virtual Controller IP: 0.0.0.0
Dynamic RADIUS proxy: Disabled
Mobility Access Switch integration: Enabled
NTP server: --
Timezone: None

Advanced

Preferred band: All
Auto join mode: Enabled
Terminal access: Disabled
LED display: Enabled
TFTP Dump Server: 0.0.0.0
Extended SSID: Disabled
Deny inter user bridging: Disabled
Deny inter user routing: Disabled

DHCP Server

Domain name: --
DNS Server(s): --
Lease time: --
Network: --
Mask: --

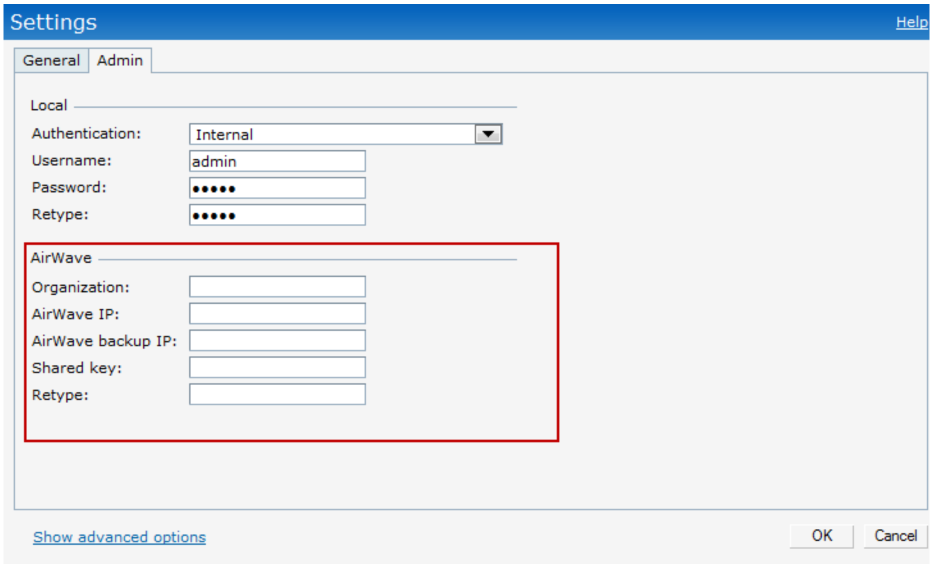
Language

The language links are provided in the login screen to allow users to select the preferred language before logging in to the Instant UI. In addition, this link is also 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 rapidly changing wireless networks. When enabled, AirWave allows you to manage the Instant network. For more information on AirWave, see Chapter 25, "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 window appears with **Admin** tab selected. For information to configure AirWave, see "Configuring AirWave" on page 207.

Figure 35 *AirWave Setup Link – AirWave Configuration*



Local

Authentication: Internal

Username: admin

Password: •••••

Retype: •••••

AirWave

Organization:

AirWave IP:

AirWave backup IP:

Shared key:

Retype:

Pause/Resume

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

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

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

Views

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

- Virtual Controller view— The Virtual Controller view is the default view. This view allows you to monitor the 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 name of the network that you want to monitor. Network view for the selected network appears.
- Instant Access Point view— The Instant Access Point view provides information that is necessary to monitor a selected IAP. All IAPs in the Aruba Instant network are listed in the **Access Points** tab. Click the name of the IAP that you want to monitor. Access Point view for that IAP appears.
- Client view— The Client view provides information that is necessary to monitor a selected client. In the Client view, all the 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 more information on the graphs and the views, see Chapter 26, “Monitoring” .

Chapter 4

Wireless Network

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

Table 4 *IEEE 802.11 Standards*

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

During start up, a wireless client searches for radio signals or beacon frames that originate from the nearest 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

NOTE

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

Employee Network

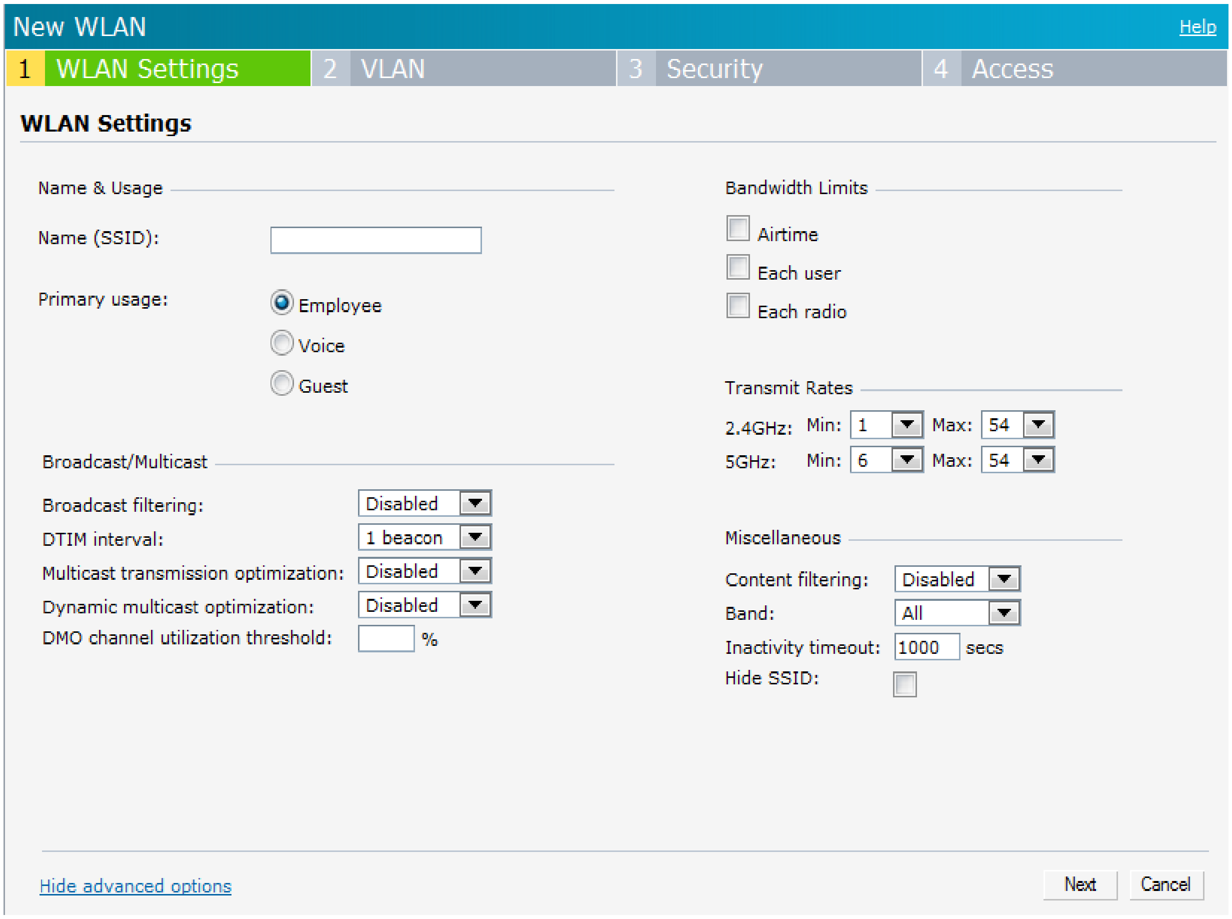
An Employee network is a classic Wi-Fi network. This network type is supported with full customization on Aruba Instant. It is used by the employees in the organization. Passphrase based or 802.1X based authentication methods are supported on this network type. Employees can access the protected data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

Adding an Employee Network

This section provides the procedure to add an employee network.

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

Figure 36 *Adding an Employee Network — Basic Info Tab*



WLAN Settings

Name & Usage

Name (SSID):

Primary usage: ● Employee ○ Voice ○ Guest

Broadcast/Multicast

Broadcast filtering: Disabled

DTIM interval: 1 beacon

Multicast transmission optimization: Disabled

Dynamic multicast optimization: Disabled

DMO channel utilization threshold: %

Bandwidth Limits

□ Airtime

□ Each user

□ Each radio

Transmit Rates

2.4GHz: Min: 1 Max: 54

5GHz: Min: 6 Max: 54

Miscellaneous

Content filtering: Disabled

Band: All

Inactivity timeout: 1000 secs

Hide SSID: □

2. In the **WLAN Settings** tab, perform the following steps:

   a. **Name (SSID)**— Enter a name that uniquely identifies a wireless network.

   b. **Primary usage**— Select **Employee** (this is selected by default) from the **Primary usage** options. This selection determines whether the network is primarily intended to be used for employee data, guest data, or voice traffic.

3. Click the **Show advanced options** link and perform the following steps.

   a. Broadcast/Multicast

   - **Broadcast filtering**— When set to **All**, the IAP drops all broadcast and multicast frames except for DHCP and ARP. When set to **ARP**, in addition to the above, the IAP converts ARP requests to unicast and send frames directly to the associated client. When **Disabled**, all broadcast and multicast traffic is forwarded.
   - **DTIM interval**— Indicates the DTIM (delivery traffic indication message) period in beacons. You can configure this option for every WLAN SSID profile. The default value is 1, which means the client checks for buffered data on the IAP at every beacon. You may choose to configure a larger DTIM value for power saving.
   - **Multicast transmission optimization**— When **Enabled**, the IAP chooses the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. The default values are 1 mbps for 2.4 GHz and 6 mbps for 5.0GHz bands. Multicast traffic can be sent at upto 24 mbps when this option is enabled. This option is disabled by default.

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

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

b. **Bandwidth Limits—** You can specify three types of bandwidth limits.

- Airtime— Indicates the aggregate amount of airtime that all clients on this Network can use to send/receive data.
- Each user— Indicates the throughput for any single user on this Network. The throughput value is specified in kbps.
- Each radio— Indicates the aggregate amount of throughput each radio (some AP models have multiple radios) is allowed to provide for all clients connected to that radio

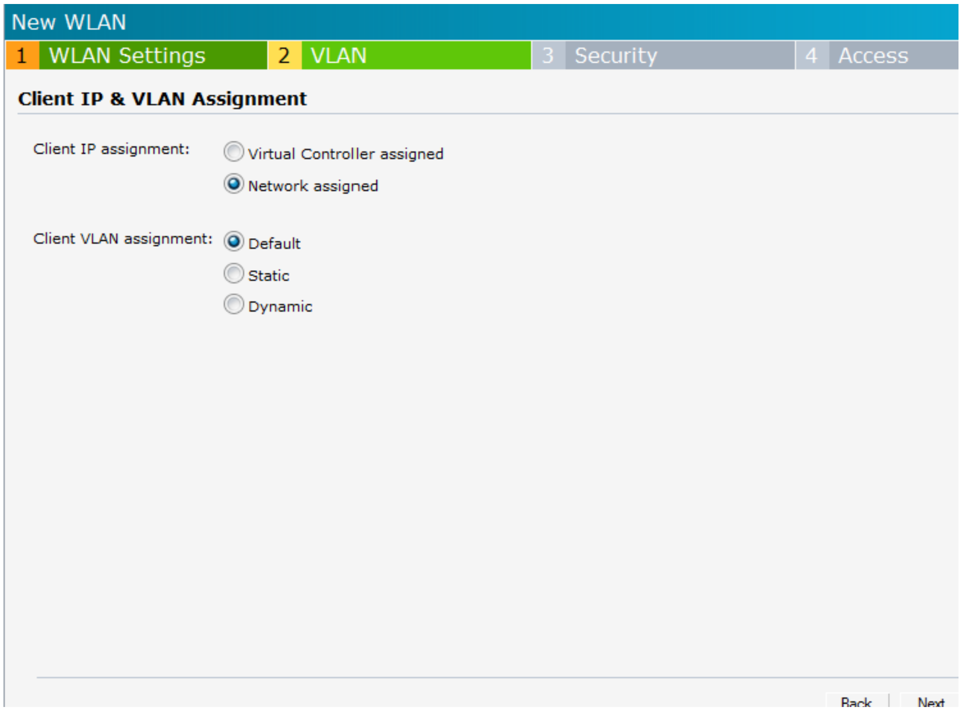
c. Transmit Rates— Indicates the ability to configure the basic and supported rates per SSID for Aruba Instant. Select to set the minimum and maximum legacy (non-802.11n) transmit rates for each band — 2.4 GHz and 5 GHz.

d. Miscellaneous

- Content filtering— When enabled, all DNS requests to non-corporate domains on this wireless network are sent to OpenDNS.
- Band**—** Set the band at which the network transmits radio signals. Available options are 2.4 GHz, 5 GHz and All. The All option is selected by default. It is also the recommended option.
- Inactivity timeout**—** Indicates the time in seconds after which an idle client ages out. The minimum value is 60 seconds and the default value is 1000 seconds.
- Hide SSID— Select this check box if you do not want the SSID (network name) to be visible to users.

4. Click **Next** to continue.

Figure 37 *Adding an Employee Network— VLAN Tab*



New WLAN

1 WLAN Settings | 2 VLAN | 3 Security | 4 Access

Client IP & VLAN Assignment

Client IP assignment: ○ Virtual Controller assigned ● Network assigned

Client VLAN assignment: ● Default ○ Static ○ Dynamic

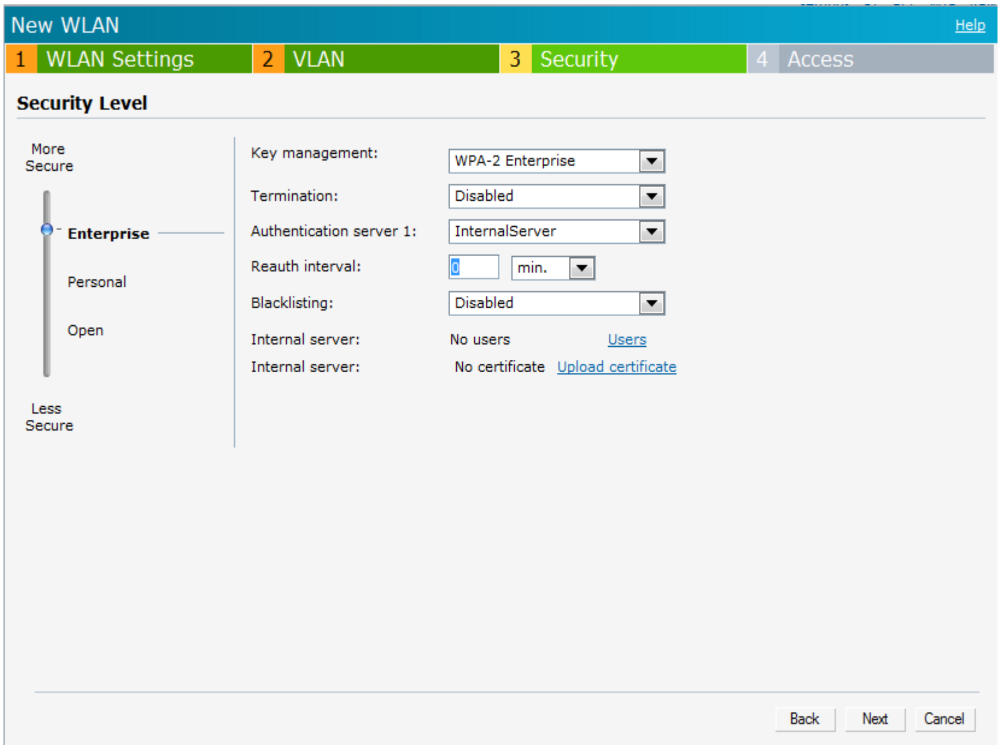
5. Select the required Client IP assignment option — **Virtual Controller assigned** or **Network assigned**.

Table 5 *Conditions for Client IP and VLAN assignment*

If	then
You select Virtual Controller assigned	The client gets the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the IAP for the wireless clients. The Virtual Controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi site wireless network. See Chapter 11, “Virtual Controller” on page 121 for configuring the DHCP server.
You select Network assigned	By default, the client VLAN is assigned to the native VLAN on the wired network. ● Default— The client gets the IP address in the same subnet as the IAPs. ● Static— Select to specify a VLAN for all clients on this network. ● Dynamic— Select to create rules for per-user VLAN assignment. See “VLAN Derivation Rule” on page 156 for more information.

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

Figure 38 *Employee Security Tab— Enterprise*



Security Level

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: InternalServer

Reauth interval: 0 min.

Blacklisting: Disabled

Internal server: No users Users

Internal server: No certificate Upload certificate

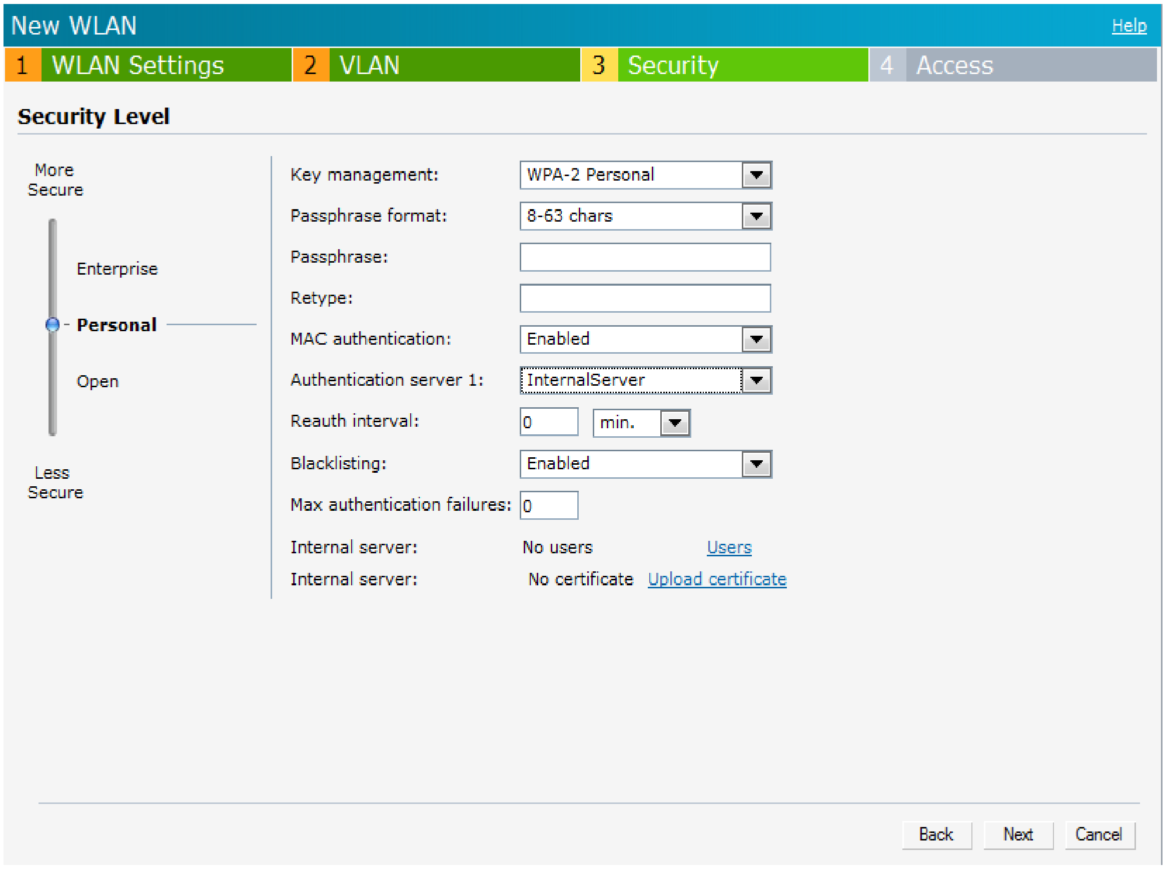
Table 6 *Conditions for Adding an Employee Network— Security Tab*

If	then,
You select the **Enterprise** security level	Perform the following steps: 1. Select the required key options from the **Key management** drop-down list. Available options are: ● WPA-2 Enterprise ● WPA Enterprise ● Both (WPA-2 & WPA) ● Dynamic WEP with 802.1X ● **Use Session Key for LEAP—** Use the **Session Key for LEAP** instead of using Session Key from the RADIUS Server to derive pair wise unicast keys. This is required for old printers that use dynamic WEP via LEAP authentication. This is **Disabled** by default. For more information on encryption and recommended encryption type, see Chapter 13, “Encryption” . 2. **Termination**— Enable this option to terminate the EAP portion of 802.1X authentication on the IAP instead of the RADIUS server. For more information, see “External RADIUS Server” on page 124. 3. **Authentication server 1—** Select the required Authentication server option from the drop-down list. Available options are: ● **New**— If you select this option, an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 12, “Authentication” . ● **InternalServer**— If you select this option, users who are required to authenticate with the internal RADIUS server must be added. Click the **Users** link to add the users. For information on adding a user, see “Adding a User” on page 251. 4. **Reauth interval—** When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients. **5.** **Blacklisting—** Select **Enabled** if you want clients to be blacklisted after a certain number of authentication failures. **6.** **Max authentication failures—** Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. **NOTE:** Navigate to **PEF > Blacklisting** in the Instant WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window. 7. Click **Upload Certificate** and browse to upload a certificate file for the internal server. See “Certificates” on page 143 for more information.

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

If	then,
You want to use the default security level, **Personal**	Perform the following steps: 1. Select the required key options from the **Key management** drop-down list. Available options are: ● WPA-2 Personal ● WPA Personal ● Both (WPA-2 & WPA) ● Static WEP— If you have selected **Static WEP**, do the following: ● Select appropriate **WEP key size** from the WEP key size drop-down list. Available options are 64-bit and 128-bit. ● Select appropriate Tx key from the **Tx Key** drop-down list. Available options are **1**, **2**, **3**,and **4**. ● Enter an appropriate **WEP key** and reconfirm. For more information on encryption and recommended encryption type, see Chapter 13, “Encryption” . 2. WPA-2 Personal— ● Select a passphrase format from the **Passphrase format** drop-down list. Available options are: ● 8-63 alphanumeric chars ● 64 hexadecimal chars 3. Enter a passphrase in the **Passphrase** text box and reconfirm. 4. Select the required option from the **MAC authentication** drop-down list. Available options are ● Enabled and Disabled When **Enabled**, user must configure at least one RADIUS server for authentication server. See “MAC Authentication” on page 141 for further details. 5. **Authentication server 1—** Select the required Authentication server option from the drop-down list. Available options are: ● **New**— If you select this option, an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 12, “Authentication” . 6. **Reauth interval—** When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients. 7. **Blacklisting**— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures. 8. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. 9. **Internal server**— If you select this option, users who are required to authenticate with the internal RADIUS server must be added. Click the **Users** link to add the users.For information on adding a user, see “Adding a User” on page 251. **NOTE:** Navigate to **PEF > Blacklisting** in the Instant WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window. 10. Click **Upload Certificate** and browse to upload a certificate file for the internal server. See “Certificates” on page 143 for more information.

Figure 39 *Employee Security Tab— Personal*



Key management: WPA-2 Personal

Passphrase format: 8-63 chars

Passphrase:

Retype:

MAC authentication: Enabled

Authentication server 1: InternalServer

Reauth interval: 0 min.

Blacklisting: Enabled

Max authentication failures: 0

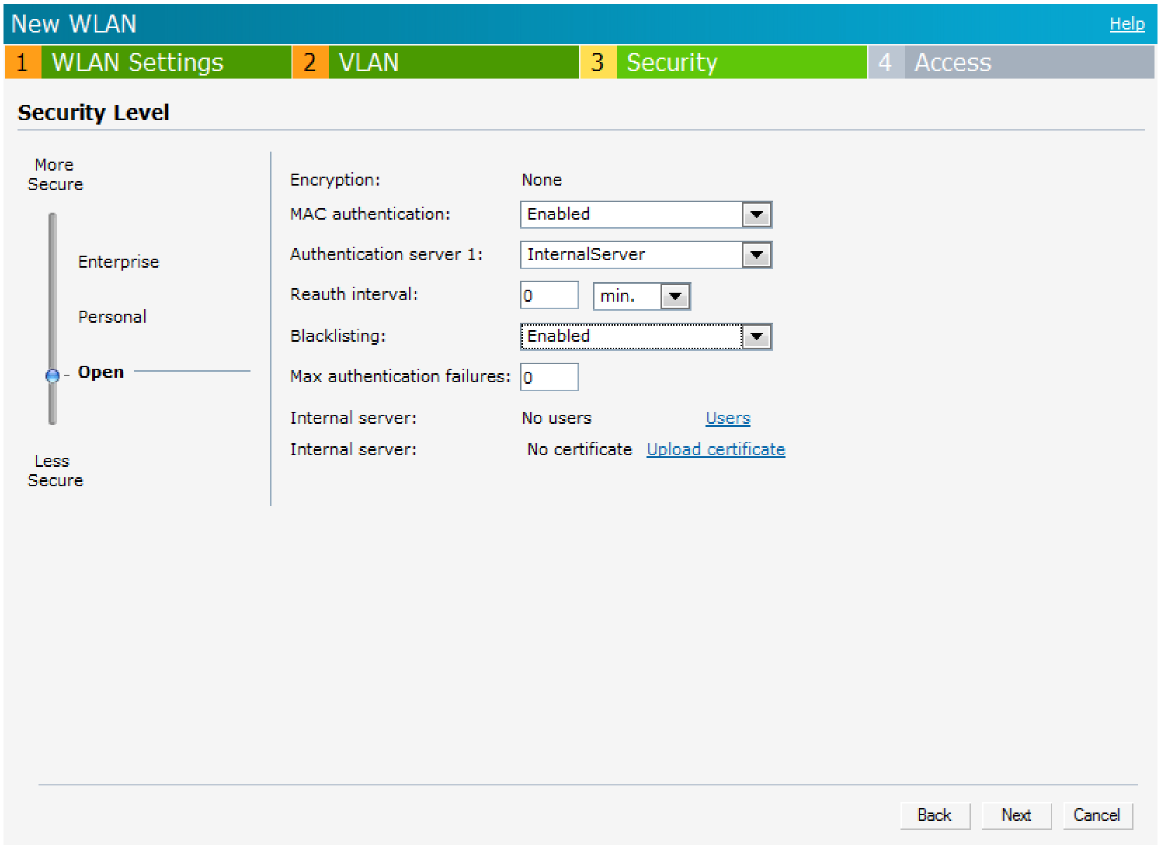
Internal server: No users Users

Internal server: No certificate Upload certificate

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

If	then,
You select the **Open** security level	1. Select the required MAC authentication from the **MAC authentication** drop-down list. Available options are— Enabled and Disabled ● When **Enabled**, user must configure at least one RADIUS server for authentication server. See "MAC Authentication" on page 141 for further details. 2. **Authentication server 1—** Select the required Authentication server option from the drop-down list. Available options are: ● **New**— If you select this option, an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 12, "Authentication" . 3. **Reauth interval—** When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients. 4. **Blacklisting**— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures. 5. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. **NOTE:** Navigate to **PEF > Blacklisting** in the Instant WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window. 6. **Internal server**— If you select this option, users who are required to authenticate with the internal RADIUS server must be added. Click the **Users** link to add the users. For information on adding a user, see "Adding a User" on page 251. 7. Click **Upload Certificate** and browse to upload a certificate file for the internal server. See "Certificates" on page 143 for more information.

Figure 40 *Employee Security Tab— Open*



Security Level

Encryption: None

MAC authentication: Enabled

Authentication server 1: InternalServer

Reauth interval: 0 min.

Blacklisting: Enabled

Max authentication failures: 0

Internal server: No users Users

Internal server: No certificate Upload certificate

8. Click **Next** to continue.
9. Use the **Access Rules** page to specify optional access rules for this network.
   1. **Network-based—** Set the slider to **Network-based** if you want the same rules to apply to all users. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. Instant Firewall treats packets based on the first rule matched. For more information, see Chapter 16, "Instant Firewall" .

   To edit the default rule:

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

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

   To define an access rule:

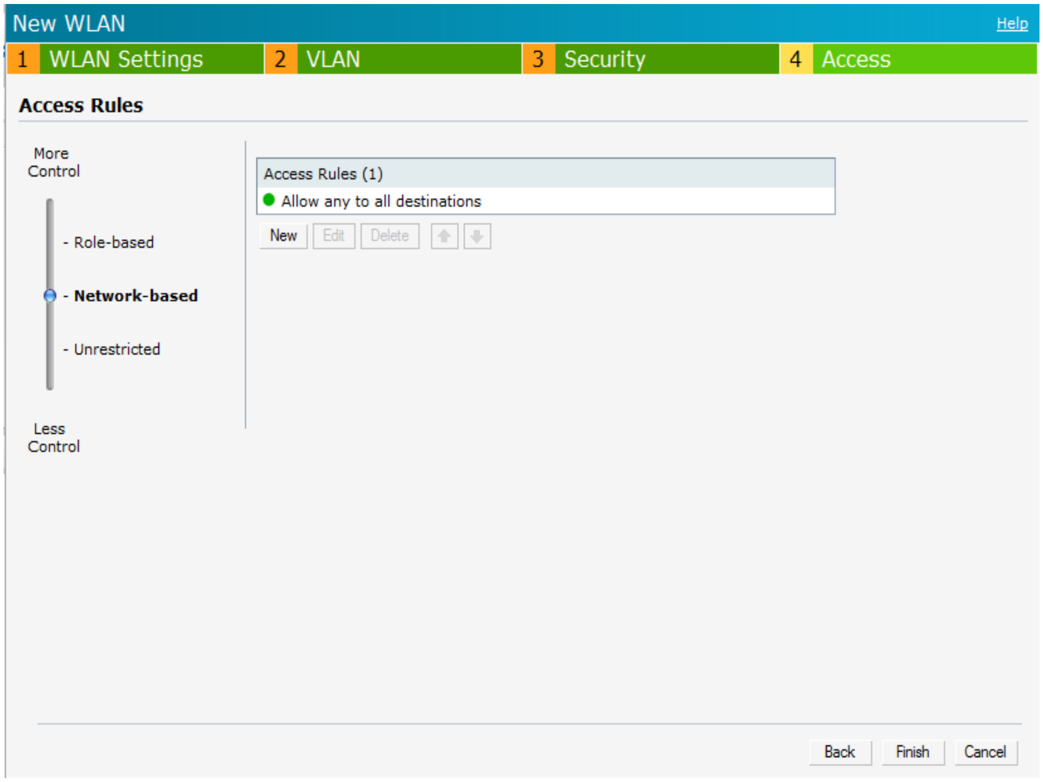
   a. Click **New**.

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

   c. Click **OK.**

   2. **Role-based—** Select **Role-based** if you want to specify per-user access rules. See "Creating a New User Role" on page 151 for more information.
   3. **Unrestricted—** Select this to set no restrictions on access based on destination or type of traffic.
10. Click **Finish**. The network is added and listed in the **Networks** tab.

Figure 41 *Adding an Employee Network— Access Rules Tab*



Access Rules (1)

● Allow any to all destinations

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

Voice Network

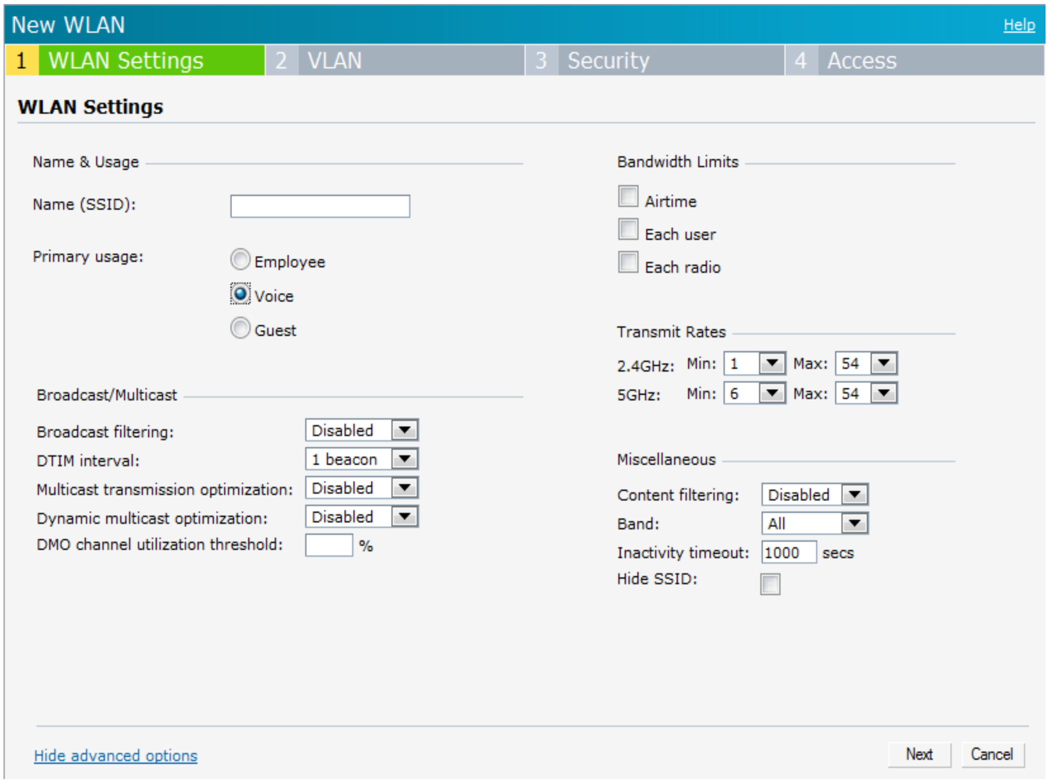
Use the Voice network type when you want devices that provide only voice services like handsets or only applications that require voice-like prioritization need connectivity.

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** window appears.

Figure 42 *Adding a Voice Network— Basic Info Tab*



WLAN Settings

Name & Usage

Name (SSID):

Primary usage: ○ Employee ● Voice ○ Guest

Broadcast/Multicast

Broadcast filtering: Disabled

DTIM interval: 1 beacon

Multicast transmission optimization: Disabled

Dynamic multicast optimization: Disabled

DMO channel utilization threshold: %

Bandwidth Limits

□ Airtime

□ Each user

□ Each radio

Transmit Rates

2.4GHz: Min: 1 Max: 54

5GHz: Min: 6 Max: 54

Miscellaneous

Content filtering: Disabled

Band: All

Inactivity timeout: 1000 secs

Hide SSID: □

2. In the **WLAN Settings** tab, perform the following steps:

   a. **Name (SSID)**— Enter a name that uniquely identifies a wireless network.

   b. **Primary usage—** Select **Employee** (this is selected by default) from the **Primary usage** options. This selection determines whether the network is primarily intended to be used for employee data, guest data, or voice traffic.

3. Click the **Show advanced options** link and perform the following steps.

   a. Broadcast/Multicast

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

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

b. **Bandwidth Limits—** You can specify three types of bandwidth limits.

- Airtime— Indicates the aggregate amount of airtime that all clients on this Network can use to send/receive data.
- Each user— Indicates the throughput for any single user on this Network. The throughput value is specified in kbps.
- Each radio— Indicates the aggregate amount of throughput each radio (some AP models have multiple radios) is allowed to provide for all clients connected to that radio

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

d. **Miscellaneous**

- Content filtering— When enabled, all DNS requests to non-corporate domains on this wireless network are sent to OpenDNS.
- Band**—** Set the band at which the network transmits radio signals. Available options are 2.4 GHz, 5 GHz and All. The All option is selected by default. It is also the recommended option.
- Inactivity timeout**—** Indicates the time in seconds after which an idle client ages out. The minimum value is 60 seconds and the default value is 1000 seconds.
- Hide SSID— Select this check box if you do not want the SSID (network name) to be visible to users.

NOTE

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

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

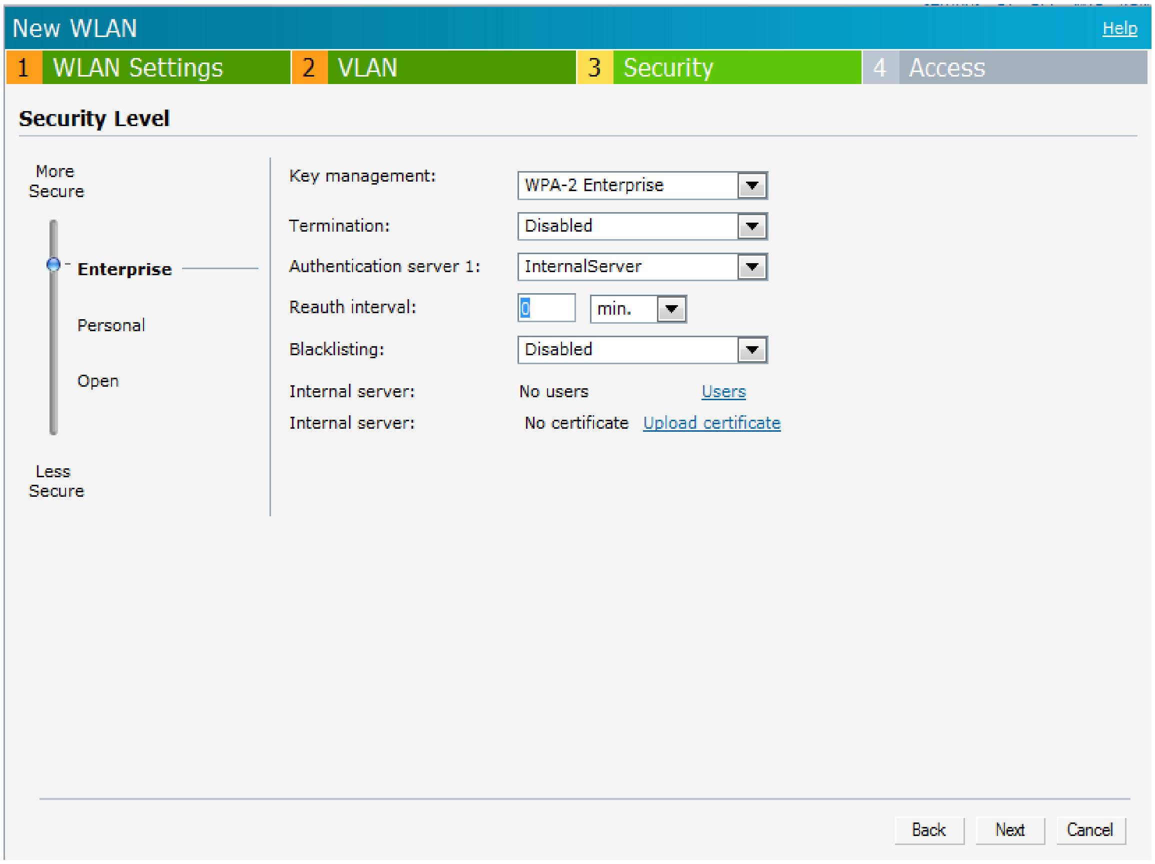
Table 8 *Conditions for Client IP and VLAN Assignment*

If	then
You select Virtual Controller assigned	The client gets the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the IAP for the wireless clients. The Virtual Controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi site wireless network. See Chapter 11, “Virtual Controller” on page 121 for configuring the DHCP server.
You select Network assigned	By default, the client VLAN is assigned to the native VLAN on the wired network. ● Default— The client gets the IP address in the same subnet as the IAPs. ● Static— Select to specify a VLAN for all clients on this network. ● Dynamic— Select to create rules for per-user VLAN assignment. See “VLAN Derivation Rule” on page 156 for more information.

6. Click **Next** to continue.

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

Figure 43 *Voice Security Tab— Enterprise*



New WLAN

1 WLAN Settings | 2 VLAN | 3 Security | 4 Access

Security Level

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: InternalServer

Reauth interval: 0 min.

Blacklisting: Disabled

Internal server: No users

Internal server: No certificate

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

If	then,
You select the **Enterprise** security level	Perform the following steps: 1. Select the required key options from the **Key management** drop-down list. Available options are: - WPA-2 Enterprise - WPA Enterprise - Both (WPA-2 & WPA) - Dynamic WEP with 802.1X - **Use Session Key for LEAP:** Use the **Session Key for LEAP** instead of using Session Key from the RADIUS Server to derive pair wise unicast keys. This is required for old printers that use dynamic WEP via LEAP authentication. This is **Disabled** by default. For more information on encryption and recommended encryption type, see Chapter 13, “Encryption” . 2. **Termination**— Enable this option to terminate the EAP portion of 802.1X authentication on the IAP instead of the RADIUS server. For more information, see “External RADIUS Server” on page 124. 3. **Authentication server 1 and 2—** Select the required Authentication server option from the drop-down list. Available options are: - **New**— If you select this option, then an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 12, “Authentication” . 4. **Reauth interval—** When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients. **5.** **Blacklisting—** Select **Enabled** if you want clients to be blacklisted after a certain number of authentication failures. **6.** **Max authentication failures—** Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. **NOTE:** Navigate to **PEF > Blacklisting** in the Instant WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.

Table 9 *Conditions for Adding a Voice Network— Security Tab (Continued)*

If	then,
You want to use the default security level, **Personal**	Perform the following steps: 1. Select the required key options from the **Key management** drop-down list. Available options are: - WPA-2 Personal - WPA Personal - Both (WPA-2 & WPA) 1. **Static WEP**— If you have selected **Static WEP**, then do the following: - Select appropriate **WEP key size** from the WEP key size drop-down list. Available options are 64-bit and 128-bit. - Select appropriate Tx key from the **Tx Key** drop-down list. Available options are 1, 2, 3,and 4. - Enter an appropriate WEP key and reconfirm. For more information on encryption and recommended encryption type, see Chapter 13, “Encryption” . 2. **WPA-2 Personal**— Select a passphrase format from the **Passphrase format** drop-down list. Available options are: - 8-63 alphanumeric chars - 64 hexadecimal chars 3. Enter a passphrase in the Passphrase text box and reconfirm. 4. Select the required option from the MAC authentication drop-down list. Available options are: Enabled and Disabled When **Enabled**, user must configure at least one RADIUS server for authentication server. See “MAC Authentication” on page 141 for further details. 5. **Authentication server 1—** Select the required Authentication server option from the drop-down list. Available options are: - **New**— If you select this option, then an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 12, “Authentication” . 6. **Reauth interval—** When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients. 7. **Blacklisting**— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures. 8. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. **NOTE:** Navigate to **PEF > Blacklisting** in the Instant WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window. 9. **InternalServer**— If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the **Users** link to add the users. For information on adding a user, see “Adding a User” on page 251.
	10. Click **Upload Certificate** and browse to upload a certificate file for the internal server. See “Certificates” on page 143 for more information.

Table 9 *Conditions for Adding a Voice Network— Security Tab (Continued)*

If	then,
You select the **Open** security level	1. Select the required MAC authentication from the **MAC authentication** drop-down list. Available options are— Enabled and Disabled ● When **Enabled**, user must configure at least one RADIUS server for authentication server. See "MAC Authentication" on page 141 for further details. 2. **Authentication server 1—** Select the required Authentication server option from the drop-down list. Available options are: ● **New**— If you select this option, then an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 12, "Authentication" . 3. **Reauth interval—** When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients. **4.** **Blacklisting—** Select **Enabled** if you want clients to be blacklisted after a certain number of authentication failures. **5.** **Max authentication failures—** Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. **NOTE:** Navigate to **PEF > Blacklisting** in the Instant WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window. 6. **InternalServer**— If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the Users link to add the users. For information on adding a user, see "Adding a User" on page 251. 7. Click **Upload Certificate** and browse to upload a certificate file for the internal server. See "Certificates" on page 143 for more information.

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

   - **Network-based—** Set the slider to **Network-based** if you want the same rules to apply to all users. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. Instant Firewall treats packets based on the first rule matched. For more information, see Chapter 16, "Instant Firewall" .

   To edit the default rule:

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

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

   To define an access rule:

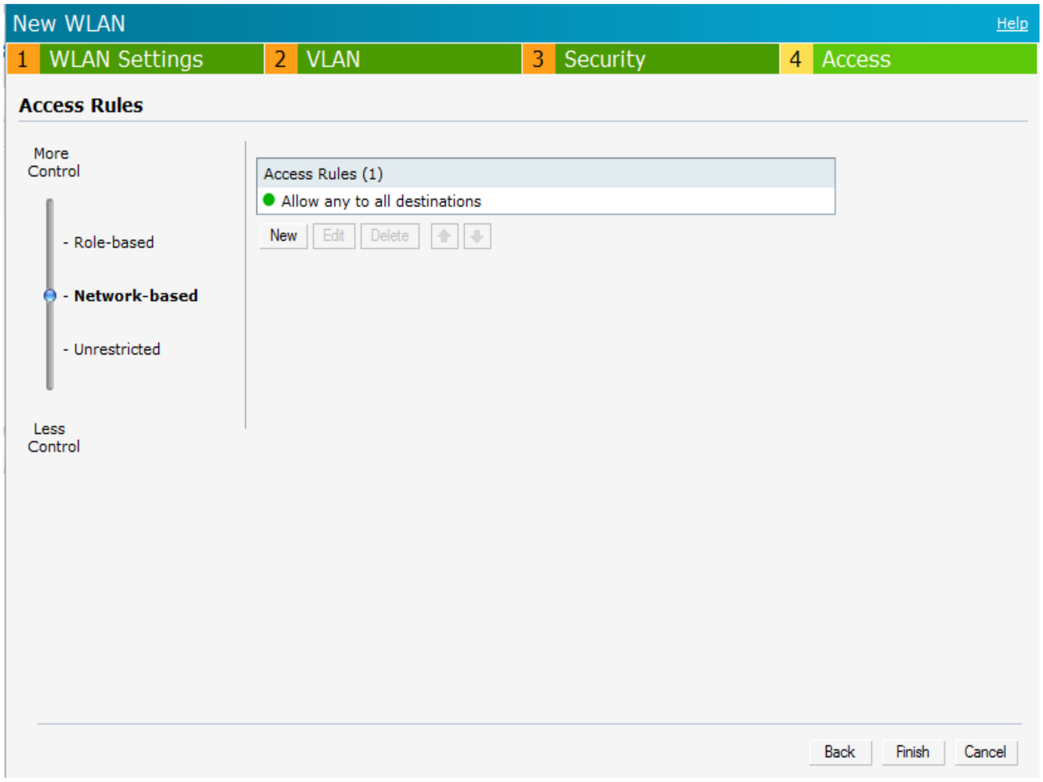
   a. Click **New**.

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

   c. Click **OK.**

   - **Role-based—** Select **Role-based** if you want to specify per-user access rules. See "Creating a New User Role" on page 151 for more information.
   - **Unrestricted—** Select this to set no restrictions on access based on destination or type of traffic.

Figure 44 *Adding a Voice Network— Access Rules Tab*



Access Rules (1)

● Allow any to all destinations

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

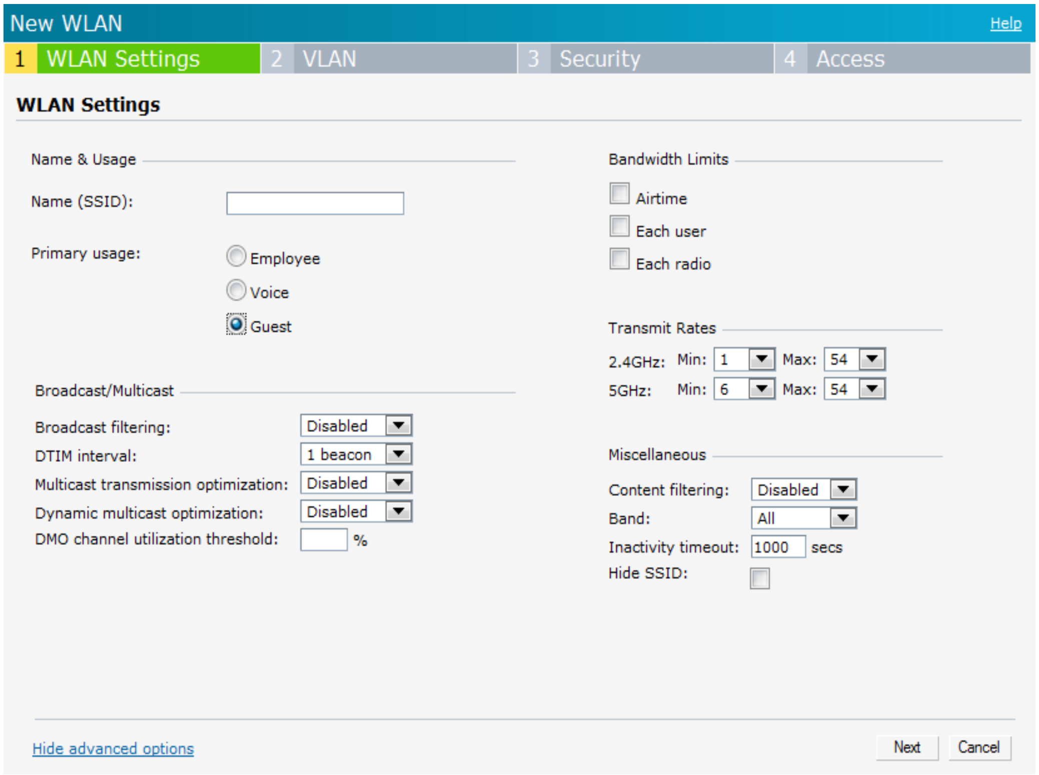
Guest Network

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

Adding a Guest Network

This section provides the procedure to add a guest network.

Figure 45 *Adding a Guest Network— Basic Info Tab*



New WLAN — Help

1 WLAN Settings | 2 VLAN | 3 Security | 4 Access

WLAN Settings

Name & Usage

Name (SSID):

Primary usage: ○ Employee ○ Voice ● Guest

Broadcast/Multicast

Broadcast filtering: Disabled

DTIM interval: 1 beacon

Multicast transmission optimization: Disabled

Dynamic multicast optimization: Disabled

DMO channel utilization threshold: %

Bandwidth Limits

□ Airtime

□ Each user

□ Each radio

Transmit Rates

2.4GHz: Min: 1 Max: 54

5GHz: Min: 6 Max: 54

Miscellaneous

Content filtering: Disabled

Band: All

Inactivity timeout: 1000 secs

Hide SSID: □

Hide advanced options

Next Cancel

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

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

b. **Bandwidth Limits—** You can specify three types of bandwidth limits.

- Airtime— Indicates the aggregate amount of airtime that all clients on this Network can use to send/receive data.
- Each user— Indicates the throughput for any single user on this Network. The throughput value is specified in kbps.
- Each radio— Indicates the aggregate amount of throughput each radio (some AP models have multiple radios) is allowed to provide for all clients connected to that radio

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

d. **Miscellaneous**

- Content filtering— When enabled, all DNS requests to non-corporate domains on this wireless network are sent to OpenDNS.
- Band**—** Set the band at which the network transmits radio signals. Available options are 2.4 GHz, 5 GHz and All. The All option is selected by default. It is also the recommended option.
- Inactivity timeout**—** Indicates the time in seconds after which an idle client ages out. The minimum value is 60 seconds and the default value is 1000 seconds.
- Hide SSID— Select this check box if you do not want the SSID (network name) to be visible to users

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

Table 10 *Conditions for Client IP and VLAN assignment*

If	then
You select Virtual Controller assigned	The client gets the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the IAP for the wireless clients. The Virtual Controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi site wireless network. See Chapter 11, “Virtual Controller” on page 121 for configuring the DHCP server.
You select Network assigned	By default, the client VLAN is assigned to the native VLAN on the wired network. ● Default— The client gets the IP address in the same subnet as the IAPs. ● Static— Select to specify a VLAN for all clients on this network. ● Dynamic— Select to create rules for per-user VLAN assignment. See “VLAN Derivation Rule” on page 156 for more information.

6. Click **Next** to continue.

7. This tab allows you to configure the captive portal page and encryption for the Guest network. Select one of the following splash page type:

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

Splash Page Type	Description and steps to set up
Internal — Authenticated	The user has to accept the terms and conditions and enter a username and password on the captive portal page. If this option is selected, then add the users who are required to use the captive portal authentication to the user database. Click the Users link to add the users. For information about adding a user, see "Adding a User" on page 251. For information on customizing the splash page, see "Customizing a Splash Page" on page 134. 1. Select the required Authentication server 1 option from the drop-down list. Available options are: ● **New** — If you select this option, then an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see "Configuring an External RADIUS Server" on page 125. ● **Internal Server** — If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the **Users** link to add the users. For information on adding a user, see "Adding a User" on page 251. 2. **Reauth interval** — When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients. 3. **Blacklisting** — Select **Enabled** if you want clients to be blacklisted after a certain number of authentication failures. 4. **Max authentication failures** — Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. 5. **For Internal users** —Click **Users** to populate the system's internal authentication server with users. For information about adding a user, see "Adding a User" on page 161. 6. Click **Upload Certificate** and browse to upload a certificate file for the internal server. See "Certificates" on page 143 for more information. 7. **Redirect URL**— Users can be redirected to a specific URL (instead of the original URL) after successful captive portal authentication. This entry is optional.

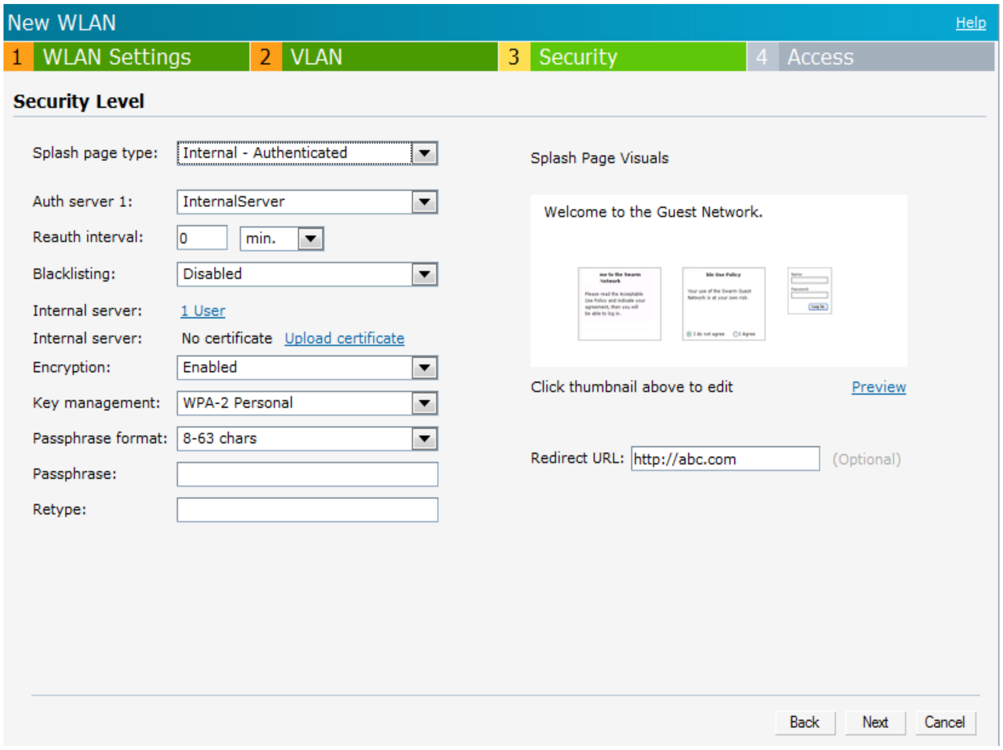
Table 11 *Conditions for Adding a Guest Network— Security Tab (Continued)*

Splash Page Type	Description and steps to set up
Internal — Acknowledged	The user has to accept the terms and conditions for this splash page type. For information on customizing the splash page, see "Customizing a Splash Page" on page 134. 1. **Encryption** —Select Enabled from the Encryption drop-down list and perform the following steps (these steps are optional): a. Select the required key management option from the Key management drop-down list. Available options are: - WPA-2 Personal - WPA Personal - Both (WPA-2 & WPA) 2. **Passphrase format**— Specify either an alphanumeric or a hexadecimal string. Ensure that the hexadecimal string must be exactly 64 digits in length. 3. **Passphrase**— Enter a pre-shared key (PSK) passphrase.
External - RADIUS Server	An external server is used to display the splash page to the user. If this option is selected, then do the following: **External splash page** - **IP or hostname**— Enter the IP or hostname of the external server in the IP or hostname text box. - **URL**— Enter the URL of the captive portal page in the URL text box. - **Port**— Enter the number of the port to be used for communicating with the external server in the Port text box. 4. **Redirect URL**— By default, after entering the requested info at the splash page, the user is redirected to the URL that was originally requested. Specify a redirect URL if you want to override the user's original request and redirect them to another URL. 5. **Auth server 1**— Select the required Authentication server 1 option from the drop-down list. Available options are: - **New**— If you select this option, then an external RADIUS server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see "Configuring an External RADIUS Server" on page 125. 6. **Reauth interval**— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients. 7. **Blacklisting**— Select **Enabled** if you want clients to be blacklisted after a certain number of authentication failures. 8. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. 9. **Walled Garden**— The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see "Walled Garden Access" on page 142.

Table 11 *Conditions for Adding a Guest Network— Security Tab (Continued)*

Splash Page Type	Description and steps to set up
External - Authentication Text	An external splash page returns a specified string to indicate successful authentication. - **IP or hostname**— Enter the IP or hostname of the external server in the IP or hostname text box. - **URL**— Enter the URL of the captive portal page in the URL text box. - **Port**— Enter the number of the port to be used for communicating with the external server in the Port text box. - **Auth text** — Indicates the text string returned by the external server after a successful authentication. - **Redirect URL**— By default, after entering the requested info at the splash page, the user is redirected to the URL that was originally requested. Specify a redirect URL if you want to override the user's original request and redirect them to another URL. 1. **Reauth interval**— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients. 2. **Blacklisting**— Select **Enabled** if you want clients to be blacklisted after a certain number of authentication failures. 3. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. 4. **Walled Garden**— The walled garden directs the user’s navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see “Walled Garden Access” on page 142.
None	Select this option if you do not want to set the captive portal authentication.

Figure 46 *Adding a Guest Network — Splash Page Settings*



Security Level

Splash page type: Internal - Authenticated

Auth server 1: InternalServer

Reauth interval: 0 min.

Blacklisting: Disabled

Internal server: 1 User

Internal server: No certificate Upload certificate

Encryption: Enabled

Key management: WPA-2 Personal

Passphrase format: 8-63 chars

Passphrase:

Retype:

Splash Page Visuals

Welcome to the Guest Network.

Click thumbnail above to edit Preview

Redirect URL: http://abc.com (Optional)

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

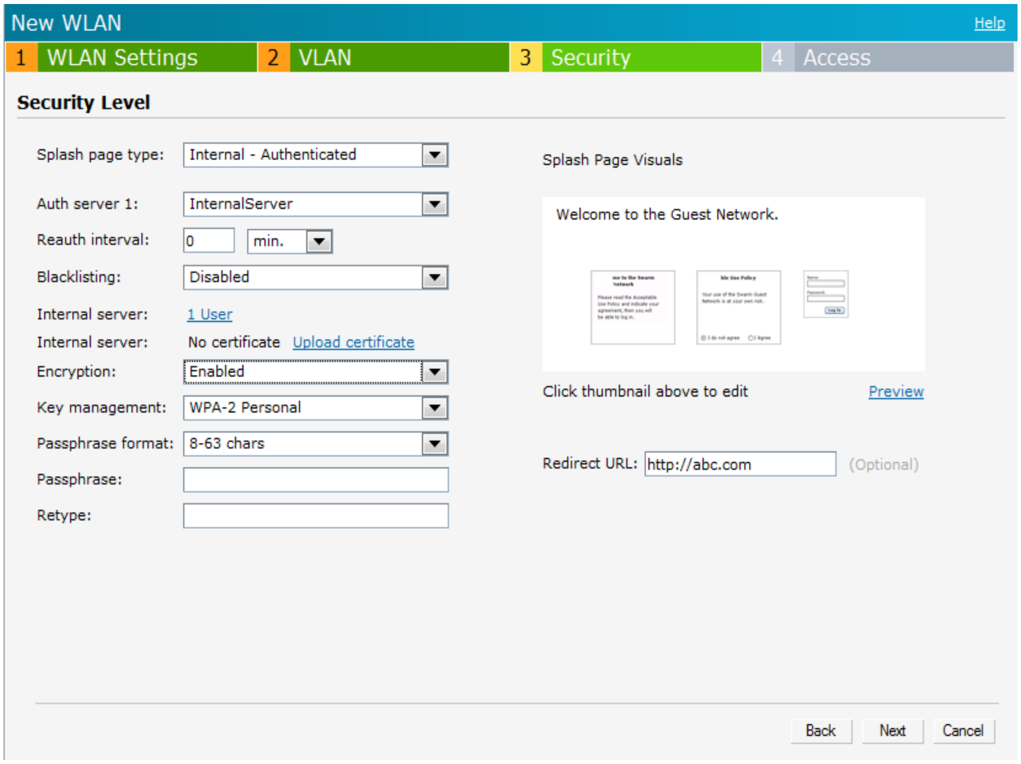
   a. Select the required key management option from the **Key management** drop-down list. Available options are:

      - WPA-2 Personal
      - WPA Personal
      - Both (WPA-2 & WPA)

   b. **Passphrase format** — Specify either an alphanumeric or a hexadecimal string. Ensure that the hexadecimal string must be exactly 64 digits in length.

   c. **Passphrase** — Enter a pre-shared key (PSK) passphrase.

Figure 47 *Configuring a Splash Page — Encryption Settings*



New WLAN

Help

1 WLAN Settings | 2 VLAN | 3 Security | 4 Access

Security Level

Splash page type: Internal - Authenticated

Auth server 1: InternalServer

Reauth interval: 0 min.

Blacklisting: Disabled

Internal server: 1 User

Internal server: No certificate Upload certificate

Encryption: Enabled

Key management: WPA-2 Personal

Passphrase format: 8-63 chars

Passphrase:

Retype:

Splash Page Visuals

Welcome to the Guest Network.

Click thumbnail above to edit Preview

Redirect URL: http://abc.com (Optional)

NOTE

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

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

   - **Network-based—** Set the slider **Network-based** if you want the same rules to apply to all users. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. Instant Firewall treats packets based on the first rule matched. For more information, see Chapter 16, “Instant Firewall” .

   To edit the default rule:

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

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

   To define an access rule:

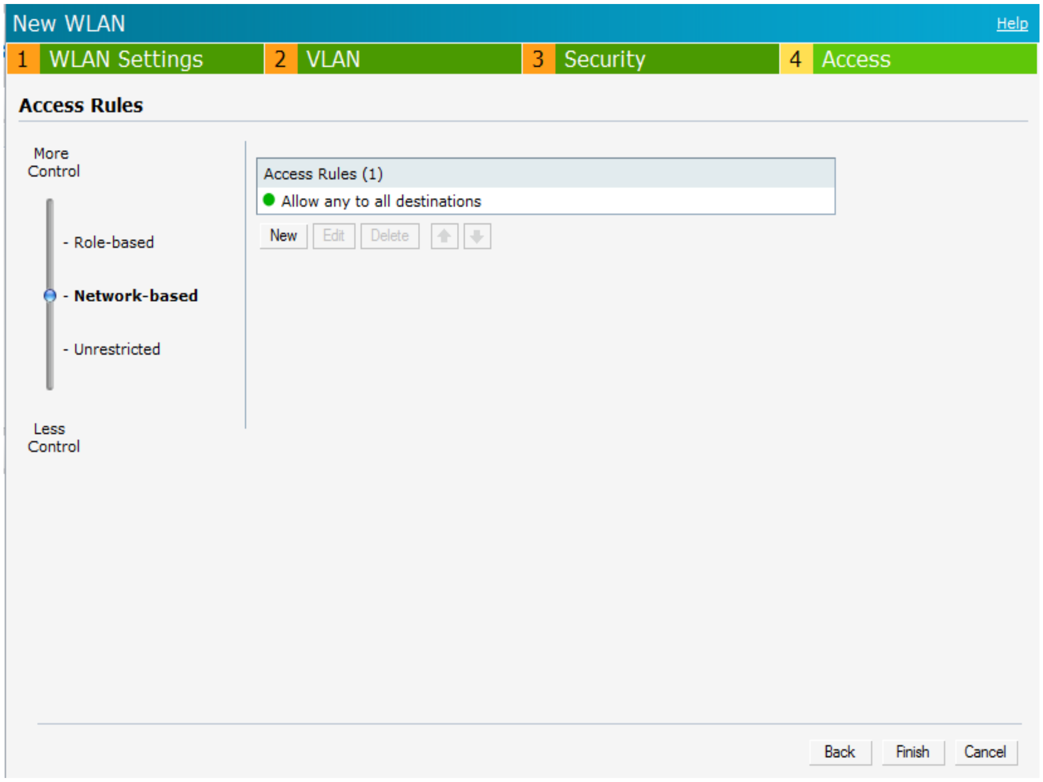
   a. Click **New**.

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

   c. Click **OK.**

   - **Role-based—** Select **Role-based** if you want to specify per-user access rules. See “Creating a New User Role” on page 151 for more information.
   - **Unrestricted—** Select this to set no restrictions on access based on destination or type of traffic.

Figure 48 *Adding a Guest Network — Access Rules Tab*



Access Rules (1)

● Allow any to all destinations

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

Editing a Network

To edit a network:

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

Deleting a Network

To delete a network:

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

Number of WLAN SSIDs supported

By default, you can create up to six networks or WLANs. You can enable the Extended SSID option and create up to 16 WLANs. IAP-175, IAP-104, and IAP-105 devices support up to 8 SSIDs and RAP-3WN, IAP-92, IAP-93, IAP-134, and IAP 135 devices support up to 16 SSIDs. After you enable this option, the number of SSIDs that become active on each IAP depends on the IAP platform.

NOTE

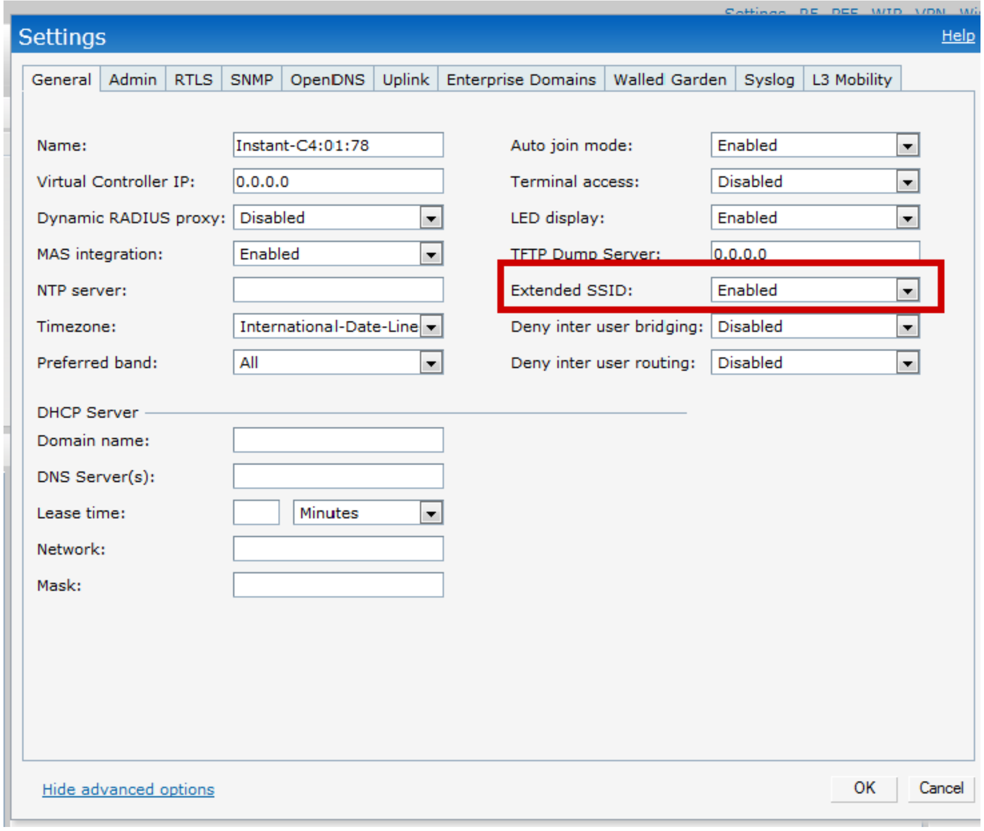
Enabling the Extended SSID option disables mesh.

Enabling the Extended SSID option

To enable the extended SSID option:

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

Figure 49 *Enabling Extended SSID.*



Name:	Instant-C4:01:78	Auto join mode:	Enabled
Virtual Controller IP:	0.0.0.0	Terminal access:	Disabled
Dynamic RADIUS proxy:	Disabled	LED display:	Enabled
MAS integration:	Enabled	TFTP Dump Server:	0.0.0.0
NTP server:		Extended SSID:	Enabled
Timezone:	International-Date-Line	Deny inter user bridging:	Disabled
Preferred band:	All	Deny inter user routing:	Disabled

DHCP Server

Domain name:	
DNS Server(s):	
Lease time:	Minutes
Network:	
Mask:	

Mesh Network

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

This chapter describes the Aruba Instant secure enterprise mesh architecture.

Mesh Instant Access Points

An Aruba Instant mesh network requires at least one valid uplink (wired or 3G) connection. The IAP with the valid uplink connection is the mesh portal. The mesh portal may also act as a Virtual Controller. The un-wired IAPs are mesh points.

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

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

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

Instant mesh functionality is supported only on dual radio IAPs and not on single radio IAPs. On dual-radio IAPs, the 5 GHz radio is always used for both mesh-backhaul and client traffic, while the 2.4 GHz radio is always used for client traffic only.

NOTE

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

The only limitation is that it has to be provisioned for the first time by plugging into the wired network. After that, mesh works on ROW IAP like any other regulatory domain.

Mesh Portals

The mesh portal (MPP) is the gateway between the wireless mesh network and the enterprise wired LAN. The mesh roles are automatically assigned based on the IAP configuration. A mesh network could have multiple mesh portals to support redundant mesh paths (mesh links between neighboring mesh points that establish the best path to the mesh portal) from the wireless mesh network to the wired LAN.

The mesh portal broadcasts a mesh services set identifier (MSSID/ mesh cluster name) to advertise the mesh network service to other IAP mesh points in that instant network. This is not configurable and is transparent to the user. The mesh points authenticate to the mesh portal and establish a link that is secured using Advanced Encryption Standard (AES) encryption.

NOTE

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

Mesh Points

The mesh point (MP), is an IAP that establishes an all-wireless path to the mesh portal. The mesh point provides traditional WLAN services (such as client connectivity, intrusion detection system (IDS) capabilities, user role association, and Quality of Service (QoS) for LAN-to-mesh communication) to clients and performs mesh backhaul/network connectivity..

NOTE

Any provisioned IAP that has a valid uplink (wired or 3G) is a mesh portal, and the IAP without an Ethernet link is a mesh point.

NOTE

Mesh point also supports LAN bridging. You can connect any wired device to the downlink port of the mesh point. In the case of single Ethernet port platforms like AP-93 and AP-105, you can convert the Eth0 uplink port to a downlink port by enabling **Eth0 Bridging**. For additional information refer to "Configuring Wired Bridging on Ethernet 0" on page 94.

Instant Mesh Setup

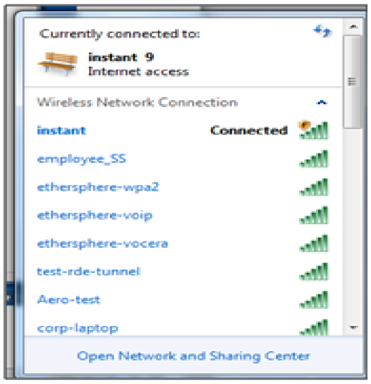
Instant mesh can be provisioned in two ways — Over-the-air provisioning and over-the-wire provisioning. Over-the-air provisioning is available when only one Aruba Instant mesh network is being advertised and it does not work for ROW version of IAPs.

The ROW IAP must have a the country code set in order to transmit/receive. Hence over-the-air provisioning is not supported on ROW IAPs at this time.

This section provides instructions on how to create a simple mesh network on Instant. To setup a mesh network:

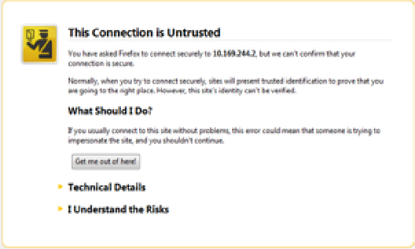
1. Connect all the IAPs to a DHCP server so that the IAPs get their IP addresses in the same subnet.
2. For over-the-air provisioning— Connect one IAP to the switch to form the mesh portal. All the other IAPs are provisioned over-the-air. Ensure that only one Virtual Controller (one subnet) is available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

Figure 50 *Open Instant SSID*



4. Type instant.arubanetworks.comin the browser.
5. Click **I understand the risks** and **Add exception** to ignore the certificate warnings that the client does not recognize the certificate authority.

Figure 51 *Untrusted Connection Window*



This Connection is Untrusted

You have asked Firefox to connect securely to 10.169.244.2, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

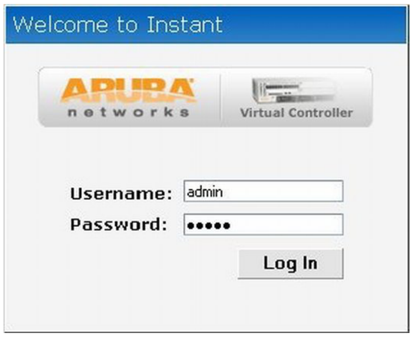
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

6. In the login screen as shown in Figure 52, enter the following credentials:

- Username— admin
- Password— admin

Figure 52 *Login Window*



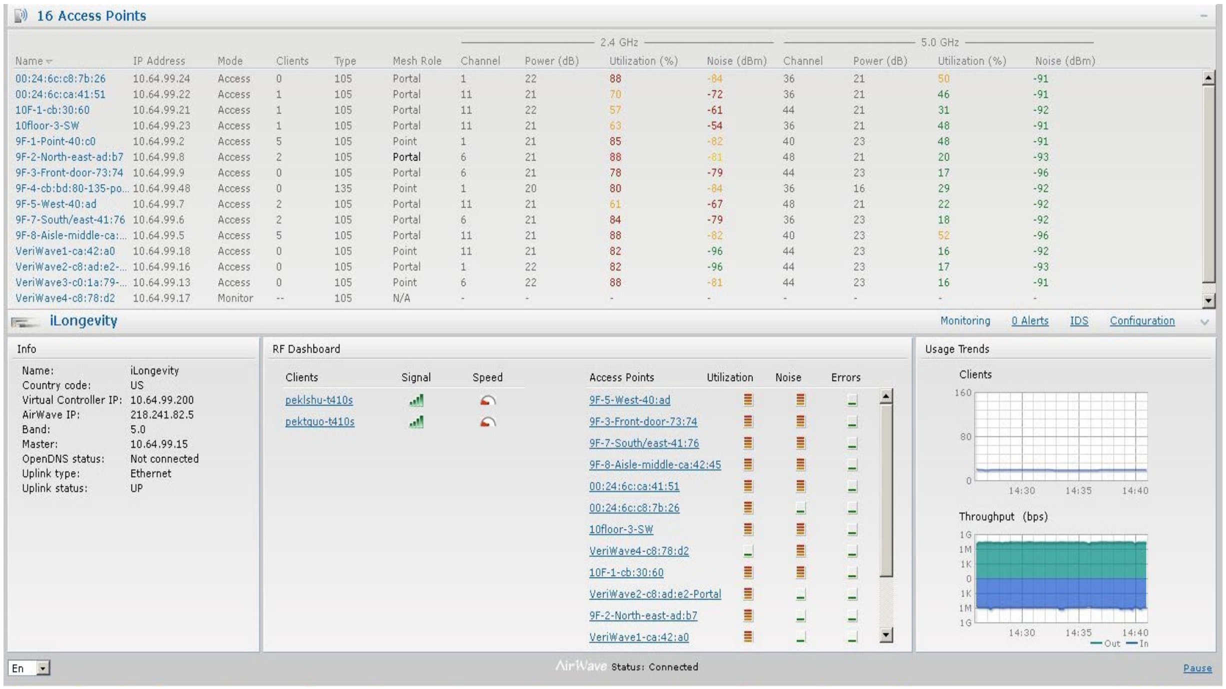
Welcome to Instant

Username: admin

Password: •••••

7. Create a new SSID and wpa-2 personal keys with **unrestricted** or **network based** access rules. Select **any permit** for basic connectivity.
8. Connect a client to the new SSID and disconnect from the **instant** SSID.
9. All the IAPs shows up on the Virtual Controller as shown in Figure 53. Disconnect the IAPs that you want to deploy as Mesh Points from the switch and place the IAPs at the desired location. The IAPs with valid uplink connections are the mesh portal.

Figure 53 *Mesh Portal*



16 Access Points

						2.4 GHz				5.0 GHz			
Name	IP Address	Mode	Clients	Type	Mesh Role	Channel	Power (dB)	Utilization (%)	Noise (dBm)	Channel	Power (dB)	Utilization (%)	Noise (dBm)
00:24:6c:c8:7b:26	10.64.99.24	Access	0	105	Portal	1	22	88	-84	36	21	50	-91
00:24:6c:ca:41:51	10.64.99.22	Access	1	105	Portal	11	21	70	-72	36	21	46	-91
10F-1-cb:30:60	10.64.99.21	Access	1	105	Portal	11	22	57	-61	44	21	31	-92
10floor-3-SW	10.64.99.23	Access	1	105	Portal	11	21	63	-54	36	21	48	-91
9F-1-Point-40:c0	10.64.99.2	Access	5	105	Point	1	21	85	-82	40	23	48	-91
9F-2-North-east-ad:b7	10.64.99.8	Access	2	105	Portal	6	21	88	-81	48	21	20	-93
9F-3-Front-door-73:74	10.64.99.9	Access	0	105	Portal	6	21	78	-79	44	23	17	-96
9F-4-cb:bd:80-135-po...	10.64.99.48	Access	0	135	Point	1	20	80	-84	36	16	29	-92
9F-5-West-40:ad	10.64.99.7	Access	2	105	Portal	11	21	61	-67	48	21	22	-92
9F-7-South/east-41:76	10.64.99.6	Access	2	105	Portal	6	21	84	-79	36	23	18	-92
9F-8-Aisle-middle-ca:...	10.64.99.5	Access	5	105	Portal	11	21	88	-82	40	23	52	-96
VeriWave1-ca:42:a0	10.64.99.18	Access	0	105	Point	11	21	82	-96	44	23	16	-92
VeriWave2-c8:ad:e2-...	10.64.99.16	Access	0	105	Portal	1	22	82	-96	44	23	17	-93
VeriWave3-c0:1a:79-...	10.64.99.13	Access	0	105	Point	6	22	88	-81	44	23	16	-91
VeriWave4-c8:78:d2	10.64.99.17	Monitor	--	105	N/A	-	-	-	-	-	-	-	-

iLongevity

Info

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

RF Dashboard

Clients	Signal	Speed
peklshu-t410s		
pektquo-t410s		

Access Points	Utilization	Noise	Errors
9F-5-West-40:ad	▤	▤	□
9F-3-Front-door-73:74	▤	▤	□
9F-7-South/east-41:76	▤	▤	□
9F-8-Aisle-middle-ca:42:45	▤	▤	□
00:24:6c:ca:41:51	▤	▤	□
00:24:6c:c8:7b:26	▤	□	□
10floor-3-SW	▤	▤	□
VeriWave4-c8:78:d2	□	▤	□
10F-1-cb:30:60	▤	▤	□
VeriWave2-c8:ad:e2-Portal	▤	□	□
9F-2-North-east-ad:b7	▤	□	□
VeriWave1-ca:42:a0	▤	□	□

Usage Trends

Status: Connected

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

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

Chapter 6

Managing IAPs

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

Preferred Band

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

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

NOTE

Reboot the IAP after configuring the radio profile settings in order for the changes to take effect.

Auto Join Mode

The Auto Join Mode feature allows IAPs to automatically,

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

The **Auto Join Mode** feature is enabled by default. When the Auto Join Mode feature is disabled, a **New** link appears in the **Access Points** tab. Click this link to add IAPs to the network. For more information, see "Adding an IAP to the Network" on page 90. In addition, when this feature is disabled, IAPs that are configured but not active appear in red.

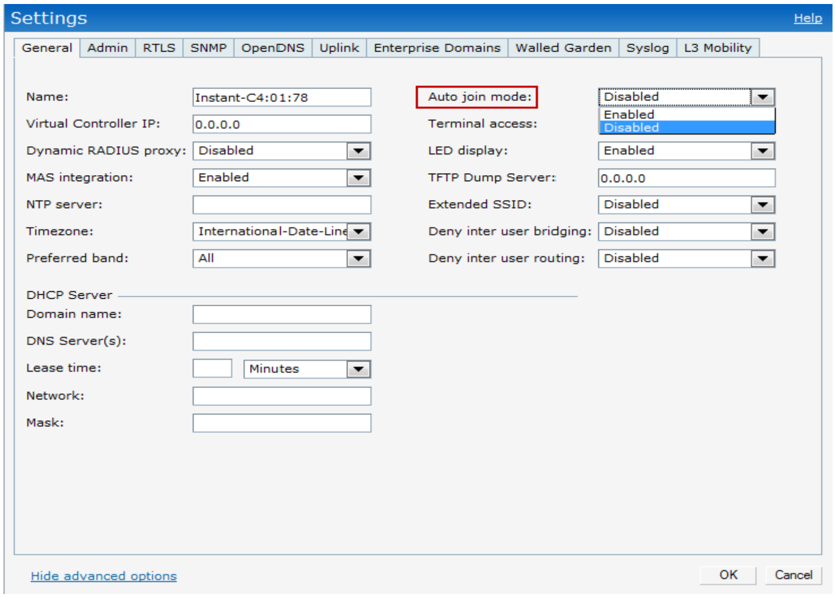
Disabling Auto Join Mode

To disable Auto Join Mode:

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

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

Figure 54 *Disabling Auto Join Mode*



Name: Instant-C4:01:78
Virtual Controller IP: 0.0.0.0
Dynamic RADIUS proxy: Disabled
MAS integration: Enabled
NTP server:
Timezone: International-Date-Line
Preferred band: All

Auto join mode: Disabled (Enabled / Disabled)
Terminal access:
LED display: Enabled
TFTP Dump Server: 0.0.0.0
Extended SSID: Disabled
Deny inter user bridging: Disabled
Deny inter user routing: Disabled

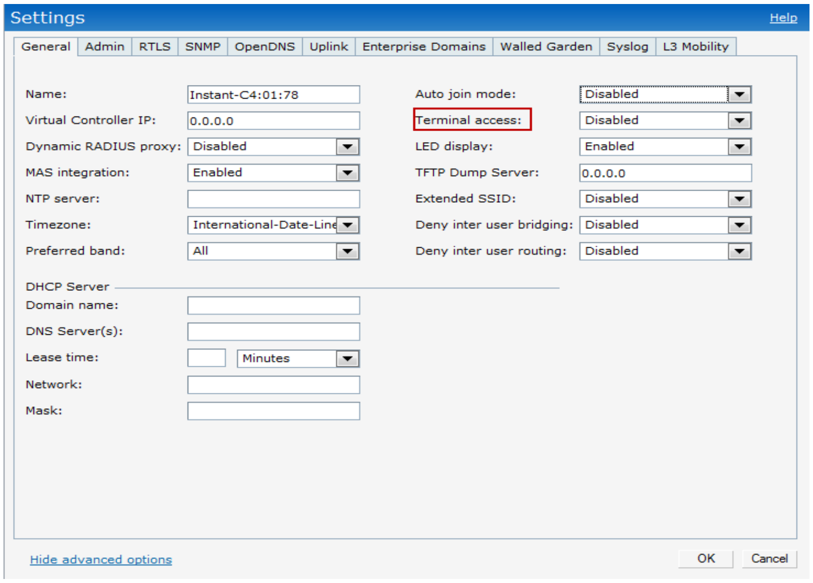
DHCP Server
Domain name:
DNS Server(s):
Lease time: Minutes
Network:
Mask:

3. Click **OK.**

Terminal Access

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

Figure 55 *Terminal Access*



Name: Instant-C4:01:78
Virtual Controller IP: 0.0.0.0
Dynamic RADIUS proxy: Disabled
MAS integration: Enabled
NTP server:
Timezone: International-Date-Line
Preferred band: All

Auto join mode: Disabled
Terminal access: Disabled
LED display: Enabled
TFTP Dump Server: 0.0.0.0
Extended SSID: Disabled
Deny inter user bridging: Disabled
Deny inter user routing: Disabled

DHCP Server
Domain name:
DNS Server(s):
Lease time: Minutes
Network:
Mask:

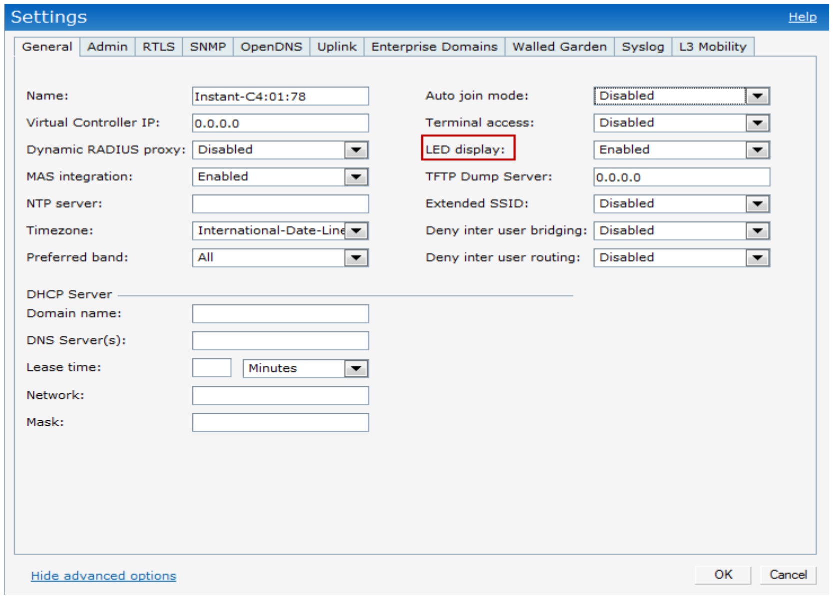
NOTE

Instant does not support configuration using CLI.

LED Display

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

Figure 56 *LED Display*



Name:	Instant-C4:01:78	Auto join mode:	Disabled
Virtual Controller IP:	0.0.0.0	Terminal access:	Disabled
Dynamic RADIUS proxy:	Disabled	LED display:	Enabled
MAS integration:	Enabled	TFTP Dump Server:	0.0.0.0
NTP server:		Extended SSID:	Disabled
Timezone:	International-Date-Line	Deny inter user bridging:	Disabled
Preferred band:	All	Deny inter user routing:	Disabled

DHCP Server

Domain name:	
DNS Server(s):	
Lease time:	Minutes
Network:	
Mask:	

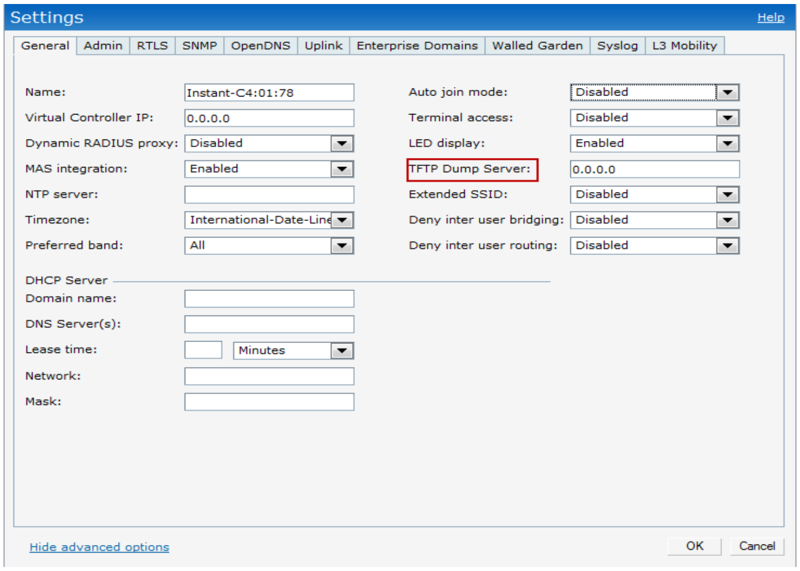
NOTE

The LED display is always in **Enabled** mode while rebooting the IAP.

TFTP Dump Server

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

Figure 57 *TFTP Dump Server*



Settings

Help
General | Admin | RTLS | SNMP | OpenDNS | Uplink | Enterprise Domains | Walled Garden | Syslog | L3 Mobility

Name: Instant-C4:01:78

Virtual Controller IP: 0.0.0.0

Dynamic RADIUS proxy: Disabled

MAS integration: Enabled

NTP server:

Timezone: International-Date-Line

Preferred band: All

Auto join mode: Disabled

Terminal access: Disabled

LED display: Enabled

TFTP Dump Server: 0.0.0.0

Extended SSID: Disabled

Deny inter user bridging: Disabled

Deny inter user routing: Disabled

DHCP Server

Domain name:

DNS Server(s):

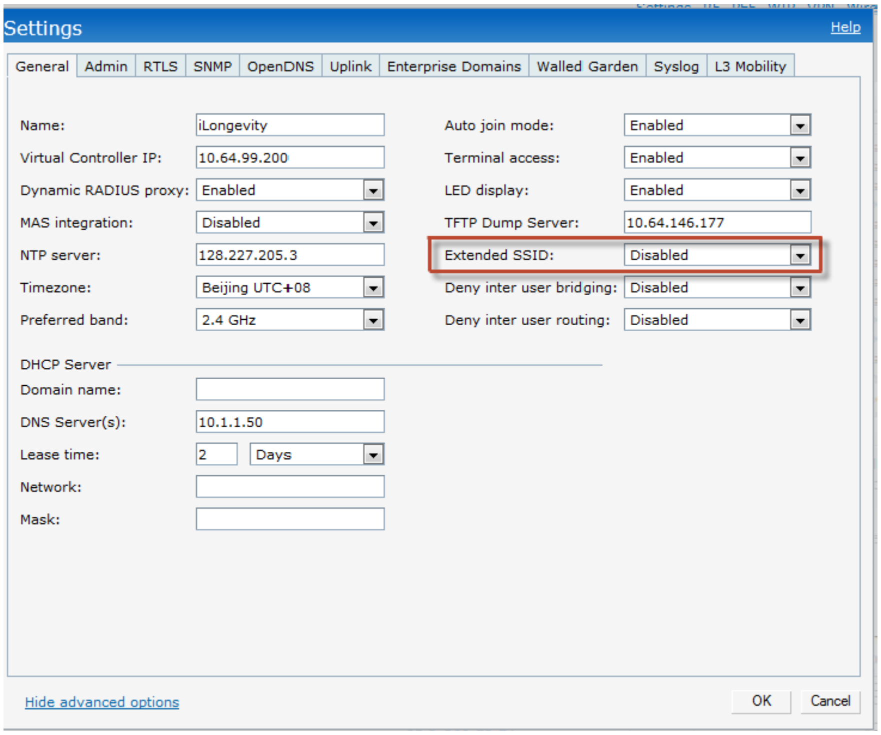
Lease time: Minutes

Network:

Mask:

Extended SSID

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



Settings

Help
General | Admin | RTLS | SNMP | OpenDNS | Uplink | Enterprise Domains | Walled Garden | Syslog | L3 Mobility

Name: iLongevity

Virtual Controller IP: 10.64.99.200

Dynamic RADIUS proxy: Enabled

MAS integration: Disabled

NTP server: 128.227.205.3

Timezone: Beijing UTC+08

Preferred band: 2.4 GHz

Auto join mode: Enabled

Terminal access: Enabled

LED display: Enabled

TFTP Dump Server: 10.64.146.177

Extended SSID: Disabled

Deny inter user bridging: Disabled

Deny inter user routing: Disabled

DHCP Server

Domain name:

DNS Server(s): 10.1.1.50

Lease time: 2 Days

Network:

Mask:

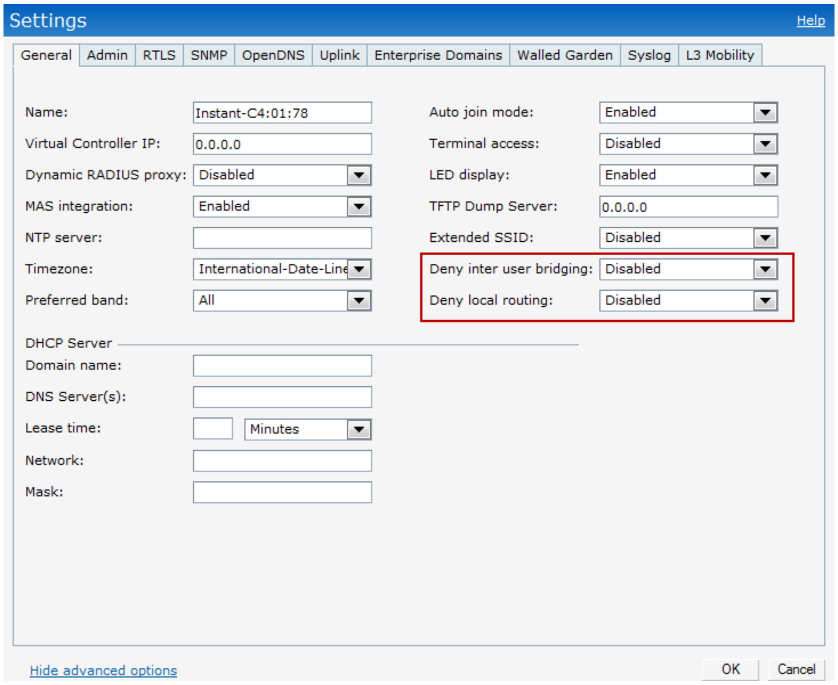
Deny Inter User Bridging and Deny Local Routing

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

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

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

Figure 58 *Deny Inter User Bridging and Deny Inter User Routing*



Name: Instant-C4:01:78
Virtual Controller IP: 0.0.0.0
Dynamic RADIUS proxy: Disabled
MAS integration: Enabled
NTP server:
Timezone: International-Date-Line
Preferred band: All

Auto join mode: Enabled
Terminal access: Disabled
LED display: Enabled
TFTP Dump Server: 0.0.0.0
Extended SSID: Disabled
Deny inter user bridging: Disabled
Deny local routing: Disabled

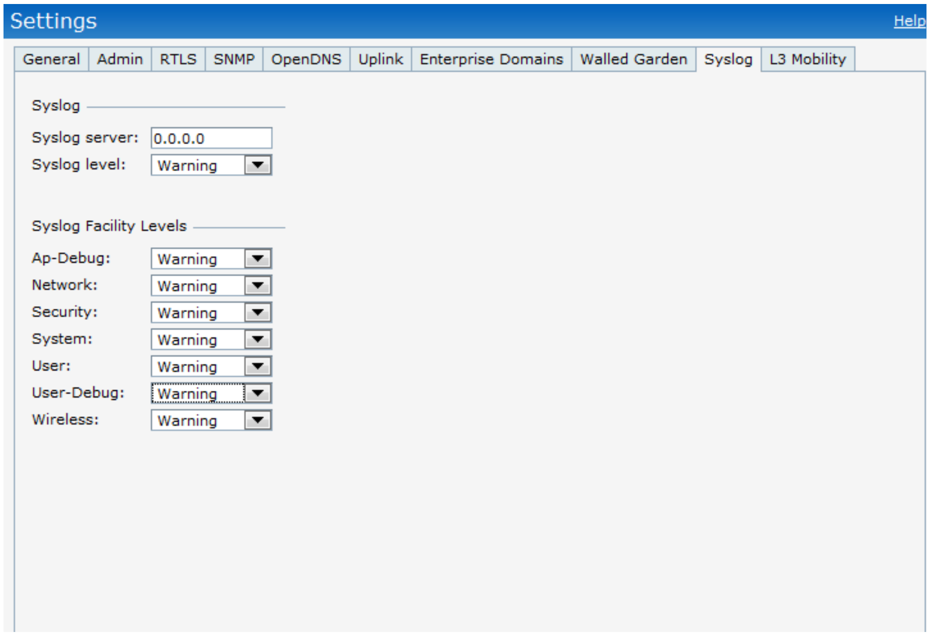
DHCP Server
Domain name:
DNS Server(s):
Lease time: Minutes
Network:
Mask:

Syslog Server

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

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

Figure 59 *Syslog Server*



Syslog
Syslog server: 0.0.0.0
Syslog level: Warning

Syslog Facility Levels
Ap-Debug: Warning
Network: Warning
Security: Warning
System: Warning
User: Warning
User-Debug: Warning
Wireless: Warning

Syslog Facility Levels

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

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

Table 12 describes the logging levels in order of severity, from most to least severe.

Table 12 *Logging Levels*

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

Adding an IAP to the Network

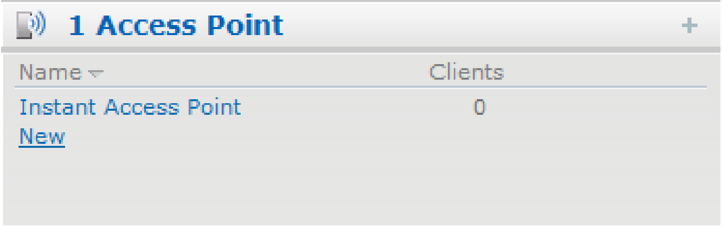
To add an IAP to the Aruba Instant network, assign an IP address. For more information, see "Assigning an IP Address to the IAP" on page 24.

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

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

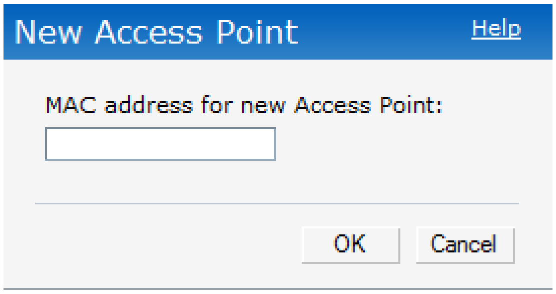
1. In the **Access Points** tab, click the **New** link.

Figure 60 *Adding an IAP to the Instant Network*



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

Figure 61 *Entering the MAC Address for the New IAP*



3. Click **OK.**

Removing an IAP from the Network

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

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.

> The deleted IAP(s) cannot join the Instant network anymore and no longer appear in the Instant WebUI. However, the master IAP cannot be deleted from the Virtual Controller.

Editing IAP Settings

This section explains the following IAP settings:

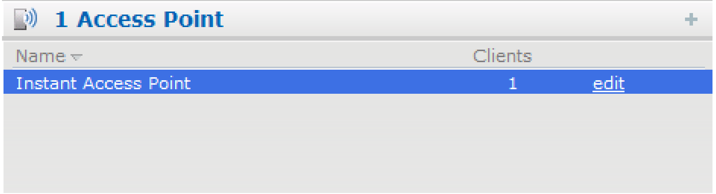
- Name
- IP Address
- Adaptive Radio Management (ARM) Configuration
- Wired Bridging on Ethernet 0 Port
- Uplink Management VLAN
- Migrating from a Virtual Controller Managed Network to Mobility Controller Managed Network

Changing IAP Name

To change the IAP name:

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

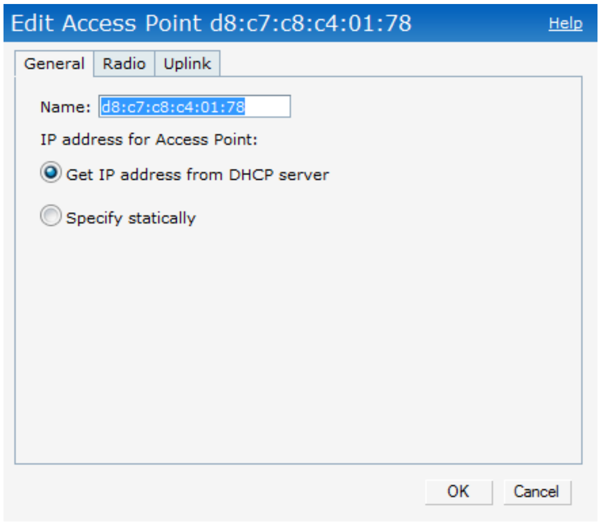
Figure 62 *Editing IAP Settings*



Name	Clients	
Instant Access Point	1	edit

2. Click the **edit** link.

Figure 63 *Changing IAP Name*



Edit Access Point d8:c7:c8:c4:01:78

Name: d8:c7:c8:c4:01:78

IP address for Access Point:

● Get IP address from DHCP server

○ Specify statically

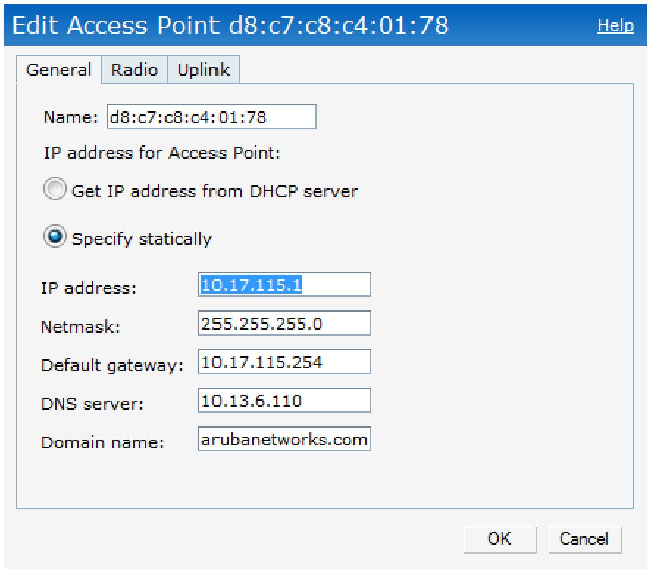
3. Edit the IAP name in the **Name** text box.
4. Click **OK.**

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:

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** window appears.

Figure 64 *Configuring IAP Settings — Connectivity Tab*



Edit Access Point d8:c7:c8:c4:01:78

Name: d8:c7:c8:c4:01:78

IP address for Access Point:

○ Get IP address from DHCP server

● Specify statically

IP address: 10.17.115.1

Netmask: 255.255.255.0

Default gateway: 10.17.115.254

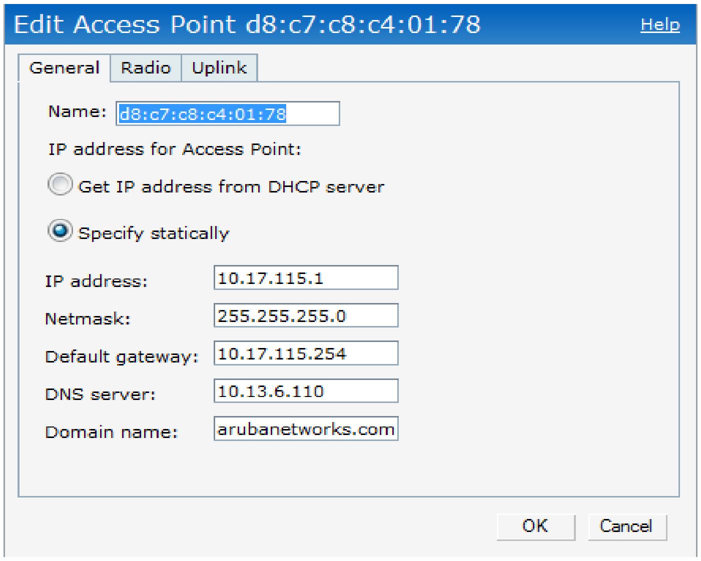
DNS server: 10.13.6.110

Domain name: arubanetworks.com

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

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

Figure 65 *Configuring IAP Connectivity Settings — Specifying Static Settings*



Name: d8:c7:c8:c4:01:78

IP address for Access Point:

○ Get IP address from DHCP server

● Specify statically

IP address: 10.17.115.1

Netmask: 255.255.255.0

Default gateway: 10.17.115.254

DNS server: 10.13.6.110

Domain name: arubanetworks.com

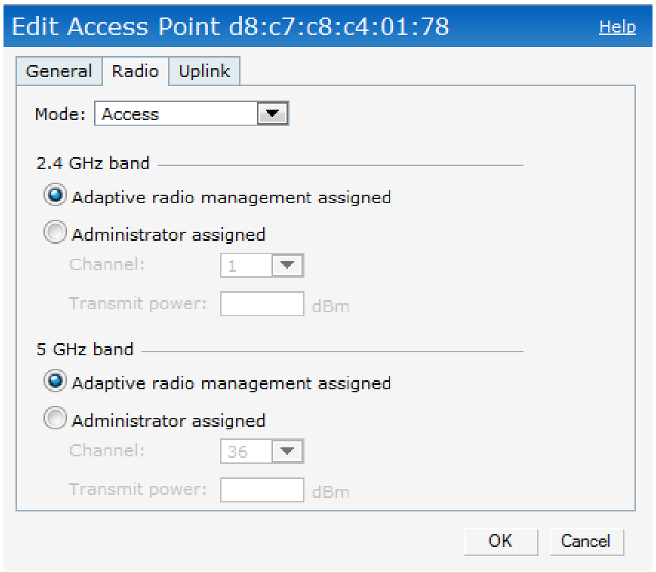
4. Click **OK** and reboot the IAP.

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.

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

Figure 66 *Configuring IAP Radio Settings Mode — Access*



Mode: Access

2.4 GHz band

● Adaptive radio management assigned

○ Administrator assigned

Channel: 1

Transmit power: dBm

5 GHz band

● Adaptive radio management assigned

○ Administrator assigned

Channel: 36

Transmit power: dBm

5. Click **OK.**

For more information about ARM, see "Adaptive Radio Management" on page 173.

Configuring Uplink Management VLAN

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

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

NOTE

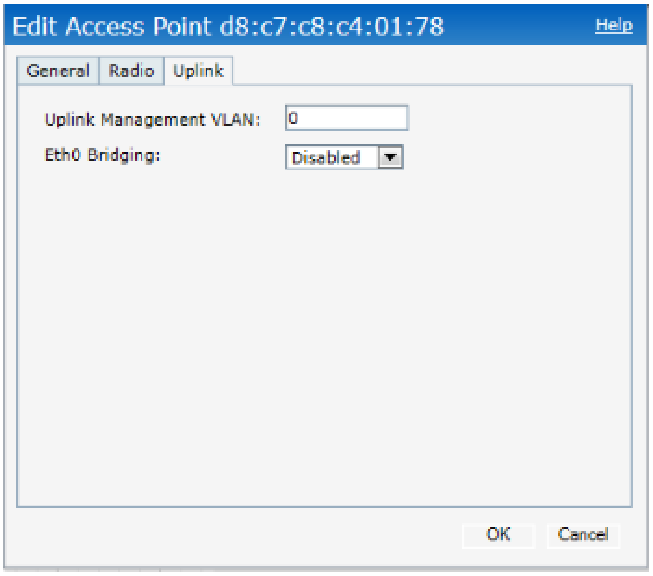
This configuration requires an IAP reboot to take effect.

Configuring Wired Bridging on Ethernet 0

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

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

Figure 67 *Configuring Wired Bridging on Ethernet 0 of an IAP*



Edit Access Point d8:c7:c8:c4:01:78

Uplink Management VLAN: 0

Eth0 Bridging: Disabled

5. Click **OK.**

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

NOTE

Reboot the IAP after the bridging is set for the configuration to take effect.

Migrating to a Mobility Controller Managed Network

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

Converting an IAP to RAP Mode

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

- If the IAP gets AirWave information via DHCP (Option 43 and Option 60), it establishes an HTTPS connection to the AirWave server and downloads the configuration and operates in IAP mode.
- If the IAP does not get AirWave information via DHCP provisioning, it tries provisioning via a firmware image server in the cloud (sends serial number MAC address). If an entry for the IAP is present in the firmware image cloud server and is provisioned as an IAP > RAP entry, the firmware image cloud server responds with controller IP address, AP group, and AP type. The IAP then contacts the controller, establishes certificate-based secure communication, and gets configuration and image from the controller. The IAP then reboots and comes up as a RAP. The IAP then establishes an IPSEC connection with the controller and begins operating in RAP mode.
- If an IAP entry for the AP is present in the firmware image cloud server, the IAP gets AirWave server information from the cloud server and downloads configuration from AirWave to operate in IAP mode.
- If there is no response from the cloud server or AirWave, the IAP comes up in Aruba Instant mode.

NOTE

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

NOTE

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

An IAP can be converted to an ArubaOS Campus AP and ArubaOS Remote AP only if the controller is running ArubaOS 6.1.4 or later.

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

Table 13 *IAP Platforms and Minimal AOS Version for IAP to CAP Conversion*

IAP Platform	AOS Version
IAP-92	6.1.4 or later
IAP-93	6.1.4 or later

Table 13 *IAP Platforms and Minimal AOS Version for IAP to CAP Conversion (Continued)*

IAP Platform	AOS Version
IAP-104	6.1.4 or later
IAP-105	6.1.4 or later
IAP-134	6.1.4 or later
IAP-135	6.1.4 or later
IAP-175AC	6.1.4 or later
IAP-175P	6.1.4 or later
RAP-3WN	6.1.4 or later
RAP-3WNP	6.1.4 or later

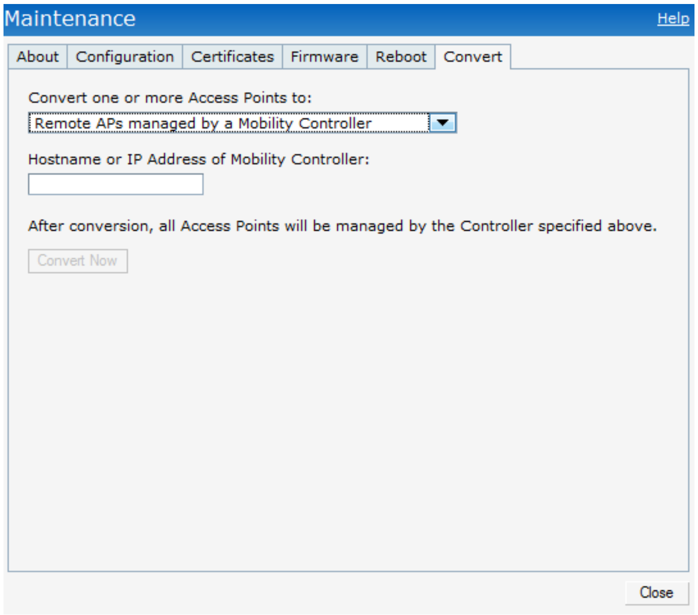
Table 14 *IAP platforms and minimal AOS version for IAP to RAP Conversion*

IAP Platform	AOS Version
IAP-92	6.1.4 or later
IAP-93	6.1.4 or later
IAP-104	6.1.4 or later
IAP-105	6.1.4 or later
IAP-134	6.1.4 or later
IAP-135	6.1.4 or later
IAP-175AC	6.1.4 or later
IAP-175P	6.1.4 or later
RAP-3WN	6.1.4 or later
RAP-3WNP	6.1.4 or later

To convert an IAP to RAP, follow the instructions below:

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

Figure 68 *Maintenance — Convert Tab*



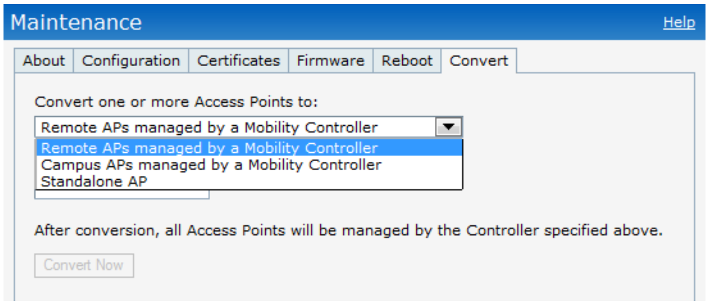
Convert one or more Access Points to:

Remote APs managed by a Mobility Controller

Hostname or IP Address of Mobility Controller:

After conversion, all Access Points will be managed by the Controller specified above.

Figure 69 *Convert options*



Convert one or more Access Points to:

Remote APs managed by a Mobility Controller

Remote APs managed by a Mobility Controller
Campus APs managed by a Mobility Controller
Standalone AP

After conversion, all Access Points will be managed by the Controller specified above.

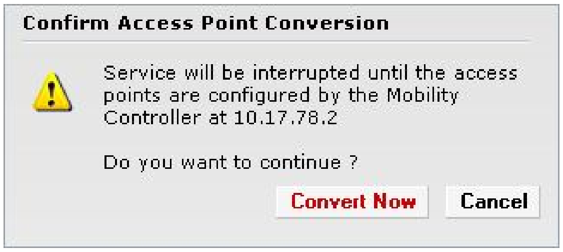
3. Select **Remote APs managed by a Mobility Controller** from the drop-down list.
4. Enter the hostname (fully qualified domain name) or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. This information is provided by your network administrator.

NOTE

Ensure the Mobility Controller IP Address is reachable by the IAPs.

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

Figure 70 *Confirm Access Point Conversion*



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 ?

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

7. After conversion, the IAP is managed by the Aruba Mobility Controller which has been specified in the Instant UI.

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

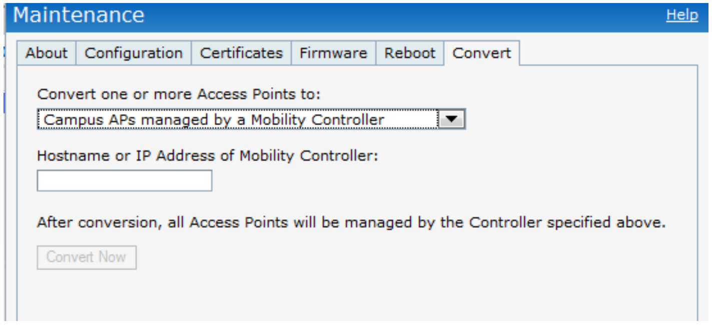
If the VPN setup fails and an error message pops up, please click **OK**, copy the error logs and share them with your Aruba support engineer.

Converting an IAP to CAP

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

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

Figure 71 *Converting an IAP to CAP*



Convert one or more Access Points to: Campus APs managed by a Mobility Controller

Hostname or IP Address of Mobility Controller:

After conversion, all Access Points will be managed by the Controller specified above.

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

Ensure the Mobility Controller IP Address is reachable by the IAPs.

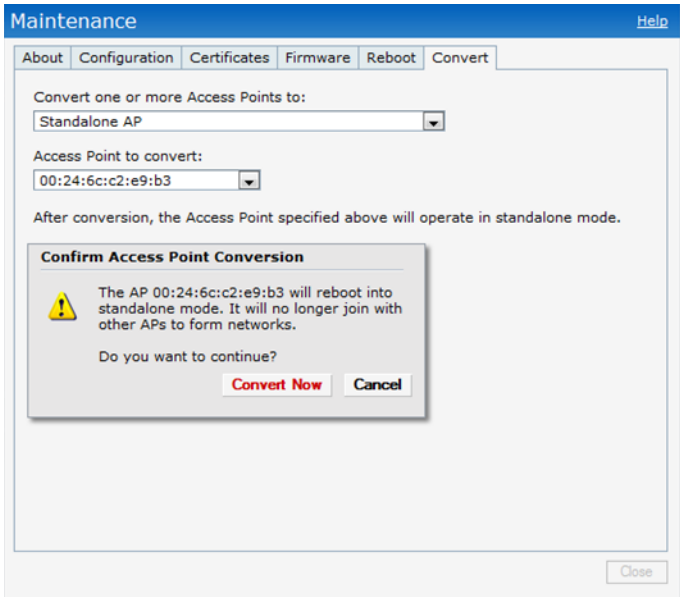
5. Click **Convert Now** to complete the conversion.

Converting an IAP to Standalone Mode

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

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

Figure 72 *Standalone AP Conversion*



Maintenance

Convert one or more Access Points to: Standalone AP

Access Point to convert: 00:24:6c:c2:e9:b3

After conversion, the Access Point specified above will operate in standalone mode.

Confirm Access Point Conversion

The AP 00:24:6c:c2:e9:b3 will reboot into standalone mode. It will no longer join with other APs to form networks.

Do you want to continue?

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

Converting back to an IAP

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

To reset an IAP, follow the instructions below:

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

The IAP then boots with the factory default settings.

NOTE

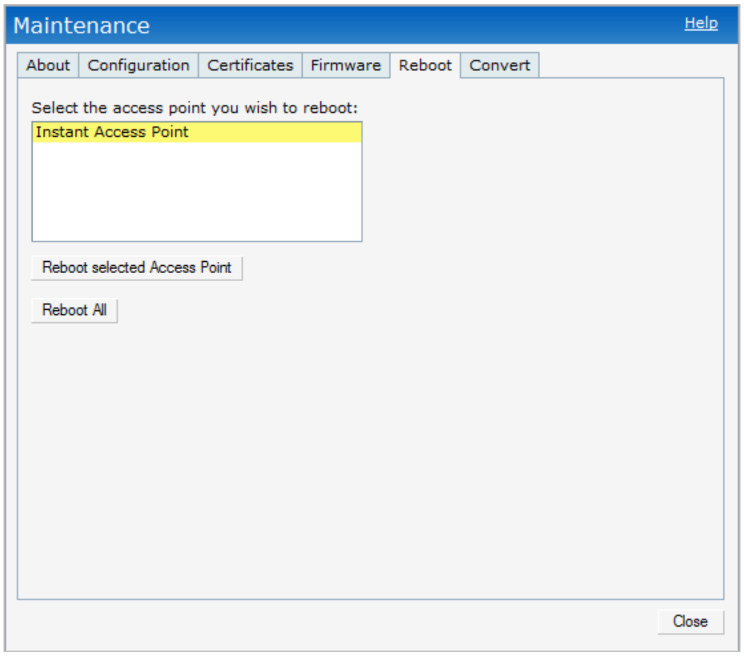
IAP-92, IAP-93, IAP-104, IAP-105, IAP-134, IAP-135, RAP-3WN, RAP-3WNP — These IAP platforms support reset button. IAP-175P and IAP-175AC do not have reset buttons. Please contact Aruba support for the backward conversion process on these IAPs.

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** window appears.
2. Click the **Reboot** tab.

Figure 73 *Rebooting the IAP*

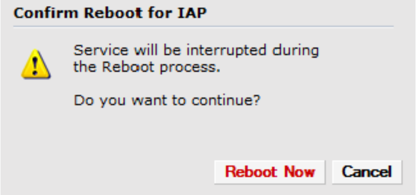


Select the access point you wish to reboot:

Instant Access Point

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

Figure 74 *Confirm Reboot message*



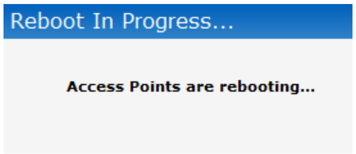
Confirm Reboot for IAP

Service will be interrupted during the Reboot process.

Do you want to continue?

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

Figure 75 *Reboot In Progress*

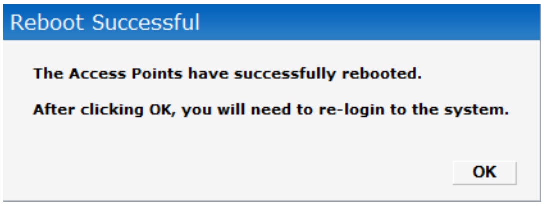


Reboot In Progress...

Access Points are rebooting...

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

Figure 76 *Reboot Successful*



Reboot Successful

The Access Points have successfully rebooted.

After clicking OK, you will need to re-login to the system.

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

Firmware Image Server in Cloud Network

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

Upgrade using AirWave and Image Server

Aruba Instant supports mixed AP-class instant deployment with RAP-3WN/3WNP, IAP-104, IAP-175P/175AC, IAP-92/93, IAP-105, and IAP-134/135 as part of the same Virtual Controller cluster.

Image management using Cloud Server

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

Image management using AirWave

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

NOTE

The Virtual Controller in Instant AP communicates with the AirWave server or Image server, depending on the user's configuration. If AirWave is not configured on the IAP, then the image is requested from the Image server. See "Configuring AirWave" on page 207 for steps on how to configure AirWave.

Automatic Firmware Image Check and Upgrade

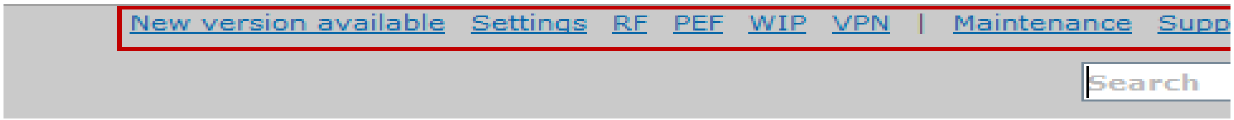
Automatic image check is enabled by default. If AirWave is configured, then the automatic image check is automatically disabled, use the manual image check option to check for the latest image. For more information, see "Upgrading to New Version" on page 102 and "Configuring AirWave" on page 207 for steps on how to configure AirWave.

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

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

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

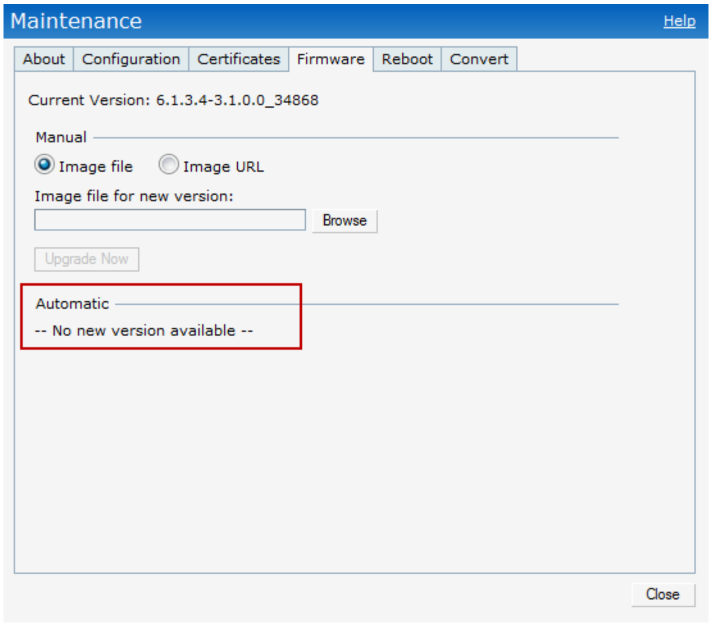
Figure 77 *Automatic Image Check — New Version Available Link*



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

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

Figure 78 *New Version Available*



Current Version: 6.1.3.4-3.1.0.0_34868

Manual

● Image file ○ Image URL

Image file for new version:

Automatic

-- No new version available --

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

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

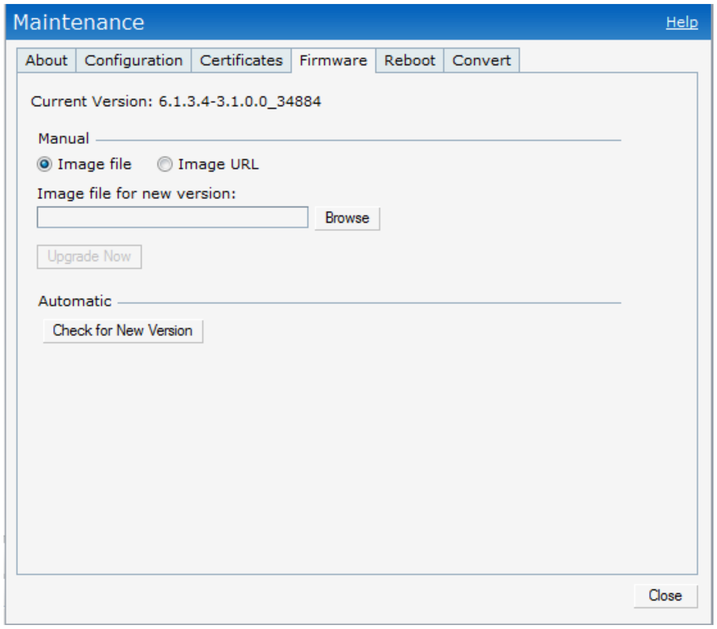
Upgrading to New Version

To manually check for a new firmware image version:

Manual

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

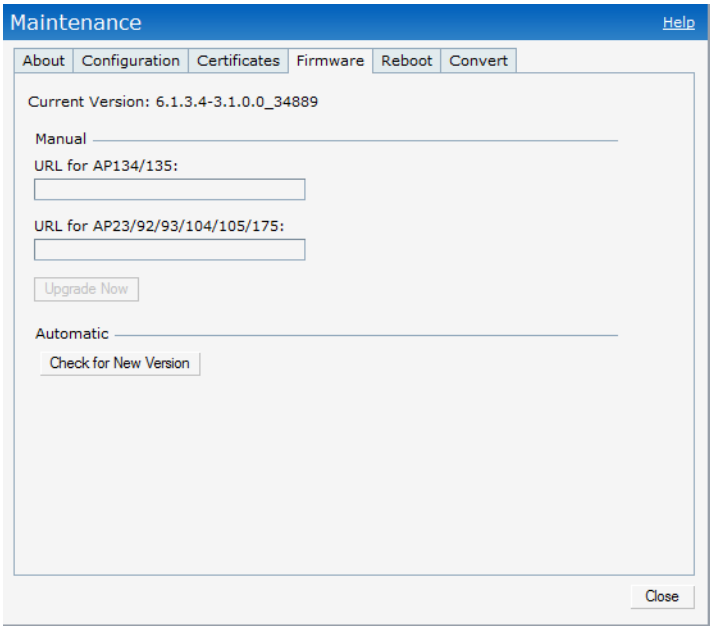
Figure 79 *Single class or Multi-class IAP Networks Firmware Upgrade*



Current Version: 6.1.3.4-3.1.0.0_34884

● Image file ○ Image URL

Figure 80 *Mixed IAP Network Firmware Upgrade*



Current Version: 6.1.3.4-3.1.0.0_34889

- **Image file—** Select to directly upload an image file. This method is only available for single-class IAPs.
  - Example: ArubaInstant_Orion_6.1.3.4-3.1.0.0_xxxx
  - Example: ArubaInstant_Cassiopeia_6.1.3.4-3.1.0.0_xxxx
- **Image URL—** Select obtain the image file from a TFTP, FTP and HTTP URL

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

TFTP:

- URL for IAP-135/134: tftp://10.64.147.8/ArubaInstant_Cassiopeia_6.1.3.4-3.1.0.0_xxxx
- URL for IAP-105/92/93: tftp://10.64.147.8/ArubaInstant_Orion_6.1.3.4-3.1.0.0_xxxx

FTP:

- ftp://10.64.147.8/ArubaInstant_Cassiopeia_6.1.3.4-3.1.0.0_xxxx

- ftp://10.64.147.8/ArubaInstant_Orion_6.1.3.4-3.1.0.0_xxxx

HTTP:

- http://10.64.160.42/ArubaInstant_Cassiopeia_6.1.3.4-3.1.0.0_xxxx
- http://10.64.160.42/ArubaInstant_Orion_6.1.3.4-3.1.0.0_xxxx

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

Automatic

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

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

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

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

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

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

Chapter 7

Mobility Access Switch Integration

Mobility Access Switch (MAS) Overview

The ArubaOS Mobility Access Switch enables secure, role-based network access for wired users and devices, independent of their location or application. Installed in wiring closets, the MAS delivers up to 384 wire-speed Gigabit Ethernet switch ports and operates as a wired access point when deployed with an Aruba Mobility Controller.

As a wired access point, users and their devices are authenticated and assigned a unique role by the Mobility Controller. These roles are consistently applied whether the user is a Wi-Fi client, or connects to a port on the Mobility Access Switch. The result is an enterprise workforce that has consistent, secure access to network resources based on who they are – no matter where they are, what device they're using or how they connect.

Two models of the Mobility Access Switch are available, the S3500 and S2500.

For more information on MAS, see the ***ArubaOS 7.1.3 User Guide***.

MAS Integration with an IAP

The Instant AP can be integrated with a MAS by plugging the Instant AP directly to the MAS port.

This section describes two main Mobility Access Switch (MAS) integration features:

- Rogue AP containment
- PoE prioritization

Rogue AP Containment

When a rogue AP is detected by Instant, it sends the MAC Address of the rogue AP to the MAS. The MAS blacklists the MAC address of the rogue AP and turns off the PoE on the port.

PoE Prioritization

When an Instant AP is plugged directly into the MAS port, the MAS should increase the PoE priority of the port. This is done only if the PoE priority is set by default in the MAS.

NOTE

The PoE Prioritization and Rogue AP Containment features is available for ArubaOS 7.2 release on **Aruba's Mobility Access Switches**.

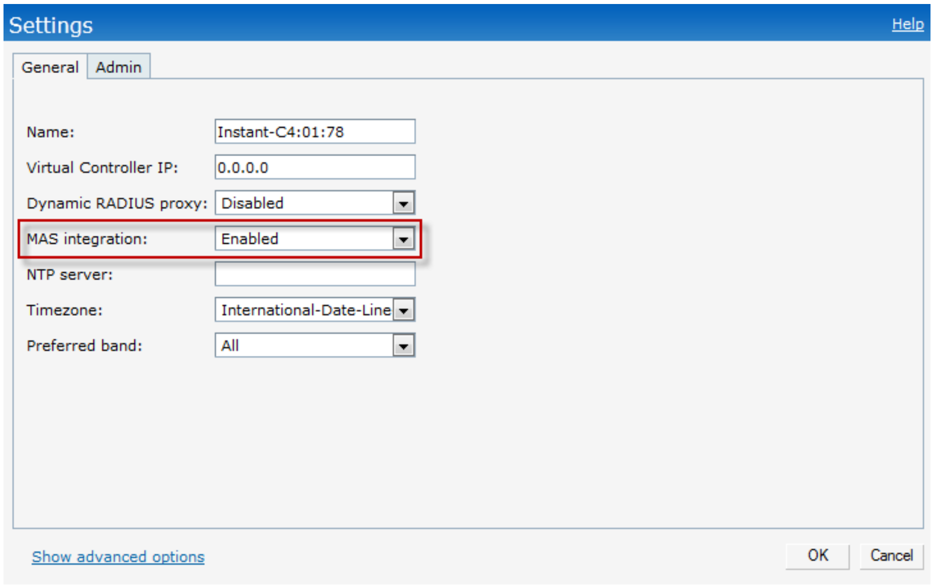
Enabling MAS Integration

This functionality enables the LLDP for the MAS integration. Using this protocol the IAPs instructs the MAS to turn off the ports where rogue APs are connected and to take actions such as increasing the PoE priority and to automatically configure the VLANs on the ports where the IAPs are connected.

To enable the MAS integration functionality, perform the following steps in the Instant UI:

1. Navigate to **Settings** at the top right corner of the Instant UI.
2. Navigate to **General** tab and select **Enabled** from the **MAS integration** drop-down list.

Figure 81 *Enabling MAS Integration with an IAP*

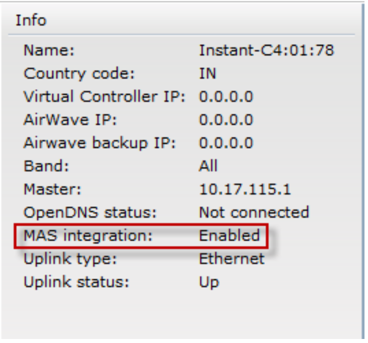


Name: Instant-C4:01:78
Virtual Controller IP: 0.0.0.0
Dynamic RADIUS proxy: Disabled
MAS integration: Enabled
NTP server:
Timezone: International-Date-Line
Preferred band: All

Viewing the MAS Integration Status

The user can view the current status of the MAS integration in the Instant UI under **Info** tab.

Figure 82 *MAS Integration Status*



Name: Instant-C4:01:78
Country code: IN
Virtual Controller IP: 0.0.0.0
AirWave IP: 0.0.0.0
Airwave backup IP: 0.0.0.0
Band: All
Master: 10.17.115.1
OpenDNS status: Not connected
MAS integration: Enabled
Uplink type: Ethernet
Uplink status: Up

Chapter 8

Layer-3 Mobility

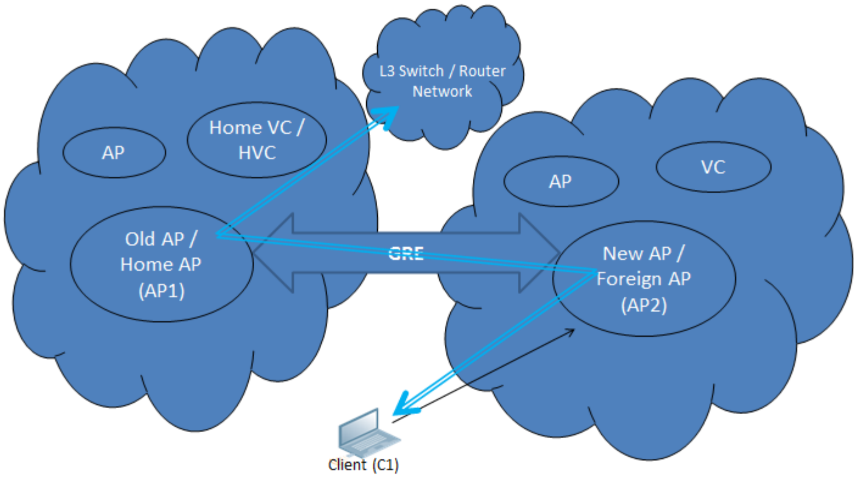
IAPs form a single Instant network when they are in the same L2 domain. As the number of clients increase, multiple subnets are required to avoid broadcast overhead. In such a scenario, a client should be allowed to roam away from the Instant network to which it first connected (home network) to another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

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

Overview

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

Figure 83 Shows the routing of traffic when the client is away from its home network



When a client first connects to an Instant network, a message is sent to all configured Virtual Controller IP addresses to see if this is an L3 roamed client. On receiving an acknowledgement from any of the configured Virtual Controller IP addresses, the client is identified as an L3 roamed client. If the AP has no GRE tunnel to this home network, a new tunnel is formed to an AP (home AP) from the client's home network.

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

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

Configuring a mobility domain

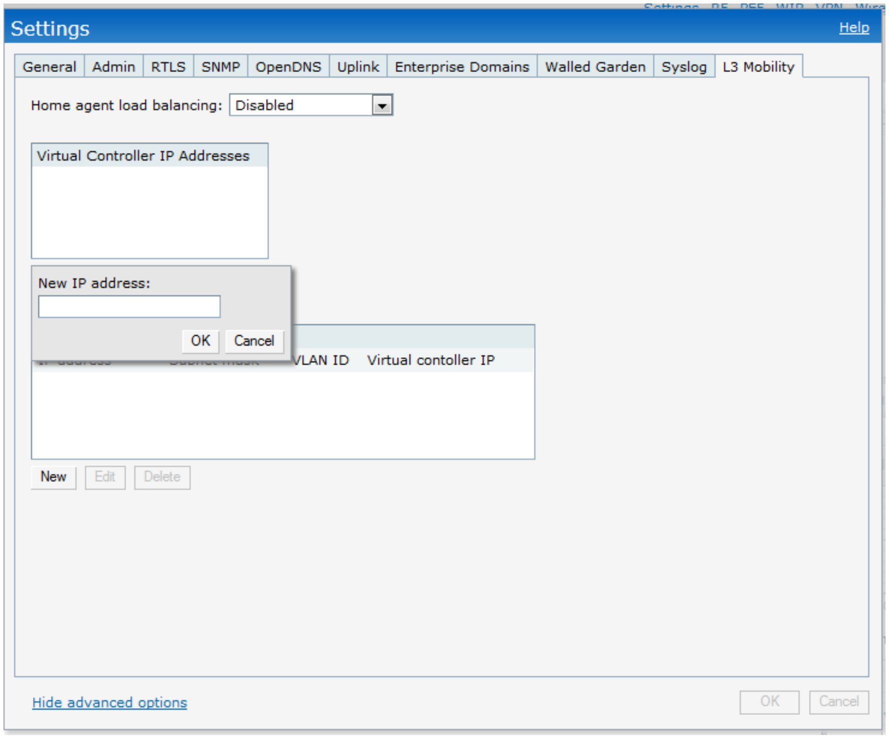
To configure a mobility domain, you have to specify the list of all Instant networks that form the mobility domain. In order to allow clients to roam seamlessly among all the APs, specify the Virtual Controller IP for each foreign subnet. You may include the local Instant/ VC IP address, so that the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

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

Perform the following steps to configure a mobility domain:

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

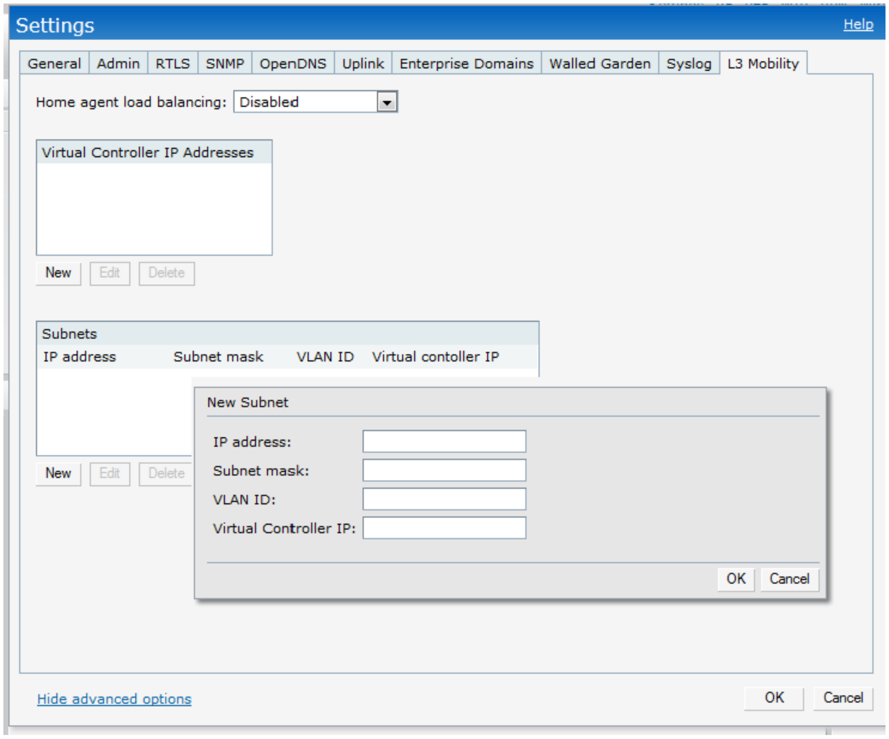
Figure 84 *Add Virtual Controller IP addresses*



Home agent load balancing: Disabled

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

Figure 85 *Add Subnets Information*



Home agent load balancing: Disabled

Virtual Controller IP Addresses

Subnets			
IP address	Subnet mask	VLAN ID	Virtual contoller IP

New Subnet

IP address:

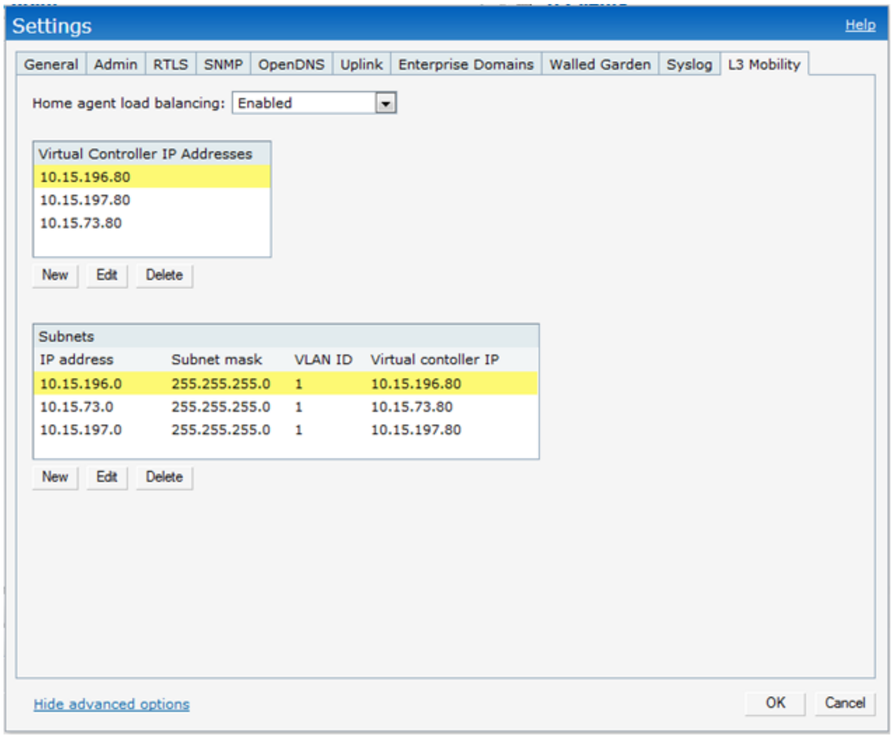
Subnet mask:

VLAN ID:

Virtual Controller IP:

6. Click **OK**.

Figure 86 *Example Layer-3 Configuration*



Home agent load balancing: Enabled

Virtual Controller IP Addresses
10.15.196.80
10.15.197.80
10.15.73.80

Subnets

IP address	Subnet mask	VLAN ID	Virtual contoller IP
10.15.196.0	255.255.255.0	1	10.15.196.80
10.15.73.0	255.255.255.0	1	10.15.73.80
10.15.197.0	255.255.255.0	1	10.15.197.80

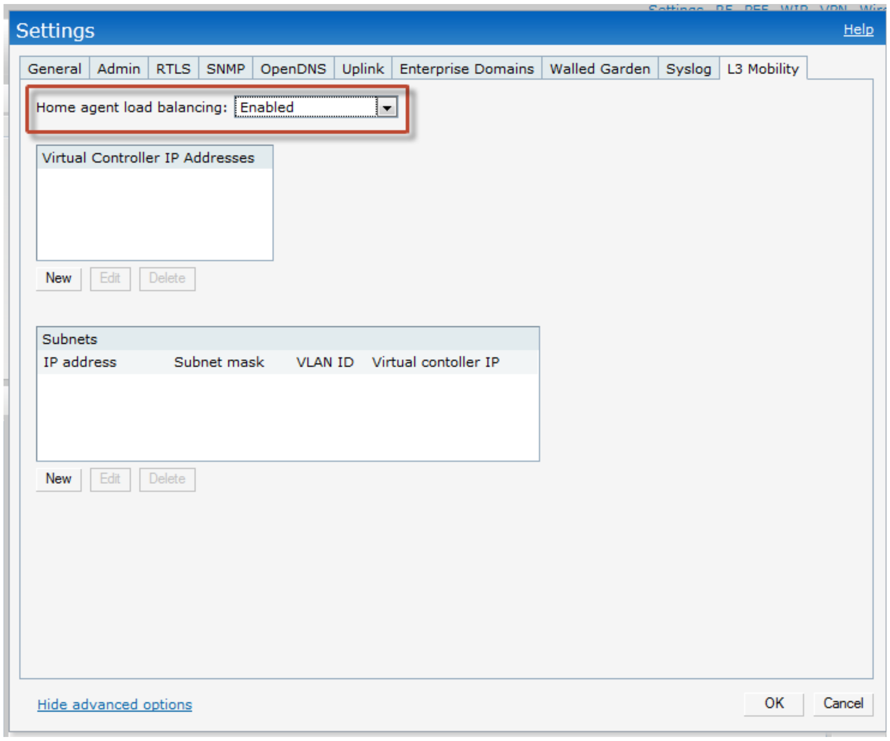
Home Agent Load Balancing

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

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

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

Figure 87 *Home Agent Load Balancing Enabled*



Home agent load balancing: Enabled

Chapter 9

Spectrum Monitor

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

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

The spectrum monitor is supported on IAP-104, IAP-105, IAP -134, and IAP-135 radios.

Creating Spectrum Monitors and Hybrid APs

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

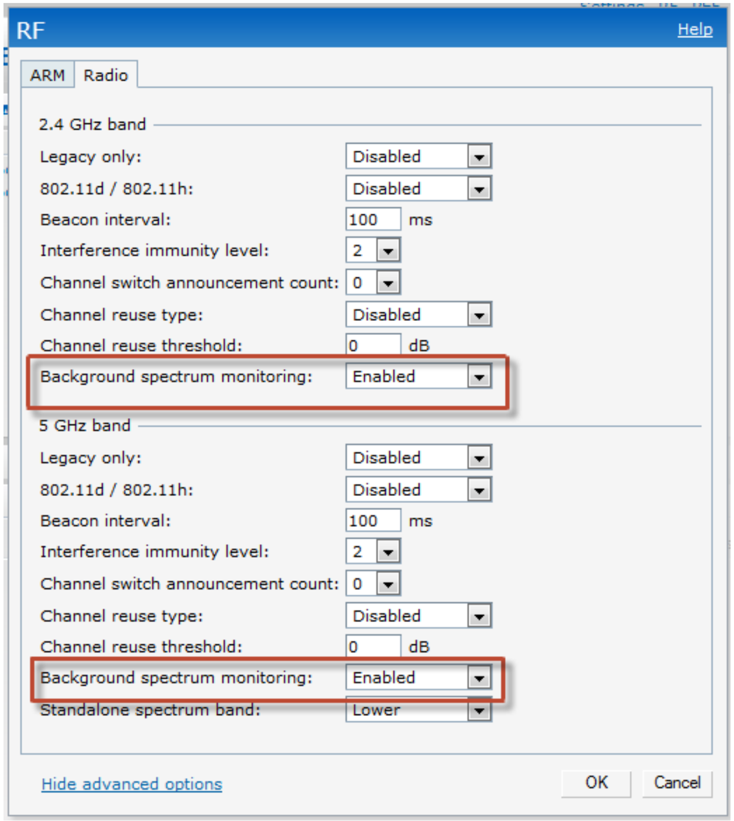
Converting IAPs into Hybrid IAPs

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

Follow the procedure below to convert IAPs in an Aruba Instant network to hybrid mode:

1. Click the **RF** link at the top right corner of the Instant WebUI.
2. Click **Show advanced options** to view the **Radio** tab.

Figure 88 *Configuring a Hybrid IAP*



2.4 GHz band

Legacy only: Disabled
802.11d / 802.11h: Disabled
Beacon interval: 100 ms
Interference immunity level: 2
Channel switch announcement count: 0
Channel reuse type: Disabled
Channel reuse threshold: 0 dB
Background spectrum monitoring: Enabled

5 GHz band

Legacy only: Disabled
802.11d / 802.11h: Disabled
Beacon interval: 100 ms
Interference immunity level: 2
Channel switch announcement count: 0
Channel reuse type: Disabled
Channel reuse threshold: 0 dB
Background spectrum monitoring: Enabled
Standalone spectrum band: Lower

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

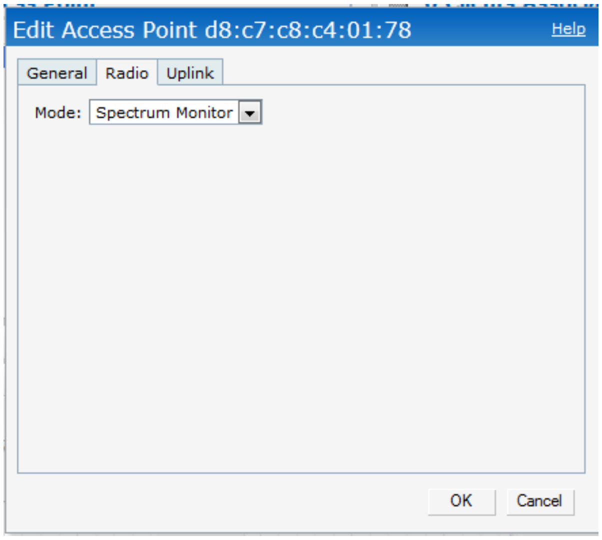
Converting an IAP to a Spectrum Monitor

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

Follow the procedure below to convert an IAP to a spectrum monitor.

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

Figure 89 *Configuring a Spectrum Monitor*



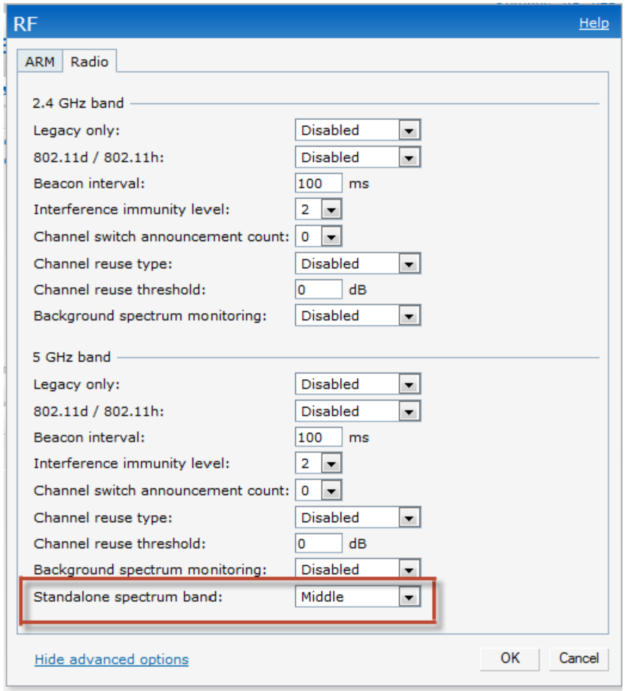
Edit Access Point d8:c7:c8:c4:01:78

Mode: Spectrum Monitor

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

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

Figure 90 *Monitor Middle Band for 5 GHz Radio.*



2.4 GHz band

Legacy only: Disabled

802.11d / 802.11h: Disabled

Beacon interval: 100 ms

Interference immunity level: 2

Channel switch announcement count: 0

Channel reuse type: Disabled

Channel reuse threshold: 0 dB

Background spectrum monitoring: Disabled

5 GHz band

Legacy only: Disabled

802.11d / 802.11h: Disabled

Beacon interval: 100 ms

Interference immunity level: 2

Channel switch announcement count: 0

Channel reuse type: Disabled

Channel reuse threshold: 0 dB

Background spectrum monitoring: Disabled

Standalone spectrum band: Middle

Spectrum Data

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

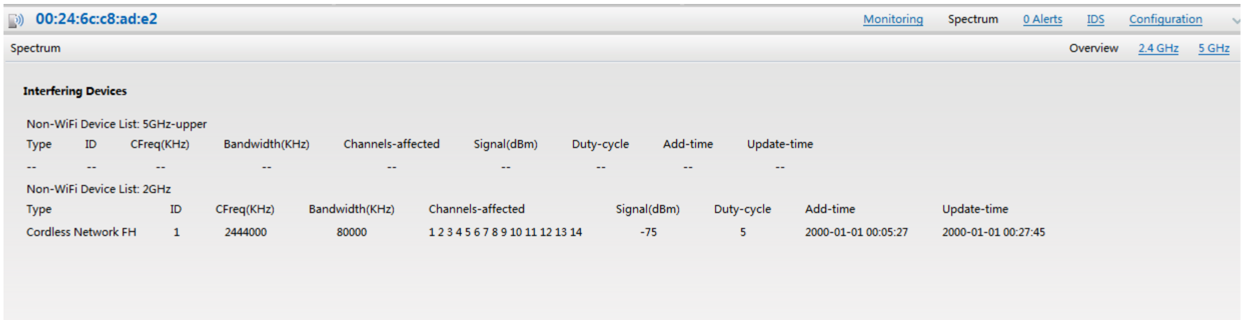
- Overview - Device list
- Channel metrics
- Channel details

Overview - Device List

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

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

Figure 91 *Device List*



Interfering Devices

Non-WiFi Device List: 5GHz-upper

Type	ID	CFreq(KHz)	Bandwidth(KHz)	Channels-affected	Signal(dBm)	Duty-cycle	Add-time	Update-time
--	--	--	--	--	--	--	--	--

Non-WiFi Device List: 2GHz

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

Table 15 shows the details of the information that is displayed:

Table 15 *Device Summary and Channel Information*

Column	Description
Type	Device type. This parameter can be any of the following: ● audio FF (fixed frequency) ● bluetooth ● cordless base FH (frequency hopper) ● cordless phone FF (fixed frequency ● cordless network FH (frequency hopper) ● generic FF (fixed frequency ● generic FH (frequency hopper) ● generic interferer ● microwave ● microwave inverter ● video ● xbox **NOTE:** For additional details about non-Wi-Fi device types shown in this table, see "Non-Wi-Fi Interferer Types" on page 115.
ID	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device.

Table 15 *Device Summary and Channel Information (Continued)*

Column	Description
Channels-affected	Radio channels affected by the wireless device.
Signal-strength	Strength of the signal sent from the device, in dBm.
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add-time	Time at which the device was first detected.
Update-time	Time at which the device's status was updated.

Non-WiFi Interferers

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

Table 16 *Non-Wi-Fi Interferer Types*

Non-Wi-Fi Interferer	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as *Fixed Frequency (Audio)*.
Fixed Frequency (Cordless Phones)	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as *Fixed Frequency (Cordless Phones)*.
Fixed Frequency (Video)	Video transmitters that continuously transmit video on a single frequency are classified as *Fixed Frequency (Video)*. These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.
Fixed Frequency (Other)	All other fixed frequency devices that do not fall into one of the above categories are classified as *Fixed Frequency (Other)*. Note that the RF signatures of the fixed frequency audio, video and cordless phone devices are very similar and that some of these devices may be occasionally classified as Fixed Frequency (Other).
Frequency Hopper (Cordless Base)	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (i.e., no active phone calls), the cordless base is classified as *Frequency Hopper (Cordless Base*).
Frequency Hopper (Cordless Network)	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as *Frequency Hopper (Cordless Network*). Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as *Frequency Hopper (Xbox*).
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into one of the above categories, it is classified as *Frequency Hopper (Other)*. Some examples include IEEE 802.11 FHSS devices, game consoles and cordless/hands-free devices that do not use one of the known cordless phone protocols.

Table 16 *Non-Wi-Fi Interferer Types (Continued)*

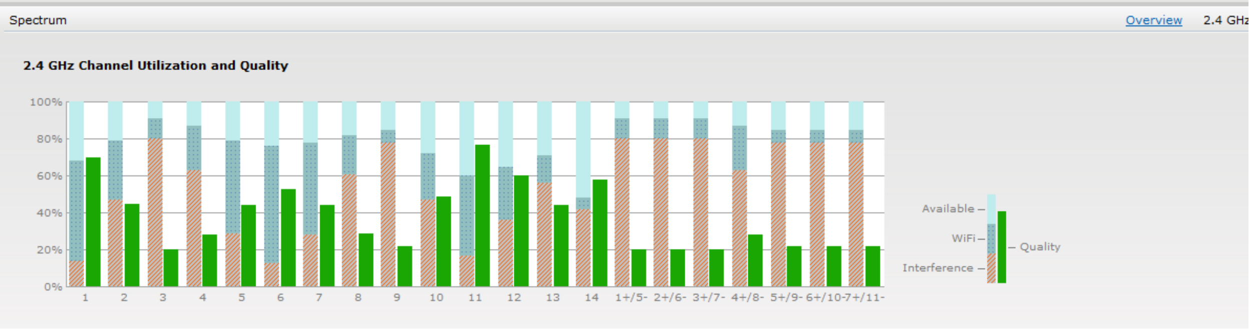
Non-Wi-Fi Interferer	Description
Microwave	Common residential microwave ovens with a single magnetron are classified as a *Microwave*. These types of microwave ovens may be used in cafeterias, break rooms, dormitories and similar environments. Some industrial, healthcare or manufacturing environments may also have other equipment that behave like a microwave and may also be classified as a Microwave device.
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as *Microwave (Inverter)*. Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as Microwave (Inverter). As in the Microwave category described above, there may be other equipment that behave like inverter microwaves in some industrial, healthcare or manufacturing environments. Those devices may also be classified as Microwave (Inverter).
Generic Interferer	Any non-frequency hopping device that does not fall into one of the other categories described in this table is classified as a *Generic Interferer*. For example a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a Generic Interferer. Similarly wide-band interfering devices may be classified as Generic Interferers.

Channel Metrics

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

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

Figure 92 *Channel Metrics for the 2.4 GHz Radio Channel*



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

Figure 93 *Channel Metrics for the 5 GHz Radio Channel*

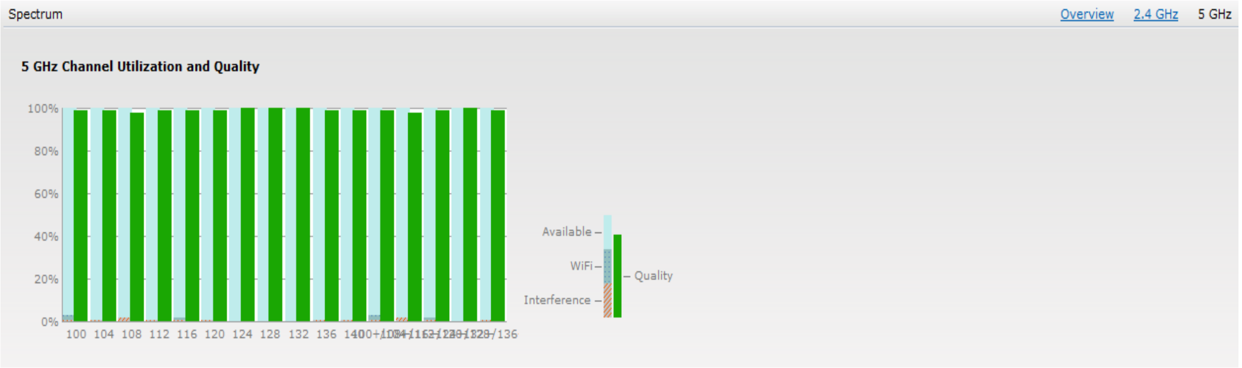


Table 17 shows the information displayed in the channel metrics graph.

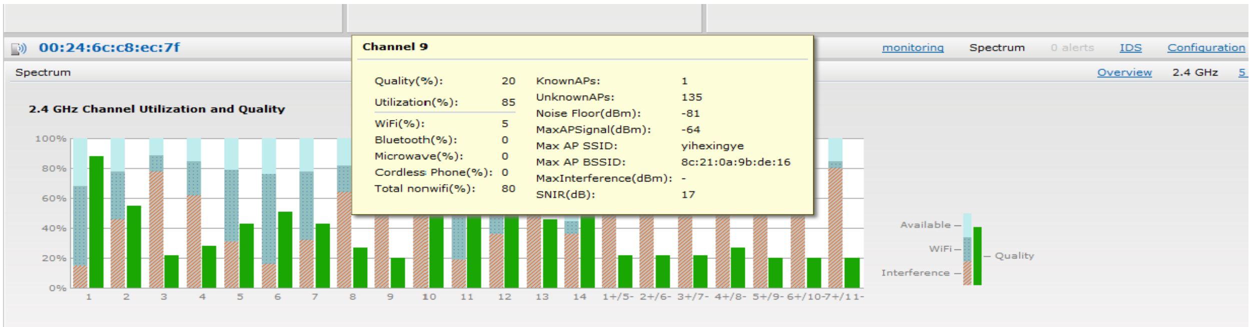
Table 17 *Channel Metrics*

Column	Description
Channel	A 2.4 GHz or 5 GHz radio channel.
Quality(%)	Current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands, as determined by the percentage of packet retries, the current noise floor, and the duty cycle for non-Wi-Fi devices on that channel.
Availability(%)	The percentage of the channel currently available for use.
Utilization(%)	The percentage of the channel being used.
WiFi Util(%)	The percentage of the channel currently being used by Wi-Fi devices.
Interference Util(%)	The percentage of the channel currently being used by non-Wi-Fi interference + Wi-Fi ACI (Adjacent Channel Interference)

Channel Details

When you hover your mouse over a channel, the channel details or the summary of the 802.11a or 802.11g channels seen by a spectrum monitor is displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference and the signal-to-noise-and-interference Ratio (SNIR). SNIR is the ratio of signal strength to the combined levels of interference and noise on that channel. Spectrum monitors display spectrum data seen on all channels in the selected band, and hybrid APs display data from the one channel they are monitoring.

Figure 94 *Channel Details*



Channel 9

Quality(%): 20
Utilization(%): 85
WiFi(%): 5
Bluetooth(%): 0
Microwave(%): 0
Cordless Phone(%): 0
Total nonwifi(%): 80

KnownAPs: 1
UnknownAPs: 135
Noise Floor(dBm): -81
MaxAPSignal(dBm): -64
Max AP SSID: yihexingye
Max AP BSSID: 8c:21:0a:9b:de:16
MaxInterference(dBm): -
SNIR(dB): 17

Table 18 shows the information that you can view in the channel details graph.

Table 18 *Channel Details Information*

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Quality(%)	Current relative quality of the channel.
Utilization(%)	The percentage of the channel being used.
Wi-Fi (%)	The percentage of the channel currently being used by Wi-Fi devices.
Type	Device type.
Total nonwifi (%)	The percentage of the channel currently being used by non Wi-Fi devices.
Known APs	Number of valid APs identified on the radio channel.
UnKnown APs	Number of invalid or rogue APs identified on the radio channel.
Channel Util (%)	Percentage of the channel currently in use.
Max AP Signal (dBm)	Signal strength of the AP that has the maximum signal strength on a channel.
Max Interference(dBm)	Signal strength of the non-Wi-Fi device that has the highest signal strength.
SNIR (db)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Spectrum Alerts

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

Chapter 10

NTP Server

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

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

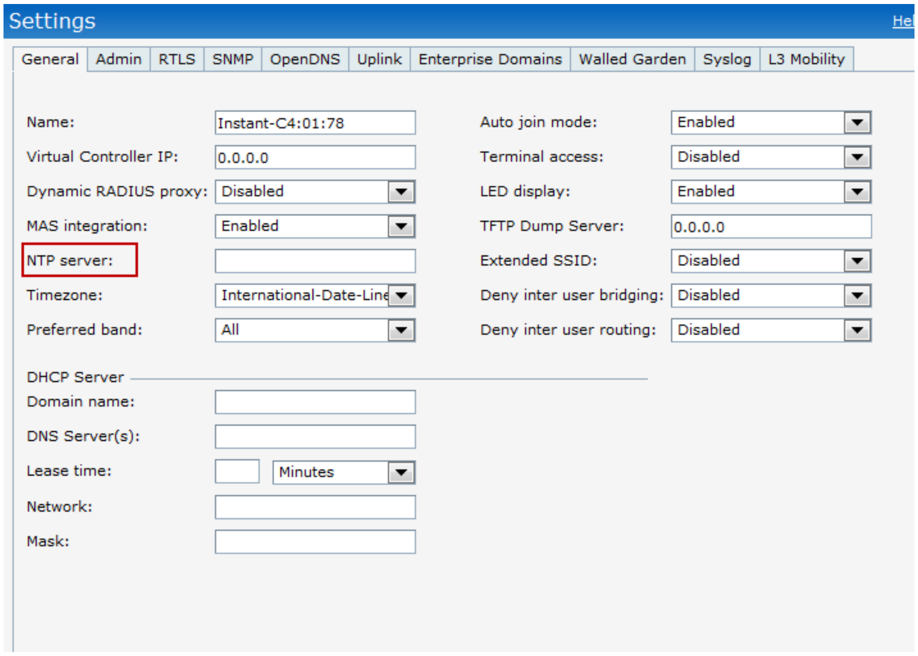
Network Time Protocol (NTP) is required to obtain the precise time from a server and to regulate the local time in each network element. If NTP server is not configured in the Aruba Instant network, an IAP reboot may lead to variation in time and data.

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. Navigate to the **Settings** tab in the top right corner of the Instant UI.
2. In the **General** tab, enter the IP address or the URL (domain name) of the NTP server in the **NTP Server** text box and click **OK.**
3. Select the timezone from the **Timezone** drop-down list. This indicates the time returned by the NTP server.

Figure 95 *Configuring NTP Server*



Name: Instant-C4:01:78
Virtual Controller IP: 0.0.0.0
Dynamic RADIUS proxy: Disabled
MAS integration: Enabled
NTP server:
Timezone: International-Date-Line
Preferred band: All

Auto join mode: Enabled
Terminal access: Disabled
LED display: Enabled
TFTP Dump Server: 0.0.0.0
Extended SSID: Disabled
Deny inter user bridging: Disabled
Deny inter user routing: Disabled

DHCP Server
Domain name:
DNS Server(s):
Lease time: Minutes
Network:
Mask:

Virtual Controller

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 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

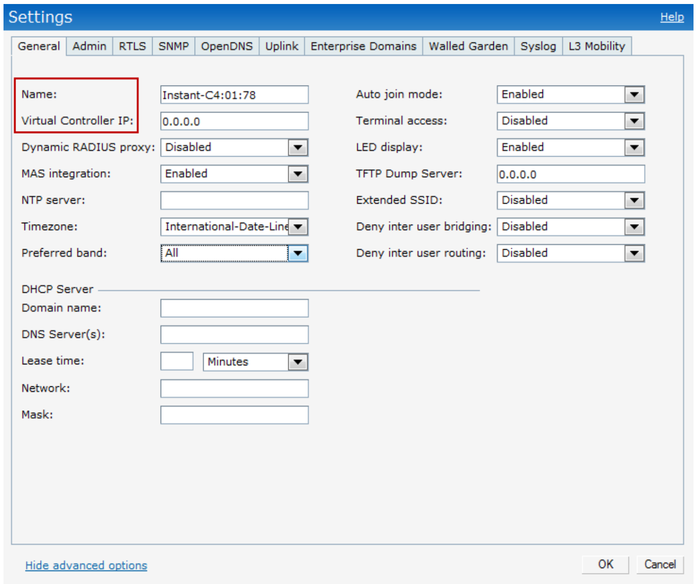
You can specify a single static IP address that can be used to manage a multi-AP Aruba Instant network. This IP address is automatically provisioned on a shadow interface on the IAP that takes the role of a Virtual Controller. When an IAP becomes a Virtual Controller, it sends three Address Resolution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

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

Figure 96 *Specifying Virtual Controller Name and IP Address*



Name:	Instant-C4:01:78	Auto join mode:	Enabled
Virtual Controller IP:	0.0.0.0	Terminal access:	Disabled
Dynamic RADIUS proxy:	Disabled	LED display:	Enabled
MAS integration:	Enabled	TFTP Dump Server:	0.0.0.0
NTP server:		Extended SSID:	Disabled
Timezone:	International-Date-Line	Deny inter user bridging:	Disabled
Preferred band:	All	Deny inter user routing:	Disabled

DHCP Server

Domain name:	
DNS Server(s):	
Lease time:	Minutes
Network:	
Mask:	

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

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

Configuring the DHCP Server

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

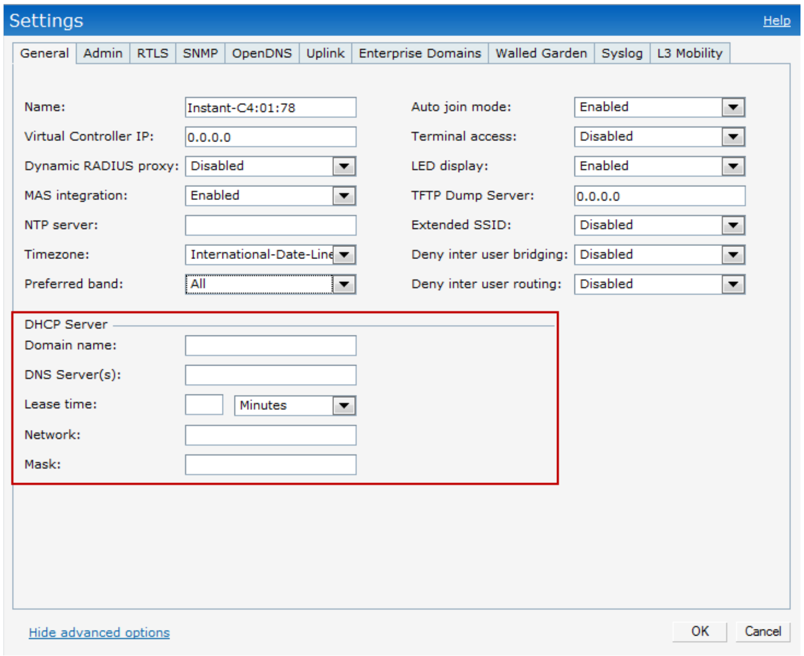
To configure the domain name, DNS server, and lease time for the DHCP server, network, and mask, perform the following steps:

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

NOTE

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

Figure 97 *Configuring the DHCP Server*



Name:	Instant-C4:01:78	Auto join mode:	Enabled
Virtual Controller IP:	0.0.0.0	Terminal access:	Disabled
Dynamic RADIUS proxy:	Disabled	LED display:	Enabled
MAS integration:	Enabled	TFTP Dump Server:	0.0.0.0
NTP server:		Extended SSID:	Disabled
Timezone:	International-Date-Line	Deny inter user bridging:	Disabled
Preferred band:	All	Deny inter user routing:	Disabled

DHCP Server

Domain name:	
DNS Server(s):	
Lease time:	Minutes
Network:	
Mask:	

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

Authentication Methods in Aruba Instant

Authentication is a process of identifying a user by having them to provide a valid username and password. Clients can also be authenticated based on their MAC addresses. The following authentication methods are supported in 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 identity and begins authentication with the client if the user identity is present in its database. The RADIUS server sends an Access-Accept message to the NAS.

   If the RADIUS server cannot identify the user, it stops the authentication process and sends an Access-Reject message to the NAS. The NAS forwards this message to the client and the client must re-authenticate with correct credentials.
5. After the client is authenticated, the RADIUS server forwards the encryption key to the NAS. The encryption key is used to encrypt or decrypt traffic sent to and from the client.

NOTE

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

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

Internal RADIUS Server

Each IAP has an instance of Free RADIUS server operating locally. When you enable the Internal RADIUS server option for the network, the 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-TLS— The Extensible Authentication Protocol- Transport Layer Security method supports the termination of EAP-TLS security using the internal RADIUS server. The EAP-TLS requires both server and certification authority (CA) certificates installed onto the IAP.The client certificate is verified on the Virtual Controller (the client certificate must be signed by a known CA) before the user name is checked on the authentication server.

- EAP-TTLS (MSCHAPv2)— The Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) method uses server-side certificates to set up authentication between clients and servers. However, the actual authentication is performed using passwords.
- EAP-PEAP (MSCHAPv2)— Protected Extensible Authentication Protocol (PEAP) is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL / TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.
- LEAP— Lightweight Extensible Authentication Protocol (LEAP) uses dynamic WEP keys for authentication between the client and authentication server.

NOTE

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

External RADIUS Server

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

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

The following authentication methods are supported in Aruba Instant network:

Authentication Terminated on IAP

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

The following EAP-Type methods are described below:

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

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

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

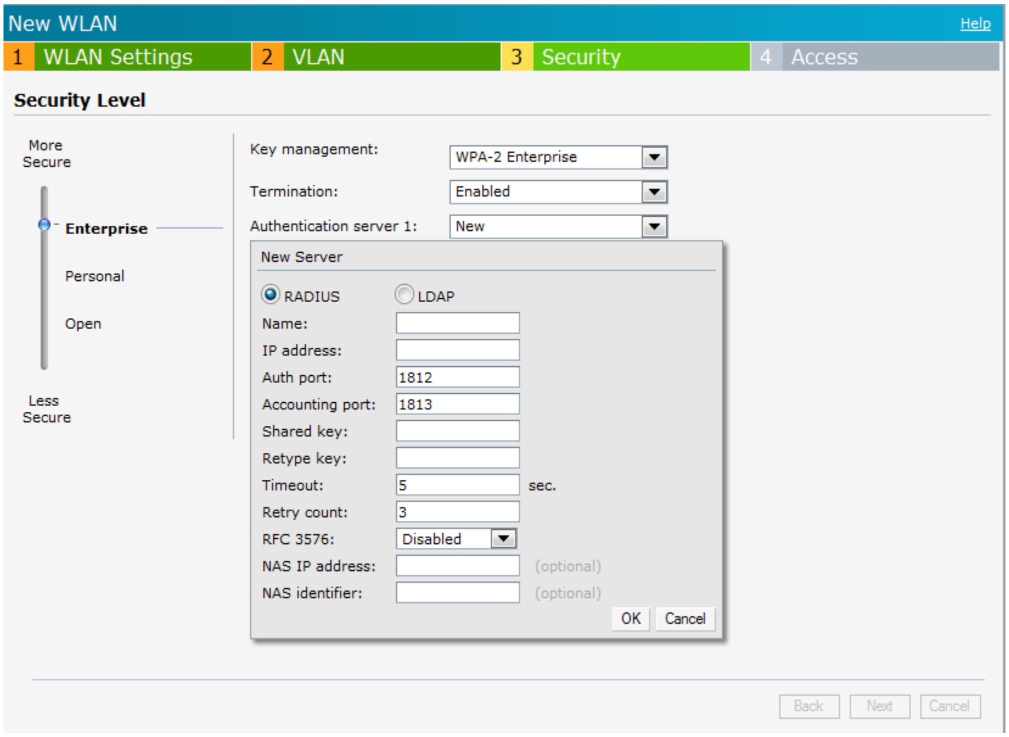
Configuring an External RADIUS Server

To configure an external RADIUS server for a wireless network:

1. Click **New** in the **Networks** tab and select the appropriate **Primary usage.**
2. Click **Next** to continue.
3. Use the **VLAN** tab to specify how the clients on this network get their IP address and VLAN.
4. Click **Next** to continue.
5. In the **Security** tab, slide the bar to **Enterprise** and update the following fields:
   a. **Key Management—** Select the type of key for encryption and authentication.
   b. **Termination—** Select **Enabled** to terminate the EAP portion of 802.1X authentication on the access point instead of RADIUS server.
   c. **Authentication server 1—** Select **New** from the drop-down list to authenticate user credentials for the RADIUS server at run time and update the following fields:
   - **RADIUS Server**
     - Name— Enter the name of the new external RADIUS server.
     - IP address— Enter the IP address of the external RADIUS server.
     - Auth port— Enter the authorization port number of the external RADIUS server. The port number is set to 1812 by default.
     - Accounting port— Enter the accounting port number. This port is used to send accounting records to the RADIUS server. The port number is set to 1813 by default
     - Shared key— Enter a shared key for communicating with the external RADIUS server.
     - Timeout— Indicates the timeout for one RADIUS request. The IAP retries to send the request several times (as configured in the "Retry count") before the user gets disconnected. e.g. If the "Timeout" is 5 sec, "Retry counter" is 3, user is disconnected after 20 sec ("Timeout" x "Retry counter + 1). The default value is 5 seconds.
     - Retry count— Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to server group, and the default value is 3 requests.
     - RFC 3576— When enabled, the Access Points process RFC 3576-compliant Change of Authorization (CoA) and Disconnect messages from the RADIUS server. Disconnect messages cause a user session to be terminated immediately, whereas CoA messages modify session authorization attributes such as data filters.
     - NAS IP address— Enter the Virtual Controller IP address. The NAS IP address is the Virtual Controller IP address that is sent in data packets. Note: If you do not enter the IP address, the Virtual Controller IP address is used by default when Dynamic RADIUS Proxy is enabled.
     - NAS identifier— Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
   - **LDAP Server**
     - Name— Enter the name of the new external RADIUS server.
     - IP address— Enter the IP address of the external RADIUS server.
     - Auth port— Enter the authorization port number of the external RADIUS server. The port number is set to 1812 by default.
     - Admin-DN— Enter a Distinguished Name for the admin user who has read/search privileges across all the entries in the LDAP database. The user may not have write privileges but is able to search the database, and read attributes of the other users in the database.
     - Admin password— Enter a admin password.
     - Base-DN— Enter a Distinguished Name of the node which contains the entire user database.

- Filter— Indicates the filter that should be applied to search for the user in the LDAP database. The default filter string is (objectclass=*).
- Key Attribute— Indicates the attribute that should be used as a key in search for the LDAP server. For Active Directory, the value is sAMAccountName.
- Timeout— Enter a value between 1 and 30 seconds. The default value is 5.
- Retry count— Enter a value between 1 and 5. The default value is 3.

Figure 98 *Configuring an External RADIUS Server*



Key management: WPA-2 Enterprise

Termination: Enabled

Authentication server 1: New

New Server

● RADIUS ○ LDAP

Name:

IP address:

Auth port: 1812

Accounting port: 1813

Shared key:

Retype key:

Timeout: 5 sec.

Retry count: 3

RFC 3576: Disabled

NAS IP address: (optional)

NAS identifier: (optional)

6. Click **OK** after updating the fields.
7. **Reauth interval** — When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.
8. **Blacklisting**— Select **Enabled** if you want clients to be blacklisted after a certain number of authentication failures.
   - **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.

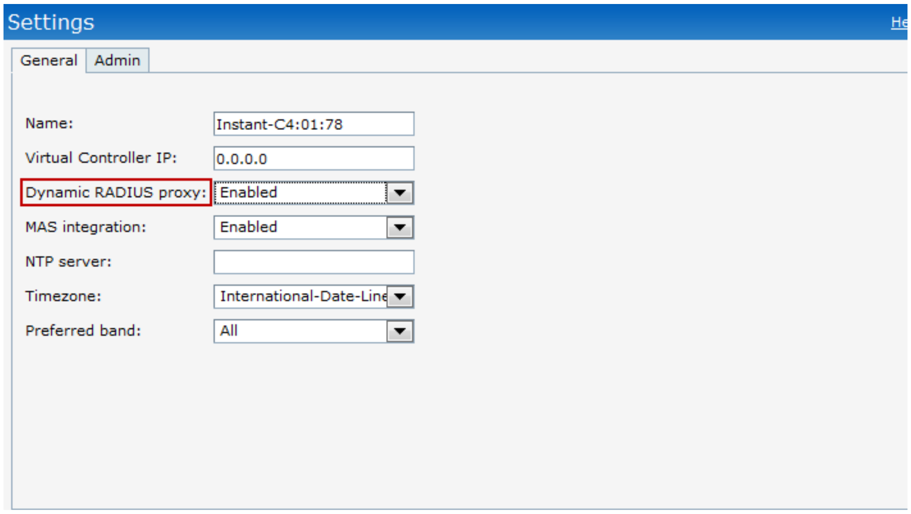
   Navigate to **PEF > Blacklisting** in the Instant WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.
9. **For Internal users—** Click **Users** to populate the system's internal authentication server with users. For information about adding a user, see "Adding a User" on page 251.
10. Click **Next** to continue and then click **Finish.**

Enabling Instant RADIUS

To enable Instant RADIUS:

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

Figure 99 *Enabling Instant RADIUS*



Name: Instant-C4:01:78

Virtual Controller IP: 0.0.0.0

Dynamic RADIUS proxy: Enabled

MAS integration: Enabled

NTP server:

Timezone: International-Date-Line

Preferred band: All

3. Click **OK**.

RADIUS Server Authentication with VSA

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

List of supported VSA

Instant supports the following types of VSA's:

- AP-Group
- AP-Name
- ARAP-Features
- ARAP-Security
- ARAP-Security-Data
- ARAP-Zone-Access
- Acct-Authentic
- Acct-Delay-Time
- Acct-Input-Gigawords
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Link-Count
- Acct-Multi-Session-Id
- Acct-Output-Gigawords
- Acct-Output-Octets
- Acct-Output-Packets
- Acct-Session-Id
- Acct-Session-Time
- Acct-Status-Type
- Acct-Terminate-Cause

- Acct-Tunnel-Packets-Lost
- Add-Port-To-IP-Address
- Aruba-AP-Group
- Aruba-Admin-Role
- Aruba-Essid-Name
- Aruba-Location-Id
- Aruba-Named-User-Vlan
- Aruba-Port-Id
- Aruba-Priv-Admin-User
- Aruba-Template-User
- Aruba-User-Role
- Aruba-User-Vlan
- CHAP-Challenge
- Callback-Id
- Callback-Number
- Class
- Connect-Info
- Connect-Rate
- Crypt-Password
- DB-Entry-State
- Digest-Response
- Domain-Name
- EAP-Message
- Error-Cause
- Event-Timestamp
- Exec-Program
- Exec-Program-Wait
- Expiration
- Fall-Through
- Filter-Id
- Framed-AppleTalk-Link
- Framed-AppleTalk-Network
- Framed-AppleTalk-Zone
- Framed-Compression
- Framed-IP-Address
- Framed-IP-Netmask
- Framed-IPX-Network
- Framed-MTU
- Framed-Protocol
- Framed-Route
- Framed-Routing

- Full-Name
- Group
- Group-Name
- Hint
- Huntgroup-Name
- Idle-Timeout
- Login-IP-Host
- Login-LAT-Node
- Login-LAT-Port
- Login-LAT-Service
- Login-Service
- Login-TCP-Port
- Menu
- Message-Auth
- NAS-Port-Type
- Password
- Password-Retry
- Port-Limit
- Prefix
- Prompt
- Rad-Authenticator
- Rad-Code
- Rad-Id
- Rad-Length
- Reply-Message
- Revoke-Text
- Server-Group
- Server-Name
- Service-Type
- Session-Timeout
- Simultaneous-Use
- State
- Strip-User-Name
- Suffix
- Termination-Action
- Termination-Menu
- Tunnel-Assignment-Id
- Tunnel-Client-Auth-Id
- Tunnel-Client-Endpoint
- Tunnel-Connection-Id
- Tunnel-Medium-Type

- Tunnel-Preference
- Tunnel-Private-Group-Id
- Tunnel-Server-Auth-Id
- Tunnel-Server-Endpoint
- Tunnel-Type
- User-Category
- User-Name
- User-Vlan
- Vendor-Specific

Management Authentication Settings

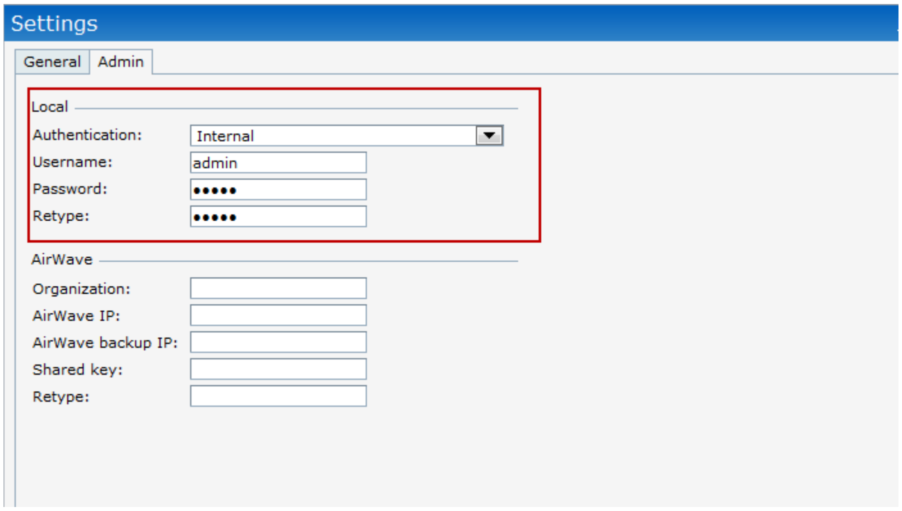
Use this page to specify authentication for access to the Virtual Controller Management user interface.

1. Navigate to the **Settings** link in the Instant UI.
2. Select the **Admin** tab.
3. In the **Authentication** drop-down list, select any one of the following:

- **Internal**— Select to specify a single set of user credentials. Enter the **Username** and **Password** for accessing the Virtual Controller Management User Interface.
- **RADIUS Server**— Specify one or two RADIUS servers to authenticate UI. If two servers are configured users can use them in primary/backup mode or load-balancing mode, this is identical to the RADIUS server configuration for SSIDs. For information on configuring external RADIUS server, see "External RADIUS Server" on page 124.
- **RADIUS server w/ fallback to internal**— Specify the RADIUS servers as well as a Username and Password. If there is no response from the RADIUS server (RADIUS server timeout), the authentication switches to **Internal**.

4. Click **OK**.

Figure 100 *Management Authentication Settings*



Local

Authentication: Internal
Username: admin
Password: •••••
Retype: •••••

AirWave

Organization:
AirWave IP:
AirWave backup IP:
Shared key:
Retype:

Captive Portal

Aruba Instant network supports captive portal authentication method for a Guest network type. In this method, a web page is displayed to a guest user who tries to access the internet. The user has to authenticate or accept company's network usage policy in the web page. Two types of captive portal authentication are supported on 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" on page 251.
- Internal Acknowledged— To gain access to the wireless network, a user must accept the terms and conditions.

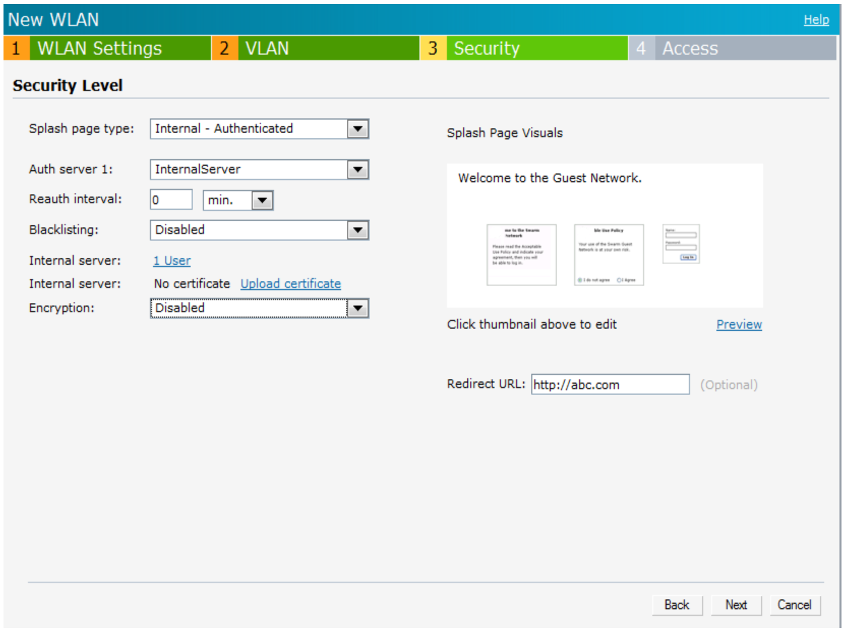
Configuring Internal Captive Portal Authentication when Adding a Guest Network

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

See "Guest Network" on page 70 for more information on the splash page type options.

Figure 101 *Configuring Captive Portal when Adding A Guest Network*



Security Level

Splash page type: Internal - Authenticated

Auth server 1: InternalServer

Reauth interval: 0 min.

Blacklisting: Disabled

Internal server: 1 User

Internal server: No certificate Upload certificate

Encryption: Disabled

Splash Page Visuals

Welcome to the Guest Network.

Click thumbnail above to edit Preview

Redirect URL: http://abc.com (Optional)

The appearance of a splash page can be customized as required. For information on customizing a splash page, see "Customizing a Splash Page" on page 134.

6. Select **InternalServer** from the **Auth server** 1 drop-down list to authenticate user credentials at run time.
7. **Reauth interval** — When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.
8. **Blacklisting** — Select Enabled if you want clients to be blacklisted after a certain number of authentication failures.
9. **Max authentication failures** — Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.
10. **Internal server** —
    - Click **User** to populate the system's internal authentication server with users. For information about adding a user, see "Adding a User" on page 251".
    - Click **Upload Certificate** and browse to upload a certificate file for the internal server.
11. **Encryption**— Select **Enabled** from the drop-down list and perform the following steps (these steps are optional):
    a. Select the required key management option from the **Key management** drop-down list. Available options are:
        - WPA-2 Personal
        - WPA Personal
        - Both (WPA-2 & WPA)

    b. **Passphrase format** — Specify either an alphanumeric or a hexadecimal string. Ensure that the hexadecimal string must be exactly 64 digits in length.

    c. **Passphrase** — Enter a pre-shared key (PSK) passphrase.
12. Click **Next** and click **Finish.**

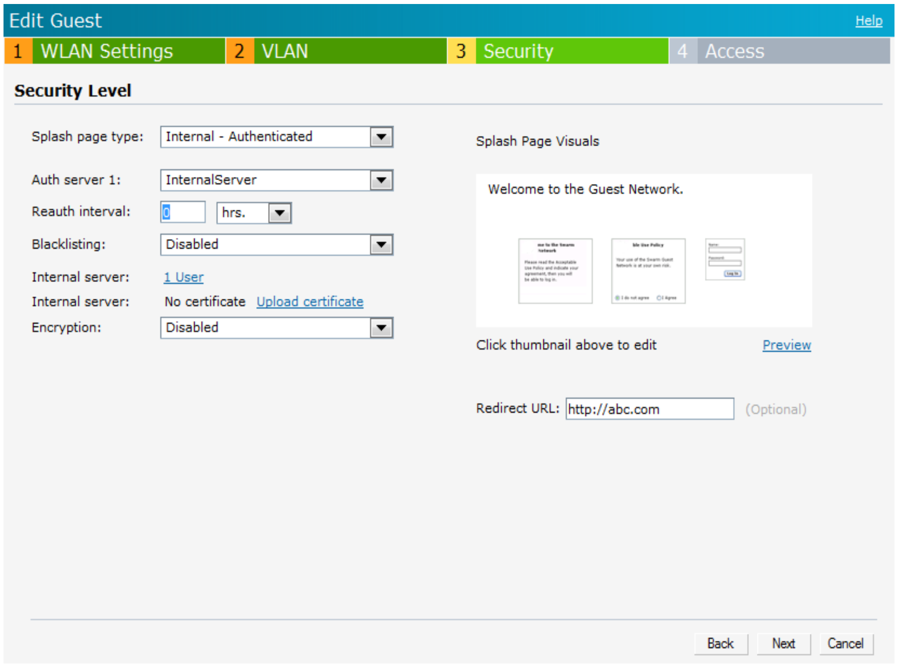
Configuring Internal Captive Portal Authentication when Editing a Guest Network

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

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

    See “Guest Network” on page 70 for more information.

Figure 102 *Configuring Captive Portal when Editing a Guest Network*



Splash page type: Internal - Authenticated
Auth server 1: InternalServer
Reauth interval: 0 hrs.
Blacklisting: Disabled
Internal server: 1 User
Internal server: No certificate Upload certificate
Encryption: Disabled

Splash Page Visuals

Welcome to the Guest Network.

Click thumbnail above to edit Preview

Redirect URL: http://abc.com (Optional)

The appearance of a splash page can be customized as required. For information on customizing a splash page, see “Customizing a Splash Page” on page 134.

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

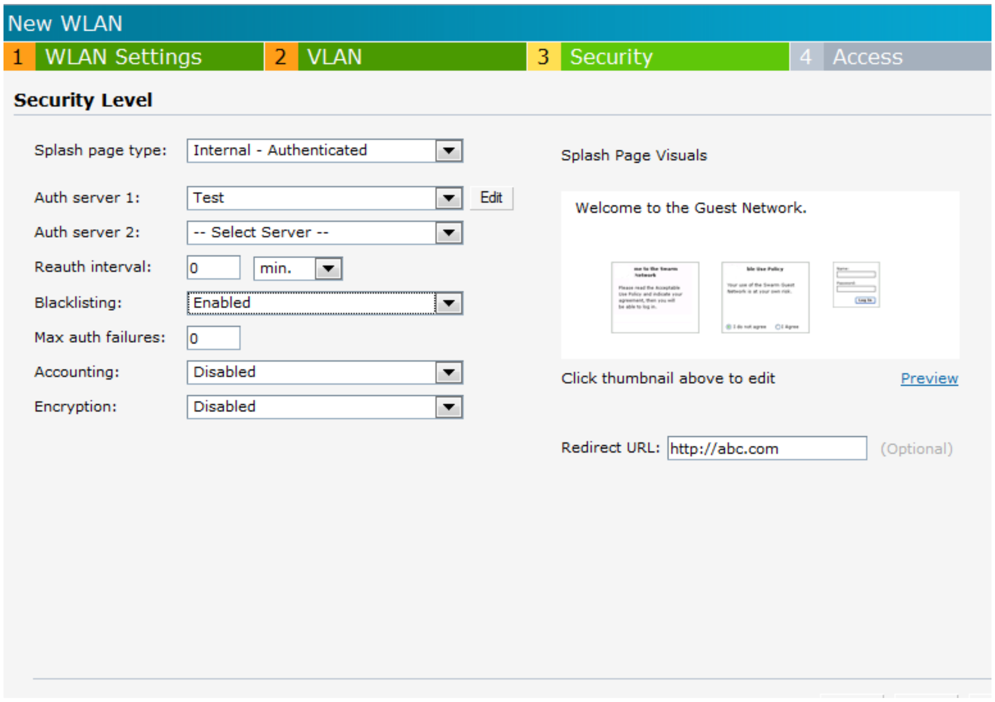
Configuring Internal Captive Portal with External RADIUS Server Authentication when Adding a Guest Network

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

1. In the **Network** tab, click the **New** link. The **New WLAN** window opens.
2. In the **WLAN Settings** tab, perform the following:
    a. Enter a name for the network in the **Name (SSID)** text box.
    b. Select **Guest** and then click **Next.**
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN.

4. Click **Next** to continue.
5. In the **Security** tab, select **Internal — Authenticated** under the splash page type.
6. Select an external RADIUS server from the Authentication server drop-down list to authenticate user credentials at run time. If there is no external RADIUS server in the drop-down list, click **New** to add a RADIUS server. For information on configuring external RADIUS server, see "External RADIUS Server" on page 124.
7. Click **Next** and then click **Finish**.

Figure 103 *Configuring Internal Captive Portal with External RADIUS Server Authentication*



New WLAN

1 WLAN Settings | 2 VLAN | 3 Security | 4 Access

Security Level

Splash page type: Internal - Authenticated

Auth server 1: Test

Auth server 2: -- Select Server --

Reauth interval: 0 min.

Blacklisting: Enabled

Max auth failures: 0

Accounting: Disabled

Encryption: Disabled

Splash Page Visuals

Welcome to the Guest Network.

Click thumbnail above to edit

Redirect URL: http://abc.com (Optional)

Customizing a Splash Page

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

NOTE

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

1. In the **Network** tab, click the network for which you want to customize the splash page. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** window for the network appears.
3. Navigate to the **Security** tab and perform the following steps:

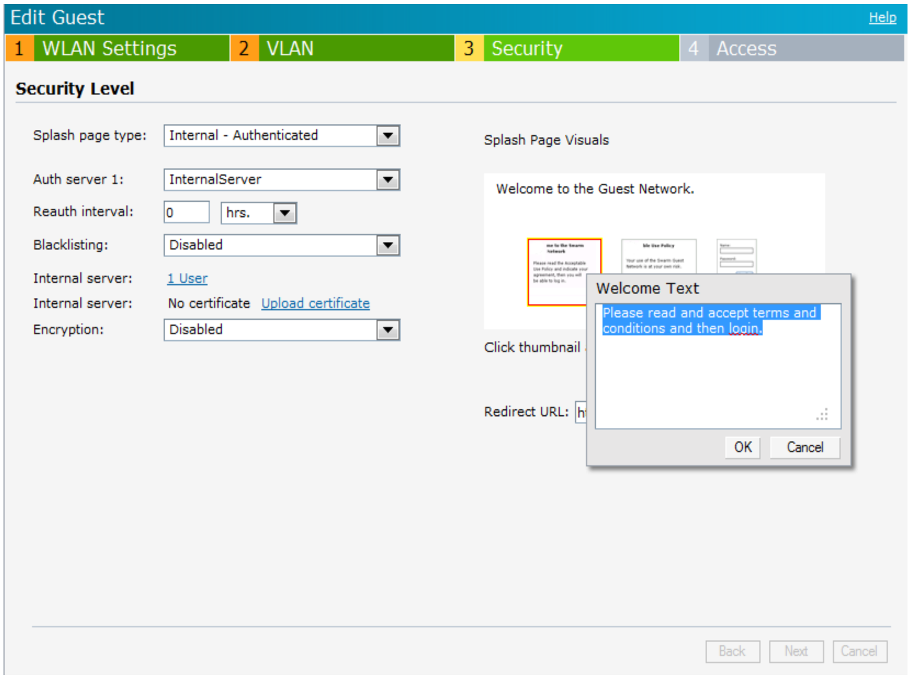
   Splash Page Visuals — Use the in-place editor below to specify text and colors for the initial page that users connecting to the network see. This page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal -Acknowledged) you set.

   a. To change the color of the splash page, click the Splash page rectangle and select the required color from the **Background Color** palette.

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

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

Figure 104 *Customizing a Splash Page*



Splash page type: Internal - Authenticated

Auth server 1: InternalServer

Reauth interval: 0 hrs.

Blacklisting: Disabled

Internal server: 1 User

Internal server: No certificate Upload certificate

Encryption: Disabled

Redirect URL: ht

Welcome Text: Please read and accept terms and conditions and then login.

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

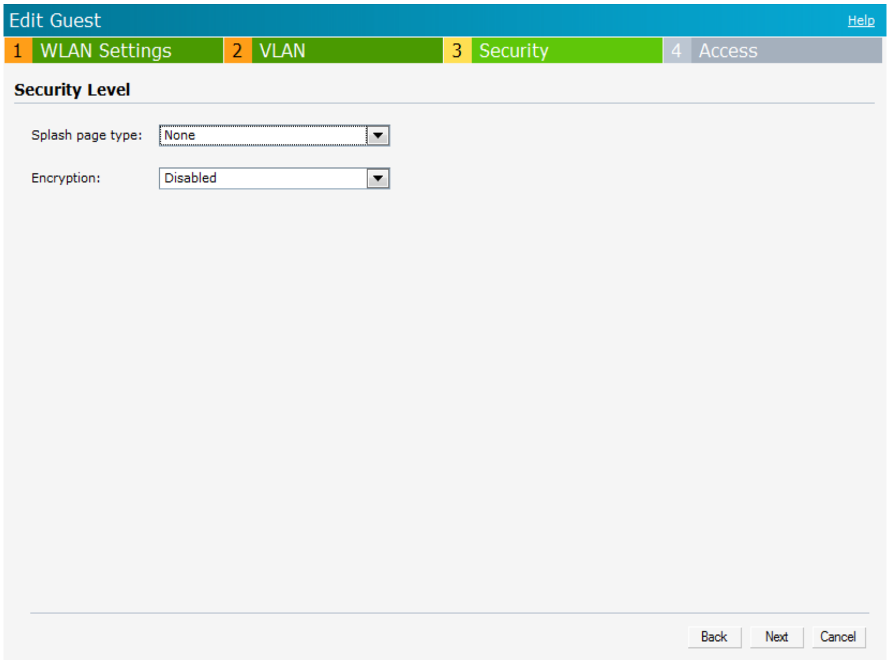
You can customize the captive portal page using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters. Click on the banner, term, or policy in the **Splash Page Visuals** to modify the text in the red box. These fields accept double-byte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

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

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

Figure 105 *Disabling Captive Portal Authentication*



Splash page type: None

Encryption: Disabled

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

External Captive Portal

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

Configuring External Captive Portal Authentication when Adding a Guest Network

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

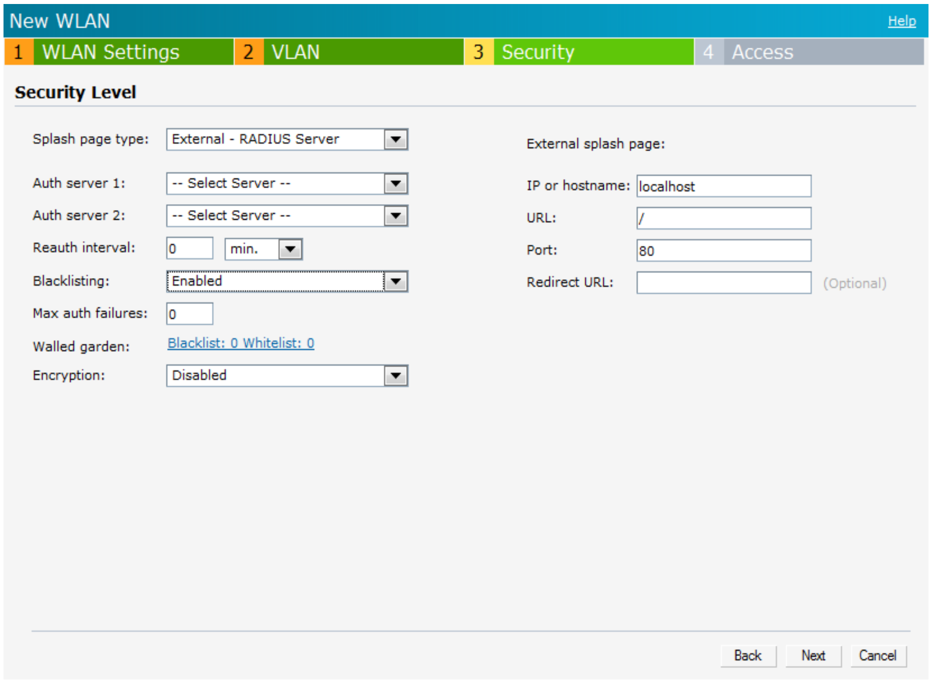
1. In the **Network** tab, click the **New** link. The **New WLAN** window appears.
2. In the **WLAN Settings** tab, perform the following:
   1. Enter a name for the network in the **Name (SSID)** text box.
   2. Select **Guest** and click **Next** to continue**.**
3. Use the **VLAN** tab to specify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

Or

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

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

Figure 106 *External Captive Portal when Adding a Guest Network - External RADIUS Server*



Security Level

Splash page type: External - RADIUS Server

Auth server 1: -- Select Server --

Auth server 2: -- Select Server --

Reauth interval: 0 min.

Blacklisting: Enabled

Max auth failures: 0

Walled garden: Blacklist: 0 Whitelist: 0

Encryption: Disabled

External splash page:

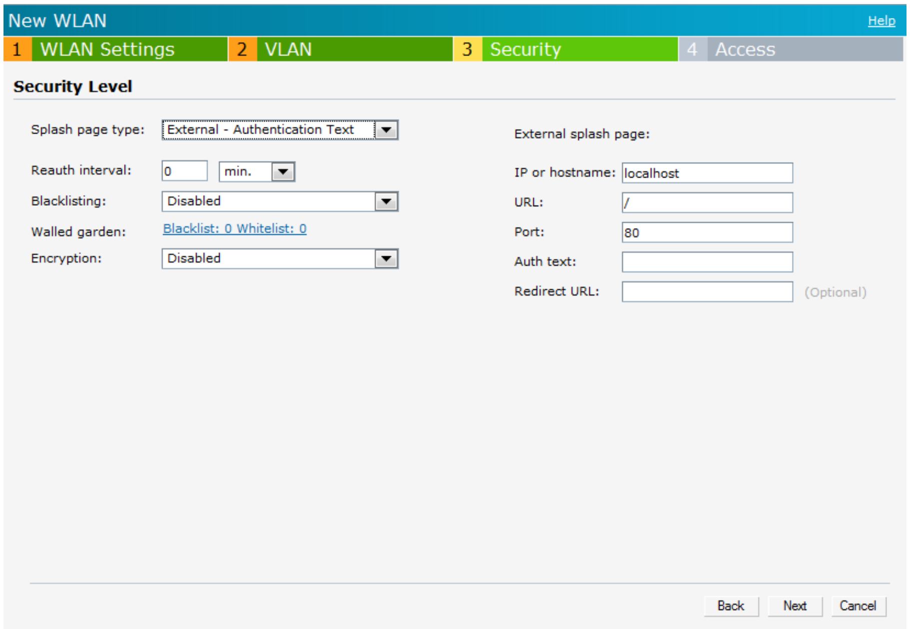
IP or hostname: localhost

URL: /

Port: 80

Redirect URL: (Optional)

Figure 107 *External Captive Portal when Adding a Guest Network - External Authentication text*



Security Level

Splash page type: External - Authentication Text

Reauth interval: 0 min.

Blacklisting: Disabled

Walled garden: Blacklist: 0 Whitelist: 0

Encryption: Disabled

External splash page:

IP or hostname: localhost

URL: /

Port: 80

Auth text:

Redirect URL: (Optional)

6. **Authentication server 1**: Select New and update the fields for the external RADIUS server to authenticate user credentials at runtime. Refer to "Configuring an External RADIUS Server" on page 125 for more details on server settings.
7. **Reauth interval** — When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.
8. **Blacklisting**— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures.
9. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10.

   Navigate to **PEF > Blacklisting** in the Instant WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.

10. **Walled garden —** Click on the link to open the **Walled Garden** window. The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see "Walled Garden Access" on page 142.

11. Click **Next** to continue and then click **Finish.**

Configuring External Captive Portal Authentication when Editing a Guest Network

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

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

   Splash page type — External - Authentication Text

   a. **Reauth interval** — When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.

   b. **Blacklisting**— Select **Enabled** if you want clients to be blacklisted after a certain number of authentication failures.

   c. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. Navigate to **PEF > Blacklisting** in the Instant WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.

   d. **Walled Garden**— Click on the link to open the **Walled Garden** window. The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see "Walled Garden Access" on page 142.

   e. **Encryption**— Select **Enabled** from the drop-down list and perform the following steps (these steps are optional). Select the required key management option from the Key management drop-down list. Available options are:

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

   External splash page

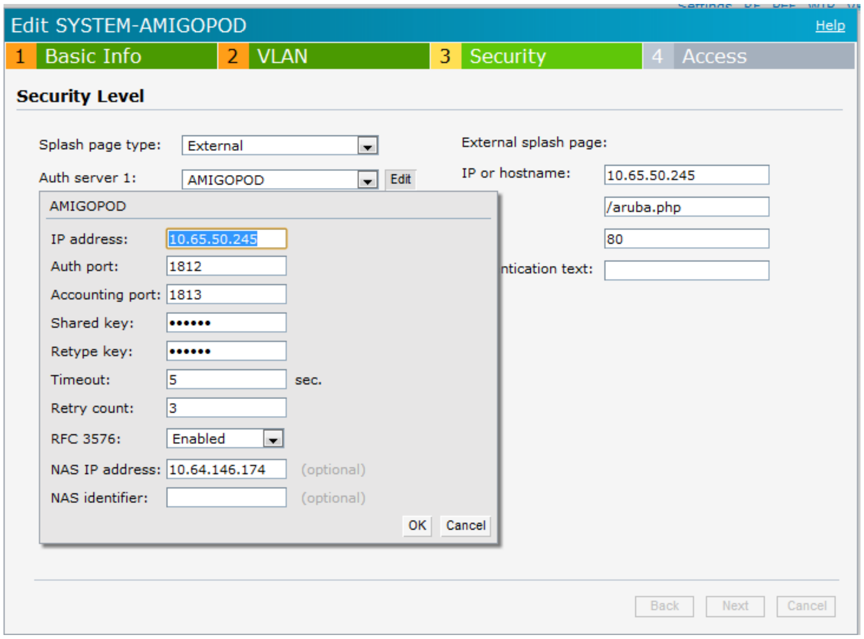
   a. **IP or hostname—** Enter the IP address or the hostname of the external splash page server.

   b. **URL—** Enter the URL for the external splash page server.

   c. **Port—** Enter the number of the port to be used for communicating with the external splash page server.

   d. **Auth text—** Enter the autentication text. This indicates the text string returned by the external server after a successful authentication.

Figure 108 *Configuring External Captive Portal Authentication when Editing a Guest Network*



Security Level

Splash page type: External

Auth server 1: AMIGOPOD

External splash page:

IP or hostname: 10.65.50.245

/aruba.php

80

ntication text:

AMIGOPOD

IP address: 10.65.50.245

Auth port: 1812

Accounting port: 1813

Shared key: ••••••

Retype key: ••••••

Timeout: 5 sec.

Retry count: 3

RFC 3576: Enabled

NAS IP address: 10.64.146.174 (optional)

NAS identifier: (optional)

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

Splash page type — External- RADIUS Server

a. **Authentication server 1**: Click **Edit** to modify the external RADIUS servers settings. Refer to "Configuring an External RADIUS Server" on page 125 for more details on server settings.

b. **Reauth interval**— When set to a value greater than zero, the Access Points periodically reauthenticate all associated and authenticated clients.

c. **Blacklisting**— Select **Enabled** if you want clients to be blacklisted after a certain number of authentication failures.

d. **Max authentication failures**— Users who fail to authenticate the number of times specified here are dynamically blacklisted. The maximum value for this entry is 10. Navigate to **PEF > Blacklisting** in the Instant WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.

e. **Walled Garden**— Click on the link to open the Walled Garden window. The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see "Walled Garden Access" on page 142.

f. **Encryption**— Select Enabled from the drop-down list and perform the following steps (these steps are optional). Select the required key management option from the Key management drop-down list. Available options are:

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

External splash page

a. **IP or hostname—** Enter the IP address or the hostname of the external splash page server.

b. **URL—** Enter the URL for the external splash page server.

c. **Port—** Enter the number of the port to be used for communicating with the external splash page server.

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

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

External Captive Portal Authentication using ClearPass Guest

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

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

Creating a Web Login page in the ClearPass Guest

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

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

Configuring the RADIUS Server in Instant

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

1. Navigate to the **Networks** tab in the Instant WebUI, click the **New** link. The **New WLAN** window appears.
2. In the **WLAN Settings** tab:
   a. Enter a name for the network in the **Name (SSID)** text box. Example: ECP
   b. Select **Guest** from the **Primary usage** options.
3. Click **Next** to continue.
4. Use the **VLAN** tab to specify how the clients on this network get their IP address and VLAN.
5. Click **Next** to continue.
6. In the **Security** tab, select **External- RADIUS Server** and update the following fields**.**
   a. Enter the IP address of the ClearPass Guest server in the **IP or hostname** field.
   The IP address is **10.65.77.245**.
   b. Enter **/page_name.php** in the **URL** field. This URL must correspond to the **Page Name** configured in the ClearPass Guest RADIUS Web Login page.
   For example, if the Page Name is **aruba**, then the URL should be **/aruba.php** in the Instant UI**.**
   c. Enter the **Port** number (generally should be **80**). The ClearPass Guest server uses this port for HTTP services.
   d. To create an external RADIUS server, select **New** from the **Authentication server 1** drop-down list. Refer to "Configuring an External RADIUS Server" on page 125 for information on the new RADIUS server parameters.

7. The new network appears in the **Networks** tab. Click the wireless network icon on your desktop and select the new network.
8. Open any browser and type any URL. Instant redirects the URL to ClearPass Guest login page.
9. Log in to the network with the username and password specified used while configuring the RADIUS server in step d.

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.

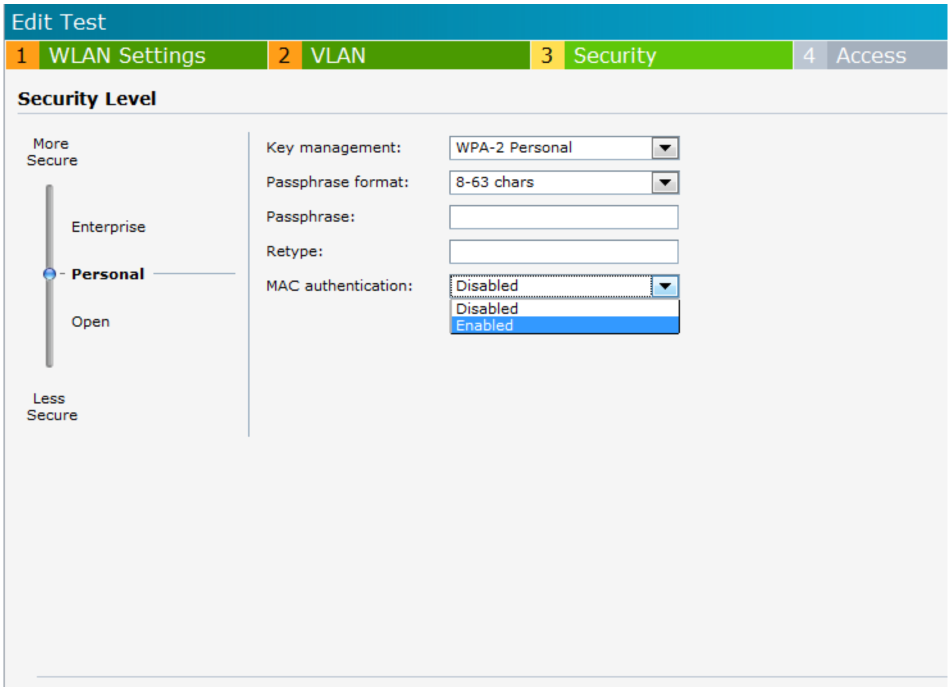
MAC authentication can be used alone, but typically it is combined with other forms of authentication, such as WEP authentication. Because MAC addresses are easily observed during transmission and easily changed on the client, this form of authentication should be considered nothing more than a minor hurdle. Aruba recommends against the use of MAC-based authentication.

Configuring MAC Authentication

To enable MAC Authentication for a wireless network:

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

Figure 109 *Configuring MAC Authentication*



Key management: WPA-2 Personal

Passphrase format: 8-63 chars

Passphrase:

Retype:

MAC authentication: Disabled

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

Walled Garden Access

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

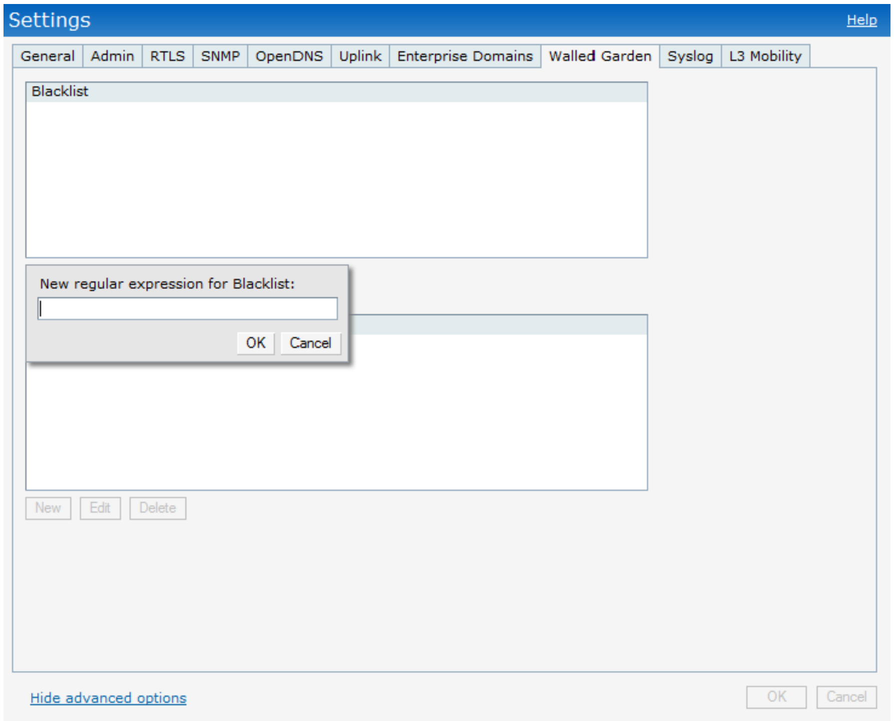
Creating a Walled Garden Access

Walled garden access is needed when an external captive portal is used. A common example could be a hotel environment where unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

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

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

Figure 110 *Walled Garden*



To create a Walled Garden access:

1. Click the **Settings** at the top right corner of the Instant UI and select **Walled Garden**.
2. To allow users access to a domain, click **New** and enter the domain name or URL in the **Whitelist** section of the window. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)), for example:
   - yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
   - www.apple.com/library/test is only allow a subset of www.apple.com site corresponding to path /library/test/*
   - favicon.ico allows access to /favicon.ico from all domains.

3. To deny users access to a domain, click **New** and enter the domain name or URL in the **Blacklist** section of the window. This prevents unauthenticated users from viewing specific websites. When a URL specified in blacklist is accessed by an unauthenticated user, Instant AP sends an HTTP 403 response to the client with a simple error message.

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

Wired Authentication on an IAP

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

The following wired authentication methods are supported:

- MAC Authentication
- Captive Portal Authentication

To configure wired authentication on an IAP:

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

NOTE

Configure bridging on the Ethernet uplink (Ethernet 0) port before you apply a profile.

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

NOTE

Wired authentication does not support WEP, WPA, and WPA2 encryption.

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 the following certificate files:

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

There are two ways to upload the certificates.

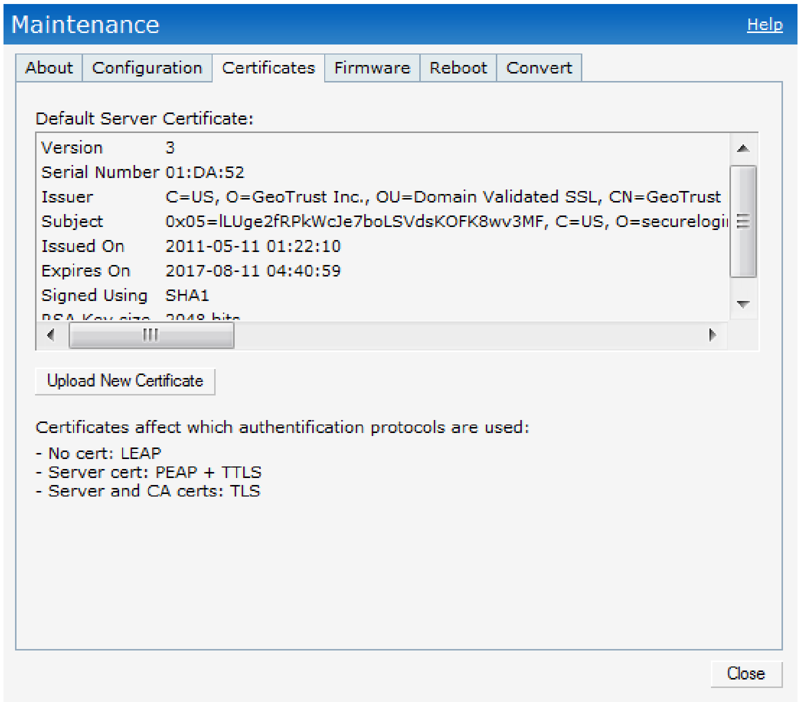
1. **Instant WebUI:** Navigate to **Maintenance > Certificates** and then click **Upload New Certificate** to directly upload the certificate. Refer Loading Certificates using Instant WebUI for further instructions.
2. **AirWave:** Navigate to **Device Setup > Certificate** and then click **Add New Certificate**. Refer Loading Certificates using AirWave for further instructions.

Loading Certificates using Instant WebUI

To load a certificate in the Instant UI:

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

Figure 111 *Loading Certificates*



Default Server Certificate:

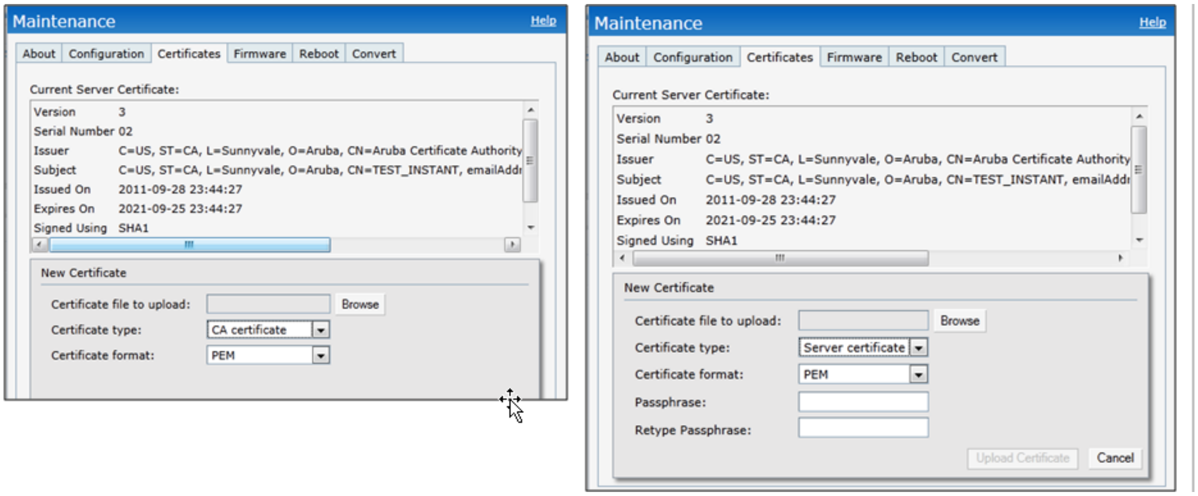
```
Version       3
Serial Number 01:DA:52
Issuer        C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust
Subject       0x05=lLUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US, O=securelogi
Issued On     2011-05-11 01:22:10
Expires On    2017-08-11 04:40:59
Signed Using  SHA1
RSA Key size  2048 bits
```

Certificates affect which authentification protocols are used:

- No cert: LEAP
- Server cert: PEAP + TTLS
- Server and CA certs: TLS

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

Figure 112 *New Certificate*



Current Server Certificate:

```
Version       3
Serial Number 02
Issuer        C=US, ST=CA, L=Sunnyvale, O=Aruba, CN=Aruba Certificate Authority
Subject       C=US, ST=CA, L=Sunnyvale, O=Aruba, CN=TEST_INSTANT, emailAddr
Issued On     2011-09-28 23:44:27
Expires On    2021-09-25 23:44:27
Signed Using  SHA1
```

New Certificate

Certificate file to upload:

Certificate type: CA certificate

Certificate format: PEM

Current Server Certificate:

```
Version       3
Serial Number 02
Issuer        C=US, ST=CA, L=Sunnyvale, O=Aruba, CN=Aruba Certificate Authority
Subject       C=US, ST=CA, L=Sunnyvale, O=Aruba, CN=TEST_INSTANT, emailAddr
Issued On     2011-09-28 23:44:27
Expires On    2021-09-25 23:44:27
Signed Using  SHA1
```

New Certificate

Certificate file to upload:

Certificate type: Server certificate

Certificate format: PEM

Passphrase:

Retype Passphrase:

3. Select the **Certificate type— CA certificate and Server certificate** from the drop-down list**.** The CA certificate is required to validate the client's certificate and the server certificate verifies the server's identity to the client.

4. Select the certificate format from the **Certificate format** drop-down list**.**

5. If you have selected **Server certificate** type, then enter a passphrase in **Passphrase** and reconfirm. The default password is **whatever**.

6. Click **Browse** and select the appropriate certificate file, and click **Upload Certificate**. The **Certificate Successfully Installed** window appears.

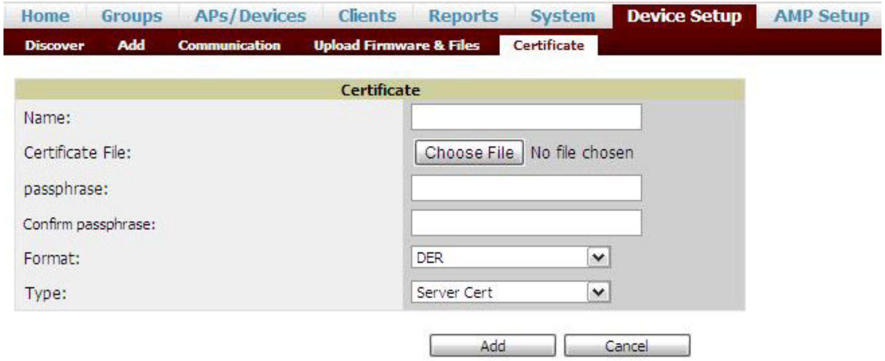
Loading Certificates using AirWave

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

To load a certificate in AirWave:

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

Figure 113 *Loading Certificate via AirWave*

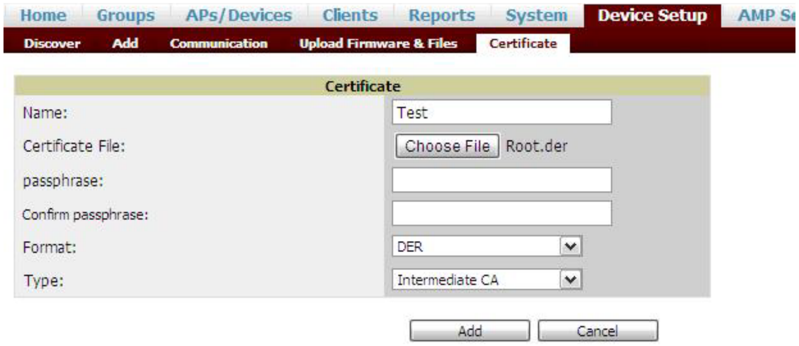


Certificate

Name:	
Certificate File:	No file chosen
passphrase:	
Confirm passphrase:	
Format:	DER
Type:	Server Cert

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

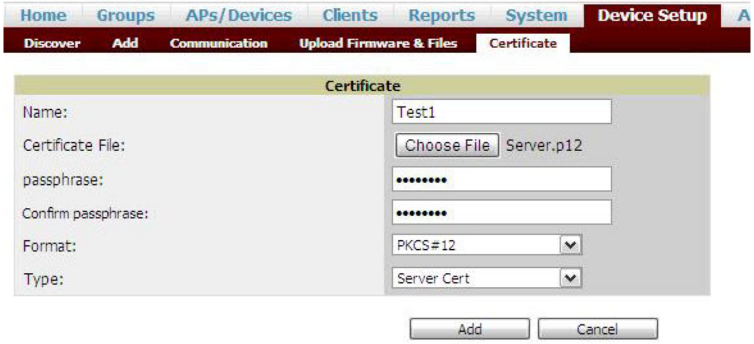
Figure 114 *CA Certificate*



Certificate

Name:	Test
Certificate File:	Choose File Root.der
passphrase:	
Confirm passphrase:	
Format:	DER
Type:	Intermediate CA

Figure 115 *Server Certificate*

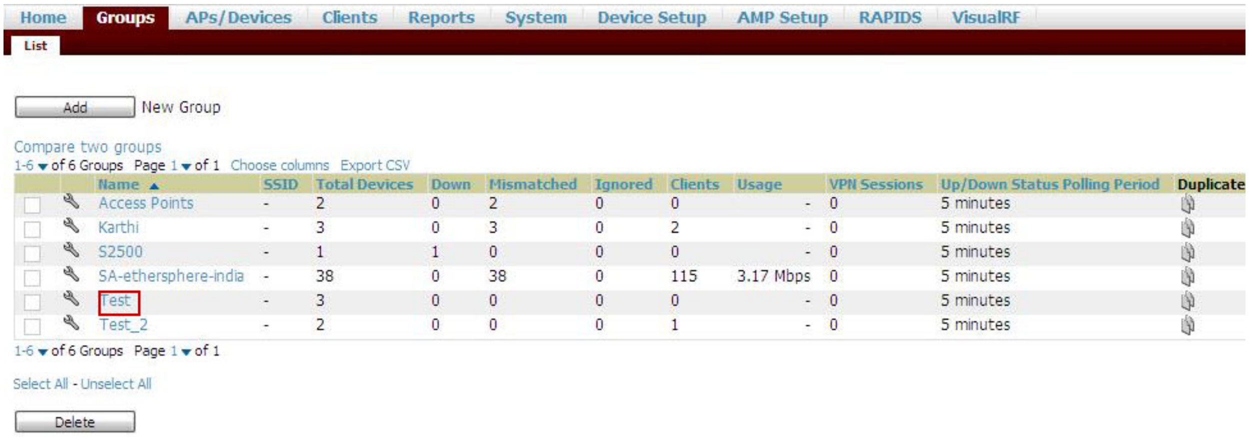


Certificate

Name:	Test1
Certificate File:	Choose File Server.p12
passphrase:	••••••••
Confirm passphrase:	••••••••
Format:	PKCS#12
Type:	Server Cert

4. After you upload the certificate, navigate to **Groups,** click on the Instant **Group** and then select **Basic**. The Group name appears only if you have entered the **Organization** name in the Instant WebUI. Refer Entering the Organization String and AMP Information into the IAP for further information.

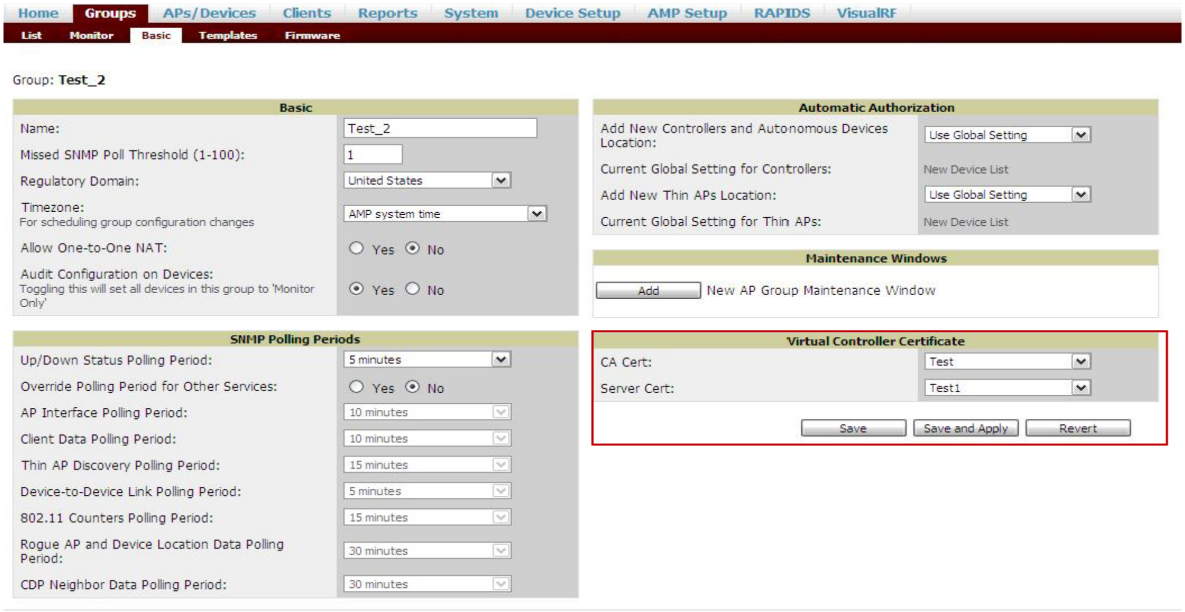
Figure 116 *Selecting the Group*



		Name ▲	SSID	Total Devices	Down	Mismatched	Ignored	Clients	Usage	VPN Sessions	Up/Down Status Polling Period	Duplicate
□		Access Points	-	2	0	2	0	0	-	0	5 minutes	
□		Karthi	-	3	0	3	0	2	-	0	5 minutes	
□		S2500	-	1	1	0	0	0	-	0	5 minutes	
□		SA-ethersphere-india	-	38	0	38	0	115	3.17 Mbps	0	5 minutes	
□		Test	-	3	0	0	0	0	-	0	5 minutes	
□		Test_2	-	2	0	0	0	1	-	0	5 minutes	

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

Figure 117 *Virtual Controller Certificate*



Group: **Test_2**

Basic

Name:	Test_2
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	United States
Timezone: For scheduling group configuration changes	AMP system time
Allow One-to-One NAT:	○ Yes ● No
Audit Configuration on Devices: Toggling this will set all devices in this group to 'Monitor Only'	● Yes ○ No

SNMP Polling Periods

Up/Down Status Polling Period:	5 minutes
Override Polling Period for Other Services:	○ Yes ● No
AP Interface Polling Period:	10 minutes
Client Data Polling Period:	10 minutes
Thin AP Discovery Polling Period:	15 minutes
Device-to-Device Link Polling Period:	5 minutes
802.11 Counters Polling Period:	15 minutes
Rogue AP and Device Location Data Polling Period:	30 minutes
CDP Neighbor Data Polling Period:	30 minutes

Automatic Authorization

Add New Controllers and Autonomous Devices Location:	Use Global Setting
Current Global Setting for Controllers:	New Device List
Add New Thin APs Location:	Use Global Setting
Current Global Setting for Thin APs:	New Device List

Maintenance Windows

New AP Group Maintenance Window

Virtual Controller Certificate

CA Cert:	Test
Server Cert:	Test1

6. Click **Save** to apply the changes only to AirWave. Click **Save and Apply** to apply the changes to the Instant AP.

NOTE

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

Encryption

Encryption Types Supported in Aruba Instant

Encryption is the process of converting data into an undecipherable format or code when it is transmitted on a network. Encryption prevents unauthorized use of the data. The following encryption types are supported in 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 that cannot support AES be upgraded or replaced so that they are capable of AES encryption.

NOTE

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

Encryption Recommendations

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 took longer than expected to complete the standard, so WPA was created based on a draft of 802.11i, which allowed people to move forward quickly to create more secure WLANs. WPA2 encompasses the full implementation of the 802.11i standard. Table 19 summarizes the differences between the two certifications. WPA2 is a superset that encompasses the full WPA feature set. WPA and WPA2 can be further classified as follows:

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

Table 19 *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 20 summarizes the recommendations for authentication and encryption combinations that should be used in Wi-Fi networks.

Table 20 *Recommended Authentication and Encryption Combinations*

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

Role Derivation

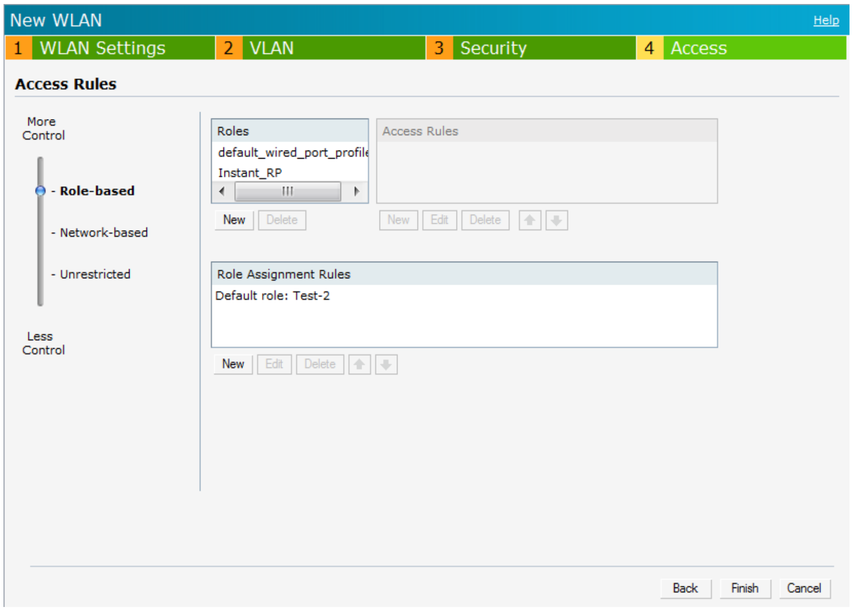
Every client in an Aruba Instant network is associated with a user role, which determines the client's network privileges, how often it must re-authenticate, and which bandwidth contracts are applicable.

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

User Roles

This section describes how to create a new user role.

Figure 118 *Access Tab - Instant User Role Settings*

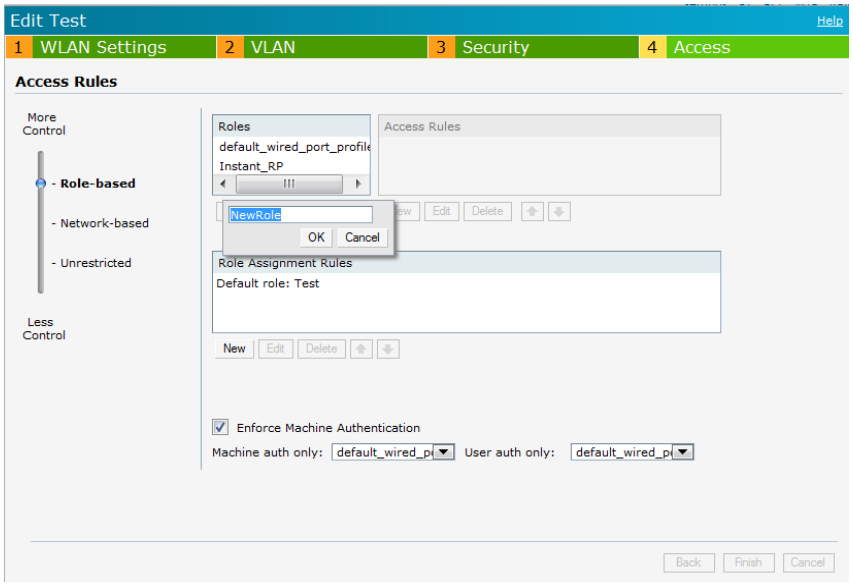


Creating a New User Role

To create a new user role:

1. Click the **New** link in the **Networks** tab.
   To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **Basic Info** tab, enter the appropriate information and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN. Click **Next** to continue.
4. Click **Next** and set appropriate values in the **Security** tab.
5. Click **Next**. The **Access** tab appears.
6. Slide to **Role-based** using the scroll bar on the left.
7. Click **New**. The **New Rule** window appears. Enter the name of the new user role. To delete a user role, select the user role and click **Delete**.

Figure 119 *Creating a New User Role*



Roles: default_wired_port_profile, Instant_RP

NewRole

Default role: Test

☑ Enforce Machine Authentication

Machine auth only: default_wired_p User auth only: default_wired_p

8. Click **OK**. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To create new access rules, see "Examples for Access Rules" on page 164.
9. **Assign pre-authentication role—** Use this option if you want to allow some access to users even before they are authenticated.
10. **Enforce Machine Authentication—** You can assign different rights to clients based on whether their hardware device supports machine authentication. Machine Authentication is only supported on Windows devices, so this can be used to distinguish between Windows devices and other devices such as iPads.

    - Machine Auth only role - This indicates a Windows machine with no user logged in. The device supports machine authentication and has a valid RADIUS account, but a user has not yet logged in and authenticated.
    - User Auth only role - This indicates a known user or a non-Windows device. The device does not support machine auth or does not have a RADIUS account, but the user is logged in and authenticated.

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

    To configure Machine Authentication, do the following:

    1. In the **Roles** window, create a role for **Machine auth only** and **User auth only**.
    2. Configure Access Rules for these roles by selecting the role, and applying the rule. Refer to "Examples for Access Rules" on page 164 for procedures to create access rules.
    3. Select **Enforce Machine Authentication** and specify these two roles.
    4. Click **Finish** to apply these changes.

Creating Role Assignment Rules

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

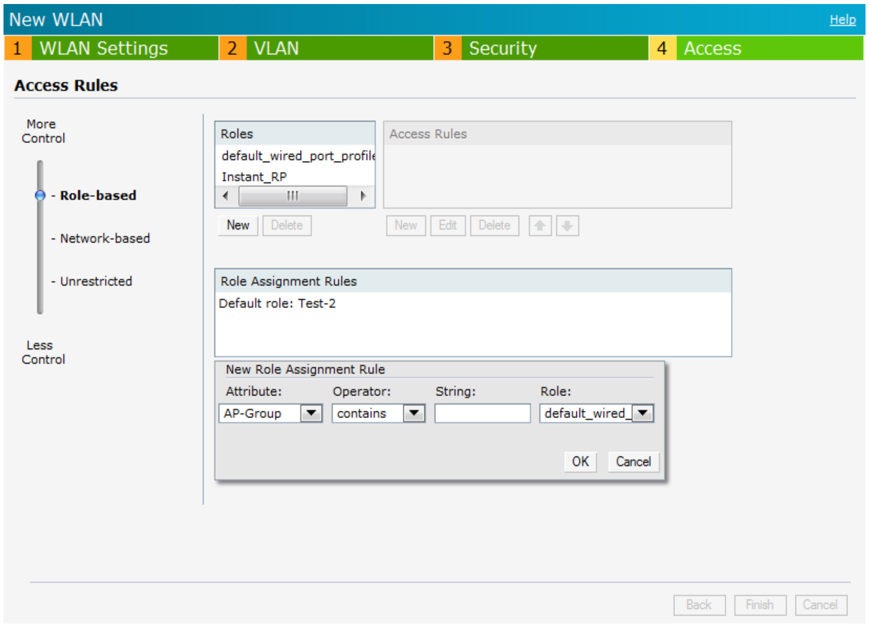
NOTE

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

To create role assignment rules for the user role:

1. Click **New** in the **Role Assignment Rules** section of the window. The default user role is the newly created user role.
2. Select the attribute from the **Attribute** drop-down list that the rule it matches against. The list of supported attributes includes RADIUS attributes (see "List of supported VSA" on page 127), DHCP-Option, and 802.1X-Authentication-Type.
3. Select the operator from the **Operator** drop-down list. The following types of operators are supported:
   - **contains**— To check if the attribute contains the operand value.
   - **Is the role**— To check if the role is same as the operand value.
   - **equals**— To check if the attribute is equal to the operand value.
   - **not-equals**— To check if the attribute is not equal to the operand value.
   - **starts-with**— To check if the attribute the starts with the operand value.
   - **ends-with**— To check if the attribute ends with the operand value.
4. Enter the string to match in the **String** text box.
5. Select the appropriate role from the **Role** drop-down list.
6. Click **OK**.

Figure 120 *Creating Role Assignment Rules*



Default role: Test-2

Attribute: AP-Group

Operator: contains

String:

Role: default_wired_

DHCP Option and DHCP Fingerprinting

The DHCP fingerprinting feature allows you to identify the operating system of a device by looking at the options in the DHCP frame. Based on the operating system type, a role can be assigned to the device.
For example, in order to create a role assignment rule with DHCP option, select **equals** from the **Operator** drop-down list and enter 370103060F77FC in the **String** text box. Since 370103060F77FC is the fingerprint for Apple iOS devices such as iPad and iPhone, IAP assigns Apple iOS devices to the role that you choose.

Table 21 *Validated DHCP Fingerprint*

Device	DHCP Option	DHCP Fingerprint
Apple iOS	Option 55	370103060F77FC

Table 21 *Validated DHCP Fingerprint (Continued)*

Device	DHCP Option	DHCP Fingerprint
Android	Option 60	3C64686370636420342E302E3135
Blackberry	Option 60	3C426C61636B4265727279
Windows 7/Vista Desktop	Option 55	37010f03062c2e2f1f2179f92b
Windows XP(SP3, Home, Professional)	Option 55	37010f03062c2e2f1f21f92b
Windows Mobile	Option 60	3c4d6963726f736f66742057696e646f777320434500
Windows 7 Phone	Option 55	370103060f2c2e2f
Apple Mac OSX	Option 55	370103060f775ffc2c2e2f

802.1X-Authentication-Type

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

NOTE

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

User VLAN Derivation

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

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

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

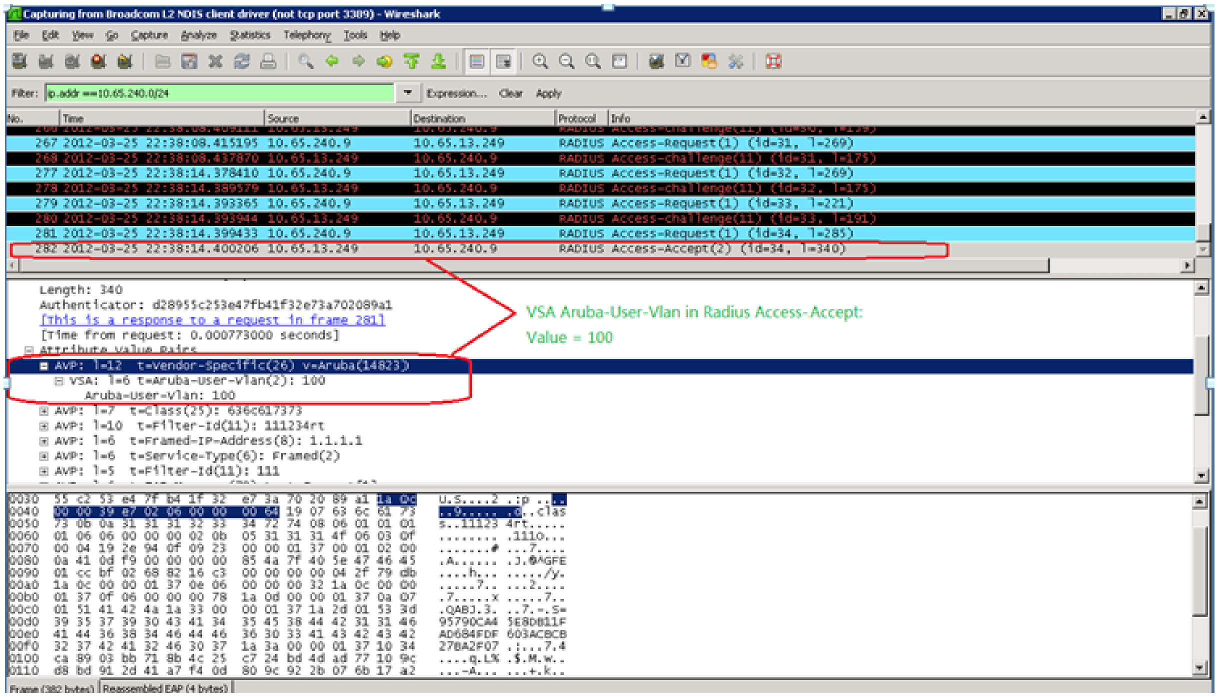
The user VLAN cannot be derived in the following scenarios:

- Captive Portal authentication
- Guest SSID network

Vendor Specific Attributes (VSA)

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

Figure 121 *RADIUS Access—Accept packets with VSA*



Filter: ip.addr ==10.65.240.0/24

```
267 2012-03-25 22:38:08.415195 10.65.240.9    10.65.13.249   RADIUS Access-Request(1) (id=31, l=269)
268 2012-03-25 22:38:08.437870 10.65.13.249   10.65.240.9    RADIUS Access-challenge(11) (id=31, l=175)
277 2012-03-25 22:38:14.378410 10.65.240.9    10.65.13.249   RADIUS Access-Request(1) (id=32, l=269)
278 2012-03-25 22:38:14.389579 10.65.13.249   10.65.240.9    RADIUS Access-challenge(11) (id=32, l=175)
279 2012-03-25 22:38:14.393365 10.65.240.9    10.65.13.249   RADIUS Access-Request(1) (id=33, l=221)
280 2012-03-25 22:38:14.393944 10.65.13.249   10.65.240.9    RADIUS Access-challenge(11) (id=33, l=191)
281 2012-03-25 22:38:14.399433 10.65.240.9    10.65.13.249   RADIUS Access-Request(1) (id=34, l=285)
282 2012-03-25 22:38:14.400206 10.65.13.249   10.65.240.9    RADIUS Access-Accept(2) (id=34, l=340)
```

```
    Length: 340
    Authenticator: d28955c253e47fb41f32e73a702089a1
    [This is a response to a request in frame 281]
    [Time from request: 0.000773000 seconds]
  ⊟ Attribute Value Pairs
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Aruba(14823)
      ⊟ VSA: l=6 t=Aruba-User-Vlan(2): 100
          Aruba-User-Vlan: 100
    ⊞ AVP: l=7  t=Class(25): 636c617373
    ⊞ AVP: l=10  t=Filter-Id(11): 111234rt
    ⊞ AVP: l=6  t=Framed-IP-Address(8): 1.1.1.1
    ⊞ AVP: l=6  t=Service-Type(6): Framed(2)
    ⊞ AVP: l=5  t=Filter-Id(11): 111
```

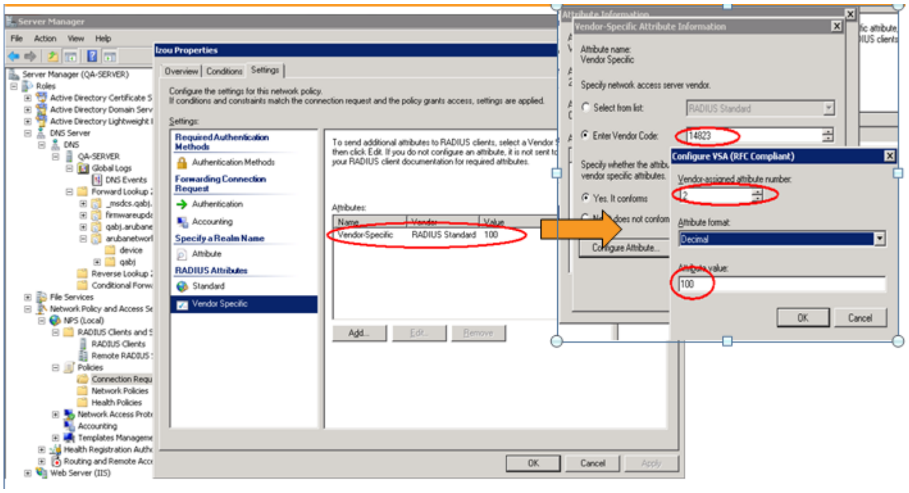
VSA Aruba-User-Vlan in Radius Access-Accept:

Value = 100

```
0030  55 c2 53 e4 7f b4 1f 32  e7 3a 70 20 89 a1 1a 0c   U.S....2 .:p ....
0040  00 00 39 e7 02 06 00 00  00 64 19 07 63 6c 61 73   ..9..... .d..clas
0050  73 0b 0a 31 31 31 32 33  34 72 74 08 06 01 01 01   s..11123 4rt.....
0060  01 06 06 00 00 00 02 0b  05 31 31 31 4f 06 03 0f   ........ .111o...
0070  00 04 19 2e 94 0f 09 23  00 00 01 37 00 01 02 00   .......# ...7....
0080  0a 41 0d f9 00 00 00 00  85 4a 7f 40 5e 47 46 45   .A...... .J.@^GFE
0090  01 cc bf 02 68 82 16 c3  00 00 00 00 04 2f 79 db   ....h... ...../y.
00a0  1a 0c 00 00 01 37 0e 06  00 00 00 32 1a 0c 00 00   .....7.. ...2....
00b0  01 37 0f 06 00 00 00 78  1a 0d 00 00 01 37 0a 07   .7.....x .....7..
00c0  01 51 41 42 4a 1a 33 00  00 01 37 1a 2d 01 53 3d   .QABJ.3. ..7.-.S=
00d0  39 35 37 39 30 43 41 34  35 45 38 44 42 31 31 46   95790CA4 5E8DB11F
00e0  41 44 36 38 34 46 44 46  36 30 33 41 43 42 43 42   AD684FDF 603ACBCB
00f0  32 37 42 41 32 46 30 37  1a 3a 00 00 01 37 10 34   27BA2F07 .:...7.4
0100  ca 89 03 bb 71 8b 4c 25  c7 24 bd 4d ad 77 10 9c   ....q.L% .$.M.w..
0110  d8 bd 91 2d 41 a7 f4 0d  80 9c 92 2b 07 6b 17 a2   ...-A... ...+.k..
```

Frame (382 bytes) | Reassembled EAP (4 bytes)

Figure 122 *Configure VSA on a RADIUS Server*



Izou Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	100

Vendor-Specific Attribute Information

Attribute name:
Vendor Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

● Enter Vendor Code: 14823

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms

○ No. It does not conform

Configure VSA (RFC Compliant)

Vendor-assigned attribute number: 2

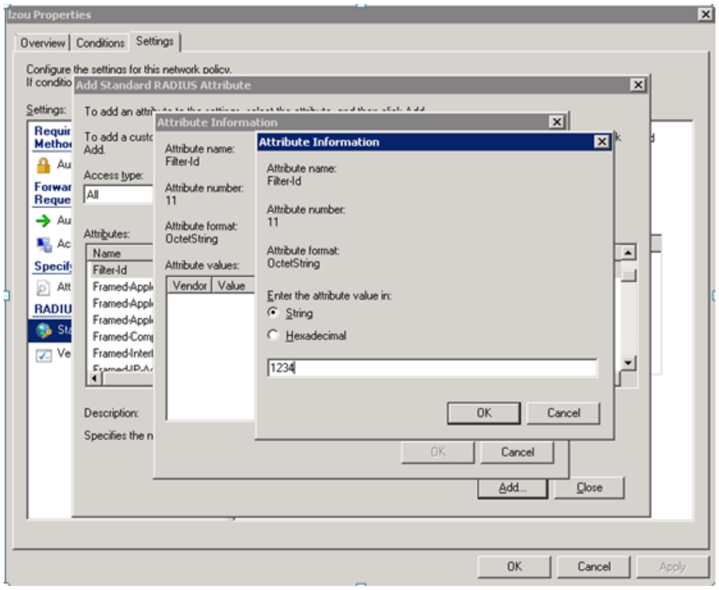
Attribute format: Decimal

Attribute value: 100

VLAN Derivation Rule

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

Figure 123 *Configuring RADIUS Attributes on the RADIUS Server*



Izou Properties

Configure the settings for this network policy.

Add Standard RADIUS Attribute

Access type: All

Attribute Information

Attribute name:
Filter-Id

Attribute number:
11

Attribute format:
OctetString

Enter the attribute value in:

● String

○ Hexadecimal

1234

Configuring VLAN Derivation Rules on an IAP

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

To configure VLAN derivation rules on an IAP:

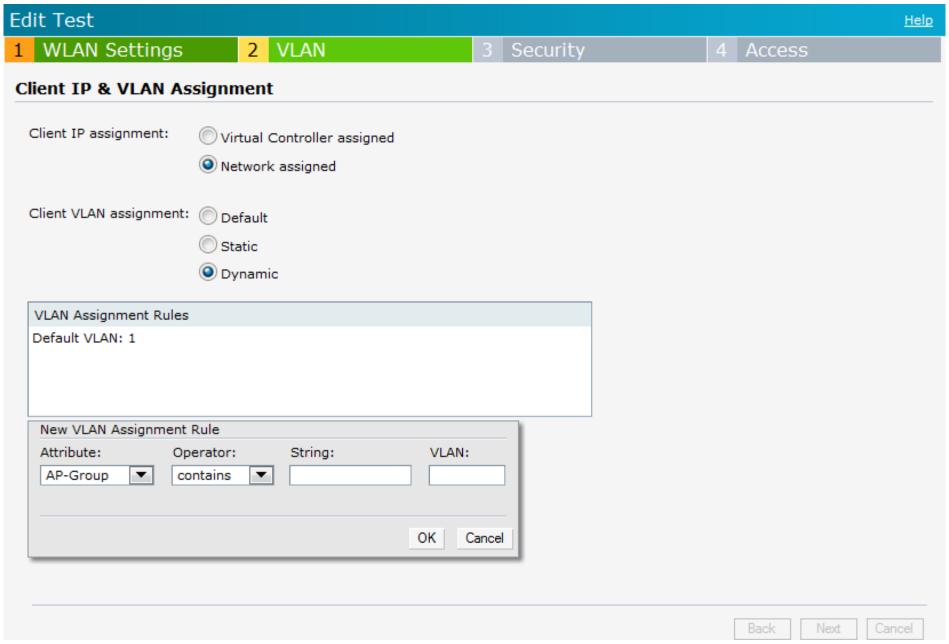
1. Select a network on the Instant UI and click on the **edit** link.
2. Select the **VLAN** tab and check the Dynamic radio button under the **client VLAN assignment.**
3. Click **New** to assign the user to a VLAN. The **New VLAN Assignment Rule** window appears.

   Enter the following information:

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

4. Click **OK**.

Figure 124 *Configuring VLAN Derivation Rules on an IAP*



Client IP & VLAN Assignment

Client IP assignment: ○ Virtual Controller assigned ● Network assigned

Client VLAN assignment: ○ Default ○ Static ● Dynamic

VLAN Assignment Rules

Default VLAN: 1

New VLAN Assignment Rule

Attribute:	Operator:	String:	VLAN:
AP-Group	contains		

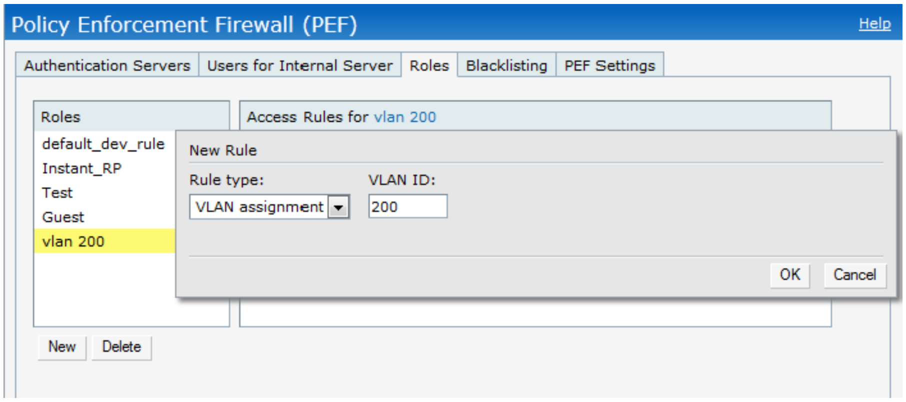
User Role

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

Configuring a User Role

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

Figure 125 *Configuring VLAN Derivation using the User Role*



Roles: default_dev_rule, Instant_RP, Test, Guest, vlan 200

Access Rules for vlan 200

New Rule

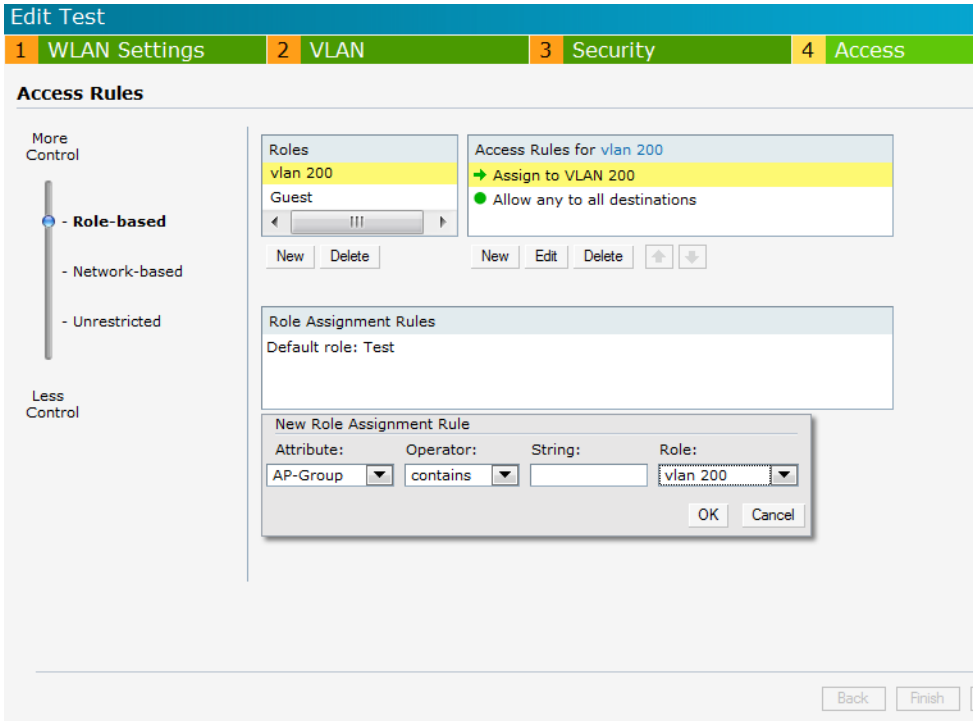
Rule type: VLAN assignment

VLAN ID: 200

To use a defined user VLAN role:

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

Figure 126 *To use a Defined User VLAN Role*



Access Rules

Roles: vlan 200, Guest

Access Rules for vlan 200: Assign to VLAN 200; Allow any to all destinations

Role Assignment Rules

Default role: Test

New Role Assignment Rule

Attribute: AP-Group

Operator: contains

String:

Role: vlan 200

SSID Profile

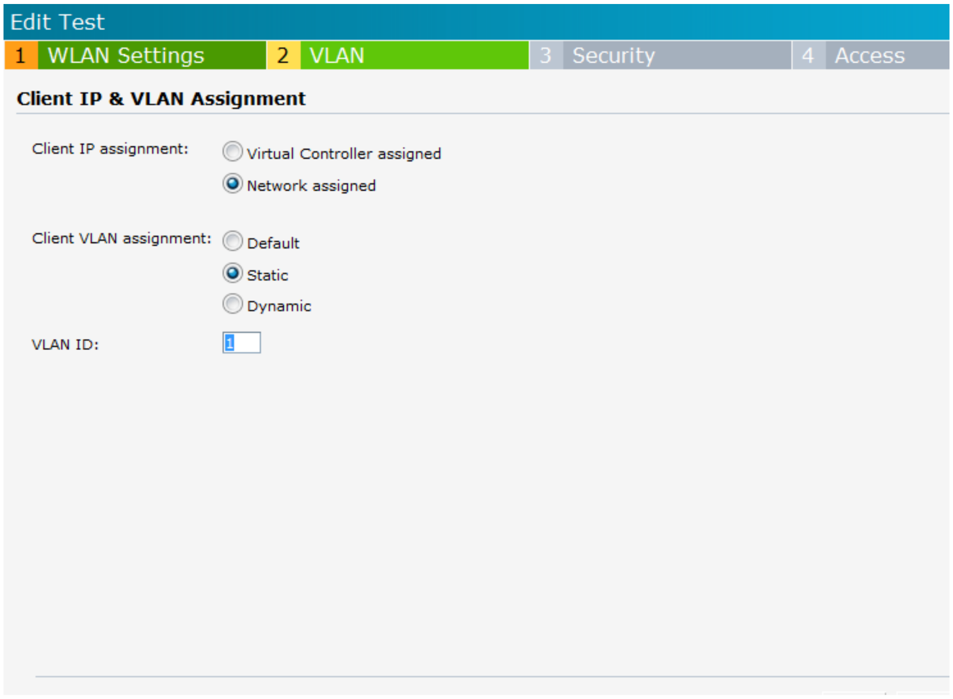
If the VSA, VLAN derivation rules are not matching, and the User Role does not contain a VLAN, then the user VLAN can be derived by the SSID profile.

Configuring VLAN Derivation Rules Using an SSID Profile

To configure VLAN derivation rules on an IAP:

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

Figure 127 *Configuring VLAN Derivation Rules Using an SSID Profile*



Client IP & VLAN Assignment

Client IP assignment: ○ Virtual Controller assigned ● Network assigned

Client VLAN assignment: ○ Default ● Static ○ Dynamic

VLAN ID: 1

Chapter 16

Instant Firewall

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

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

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

The New Rule window consists of the following options:

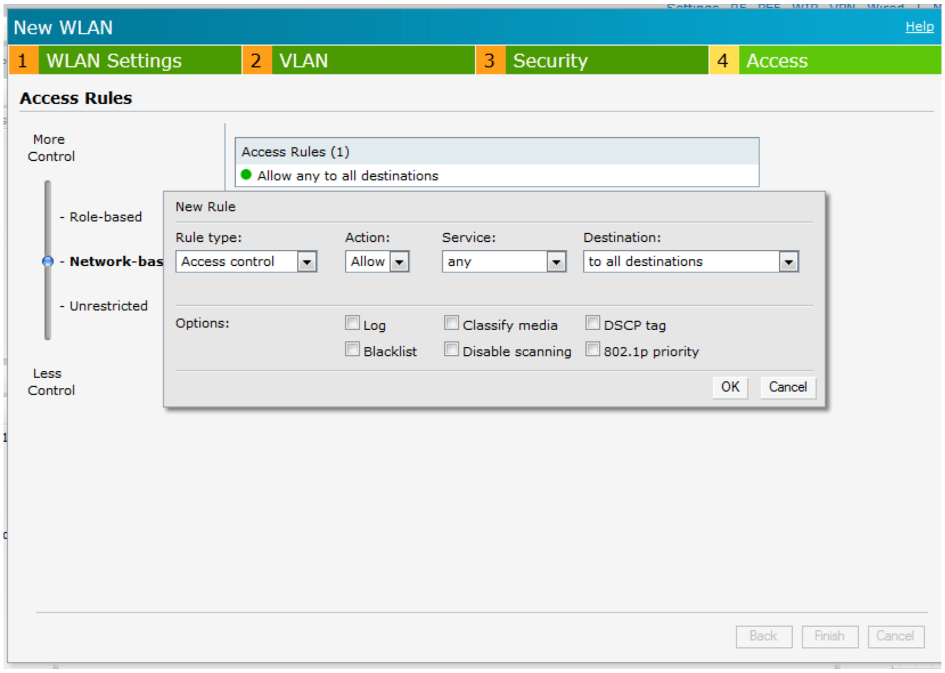
- **Rule type—** Select the rule type (Access control, VLAN assignment) from the drop-down list.
- **Action—** Select **Allow** or **Deny** from the drop-down list to allow or deny traffic with the specified service type and destination.
- **Log—** Select this checkbox if you want a log entry to be created when this rule is triggered. Instant firewall supports firewall based logging function. Firewall logs on IAP are generated as syslog messages.
- **Blacklist—** Select this checkbox if you want the client to be blacklisted when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist** time on the Blacklisting tab of the **PEF** window. See "Client Blacklisting" on page 239 for more information.
- **Classify media**— Select this checkbox if you want to prioritize video and voice traffic. When enabled, deep packet inspection is performed on all non-NATed traffic, and the traffic is marked as follows:
  - Video: Priority 5 (Critical)
  - Voice: Priority 6 (Internetwork Control)
- **Disable scanning**— Select this checkbox if you want ARM scanning to be paused when this rule is triggered, to optimize performance.

NOTE

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

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

Figure 128 *Access Tab - Instant Firewall Settings*



Access Rules

Access Rules (1)

● Allow any to all destinations

New Rule

Rule type: Access control

Action: Allow

Service: any

Destination: to all destinations

Options: □ Log □ Classify media □ DSCP tag □ Blacklist □ Disable scanning □ 802.1p priority

OK Cancel

Service Options

Table 22 lists the set of service options available in the Instant UI. You can allow or deny access to any or all of these services depending on your requirements.

Table 22 *Network Service Options*

Service	Description
any	Access is allowed or denied to all services.
custom	Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If you select the **Other** option, enter the appropriate ID.
adp	Application Distribution Protocol
bootp	Bootstrap Protocol
dhcp	Dynamic Host Configuration Protocol
dns	Domain Name Server
esp	Encapsulating Security Payload
ftp	File Transfer Protocol
gre	Generic Routing Encapsulation
h323-tcp	H.323-Transmission Control Protocol
h323-udp	H.323-User Datagram Protocol
http-proxy2	Hypertext Transfer Protocol-proxy2

Table 22 *Network Service Options (Continued)*

Service	Description
http-proxy3	Hypertext Transfer Protocol-proxy3
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
icmp	Internet Control Message Protocol
ike	Internet Key Exchange
kerberos	Computer network authentication protocol
l2tp	Layer 2 Tunneling Protocol
lpd-tcp	Line Printer Daemon protocol-Transmission Control Protocol
lpd-udp	Line Printer Daemon protocol-User Datagram Protocol
msrpc-tcp	Microsoft Remote Procedure Call-Transmission Control Protocol
msrpc-udp	Microsoft Remote Procedure Call-User Datagram Protocol
netbios-dgm	Network Basic Input/Output System-Datagram Service
netbios-ns	Network Basic Input/Output System-Name Service
netbios-ssn	Network Basic Input/Output System-Session Service
ntp	Network Time Protocol
papi	Point of Access for Providers of Information
pop3	Post Office Protocol 3
pptp	Point-to-Point Tunneling Protocol
rtsp	Real Time Streaming Protocol
sccp	Skinny Call Control Protocol
sip	Session Initiation Protocol
sip-tcp	Session Initiation Protocol-Transmission Control Protocol
sip-udp	Session Initiation Protocol-User Datagram Protocol
smb-tcp	Server Message Block-Transmission Control Protocol
smb-udp	Server Message Block-User Datagram Protocol
smtp	Simple mail transfer protocol
snmp	Simple network management protocol
snmp-trap	Simple network management protocol-trap

Table 22 *Network Service Options (Continued)*

Service	Description
svp	Software Validation Protocol
tftp	Trivial file transfer protocol

Destination Options

Table 23 lists the destination options available in the Instant UI. You can allow or deny access to any or all of these destinations depending on your requirements.

Table 23 *Destination Options*

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

Examples for Access Rules

This section provides procedures to create the following access rules.

- Allow TCP Service to a Particular Network
- 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. and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN.Click **Next** to continue.
4. Click **Next** and set appropriate values in the **Security** tab.
5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define allow TCP service access rule to a particular network:
   a. Click **New**, the **New Rule** window appears.

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

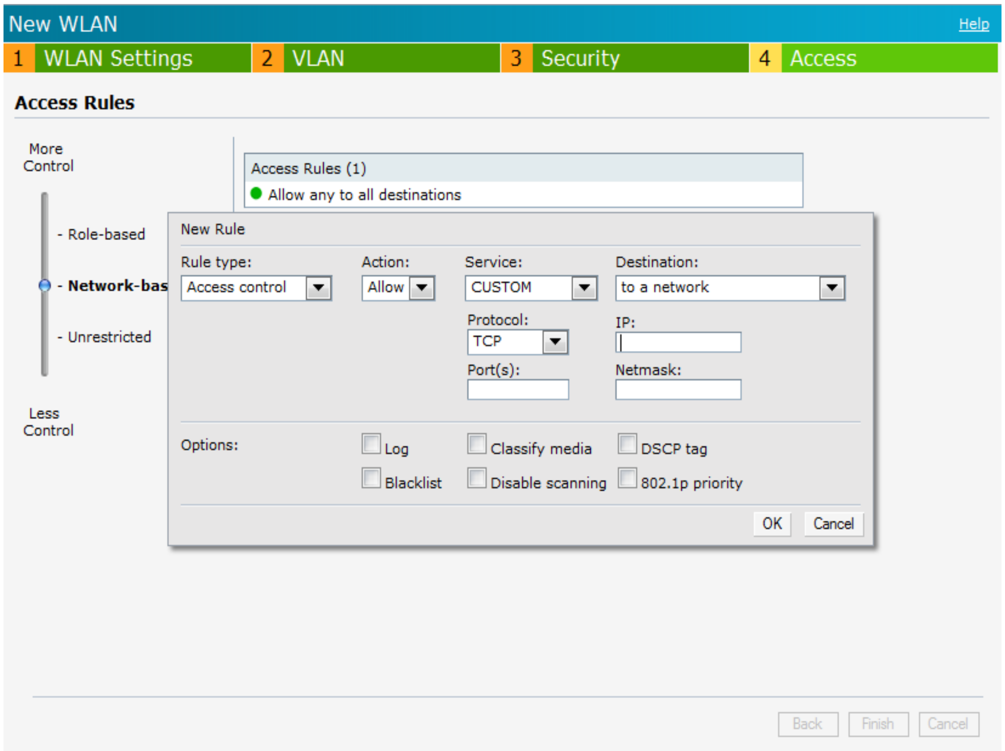
c. Select **custom** from the **Service** drop-down list.

- Select TCP from the Protocol drop-down list.
- Enter appropriate port number in the Port(s) text box.

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

- Enter appropriate IP address in the IP text box.
- Enter appropriate netmask in the Netmask text box.

Figure 129 *Defining Rule — Allow TCP Service to a Particular Network*



New WLAN

Access Rules

Access Rules (1)

● Allow any to all destinations

New Rule

Rule type: Access control

Action: Allow

Service: CUSTOM

Destination: to a network

Protocol: TCP

Port(s):

IP:

Netmask:

Options: □ Log □ Classify media □ DSCP tag □ Blacklist □ Disable scanning □ 802.1p priority

e. Click **OK.**

6. Click **Finish**.

Allow PoP3 Service to a Particular Server

1. Click the **New** link in the **Networks** tab.
   To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **Basic Info** tab, enter the appropriate information and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN.Click **Next** to continue.
4. Click **Next** and slide to set the appropriate security levels in the **Security** tab.
5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define allow POP3 service access rule to a particular server:

a. Click **New**, the **New Rule** window appears.

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

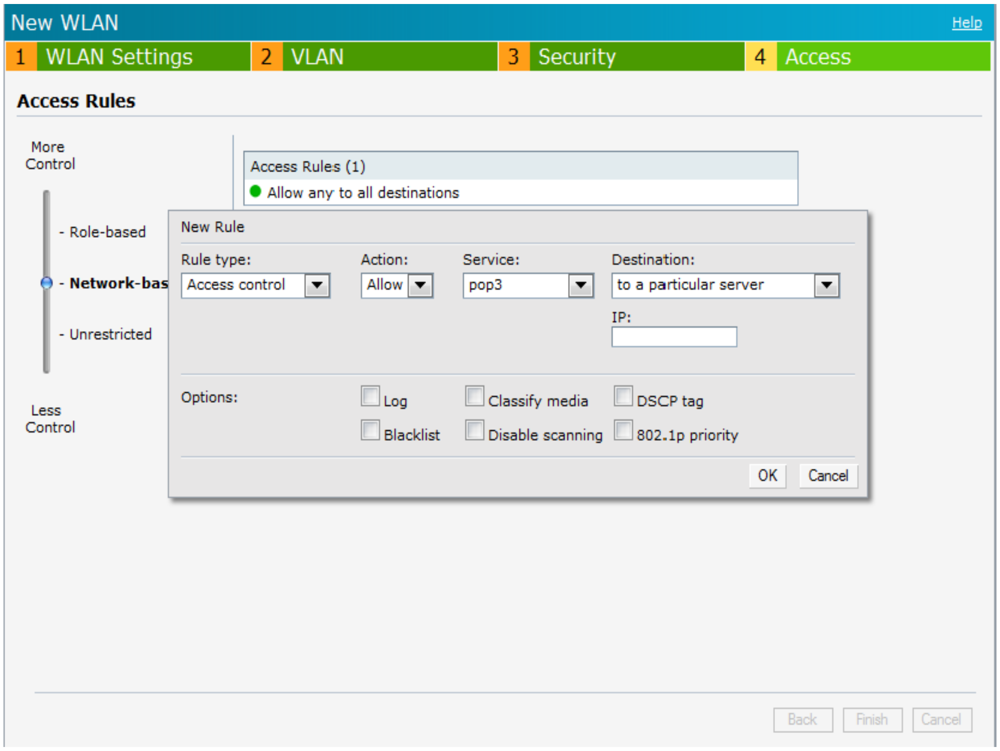
c. Select **pop3** from the **Service** drop-down list.

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

e. Click **OK**.

6. Click **Finish**.

Figure 130 *Defining Rule — Allow POP3 Service to a Particular Server*



New WLAN

Access Rules

Access Rules (1)

● Allow any to all destinations

New Rule

Rule type: Access control

Action: Allow

Service: pop3

Destination: to a particular server

IP:

Options: □ Log □ Classify media □ DSCP tag □ Blacklist □ Disable scanning □ 802.1p priority

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 and click **Next** to continue.

3. Use the **VLAN** tab, to specify how the clients on this network get their IP address and VLAN.Click **Next** to continue.

4. Click **Next** and set appropriate security levels using the slider bar in the **Security** tab.

5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define deny FTP service access rule except to a particular server:

   a. Click **New**, the **New Rule** window appears.

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

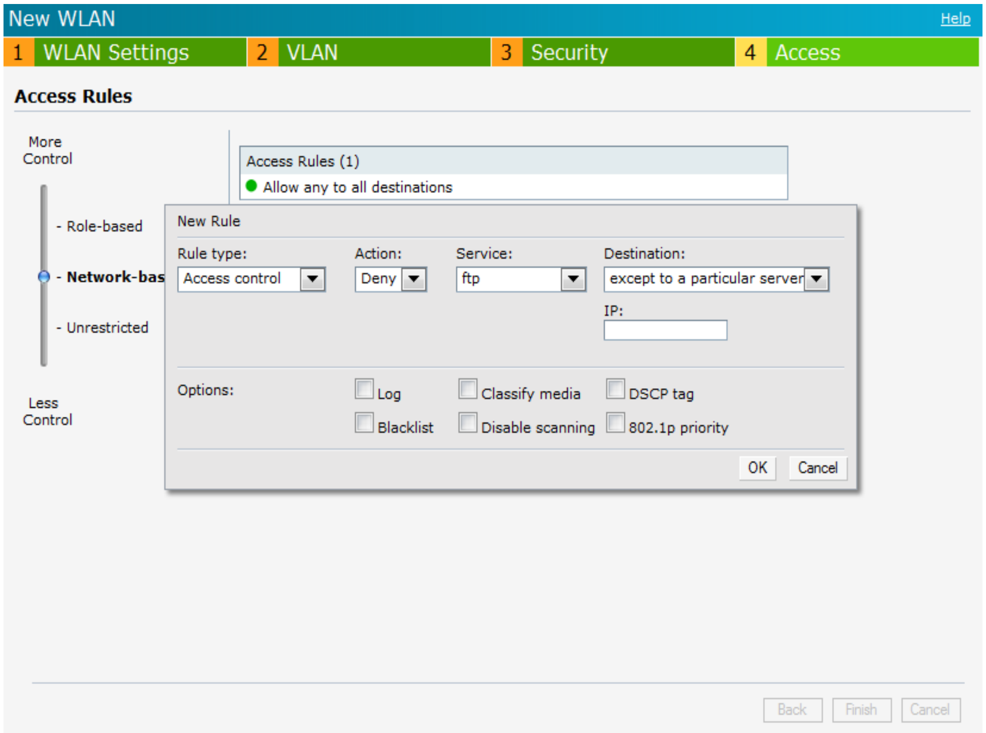
   c. Select **ftp** from the **Service** drop-down list.

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

   e. Click **OK**

6. Click **Finish**

Figure 131 *Defining Rule — Deny FTP Service Except to a Particular Server*



Access Rules (1)

● Allow any to all destinations

Rule type: Access control

Action: Deny

Service: ftp

Destination: except to a particular server

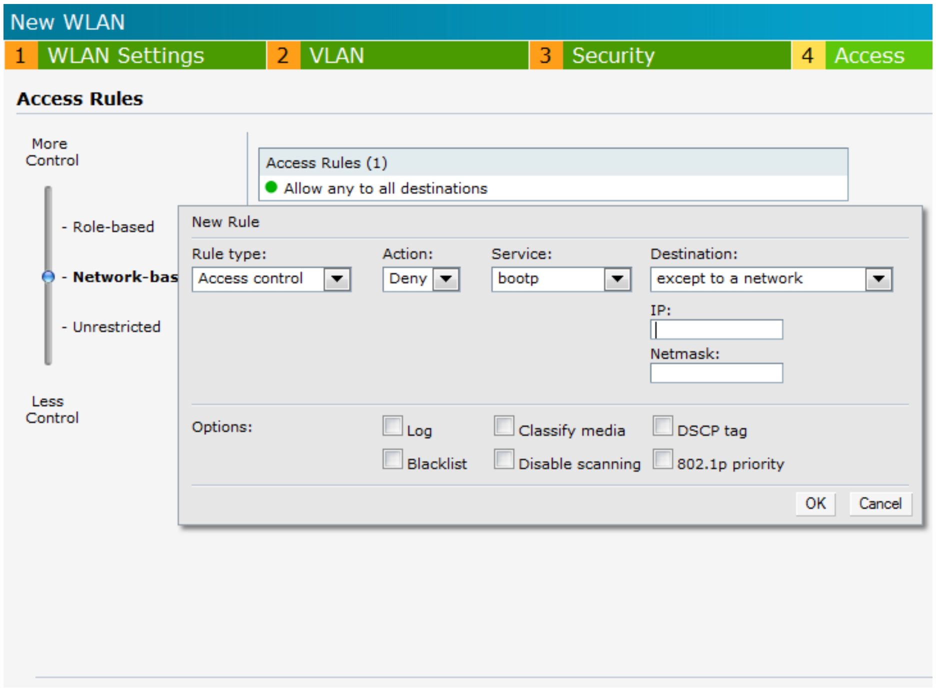
IP:

Options: □ Log □ Classify media □ DSCP tag □ Blacklist □ Disable scanning □ 802.1p priority

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

Figure 132 *Defining Rule — Deny bootp Service Except to a Network*



Access Rules

Access Rules (1)

● Allow any to all destinations

New Rule

Rule type: Access control

Action: Deny

Service: bootp

Destination: except to a network

IP:

Netmask:

Options: □ Log □ Classify media □ DSCP tag □ Blacklist □ Disable scanning □ 802.1p priority

Chapter 17

Content Filtering

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

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

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

NOTE

Regardless of whether content filtering is disabled or enabled, instant.arubanetworks.com is always resolved internally on Instant.

Enabling Content Filtering

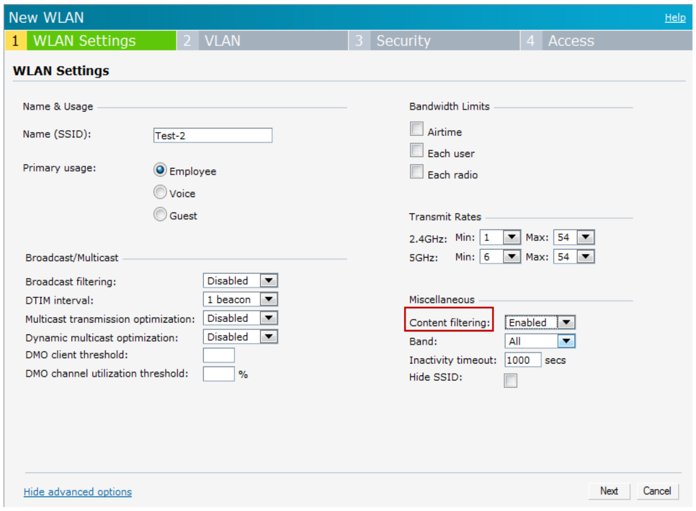
To enable content filtering per SSID:

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

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

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

Figure 133 *Enabling Content Filtering*



WLAN Settings

Name & Usage

Name (SSID): Test-2

Primary usage: ● Employee ○ Voice ○ Guest

Broadcast/Multicast

Broadcast filtering: Disabled

DTIM interval: 1 beacon

Multicast transmission optimization: Disabled

Dynamic multicast optimization: Disabled

DMO client threshold:

DMO channel utilization threshold: %

Bandwidth Limits

□ Airtime

□ Each user

□ Each radio

Transmit Rates

2.4GHz: Min: 1 Max: 54

5GHz: Min: 6 Max: 54

Miscellaneous

Content filtering: Enabled

Band: All

Inactivity timeout: 1000 secs

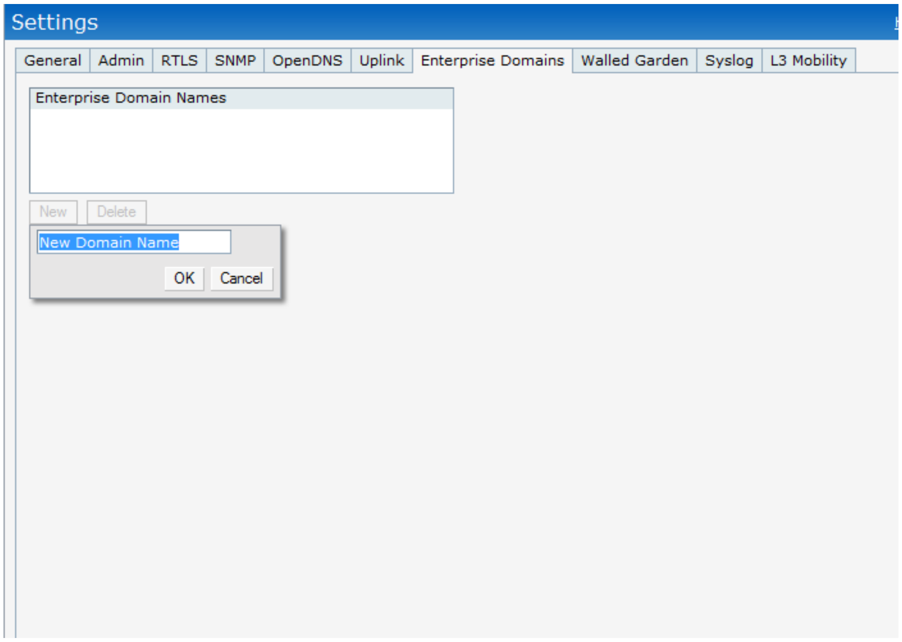
Hide SSID: □

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 Aruba Instant WebUI.

Enterprise Domains

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

Figure 134 *Enterprise Domains*



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

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

Chapter 18A

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:

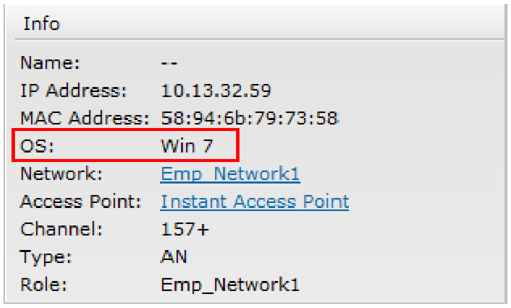
- Identifying rogue clients— Helps to identify clients that are running on forbidden operating systems.
- Identifying outdated operating systems— Helps to locate outdated and unexpected OS in the company network.
- Locating and patching vulnerable operating systems— Assists in locating and patching specific 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
- iOS
- Android
- Blackberry
- Linux

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

Figure 135 *OS Fingerprinting*



Info

Name:	--
IP Address:	10.13.32.59
MAC Address:	58:94:6b:79:73:58
OS:	Win 7
Network:	Emp_Network1
Access Point:	Instant Access Point
Channel:	157+
Type:	AN
Role:	Emp_Network1

Chapter 19

Adaptive Radio Management

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

ARM Features

This section describes ARM features that are available in 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 operations when RF conditions change.

Voice Aware Scanning

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

Load Aware Scanning

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

Band Steering Mode

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

Band steering supports the following three different band steering modes:

- **Prefer 5 GHz**— If you configure the IAP to use prefer-5 GHz band steering mode, the IAP steers the client to 5 GHz band (if the client is 5 GHz capable) but lets the client connect on the 2.4 GHz band if the client persists in 2.4 GHz association attempts.
- **Force 5 GHz**— When the IAP is configured in force-5 GHz band steering mode, the IAP forces 5 GHz-capable IAPs to use that radio band.
- **Balance Bands**— In this band steering mode, the IAP tries to balance the clients across the two radios in order to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the

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

- **Disabled—** Disabled means that the clients selects which band to use.

Airtime Fairness Mode

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

NOTE

Reboot the IAP after configuring the radio profile settings in order for the changes to take effect.

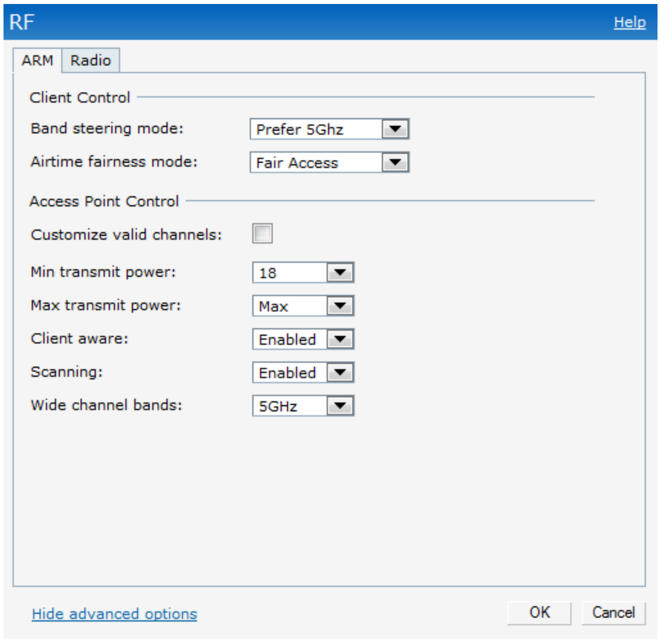
Airtime Fairness Modes

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

The Airtime fairness consists of the following modes:

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

Figure 136 *Airtime Fairness Mode*



Client Control

Band steering mode: Prefer 5Ghz

Airtime fairness mode: Fair Access

Access Point Control

Customize valid channels: □

Min transmit power: 18

Max transmit power: Max

Client aware: Enabled

Scanning: Enabled

Wide channel bands: 5GHz

Access Point Control

Customize Valid Channels

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

Min Transmit Power

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

The default value is18 dBm.

Max Transmit Power

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

Default value: 127 dBm

Client Aware

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

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

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

NOTE

When the Client Aware ARM is disabled, channels can be changed even when the clients are active on BSSID.

Scanning

When ARM is enabled, the IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and reports everything it sees to the IAP on each channel it scans. This includes, but is not limited to, data regarding WLAN coverage, interference, and intrusion detection.

Wide Channel Bands

This feature allows administrators to configure 40 MHz channels in the 2.4 GHz and 5.0 GHz bands. 40 MHz channels are essentially two 20 MHz adjacent channels that are bonded together. 40 MHz channel effectively doubles the frequency bandwidth available for data transmission.

Monitoring the Network with ARM

When ARM is enabled, an IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and provides reports for network (WLAN) coverage, interference, and intrusion detection, to a Virtual Controller.

ARM Metrics

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

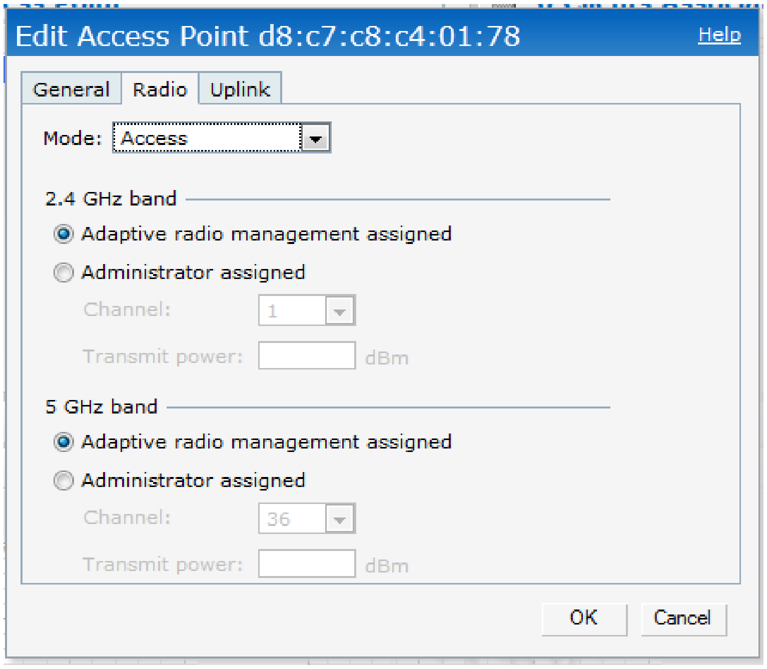
Configuring Administrator Assigned Radio Settings for IAP

Adaptive Radio Management (ARM) is enabled on Aruba Instant by default. It automatically assigns appropriate channel and power settings for the IAPs.

To manually configure radio settings:

1. In the **Access Points** tab, click the AP for which you want to enable ARM. The **edit** link appears.
2. Click the **edit** link. The **Edit AP** window appears.
3. Click the **Radio** tab.

Figure 137 *Configuring Administrator Assigned Radio Settings for IAP*



Edit Access Point d8:c7:c8:c4:01:78

Mode: Access

2.4 GHz band

● Adaptive radio management assigned

○ Administrator assigned

Channel: 1

Transmit power: dBm

5 GHz band

● Adaptive radio management assigned

○ Administrator assigned

Channel: 36

Transmit power: dBm

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

   By default the access point's channel and power are optimized dynamically using Adaptive Radio Management (ARM). You can override ARM on the 2.4 GHz and 5 GHz bands and set the channel and power manually if desired.

Table 24 *Mode, Spectrum and AP Operation*

Mode	Spectrum	AP Operation
Access	Disabled	AP serves clients, while also monitoring for rogue APs in the background.
Access	Enabled	AP monitors all RF interference on its current channel, while simultaneously providing normal access services to clients.

Table 24 *Mode, Spectrum and AP Operation (Continued)*

Mode	Spectrum	AP Operation
Monitor	Disabled	AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring APs or from non-WiFi devices such as microwaves and cordless phones.
Monitor	Enabled	AP does not provide access service to clients.

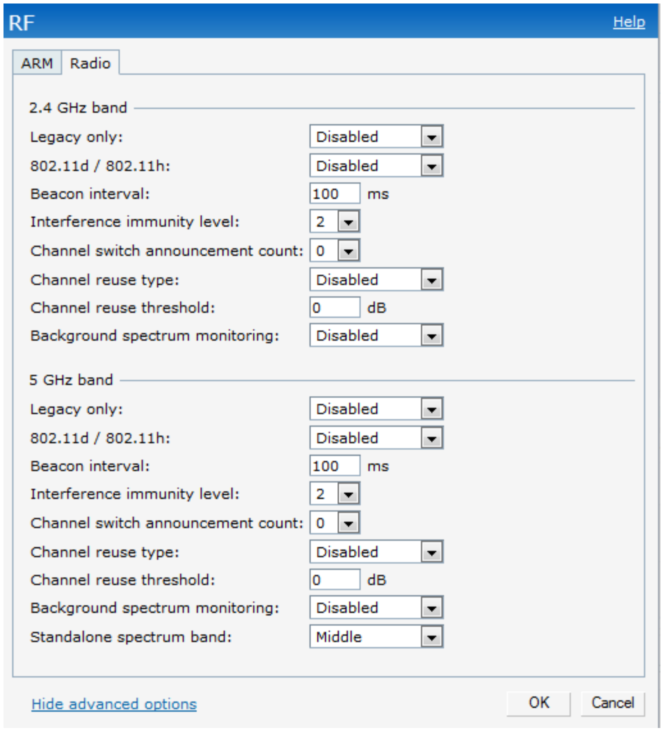
5. Select **Administrator assigned** in **2.4 GHz** and **5 GHz** band sections.
6. Select appropriate channel number from the **Channel** drop-down list for both **2.4 GHz** and **5 GHz** band sections.
7. Enter appropriate transmit power value in the **Transmit power** text box in **2.4 GHz** and **5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

Configuring Radio Profiles in Instant

Aruba Instant supports radio profile configuration. The radio settings are available for both the 2.4-GHz and the 5-GHz radio profiles. You can configure the radios separately, using the parameters described in table on each radio.

Use the following procedure to configure Instant's radio attributes for the 2.4 GHz and 5 GHz frequency bands.

Figure 138 *Radio Profile*



2.4 GHz band

Legacy only:	Disabled
802.11d / 802.11h:	Disabled
Beacon interval:	100 ms
Interference immunity level:	2
Channel switch announcement count:	0
Channel reuse type:	Disabled
Channel reuse threshold:	0 dB
Background spectrum monitoring:	Disabled

5 GHz band

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

1. Navigate to **RF** which is at the top right corner of the Instant WebUI.
2. Click **Show advanced options** to view the **Radio** tab.

3. Refer to the table below to configure the radio settings for bands 2.4 GHz and 5 GHz.

Table 25 *Radio Profile Configuration Parameters*

Parameter	Description
Legacy only	Enable to run the radio in non-802.11n mode. This is disabled by default.
802.11d / 802.11h	Enable the radio to advertise its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This is disabled by default.
Beacon interval	Enter the Beacon period (60ms to 500ms) for the IAP in msec. This indicates how often the 802.11 beacon management frames are transmitted by the access point. The default value is 100 msec.
Interference immunity level	Select to increase the immunity level to improve performance in high-interference environments. The default immunity level is 2. **NOTE:** Increasing the immunity level makes the AP slightly "deaf" to its surroundings, causing the AP to lose a small amount of range. ● Level 0— no ANI adaptation. ● Level 1— Noise immunity only. This level enables power-based packet detection by controlling the ● amount of power increase that makes a radio aware that it has received a packet. ● Level 2— Noise and spur immunity. This level also controls the detection of OFDM packets, and is the ● default setting for the Noise Immunity feature. ● Level 3— Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ● Level 4— Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ● Level 5— The AP completely disables PHY error reporting, improving performance by eliminating the time the IAP would spend on PHY processing.
Channel switch announcement count	Indicates the number of channel switching announcements that must be sent prior to switching to a new channel. This allows associated clients to recover gracefully from a channel change.
Channel reuse type	When set to **Dynamic**, the access point, when busy, automatically adjust its Clear Channel Assessment (CCA) threshold to accommodate transmissions to the most distant associated client. When set to **Static**, the access point sets its CCA threshold to the value specified in **Channel reuse threshold**.
Channel reuse threshold	When set to **Static,** this value specifies the tolerable interference that must be maintained.

Table 25 *Radio Profile Configuration Parameters (Continued)*

Parameter	Description
Background spectrum monitoring	When background spectrum monitoring is enabled, the APs in access mode continue to provide normal access service to clients, while performing additional function of monitoring RF interference (from both neigh bo uri ng APs and non-WiFi sources such as, microwaves and cordless phones) on the channel they are currently serving clients on.
Standalone spectrum band	For background spectrum monitoring on the 5 GHz band, it is necessary to specify which portion of the channel to monitor: upper, middle, or lower.

NOTE

Reboot the IAP after configuring the radio profile settings in order for the changes to take effect.

Chapter 20

Intrusion Detection System

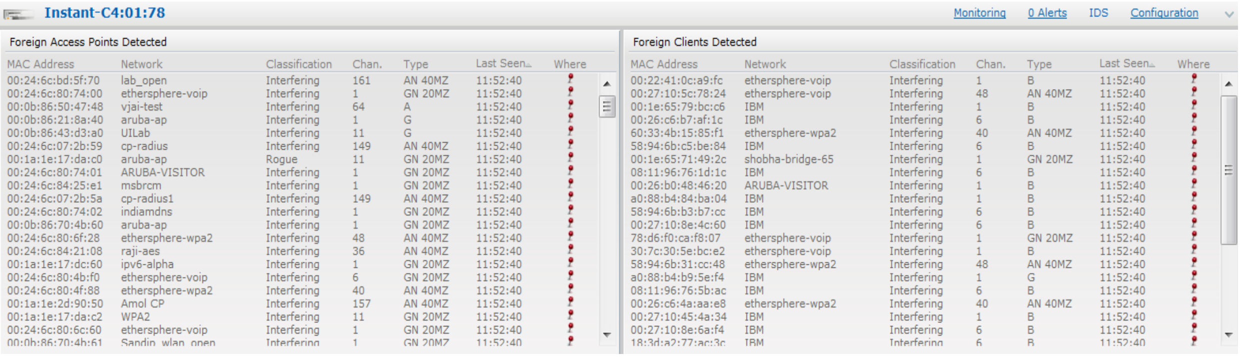
Intrusion Detection System (IDS) is a feature that monitors the network for the presence of unauthorized IAPs and clients. It also logs information about the unauthorized IAPs and clients, and generates reports based on the logged information.

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.

Navigate to **IDS** in the Instant UI and click the **IDS** link. The built-in IDS scans for access points that are not controller by this Virtual Controller. These are listed below and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

Figure 139 *Intrusion Detection*



Foreign Access Points Detected

MAC Address	Network	Classification	Chan.	Type	Last Seen	Where
00:24:6c:bd:5f:70	lab_open	Interfering	161	AN 40MZ	11:52:40	📍
00:24:6c:80:74:00	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40	📍
00:0b:86:50:47:48	vjai-test	Interfering	64	A	11:52:40	📍
00:0b:86:21:8a:40	aruba-ap	Interfering	1	G	11:52:40	📍
00:0b:86:43:d3:a0	UILab	Interfering	11	G	11:52:40	📍
00:24:6c:07:2b:59	cp-radius	Interfering	149	AN 40MZ	11:52:40	📍
00:1a:1e:17:da:c0	aruba-ap	Rogue	11	GN 20MZ	11:52:40	📍
00:24:6c:80:74:01	ARUBA-VISITOR	Interfering	1	GN 20MZ	11:52:40	📍
00:24:6c:84:25:e1	msbrcm	Interfering	1	GN 20MZ	11:52:40	📍
00:24:6c:07:2b:5a	cp-radius1	Interfering	149	AN 40MZ	11:52:40	📍
00:24:6c:80:74:02	indiamdns	Interfering	1	GN 20MZ	11:52:40	📍
00:0b:86:70:4b:60	aruba-ap	Interfering	1	GN 20MZ	11:52:40	📍
00:24:6c:80:6f:28	ethersphere-wpa2	Interfering	48	AN 40MZ	11:52:40	📍
00:24:6c:84:21:08	raji-aes	Interfering	36	AN 40MZ	11:52:40	📍
00:1a:1e:17:dc:60	ipv6-alpha	Interfering	1	GN 20MZ	11:52:40	📍
00:24:6c:80:4b:f0	ethersphere-voip	Interfering	6	GN 20MZ	11:52:40	📍
00:24:6c:80:4f:88	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40	📍
00:1a:1e:2d:90:50	Amol CP	Interfering	157	AN 40MZ	11:52:40	📍
00:1a:1e:17:da:c2	WPA2	Interfering	11	GN 20MZ	11:52:40	📍
00:24:6c:80:6c:60	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40	📍
00:0b:86:70:4b:61	Sandip_wlan_open	Interfering	1	GN 20MZ	11:52:40	📍

Foreign Clients Detected

MAC Address	Network	Classification	Chan.	Type	Last Seen	Where
00:22:41:0c:a9:fc	ethersphere-voip	Interfering	1	B	11:52:40	📍
00:27:10:5c:78:24	ethersphere-voip	Interfering	48	AN 40MZ	11:52:40	📍
00:1e:65:79:bc:c6	IBM	Interfering	1	B	11:52:40	📍
00:26:c6:b7:af:1c	IBM	Interfering	6	B	11:52:40	📍
60:33:4b:15:85:f1	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40	📍
58:94:6b:c5:be:84	IBM	Interfering	6	B	11:52:40	📍
00:1e:65:71:49:2c	shobha-bridge-65	Interfering	1	GN 20MZ	11:52:40	📍
08:11:96:76:1d:1c	IBM	Interfering	6	B	11:52:40	📍
00:26:b0:48:46:20	ARUBA-VISITOR	Interfering	1	B	11:52:40	📍
a0:88:b4:84:ba:04	IBM	Interfering	1	B	11:52:40	📍
58:94:6b:b3:b7:cc	IBM	Interfering	6	B	11:52:40	📍
00:27:10:8e:4c:60	IBM	Interfering	6	B	11:52:40	📍
78:d6:f0:ca:f8:07	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40	📍
30:7c:30:5e:bc:e2	ethersphere-voip	Interfering	1	B	11:52:40	📍
58:94:6b:31:cc:48	ethersphere-wpa2	Interfering	48	AN 40MZ	11:52:40	📍
a0:88:b4:b9:5e:f4	IBM	Interfering	1	G	11:52:40	📍
08:11:96:76:5b:ac	IBM	Interfering	6	B	11:52:40	📍
00:26:c6:4a:aa:e8	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40	📍
00:27:10:45:4a:34	IBM	Interfering	1	B	11:52:40	📍
00:27:10:8e:6a:f4	IBM	Interfering	6	B	11:52:40	📍
18:3d:a2:77:ac:3c	IBM	Interfering	6	B	11:52:40	📍

Wireless Intrusion Protection (WIP)

WIP offers a wide selection of intrusion detection and protection features to protect the network against wireless threats. Like most other security-related features of the Aruba network, the WIP configuration can be done on the IAP.

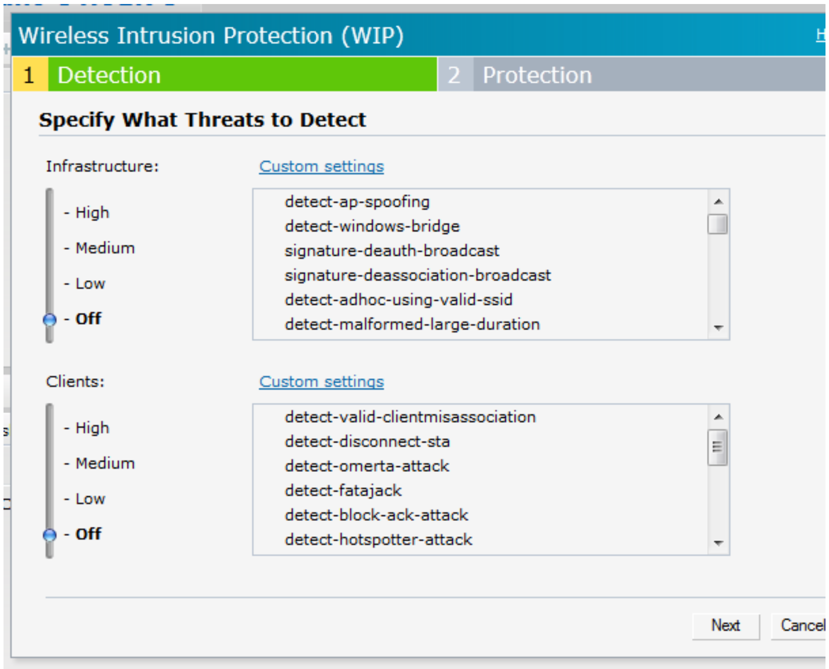
An administrator can configure the following five main options.

- **Infrastructure Detection Policies**— Specifies which wireless attacks on access points to detect
- **Client Detection Policies**— Specifies which wireless attacks on clients to detect
- **Infrastructure Protection Policies**— Specifies which wireless attacks on access points to protect against
- **Client Protection Policies**— Specifies which wireless attacks on clients to protect against
- **Containment Methods**— Prevents unauthorized stations from connecting to your Instant network.

In each of these options there are several default levels that enable different sets of policies. An administrator can customize (enable/disable) these options accordingly.

Four levels of detection can be configured in the WIP Detection page— **Off**, **Low**, **Medium**, and **High** (as shown in Figure 140).

Figure 140 *Wireless Intrusion Protection— Detection*



Specify What Threats to Detect

Infrastructure: Custom settings

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

Clients: Custom settings

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

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

Table 26 *Infrastructure Detection Policies*

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

Table 26 *Infrastructure Detection Policies* (Continued)

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

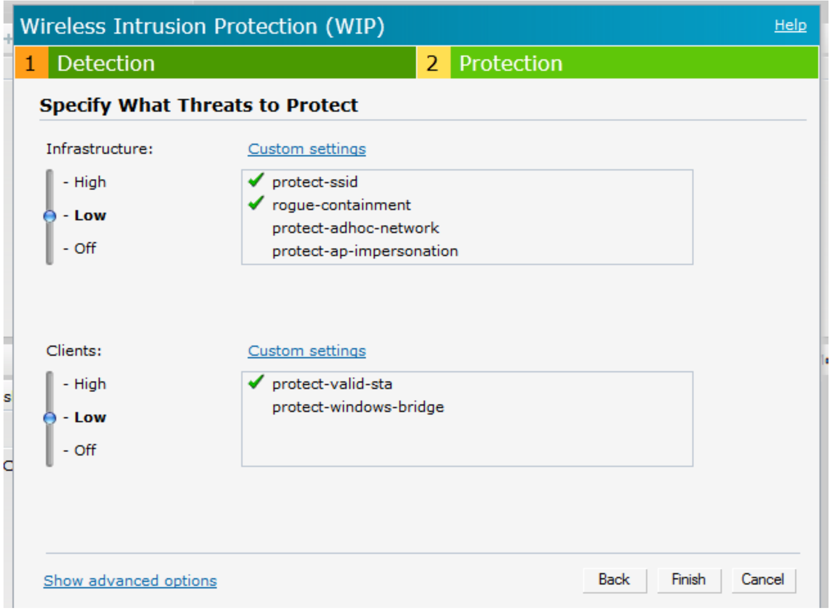
The following table describes the detection policies that are enabled in Client Detection **Custom settings** field.

Table 27 *Client Detection Policies*

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

Three levels of detection can be configured in the WIP Protection page— **Off**, **Low**, and **High** (as shown in Figure 141).

Figure 141 *Wireless Intrusion Protection— Protection*



Specify What Threats to Protect

Infrastructure: Custom settings

- High
- **Low**
- Off

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

Clients: Custom settings

- High
- **Low**
- Off

✓ protect-valid-sta
protect-windows-bridge

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

Table 28 *Infrastructure Protection Policies*

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

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

Table 29 *Client Protection Policies*

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

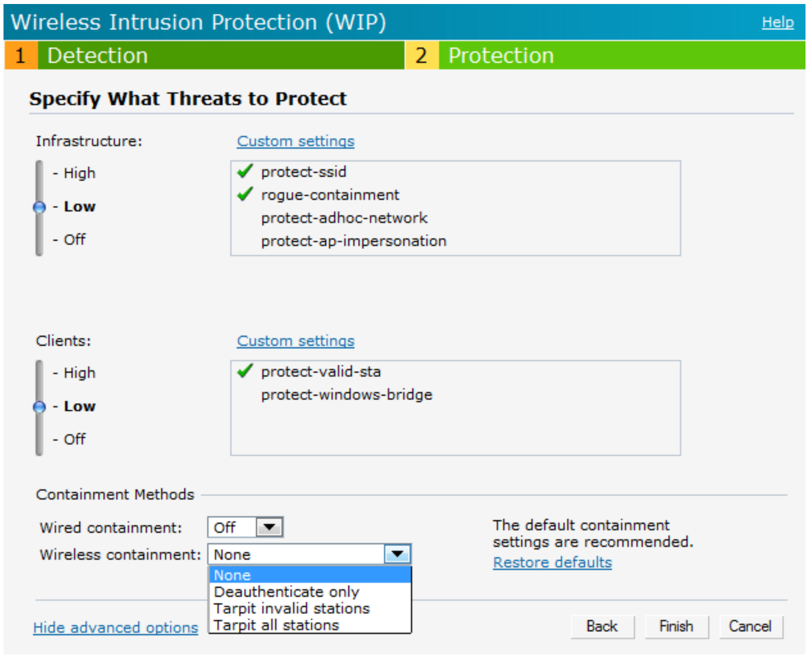
Containment Methods

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

Instant supports the following types of containment mechanisms:

- Wired containment— When enabled, Aruba Access Points generate ARP packets on the wired network to contain wireless attacks.
- Wireless containment— When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified Access Point.
  - None— Disables all the containment mechanisms.
  - Deauthenticate only— With deauthentication containment, the Access Point or client is contained by disrupting the client association on the wireless interface.
  - Tarpit containment— With Tarpit containment, the Access Point is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the Access Point being contained.

Figure 142 *Containment Methods*



Wireless Intrusion Protection (WIP)

1 Detection

2 Protection

Specify What Threats to Protect

Infrastructure: Low

✓ protect-ssid

✓ rogue-containment

protect-adhoc-network

protect-ap-impersonation

Clients: Low

✓ protect-valid-sta

protect-windows-bridge

Containment Methods

Wired containment: Off

Wireless containment: None

The default containment settings are recommended.

Chapter 21

SNMP

Aruba Instant supports SNMPv1, SNMPv2c, and SNMPv3 for reporting purposes only. An IAP cannot use SNMP to set values in an Aruba system.

SNMP Parameters for IAP

You can configure the following parameters for IAP.

Table 30 *SNMP Parameters for IAP*

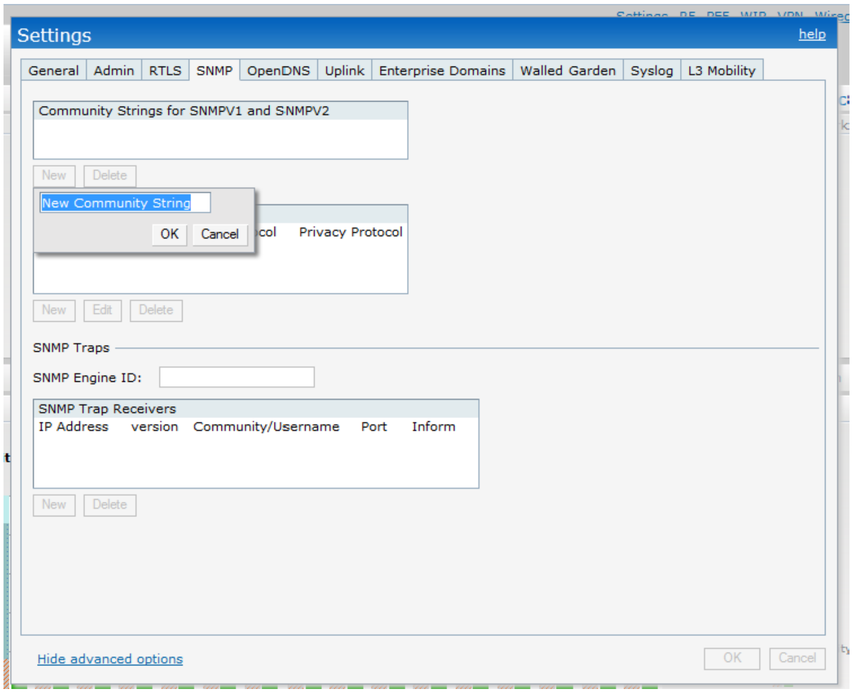
Field	Description
Community Strings for SNMPV1 and SNMPV2	An SNMP Community string is a text string that acts as a password, and is used to authenticate messages sent between the Virtual Controller and the SNMP agent.
If you are using SNMPv3 to obtain values from the Aruba Instant, you can configure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

Follow the steps below to create community strings for SNMPV1 and SNMPV2

1. In the Settings tab, click the **SNMP** tab.
2. Click **New** in the Community Strings for SNMPV1 and SNMPV2 box.
3. Enter the string in the **New Community String** text box.
4. Click **OK.**

To delete a community string, select the string and click **Delete**.

Figure 143 *Creating Community Strings for SNMPV1 and SNMPV2*

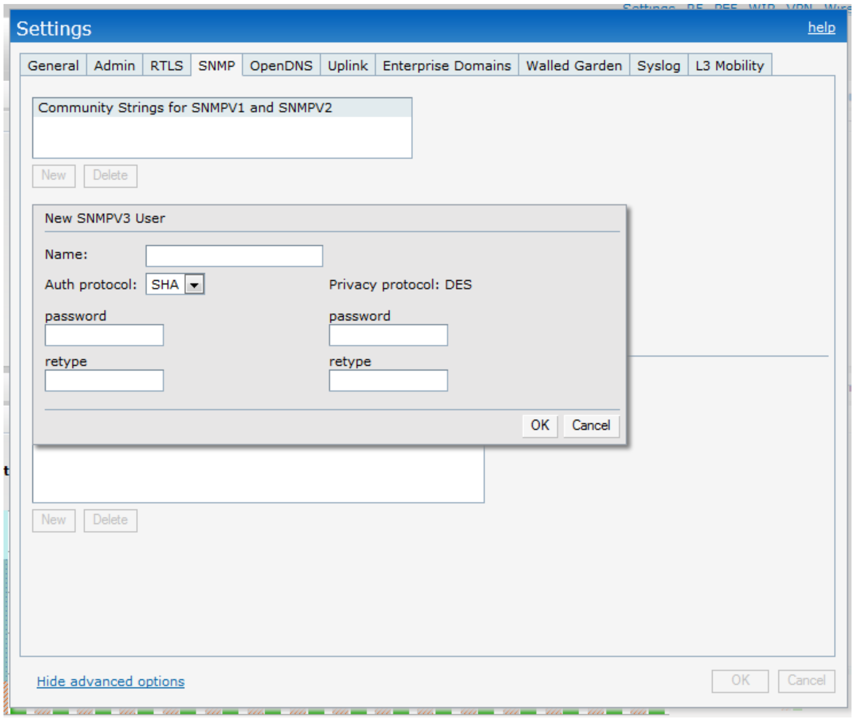


Follow the procedure below to create, edit, and delete users for SNMPV3.

1. In the **Settings** tab, click the **SNMP** tab.
2. Click **New** in the **Users for SNMPV3** box.
3. Enter the name of the user in the **Name** text box.
4. Select the type of authentication protocol from the **Auth protocol** drop-down list.
5. Enter the authentication password in the **Password** tex box and retype the password in the **Retype** tex box.
6. Select the type of privacy protocol from the **Privacy protocol** drop-down list.
7. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box.
8. Click **OK.**

To edit the details for a particular user, select the user and click **Edit**. To delete a particular user, select the user and click **Delete**.

Figure 144 *Creating Users for SNMPV3*



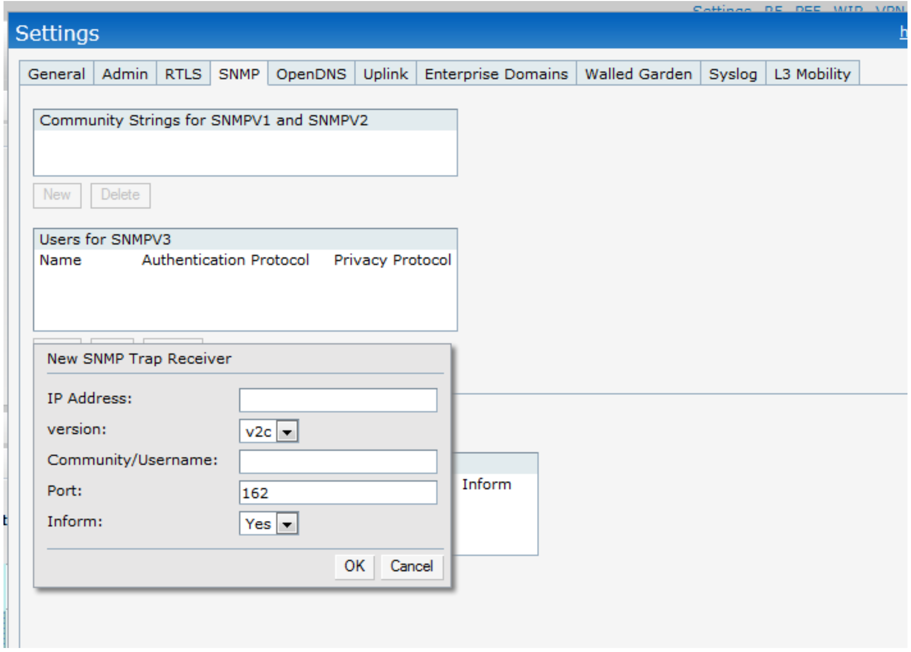
Auth protocol: SHA

Privacy protocol: DES

SNMP Traps

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

Figure 145 *SNMP Traps*



version: v2c

Port: 162

Inform: Yes

To configure an SNMP trap receiver:

1. Enter a name in the **SNMP Engine ID** text box. It indicates the name of the SNMP agent on the access point. SNMPV3 agent has an engine ID that uniquely identifies the agent in the device and is unique to that internal network.
2. Click **New** and update the following fields:

   1. **IP Address—** Enter the **IP Address** of the new SNMP Trap receiver.
   2. **Version—** Select the SNMP version— **v1, v2c, v3** from the drop-down list. The version specifies the format of traps generated by the access point.
   3. **Community/Username—** Specify the community string for SNMPV1 and SNMPV2c traps and a username for SNMPV3 traps.
   4. **Port—** Enter the port to which the traps are sent. The default value is 162.
   5. **Inform—** When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPV3 only. The default value is **Yes**.
3. Click **OK** to view the trap receiver information in the **SNMP Trap Receivers** window.

Aruba-specific management information bases (MIBs) describe the objects that can be managed using SNMP. See the *Aruba Instant 6.1.3.4-3.1.0.0 MIB Reference Guide* for information about the Aruba MIBs and SNMP traps.

Chapter 22

Hierarchical Deployment

In earlier releases of Aruba Instant, an IAP could be connected to another IAP via the uplink port through a wired switch. If there is no wired infrastructure (Ethernet connection with a L3 NAT router), then multiple IAPs could not be deployed.

An IAP-130 series or RAP-3WN AP (with more than one wired port) can now be connected to the downlink wired port of another IAP (ethX). You can provision an IAP with a single Ethernet port (like IAP-90 or IAP-100 series devices) to use enet0_bridging, so that Eth0 is converted do a downlink wired port. In such single Ethernet port platform deployments, the root AP must use the 3G uplink.

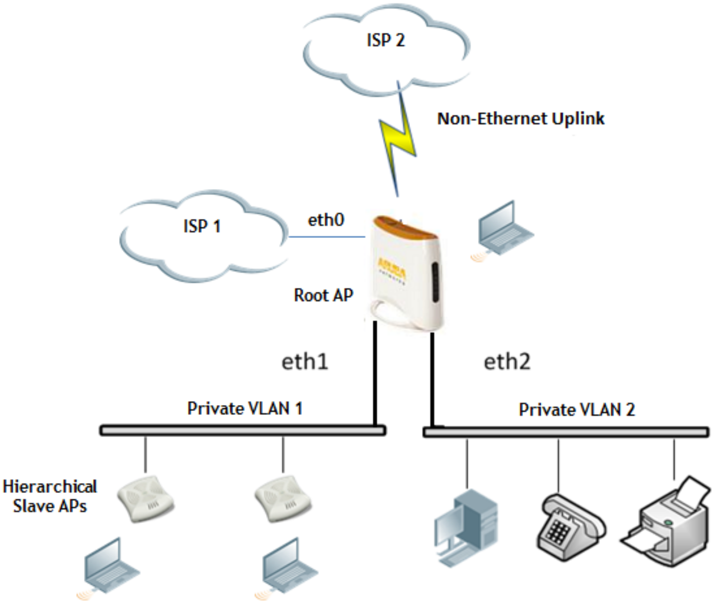
In this release of Aruba Instant, you can form an IAP network by connecting the downlink port of an AP to other APs. Only one AP in the network uses its downlink port to connect to the other APs. This AP (called the root AP) acts as the wired device for the network, provides DHCP service and an L3 connection to the ISP uplink with NAT. The root AP is always the master of the Instant network. On a single Ethernet port platform, you can use enet0_bridging so that Eth0 is converted to a downlink wired port and the root AP must have the 3G uplink configured.

Deployment

A typical hierarchical deployment is comprised of the following:

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

Figure 146 *Hierarchical Deployment*



Ethernet Downlink

Ethernet Downlink Overview

The Ethernet downlink ports allow third party devices such as VoIP phones or printers (which support only wired connections) to connect to the wireless network. Additionally, an Access Control List (ACL) can be configured for added security on the Ethernet downlink.

NOTE

This release of Instant supports only the OpenAuth mechanism.

Ethernet Downlink Profile Parameters

To create a new Ethernet downlink profile:

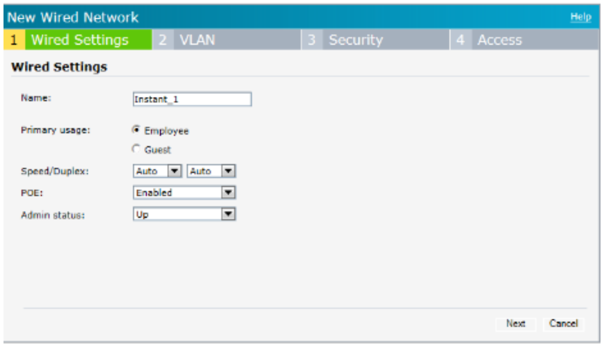
1. Click on the **Wired** link on the top right corner of the Instant UI.
2. Click on the **New** button below the **Wired Networks** window and enter the following information in the **Wired** tab.

Table 31 *Ethernet Downlink Profile Parameters - Wired Tab*

Field	Description
Name	Name of the Ethernet downlink profile.
Primary Usage	● **Employee** — Employee access. ● **Guest**— Guest access.
Speed/Duplex	Only experienced network administrators should change the speed and duplex parameters manually.
POE	When enabled, the system passes electric power along with the data on the Ethernet cable. **NOTE:** The Power Sourcing Equipment (PSE) functionality is available only for the Ethernet port2 on RAP-3WNP.
Admin Status	Displays the status of the admin.

The following figure displays the wired parameters of the Ethernet profile configuration:

Figure 147 *Ethernet Profile Configuration - Wired Tab*



New Wired Network

Wired Settings

Name: Instant_1

Primary usage: ● Employee ○ Guest

Speed/Duplex: Auto Auto

POE: Enabled

Admin status: Up

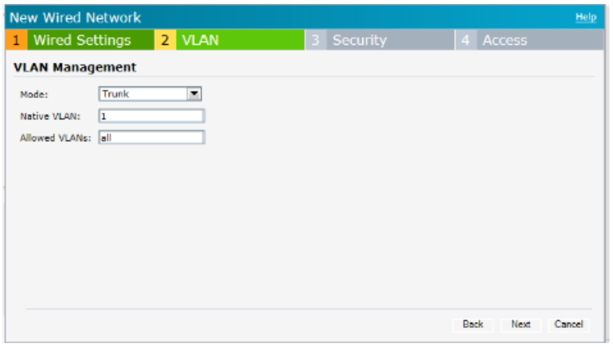
3. Click the **VLAN** tab or click **Next** and enter the following information:

Table 32 *Ethernet Downlink Profile Parameters - VLAN Tab*

Field	Description
Mode	- In **Access mode** the port carries a single VLAN, specified as the Native VLAN. - In **Trunk mode** the port carries packets for multiple VLANs, specified as the Allowed VALN.
Native VLAN	Specifies the VLAN carried by the port in Access mode.
Allowed VLANs	Specifies the VLAN carried by the port in Trunk mode.

The following figure displays the VLAN parameters of the Ethernet profile configuration:

Figure 148 *Ethernet Profile Configuration — VLAN Tab*



VLAN Management

Mode: Trunk

Native VLAN: 1

Allowed VLANs: all

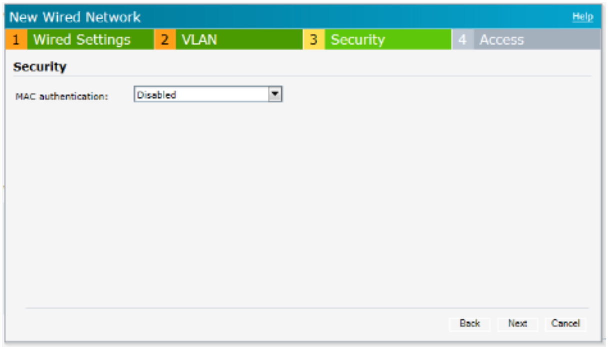
4. Click on **Security** tab or click on **Next** and enter the following information:

Table 33 *Ethernet Downlink Profile Parameters - Security Tab*

Field	Description
MAC authentication	- Disable— Disable MAC Authentication on the profile (default). - Enable— Enable MAC Authentication on the profile.

The following figure displays the security parameters of the Ethernet profile configuration:

Figure 149 *Ethernet Profile Configuration - Security Tab*



Security

MAC authentication: Disabled

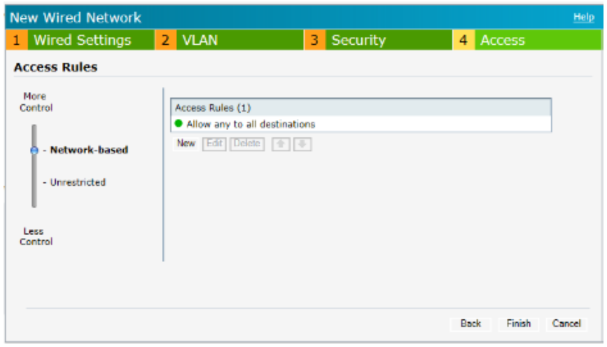
5. Click the **Access** tab and configure the access rule for the profile.

Table 34 *Ethernet Downlink Profile Parameters - Access Tab*

Field	Description
Access Rules	- **Unrestricted**— User gets unrestricted access on the port. - **Network-based**— User is authenticated using the access rules defined here.

The following figure displays the access parameters of the Ethernet profile configuration:

Figure 150 *Ethernet Profile Configuration - Access Tab*



Allow any to all destinations

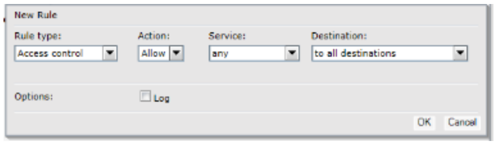
6. Click **New** in the **Access Rules** window to create a new rule and enter the following:

Table 35 *Access Rule Parameters*

Field	Description
Rule type	**Access Control**
Action	- **Allow**— Allow users based on the access rule. - **Deny**— Deny users based on the access rule.
Service	Type of service.
Destination	Specify the destination.
Options	Disable or enable logging.

The following figure displays the parameters of the access rule configuration:

Figure 151 *Access Rule Parameters*



Rule type: Access control

Action: Allow

Service: any

Destination: to all destinations

Options: □ Log

7. Click **Finish** to configure the new network profile.

8. To edit an Ethernet downlink profile, select the configured Ethernet downlink profile and click the **Edit** button below the **Wired Networks** window.

9. To delete an Ethernet downlink profile, select the configured Ethernet downlink profile and click the **Delete** button below the **Wired Networks** window.

Assigning a Profile to the Ethernet Port

You can assign the configured profiles to the Ethernet ports under the **Network Assignments** window.

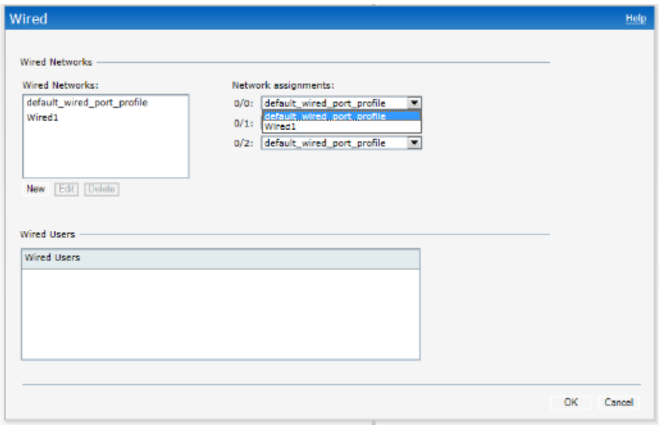
- To assign an Ethernet downlink profile to Ethernet 0 port:
  1. Enable wired bridging on the port. See "Configuring Wired Bridging on Ethernet 0" on page 94.
  2. Select and assign a profile from the **0/0** drop down list.

NOTE

Wired bridging must be enable on Ethernet 0 (0/0) port before you can assign a Ethernet downlink profile.

- To assign an Ethernet downlink profile to Ethernet 1 port, select the profile from the **0/1** drop down list.
- To assign an Ethernet downlink profile to Ethernet 2 port, select the profile from the **0/2** drop down list.

Figure 152 *Assigning a Profile to the Ethernet Ports*



Wired Networks:
default_wired_port_profile
Wired1

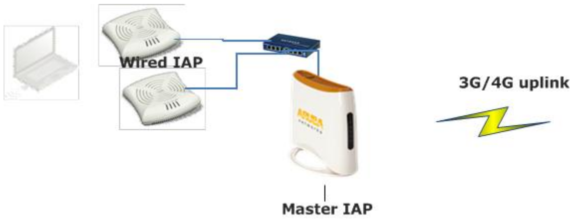
Network assignments:
0/0: default_wired_port_profile
0/1: default_wired_port_profile
Wired1
0/2: default_wired_port_profile

Uplink Configuration Overview

The Aruba Instant network supports Ethernet and 3G/4G USB modems for the corporate Instant network. The 3G/4G USB modems can be used to extend the connectivity to places where an Ethernet uplink cannot be configured, allowing the client traffic to reach the internet and the corporate network. It also provides a reliable backup link for the Ethernet based Instant network.

The following figure describes the IAP when the Ethernet connection is not configurable on an IAP network. The other IAPs also join the Virtual Controller as slave IAPs via a wired uplink.

Figure 153 *Uplink Types*



The following types of uplinks are supported on Instant:

- Ethernet
  - PPPoE
  - DHCP
  - Static IP
- 3G/4G LTE modem

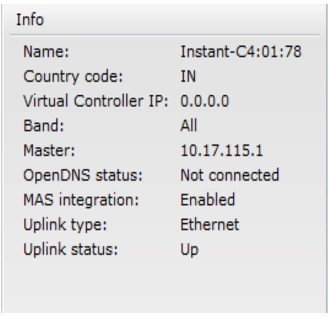
Ethernet Uplink

The Ethernet 0 port on an IAP is enabled as an uplink port by default.

NOTE: Instant does not support configuration of an Eth0 uplink.

View the type of uplink and the status of the uplink in the Instant UI in the **Info** tab.

Figure 154 *Uplink Status*



Info

Name:	Instant-C4:01:78
Country code:	IN
Virtual Controller IP:	0.0.0.0
Band:	All
Master:	10.17.115.1
OpenDNS status:	Not connected
MAS integration:	Enabled
Uplink type:	Ethernet
Uplink status:	Up

3G/4G Uplink

Instant now supports the use of 3G/4G USB modems to provide internet backhaul to an Instant network. The 3G/4G USB modems extend client connectivity to places where an Ethernet uplink is not feasible. This enables the RAP-3 to choose the available network in an area automatically. For 4G LTE modem, 4G takes precedence over 3G when the RAP-3 tries to auto-select the network

NOTE

The 3G and 4G LTE USB modems can be provisioned only on RAP-3.

Types of Modems

Instant supports the following three types of 3G modems:

- **True Auto Detect**— Modems of this type can be used only in one country and for a specific ISP. The parameters are configured automatically and hence no configuration is necessary (Plug and Play).
- **Auto-detect + ISP/country**— Modems of this type require the user to specify the Country and ISP. The same modem is used for different ISPs with different parameters configured for each of them.
- **No Auto-detect**—Modems of this type are used where the modems share the same Device-ID, Country, and ISP, but need to configure different parameters for each of them. These modems work with Instant provided the correct parameters are configured. All the new auto-detected modems falls under this category as the parameter necessary to automatically configure them are unknown.

The following table lists the types of supported 3G modems:

Table 36 *List of Supported 3G Modems*

Modem Type	Supported 3G Modems
True Auto Detect	● USBConnect 881 (Sierra 881U) ● Quicksilver (Globetrotter ICON 322) ● UM100C (UTstarcom) ● Icon 452 ● Aircard 250U (Sierra) ● USB 598 (Sierra) ● U300 (Franklin wireless) ● U301 (Franklin wireless) ● USB U760 for Virgin (Novatel) ● USB U720 (Novatel/Qualcomm) ● UM175 (Pantech) ● UM150 (Pantech) ● UMW190(Pantech) ● SXC-1080 (Qualcomm) ● Globetrotter ICON 225 ● UMG181 ● NTT DoCoMo L-05A (LG FOMA L05A) ● NTT DoCoMo L-02A ● ZTE WCDMA Technologies MSM (MF668?) ● Fivespot (ZTE) ● c-motech CNU-600 ● ZTE AC2736 ● SEC-8089 (EpiValley) ● Nokia CS-10 ● NTT DoCoMo L-08C (LG) ● NTT DoCoMo L-02C (LG) ● Novatel MC545 ● Huawei E220 for Movistar in Spain ● Huawei E180 for Movistar in Spain ● ZTE-MF820 ● Huawei E173s-1 ● Sierra 320 ● Longcheer WM72 ● U600 (3G mode)

Table 36 *List of Supported 3G Modems (Continued)*

Modem Type	Supported 3G Modems
Auto-detect + ISP/country	- Sierra USB-306 (HK CLS/1010 (HK)) - Sierra 306/308 (Telstra (Aus)) - Sierra 503 PCIe (Telstra (Aus)) - Sierra 312(Telstra (Aus)) - Aircard USB 308 (AT&T's Shockwave) - Compass 597(Sierra) (Sprint) - U597 (Sierra) (Verizon) - Tstick C597(Sierra) (Telecom(NZ)) - Ovation U727 (Novatel) (Sprint) - USB U727 (Novatel) (Verizon) - USB U760 (Novatel) (Sprint) - USB U760 (Novatel) (Verizon) - Novatel MiFi 2200 (Verizon Mifi 2200) - Huawei E272, E170, E220 (ATT) - Huawei E169, E180,E220,E272 (Vodafone/SmarTone (HK)) - Huawei E160 (O2(UK)) - Huawei E160 (SFR (France)) - Huawei E220 (NZ and JP) - Huawei E176G (Telstra (Aus)) - Huawei E1553, E176 (3/HUTCH (Aus)) - Huawei K4505 (Vodafone/SmarTone (HK)) - Huawei K4505 (Vodafone (UK)) - ZTE MF656 (Netcom (norway)) - ZTE MF636 (HK CSL/1010) - ZTE MF633/MF636 (Telstra (Aus)) - ZTE MF637 (Orange in Israel) - Huawei E180, E1692,E1762 (Optus (Aus)) - Huawei E1731 (Airtel-3G (India)) - Huawei E3765 (Vodafone (Aus)) - Huawei E3765 (T-Mobile (Germany) - Huawei E1552 (SingTel) - Huawei E1750 (T-Mobile (Germany)) - UGM 1831 (TMobile) - Huawei D33HW (EMOBILE(Japan)) - Huawei GD01 (EMOBILE(Japan)) - Huawei EC150 (Reliance NetConnect+ (India)) - KDDI DATA07(Huawei) (KDDI (Japan)) - Huawei E353 (China Unicom) - Huawei EC167 (China Telecom) - Huawei E367 (Vodafone (UK)) - Huawei E352s-5 (T-Mobile (Germany))
No auto-detect	- Huawei D41HW - ZTE AC2726

Provisioning 3G/4G Uplink Manually

To provision a 3G/4G uplink manually, configure the modem parameters. The IAP has to be rebooted if you configure USB modem parameter from the Instant WebUI.

Use the following procedure to provision 3G/4G uplink manually:

1. In the **settings** tab, click the **show advanced settings** hyperlink.

2. Select the **Uplink** tab. Under **3G/4G** tab, enter the parameters:

a. Enter the type of the 3G/4G modem driver type:
   - To provision 3G modem, enter the type of 3G modem in the **USB type** text box
   - To provision 4G modem, enter the type of 4G modem in the **4G USB type** text box

NOTE

This release of Instant supports only the Pantech UML 290 4G card and is a True Auto Detect modem.

b. Enter the identifier of the modem device in the **USB dev** text box.

c. Enter the TTY port of the modem in the **USB tty** text box.

d. Enter the parameter to initialize the modem in the **USB init** text box.

e. Enter the parameter to dial the cell tower in the **USB dial** text box.

f. Enter the username used to dial the ISP in the **USB user** text box.

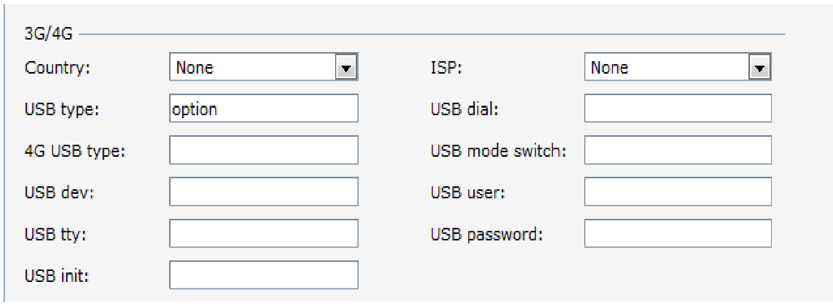
g. Enter the password used to dial the ISP in the **USB password** text box.

h. Enter the parameter used to switch modem from storage mode to modem mode in the **USB switch mode** text box.

NOTE

The parameter details are available from the manufacturer of your modem or from your IT administrator.

Figure 155 *Provisioning 3G/4G Uplink— Manually*



3G/4G

Country:	None	ISP:	None
USB type:	option	USB dial:	
4G USB type:		USB mode switch:	
USB dev:		USB user:	
USB tty:		USB password:	
USB init:			

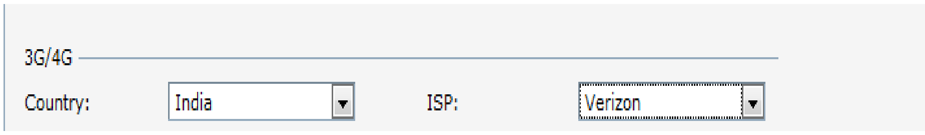
NOTE

You must reboot the IAP after manually provisioning the IAP.

Provisioning 3G Uplink Automatically

To provision a 3G uplink automatically, select only the **Country** and **ISP**. The IAP finds the parameters automatically.

Figure 156 *Provisioning 3G Uplink— Automatically*



3G/4G

Country:	India	ISP:	Verizon

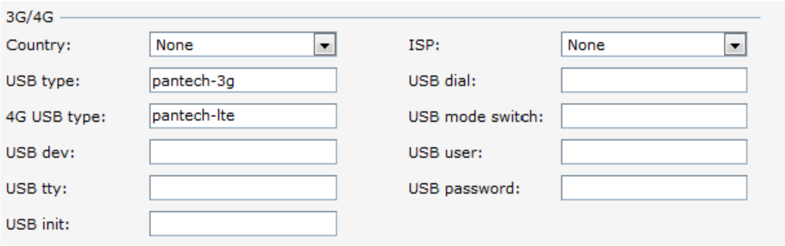
NOTE

In the Instant UI, you can view the list of country or ISP in the country and ISP drop-down lists. You can either use the country or ISP to configure the modem, or configure the individual modem parameters manually. If you cannot view the list of country or ISP from the drop-down list, then configure the modem parameters manually.

Provisioning a 3G/4G Switch Network

To provision a 3G/4G switch network, provide the driver type for the 3G modem in the **USB type** text box and the driver type for 4G modem in the **4G USB type** text box and click **OK**.

Figure 157 *3G/4G Switch Network*



3G/4G

Country:	None	ISP:	None
USB type:	pantech-3g	USB dial:	
4G USB type:	pantech-lte	USB mode switch:	
USB dev:		USB user:	
USB tty:		USB password:	
USB init:			

Uplink Switchover

The default priority for uplink switchover is Ethernet and then 3G/4G. The IAP has the ability to switch to the lower priority uplink if the current uplink is down.

NOTE

An IAP reboot is not required for uplink switchover process.

NOTE

If VPN is configured, IAP monitors the VPN status, once VPN status is down for 3 minutes, the uplink switches over (if low priority uplink is detected, and the uplink preference is none).

Uplink Switching based on VPN Status

Instant supports switching uplinks based on the VPN status when deploying mixed uplinks (Eth0, 3G/4G). When VPN is used with multiple backhaul options, the IAP switches to an uplink connection based on the VPN connection status instead of only using Eth0, the physical backhaul link. The behavior of the uplink switching is described as follows:

- If the current uplink is Eth0, this uplink is used until the VPN connection is down. When the VPN connection is down at which point a different uplink (3G) is selected.
- If the current uplink is 3G, and Eth0 has a physical link, the IAP periodically suspends user traffic to try and connect to the VPN on the Eth0. If the IAP succeeds, then the IAP switches to Eth0. If the IAP does not succeed, then the IAP restores the VPN connection to the current uplink.

NOTE

This feature is automatically enabled when a VPN is configured in the IAP.

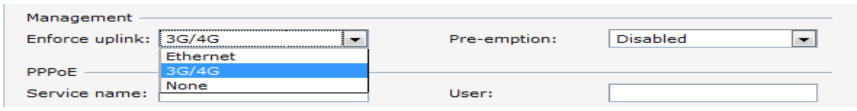
Uplink Preemption

With this feature, the IAP tries to get a higher priority link every ten minutes even if the current uplink is up. This does not affect the current uplink connection. If the higher uplink is usable the IAP switches over to that uplink. Preemption is enabled by default and the user can disable it by configuration.

Uplink Preference

Select the type of uplink from the **uplink preference** drop-down list under **Management.** To use a 3G/4G uplink, select **3G/4G** from the **Uplink preference** drop-down list.

Figure 158 *Uplink Preference*



Management

Enforce uplink: 3G/4G

Pre-emption: Disabled

PPPoE

Service name:

User:

NOTE

Uplink preferences can be set manually. This forces the IAP to use that uplink. Switchover and preemption do not work in this configuration.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a method of connecting to the internet typically used with DSL services where the client connects to the DSL modem. You can use PPPoE for your uplink connectivity in both normal IAP and VPN IAP deployments. PPPoE is supported only in a single AP deployment.

NOTE

Uplink redundancy with the PPPoE link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. Once the PPPoE settings are configured, PPPoE has the highest priority for the uplink. The IAP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP). Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After you configure PPPoE, you have to reboot the IAP for the configuration to take effect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during bootup and if found incorrect, Ethernet is used for the uplink connection.

NOTE

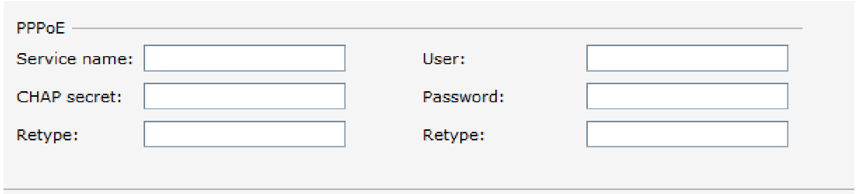
When you use PPPoE, do not configure the IP address of the Virtual Controller.
When you use PPPoE, do not use Dynamic RADIUS Proxy.
An SSID created with default VLAN is not supported with PPPoE.

Configuring PPPoE

To configure the PPPOE settings:

1. Click the **Settings** link at the upper right corner of the Instant WebUI.
2. Click the **Show advanced options** link.
3. In the **Uplink** tab, perform the following steps in the **PPPoE** section:
    a. Enter the **PPPoE service name** provided to you by your service provider in the **Service name** field.
    b. In the **CHAP secret** and **Retype** fields, enter the CHAP secret and confirm it.
    c. Enter the user name for the PPPoE connection in the **User** field.
    d. In the **Password** and **Retype** fields, enter the PPPoE password and confirm it.
4. Click **OK**.
5. Reboot the IAP for the configuration to take effect.

Figure 159 *PPPoE Settings*



PPPoE

Service name:		User:	
CHAP secret:		Password:	
Retype:		Retype:	

Chapter 25

AirWave Integration and Management

AirWave is a powerful and easy-to-use network operations system that manages Aruba wireless, wired, and remote access networks, as well as wired and wireless infrastructures from a wide range of third-party manufacturers. With its easy-to-use interface, AirWave provides real-time monitoring, proactive alerts, historical reporting, and fast, efficient troubleshooting. It also offers tools that manage RF coverage, strengthen wireless security, and demonstrate regulatory compliance.

Aruba IAPs communicate with AirWave using the HTTPS protocol. This allows an AirWave server to be deployed in the cloud across a NAT device, such as a router.

AirWave Features

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

Image Management

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

The following models can be used to upgrade the firmware:

- Automatic— In this model, the Virtual Controller (VC) periodically checks for newer updates from a configured URL and automatically initiates upgrade of the network.
- Manual— In this model, the user can manually start a firmware upgrade on a VC-by-VC basis or set the desired firmware preference per group of devices.

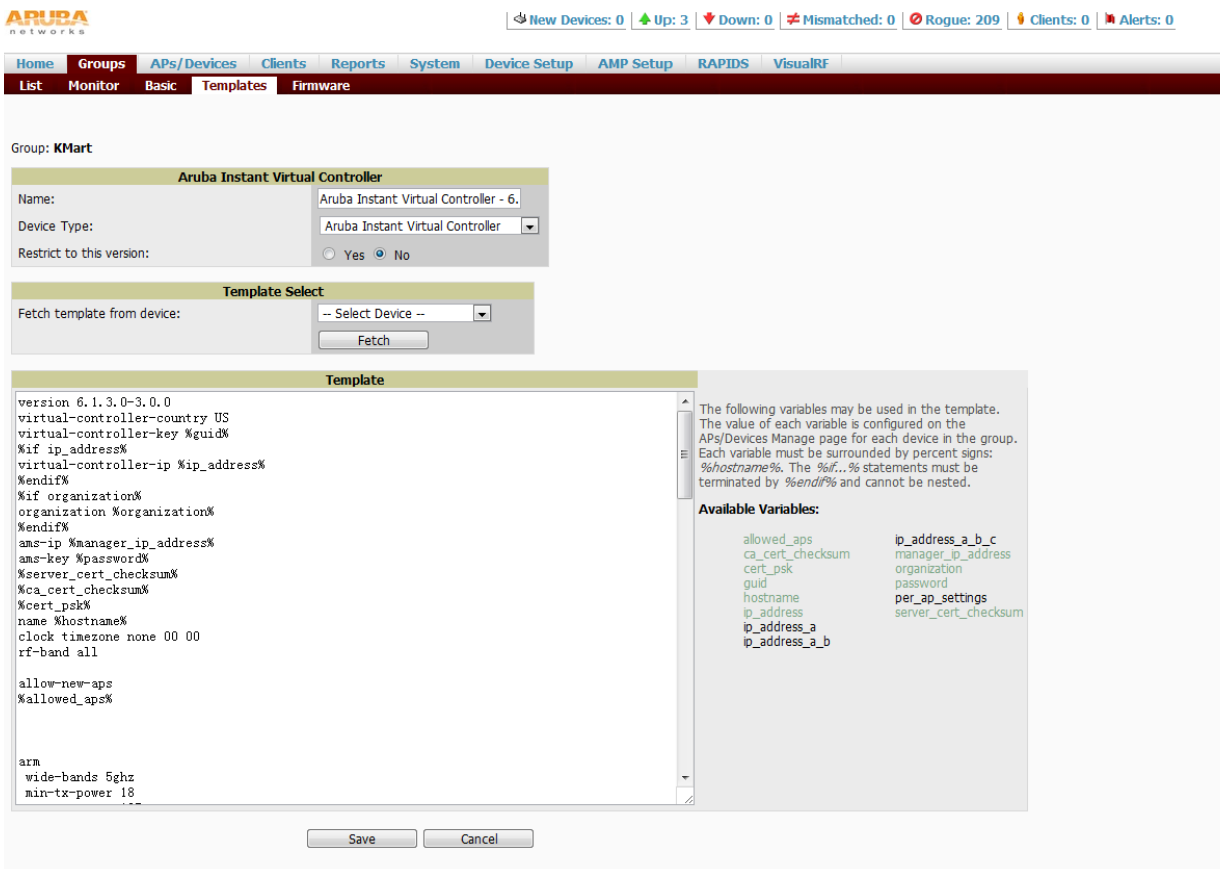
IAP and Client Monitoring

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

Template-based Configuration

AirWave automatically creates a configuration template based on any of the existing IAPs, and it applies that template across the network as shown in Figure 160. It audits every device on an ongoing basis to ensure that configurations never vary from the enterprise policies. It alerts you whenever a violation is detected and automatically repairs the misconfigured device.

Figure 160 *Template-based Configuration*



Group: **KMart**

Aruba Instant Virtual Controller

Name:	Aruba Instant Virtual Controller - 6.
Device Type:	Aruba Instant Virtual Controller
Restrict to this version:	○ Yes ● No

Template Select

Fetch template from device: -- Select Device --

Template

```
version 6.1.3.0-3.0.0
virtual-controller-country US
virtual-controller-key %guid%
%if ip_address%
virtual-controller-ip %ip_address%
%endif%
%if organization%
organization %organization%
%endif%
ams-ip %manager_ip_address%
ams-key %password%
%server_cert_checksum%
%ca_cert_checksum%
%cert_psk%
name %hostname%
clock timezone none 00 00
rf-band all

allow-new-aps
%allowed_aps%



arm
 wide-bands 5ghz
 min-tx-power 18
```

The following variables may be used in the template. The value of each variable is configured on the APs/Devices Manage page for each device in the group. Each variable must be surrounded by percent signs: *%hostname%*. The *%if...%* statements must be terminated by *%endif%* and cannot be nested.

Available Variables:

allowed_aps
ca_cert_checksum
cert_psk
guid
hostname
ip_address
ip_address_a
ip_address_a_b
ip_address_a_b_c
manager_ip_address
organization
password
per_ap_settings
server_cert_checksum

Trending Reports

AirWave saves up to 14 months of actionable information, including network performance data and user roaming patterns, so you can analyze how network usage and performance trends have changed over time. It also provides detailed capacity reports with which you can plan the capacity and appropriate strategies for your organization.

Intrusion Detection System

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

Wireless Intrusion Detection System (WIDS) Event Reporting to AirWave

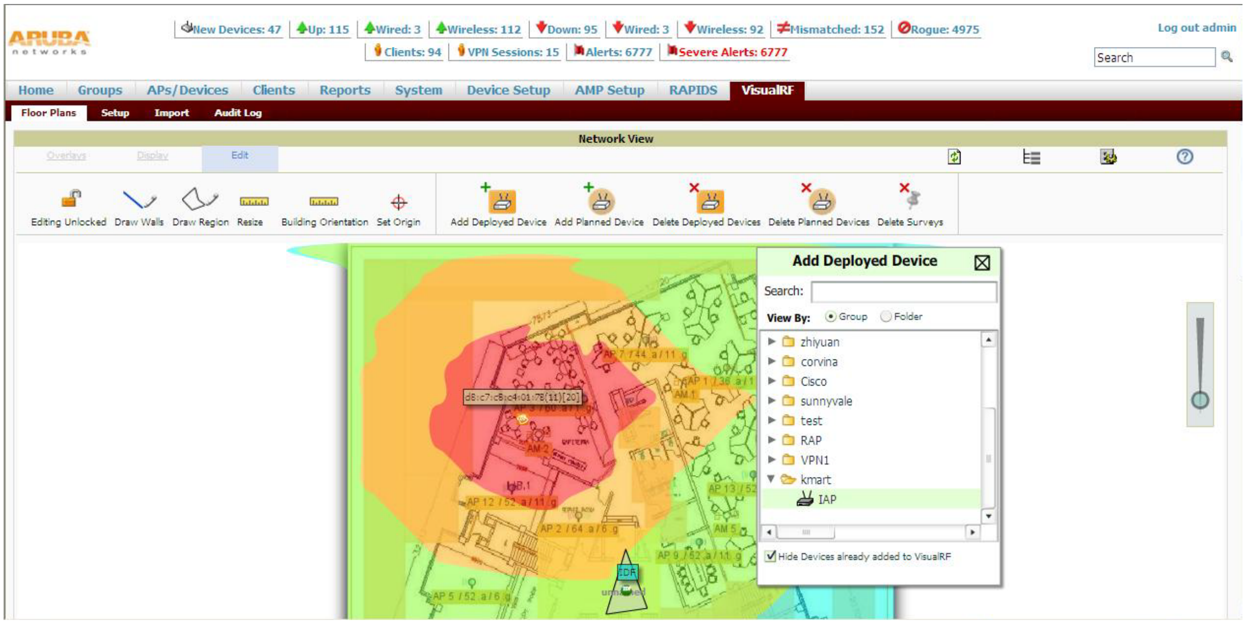
AirWave supports Wireless Intrusion Detection System(WIDS) Event Reporting, which is provided by Aruba Instant. This includes WIDS classification integration with the RAPIDS (Rogue Access Point Detection Software) module. RAPIDS is a powerful and easy-to-use tool for automatic detection of unauthorized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

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

RF Visualization Support for Aruba Instant

AirWave supports RF visualization for Aruba Instant. The VisualRF module provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. VisualRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every Instant device in range. VisualRF provides graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network.

Figure 161 *Adding an IAP in VisualRF*



Configuring AirWave

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

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

Creating your Organization String

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

- AMP Role— "Org Admin" (initially disabled)
- AMP User— "Org Admin" (assigned to the role "Org Admin")
- Folder— "Org" (under the Top folder in AMP)
- Configuration Group— "Org"

Additional strings in the Organization String are used to create a hierarchy of sub folders under the folder named "Org":

- subfolder1 would be a folder under the "Org" folder
- subfolder2 would be a folder under subfolder1

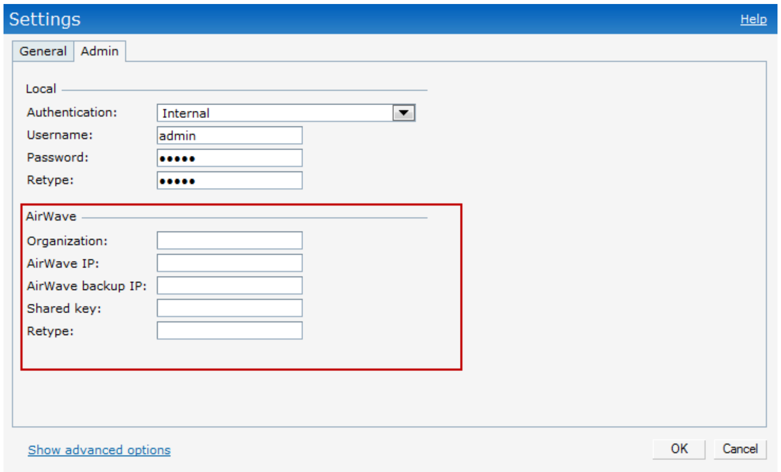
About Shared Key

The Shared Secret key is used by the administrator to manually authorize the first Virtual Controller for an organization. Any string is acceptable.

Entering the Organization String and AMP Information into the IAP

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

Figure 162 *Configuring AirWave*



Authentication: Internal

Username: admin

Password: •••••

Retype: •••••

2. Enter the name of your organization in the **Organization** name text box. This name automatically appears in AirWave under Groups list.
3. Enter the IP address of the AirWave server in the **AirWave IP** text box.
4. Enter the IP address of a backup AirWave server in the **AirWave backup IP** text box. The backup server provides connectivity when the primary server is down. If the IAP cannot send data to the primary server, the Virtual Controller switches to the backup server automatically.
5. Enter the shared key in the **Shared key** text box and reconfirm. This shared key is used for configuring the first AP in the Aruba Instant network.
6. Click **OK**.

AirWave Discovery through DHCP Option

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

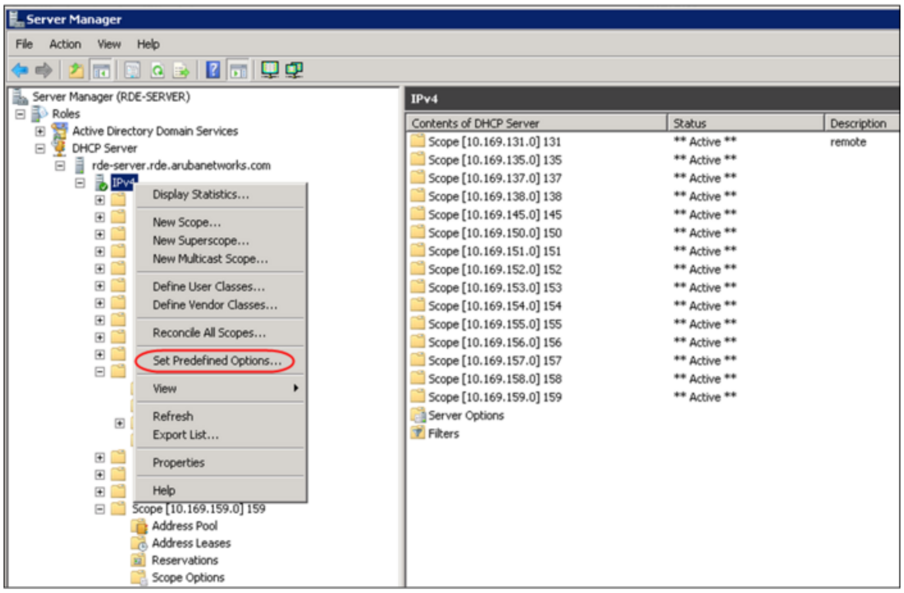
On the DHCP server, the format for option 60 is "**ArubaInstantAP**", and the format for option 43 is "**ams-ip,ams-key**".

Standard DHCP option 60 and 43 on Windows Server 2008

In networks that are not using DHCP option 60 and 43, it is easy to use the standard DHCP options 60 and 43 for Aruba AP or Aruba Instant AP. For Aruba APs these options can be used to indicate the, master controller or the local controller. For IAP, this can be used to define the AirWave IP, group and password.

1. From a server running Windows Server 2008 navigate to **Server Manager > Roles > DHCP sever >** domain **DHCP Server** (rde-server.rde.arubanetworks.com) **> IPv4**
2. Right click on **IPv4** and select **Set Predefined Options.**

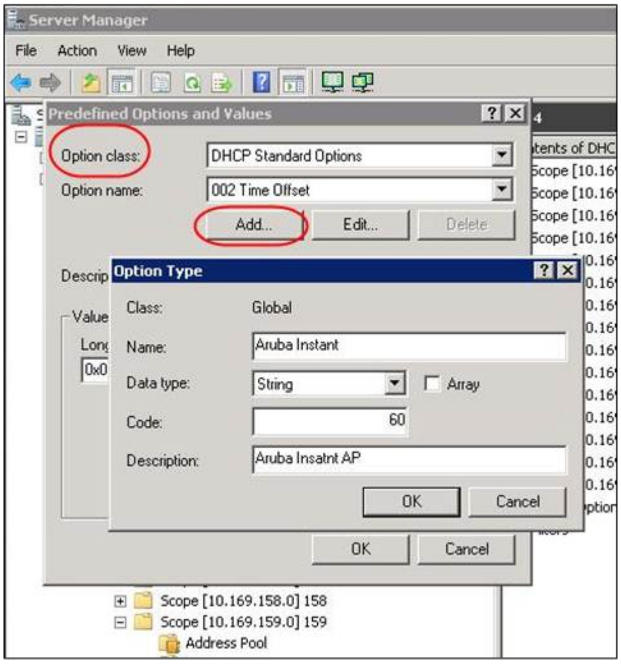
Figure 163 *Instant and DHCP options for AirWave— Set Predefined Options*



Contents of DHCP Server	Status	Description
Scope [10.169.131.0] 131	** Active **	remote
Scope [10.169.135.0] 135	** Active **	
Scope [10.169.137.0] 137	** Active **	
Scope [10.169.138.0] 138	** Active **	
Scope [10.169.145.0] 145	** Active **	
Scope [10.169.150.0] 150	** Active **	
Scope [10.169.151.0] 151	** Active **	
Scope [10.169.152.0] 152	** Active **	
Scope [10.169.153.0] 153	** Active **	
Scope [10.169.154.0] 154	** Active **	
Scope [10.169.155.0] 155	** Active **	
Scope [10.169.156.0] 156	** Active **	
Scope [10.169.157.0] 157	** Active **	
Scope [10.169.158.0] 158	** Active **	
Scope [10.169.159.0] 159	** Active **	
Server Options		
Filters		

3. Select **DHCP Standard Options** in the **Option class** drop-down list and then click **Add.** Enter the following information:
   - Name— Aruba Instant
   - Data Type— String
   - Code— 60
   - Description— Aruba Instant AP

Figure 164 *Instant and DHCP options for AirWave— Predefined Options and Values*

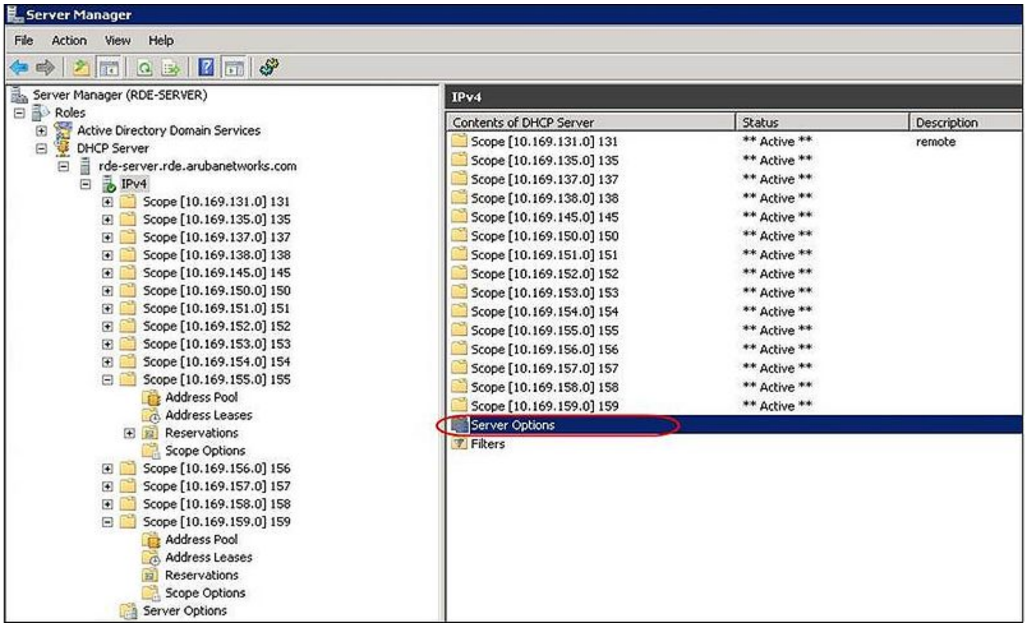


Option class: DHCP Standard Options
Option name: 002 Time Offset

Class: Global
Name: Aruba Instant
Data type: String □ Array
Code: 60
Description: Aruba Insatnt AP

4. Navigate to **Server Manager** and select **Server Options** in the **IPv4** window. (This sets the value globally. Use options on a per-scope basis to override the global options.)
5. Right click on **Server Options** and select the configuration options.

Figure 165 *Instant and DHCP options for AirWave— Server Options*



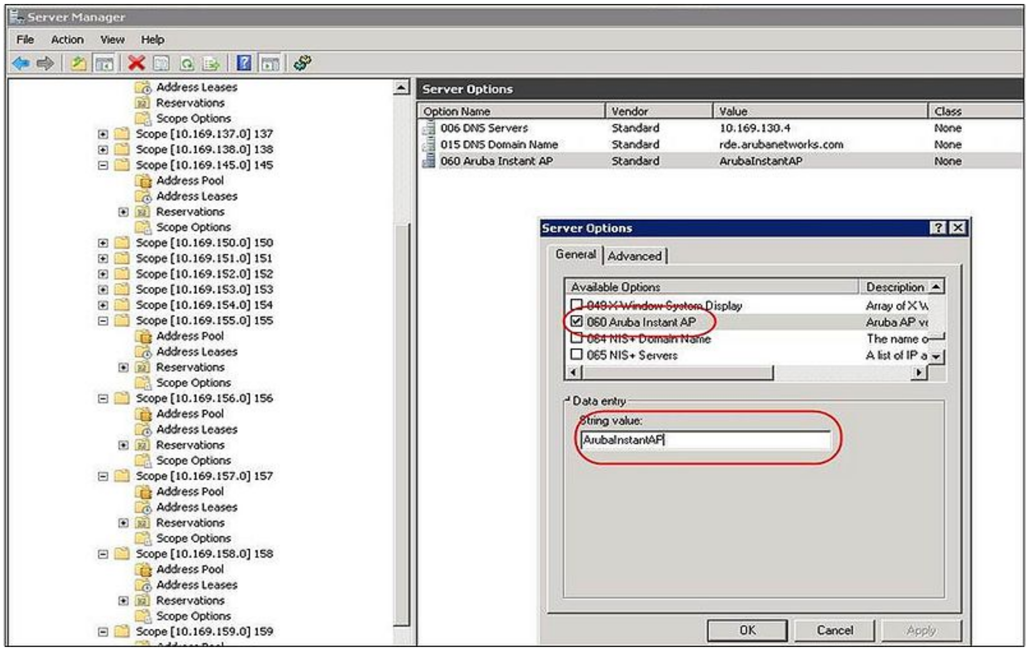
Server Manager (RDE-SERVER)
- Roles
  - Active Directory Domain Services
  - DHCP Server
    - rde-server.rde.arubanetworks.com
      - IPv4
        - Scope [10.169.131.0] 131
        - Scope [10.169.135.0] 135
        - Scope [10.169.137.0] 137
        - Scope [10.169.138.0] 138
        - Scope [10.169.145.0] 145
        - Scope [10.169.150.0] 150
        - Scope [10.169.151.0] 151
        - Scope [10.169.152.0] 152
        - Scope [10.169.153.0] 153
        - Scope [10.169.154.0] 154
        - Scope [10.169.155.0] 155
          - Address Pool
          - Address Leases
          - Reservations
          - Scope Options
        - Scope [10.169.156.0] 156
        - Scope [10.169.157.0] 157
        - Scope [10.169.158.0] 158
        - Scope [10.169.159.0] 159
          - Address Pool
          - Address Leases
          - Reservations
          - Scope Options
        - Server Options

IPv4

Contents of DHCP Server	Status	Description
Scope [10.169.131.0] 131	** Active **	remote
Scope [10.169.135.0] 135	** Active **	
Scope [10.169.137.0] 137	** Active **	
Scope [10.169.138.0] 138	** Active **	
Scope [10.169.145.0] 145	** Active **	
Scope [10.169.150.0] 150	** Active **	
Scope [10.169.151.0] 151	** Active **	
Scope [10.169.152.0] 152	** Active **	
Scope [10.169.153.0] 153	** Active **	
Scope [10.169.154.0] 154	** Active **	
Scope [10.169.155.0] 155	** Active **	
Scope [10.169.156.0] 156	** Active **	
Scope [10.169.157.0] 157	** Active **	
Scope [10.169.158.0] 158	** Active **	
Scope [10.169.159.0] 159	** Active **	
Server Options		
Filters		

6. Select **060 Aruba Instant AP** in the **Server Options** window and enter **ArubaInstantAP** in the String Value.

Figure 166 *Instant and DHCP options for AirWave—060 Aruba Instant AP in Server Options*



- Address Leases
- Reservations
- Scope Options
- Scope [10.169.137.0] 137
- Scope [10.169.138.0] 138
- Scope [10.169.145.0] 145
  - Address Pool
  - Address Leases
  - Reservations
  - Scope Options
- Scope [10.169.150.0] 150
- Scope [10.169.151.0] 151
- Scope [10.169.152.0] 152
- Scope [10.169.153.0] 153
- Scope [10.169.154.0] 154
- Scope [10.169.155.0] 155
  - Address Pool
  - Address Leases
  - Reservations
  - Scope Options
- Scope [10.169.156.0] 156
  - Address Pool
  - Address Leases
  - Reservations
  - Scope Options
- Scope [10.169.157.0] 157
  - Address Pool
  - Address Leases
  - Reservations
  - Scope Options
- Scope [10.169.158.0] 158
  - Address Pool
  - Address Leases
  - Reservations
  - Scope Options
- Scope [10.169.159.0] 159

Server Options

Option Name	Vendor	Value	Class
006 DNS Servers	Standard	10.169.130.4	None
015 DNS Domain Name	Standard	rde.arubanetworks.com	None
060 Aruba Instant AP	Standard	ArubaInstantAP	None

Server Options

General | Advanced

Available Options	Description
□ ~~049 X Window System~~ Display	Array of X W
☑ 060 Aruba Instant AP	Aruba AP vc
□ ~~064 NIS+ Domain Name~~	The name o
□ 065 NIS+ Servers	A list of IP a

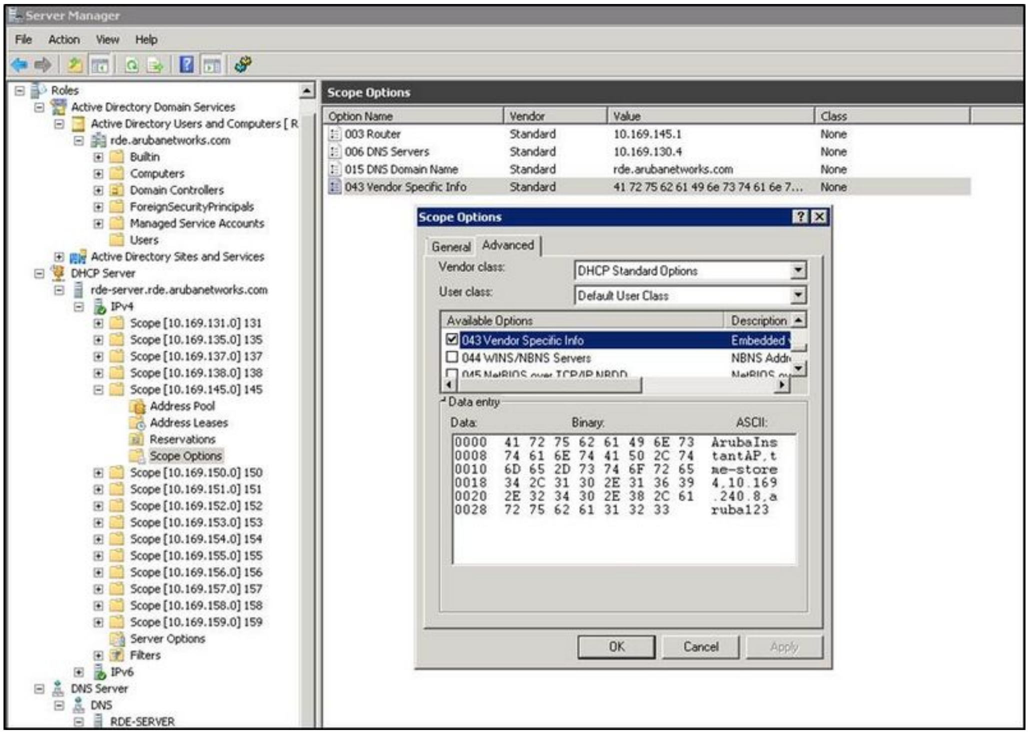
Data entry

String value:

ArubaInstantAP

7. Select **043 Vendor Specific Info** and enter a value for **airwave-orgn, airwave-ip, airwave-key** in the ASCII field (for example: tme-instant-store1,10.169.240.8,aruba123).

Figure 167 *Instant and DHCP options for AirWave— 043 Vendor Specific Info*



Scope Options

Option Name	Vendor	Value	Class
003 Router	Standard	10.169.145.1	None
006 DNS Servers	Standard	10.169.130.4	None
015 DNS Domain Name	Standard	rde.arubanetworks.com	None
043 Vendor Specific Info	Standard	41 72 75 62 61 49 6e 73 74 61 6e 7...	None

Vendor class: DHCP Standard Options

User class: Default User Class

Available Options	Description
☑ 043 Vendor Specific Info	Embedded v
□ 044 WINS/NBNS Servers	NBNS Addr
□ 045 NetBIOS over TCP/IP NBDD	NetBIOS ov

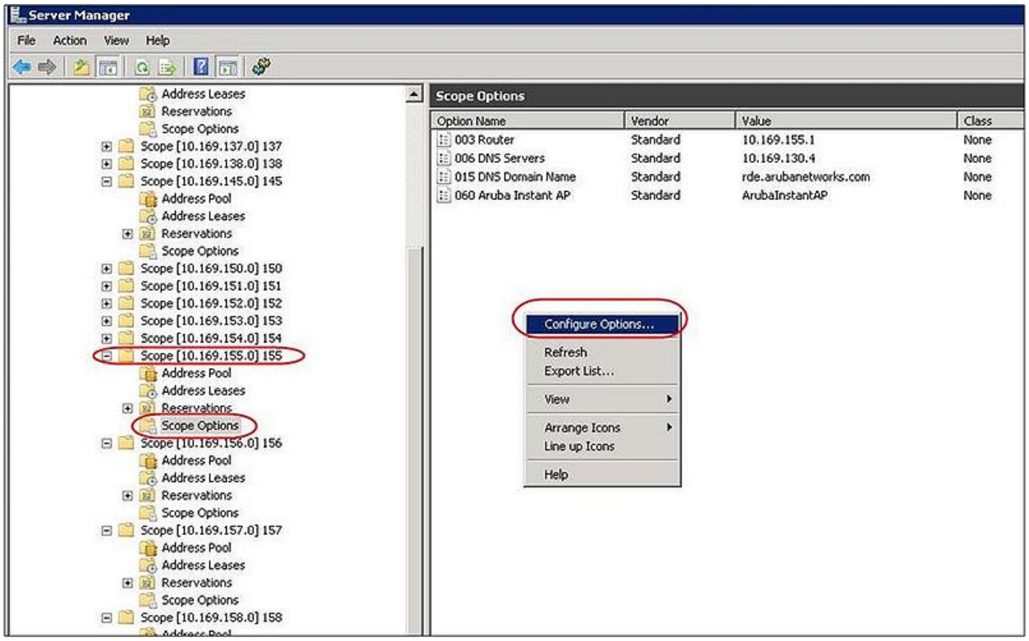
Data entry

Data: Binary: ASCII:

```
0000  41 72 75 62 61 49 6E 73  ArubaIns
0008  74 61 6E 74 41 50 2C 74  tantAP,t
0010  6D 65 2D 73 74 6F 72 65  me-store
0018  34 2C 31 30 2E 31 36 39  4,10.169
0020  2E 32 34 30 2E 38 2C 61  .240.8,a
0028  72 75 62 61 31 32 33     ruba123
```

This creates a DHCP option 60 and 43 on a global basis. You can do the same on a per-scope basis. The per-scope option overrides the global option.

Figure 168 *Instant and DHCP options for AirWave— Scope Options*



Scope Options

Option Name	Vendor	Value	Class
003 Router	Standard	10.169.155.1	None
006 DNS Servers	Standard	10.169.130.4	None
015 DNS Domain Name	Standard	rde.arubanetworks.com	None
060 Aruba Instant AP	Standard	ArubaInstantAP	None

Alternate Method for Defining Vendor-Specific DHCP Options

This section describes how to add vendor-specific DHCP options for Aruba Instant APs in a network that already uses DHCP options 60 and 43 for other services. Some networks use DHCP standard options 60 and 43 to give the DHCP clients info about certain services such as PXE to the DHCP clients. In such an environment, it is not possible to use the standard DHCP options 60 and 43 for Aruba APs.

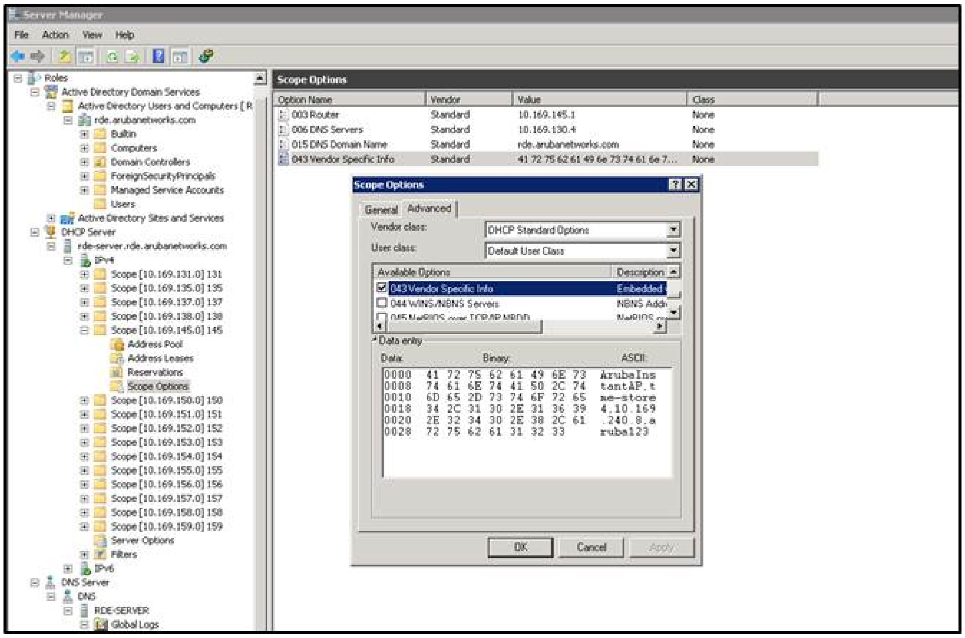
This method describes how to set up a DHCP server to send option 43 with AirWave information to Aruba Instant IAP. This section assumes that option 43 is sent per scope because option 60 is being shared by other devices as well.

NOTE

This scope should be specific to Instant, and the PXE devices that use options 60 and 43 should not connect to the subnet defined by this scope. This is because you can specify only one option 43 for a scope, and if other devices that use option 43 connect to this subnet, they are presented with Instant-specific information.

1. In server 2008, navigate to **Server Manager > Roles > DHCP Server > Domain DHCP Server** (rde-server.rde.arubanetworks.com) **> IPv4**.
2. Select a scope (subnet). Scope (10.169.145.0)145 is selected in the example shown in Figure below.
3. Right click and select **Advanced,** and then specify the following options:
   - Vendor class— DHCP Standard Options
   - User class— Default User Class
   - Available options— Select 043 Vendor-Specific Info
   - String Value— ArubaInstantAP, tme-store4, 10.169.240.8, aruba123 (which is the AP description, organization string, AirWave IP address, Pre-shared key for AirWave)

Figure 169 *Vendor Specific DHCP options*



Scope Options

Option Name	Vendor	Value	Class
003 Router	Standard	10.169.145.1	None
006 DNS Servers	Standard	10.169.130.4	None
015 DNS Domain Name	Standard	rde.arubanetworks.com	None
043 Vendor Specific Info	Standard	41 72 75 62 61 49 6e 73 74 61 6e 7...	None

Scope Options

Vendor class: DHCP Standard Options

User class: Default User Class

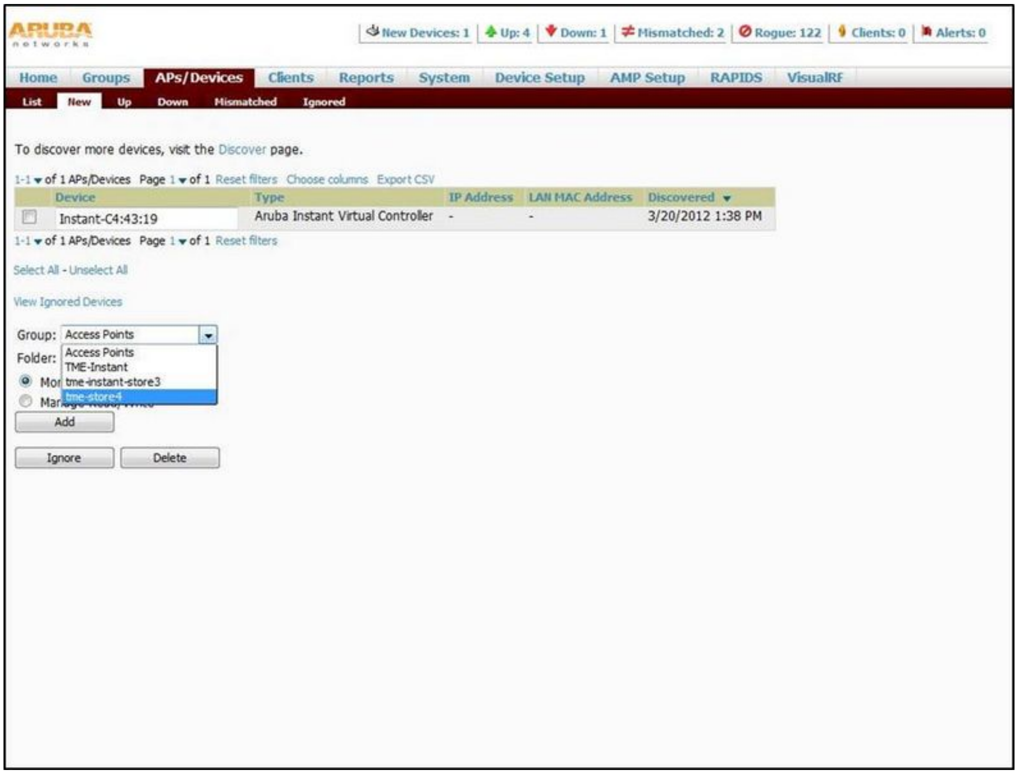
Available Options	Description
☑ 043 Vendor Specific Info	Embedded
☐ 044 WINS/NBNS Servers	NBNS Addr
☐ 045 NetBIOS over TCP/IP NBDD	NetBIOS

Data entry

```
Data:   Binary:                   ASCII:
0000  41 72 75 62 61 49 6E 73   ArubaIns
0008  74 61 6E 74 41 50 2C 74   tantAP,t
0010  6D 65 2D 73 74 6F 72 65   me-store
0018  34 2C 31 30 2E 31 36 39   4,10.169
0020  2E 32 34 30 2E 38 2C 61   .240.8,a
0028  72 75 62 61 31 32 33      ruba123
```

Upon completion, the IAP shows up as a new device in AirWave, and a new group called **tme-store4** is created. Navigate to **APs/Devices > New > Group** to view this group.

Figure 170 *AirWave — New Group*



To discover more devices, visit the Discover page.

1-1 ▾ of 1 APs/Devices Page 1 ▾ of 1 Reset filters Choose columns Export CSV

	Device	Type	IP Address	LAN MAC Address	Discovered ▾
□	Instant-C4:43:19	Aruba Instant Virtual Controller	-	-	3/20/2012 1:38 PM

1-1 ▾ of 1 APs/Devices Page 1 ▾ of 1 Reset filters

Select All - Unselect All

View Ignored Devices

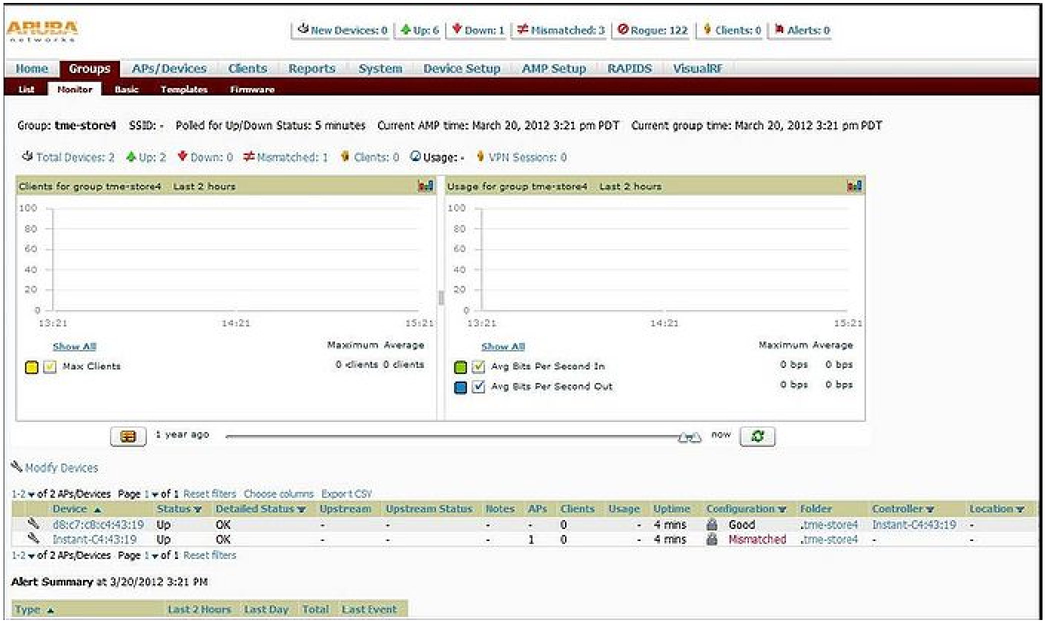
Group: Access Points

Folder:

● Mor

○ Mar

Figure 171 *AirWave —Monitor*



Group: tme-store4 SSID: - Polled for Up/Down Status: 5 minutes Current AMP time: March 20, 2012 3:21 pm PDT Current group time: March 20, 2012 3:21 pm PDT

Total Devices: 2 Up: 2 Down: 0 Mismatched: 1 Clients: 0 Usage: - VPN Sessions: 0

	Maximum	Average
🟨 ☑ Max Clients	0 clients	0 clients

	Maximum	Average
🟩 ☑ Avg Bits Per Second In	0 bps	0 bps
🟦 ☑ Avg Bits Per Second Out	0 bps	0 bps

Modify Devices

1-2 ▾ of 2 APs/Devices Page 1 ▾ of 1 Reset filters Choose columns Export CSV

	Device ▴	Status ▾	Detailed Status ▾	Upstream	Upstream Status	Notes	APs	Clients	Usage	Uptime	Configuration ▾	Folder	Controller ▾	Location ▾
	d8:c7:c8:c4:43:19	Up	OK	-	-	-	-	0	-	4 mins	Good	.tme-store4	Instant-C4:43:19	-
	Instant-C4:43:19	Up	OK	-	-	-	1	0	-	4 mins	Mismatched	.tme-store4	-	-

1-2 ▾ of 2 APs/Devices Page 1 ▾ of 1 Reset filters

Alert Summary at 3/20/2012 3:21 PM

Type ▴	Last 2 Hours	Last Day	Total	Last Event

Chapter 26

Monitoring

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

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

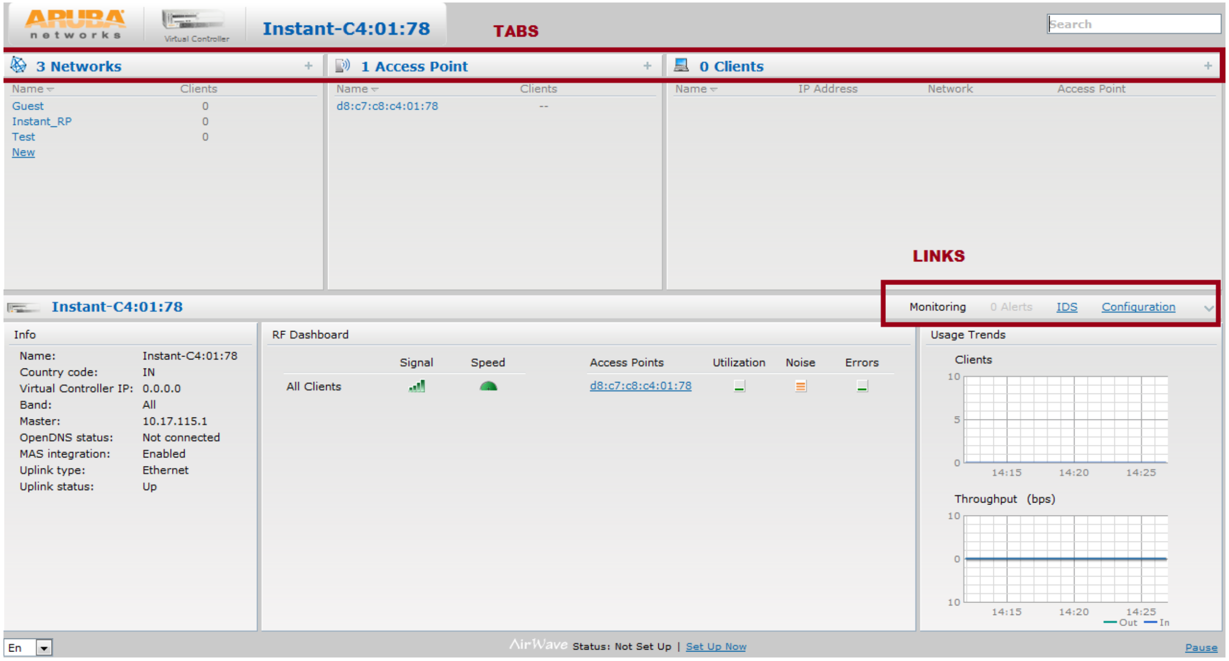
This chapter provides information about the parameters that can be monitored using these views. It also provides procedures to monitor these parameters.

Virtual Controller View

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

- Tabs— Contains three tabs— Networks, Access Points, and Clients. For detailed information about the tabs, see Chapter 3, “Instant User Interface” .
- Links— Contains three links— Monitoring, Client Alerts, and IDS. The Spectrum link is visible if you have configured the IAP as a spectrum monitor. These links allow you to monitor the 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 , IDS Link , Client Alerts Link , Configuration Link sections. For detailed information about spectrum monitoring, see “Spectrum Monitor” on page 111.

Figure 172 *Virtual Controller View*



3 Networks

Name	Clients
Guest	0
Instant_RP	0
Test	0
New	

1 Access Point

Name	Clients
d8:c7:c8:c4:01:78	--

0 Clients

Name	IP Address	Network	Access Point

Instant-C4:01:78

Info

Name:	Instant-C4:01:78
Country code:	IN
Virtual Controller IP:	0.0.0.0
Band:	All
Master:	10.17.115.1
OpenDNS status:	Not connected
MAS integration:	Enabled
Uplink type:	Ethernet
Uplink status:	Up

RF Dashboard

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

Usage Trends

Status: Not Set Up | Set Up Now

Monitoring Link

This link is selected by default and the following sections are displayed. These sections provide information about the Virtual Controller and allow you to monitor the network.

- Info
- RF Dashboard
- Usage Trends

Info

The **Info** section displays the following information about the Virtual Controller:

- **Name**— Displays the Virtual Controller name.
- **Country Code**— Displays the Country in which the Virtual Controller is operating.
- **Virtual Controller IP address**— Displays the IP address of the Virtual Controller.
- **AirWave IP**— Displays the IP address of the AirWave server.
- **Band**— Displays the band in which the Virtual Controller is operating— 2.4 GHz band, 5.4 GHz band, or both.
- **Master**— Displays the IP address of the Access Point acting as a Virtual Controller.
- **OpenDNS Status**— Displays the OpenDNS status. If the OpenDNS is **Not connected**, make sure you have provided the correct credentials on the **OpenDNS** tab of the **Settings** window. In addition, please check if the internet connection is up.
- **MAS integration**— Displays the status of the MAS integration feature.
- **Uplink type**— Displays the type of uplink— Ethernet and 3G
- **Uplink status**— Displays whether the uplink is up or down.

RF Dashboard

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

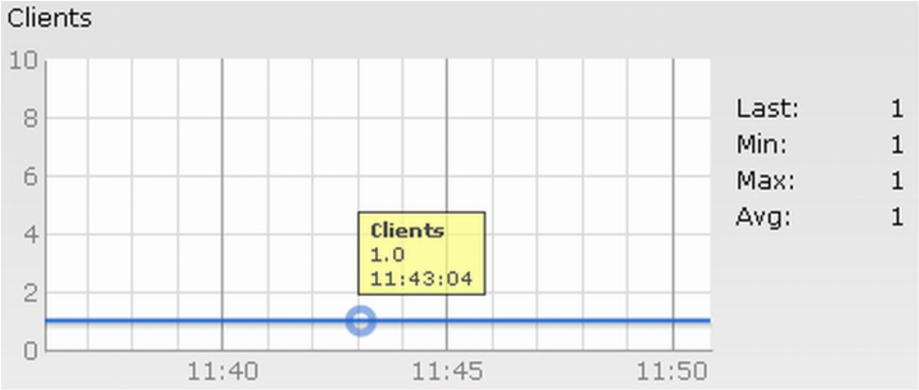
- IP address, Signal, and Speed information about the clients in the Aruba Instant network. If the speed or signal strength of a client is low, IP address of the client appears as a link. Click the link to monitor the client. For more information, see “Client View” on page 228.
- Instant Access Points, Utilization, Noise, and Errors information about the IAPs in the Aruba Instant network. If utilization, noise or errors of an IAP are not within the specified threshold, the IAP name appears as a link. Click the link to monitor the IAP. For more information, see “Instant Access Point View” on page 220.

Usage Trends

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

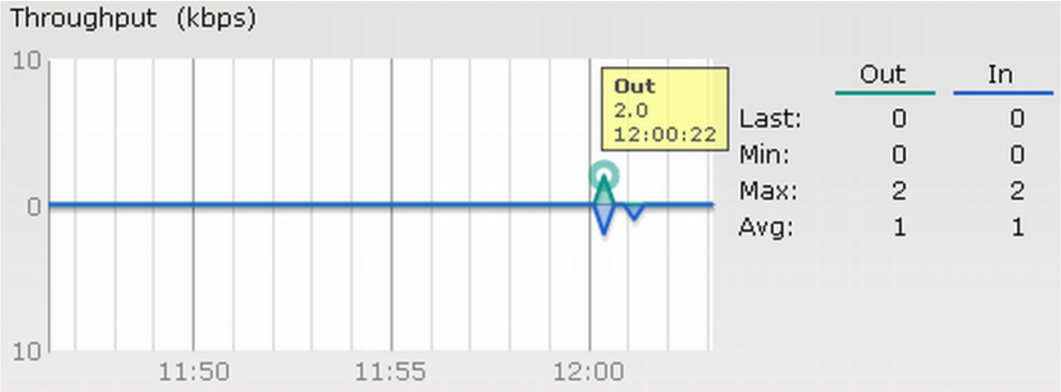
- Clients Graph

Figure 173 *Clients Graph*



- Throughput Graph

Figure 174 *Throughput Graph*



For more information about the graphs in the Virtual Controller view and for monitoring procedures, see Table 37.

Table 37 *Virtual Controller View — Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients	The Clients graph shows the number of clients associated with the Virtual Controller for the last 15 minutes. To see an enlarged view, click the graph. ● The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the Virtual Controller for the last 15 minutes. ● To see the exact number of clients in the Aruba Instant network at a particular time, hover the cursor over the graph line.	To check the number of clients associated with the Virtual Controller for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. Study the Clients graph in the **Usage Trends** pane. For example, the graph shows that one client is associated with the Virtual Controller at 11:43 hours.

Table 37 *Virtual Controller View — Graphs and Monitoring Procedures (Continued)*

Graph Name	Description	Monitoring Procedure
Throughput	The Throughput graph shows the throughput of all networks and IAPs associated with the Virtual Controller for the last 15 minutes. ● Outgoing traffic — Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. ● Incoming traffic — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. ● The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the Virtual Controller for the last 15 minutes. To see the exact throughput of the 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 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 “Clients Tab” on page 31 and Chapter 27, “Alert Types and Management” chapters.

IDS Link

For information about the IDS link, see “IDS” on page 50.

Network View

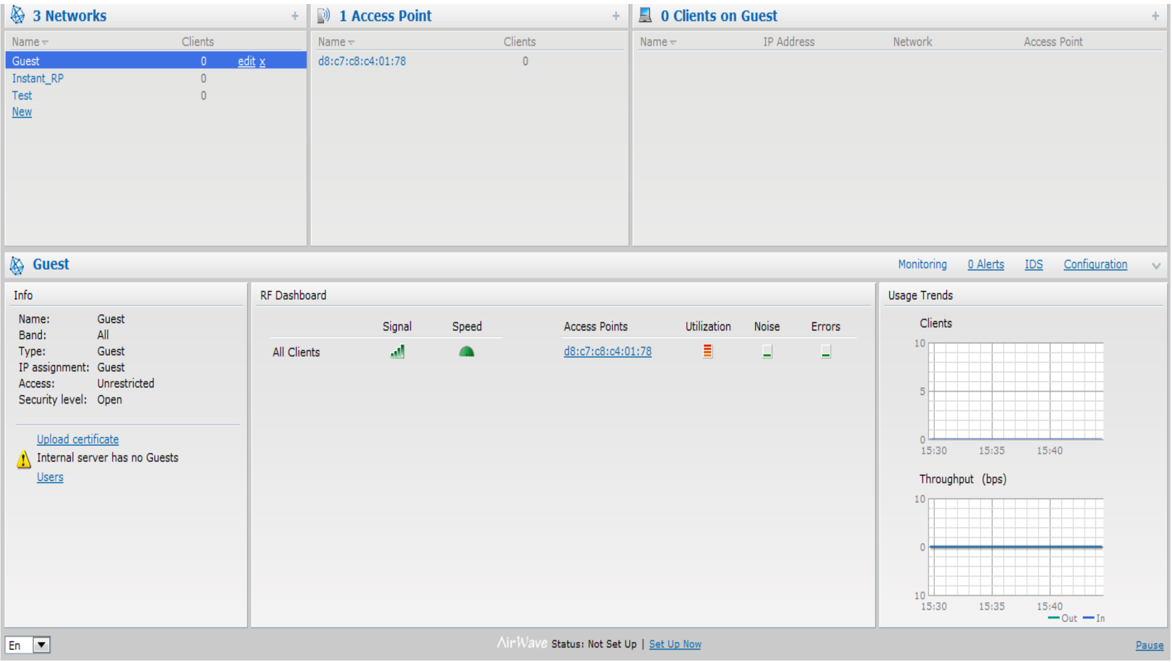
All Wi-Fi networks in the Aruba Instant network are listed in the **Networks** tab. Click the network that you want to monitor. Network View for the selected network appears.

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 175 *Network View*



3 Networks +

Name	Clients	
Guest	0	edit x
Instant_RP	0	
Test	0	
New		

1 Access Point +

Name	Clients
d8:c7:c8:c4:01:78	0

0 Clients on Guest +

Name	IP Address	Network	Access Point

Guest — Monitoring | 0 Alerts | IDS | Configuration

Info

Name:	Guest
Band:	All
Type:	Guest
IP assignment:	Guest
Access:	Unrestricted
Security level:	Open

Upload certificate

⚠ Internal server has no Guests

Users

RF Dashboard

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

Usage Trends

En ▼ AirWave Status: Not Set Up | Set Up Now Pause

Info

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

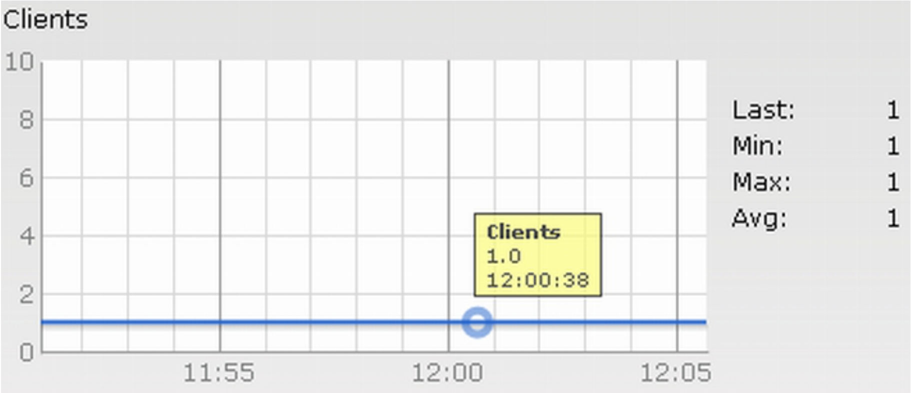
- **Name**— Name of the network.
- **Band**— Band in which the network is broadcast: 2.4 GHz band, 5.4 GHz band, or both.
- **Type**— Network type: Employee, Guest, or Voice.
- **IP Assignment**— Source of IP address for the client.
- **Access**— The level of access control for this network.
- **Security level**— The type of user authentication and data encryption for this network.

Usage Trends

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

- Clients

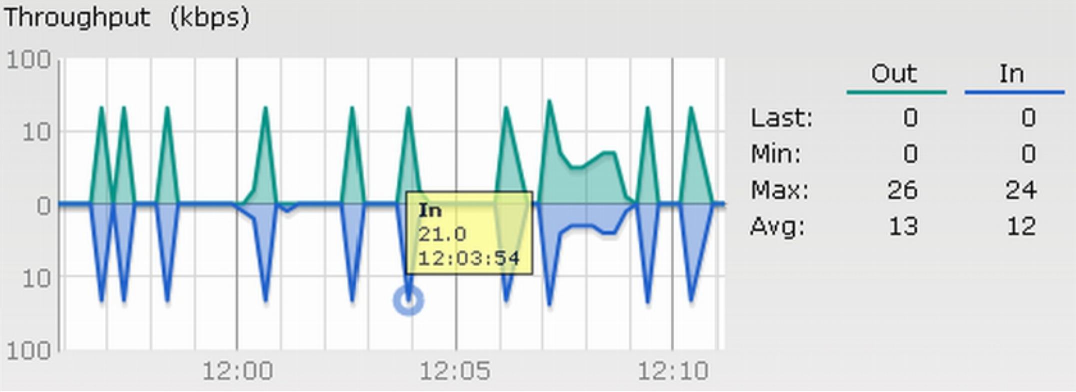
Figure 176 *Clients Graph*



Last:	1
Min:	1
Max:	1
Avg:	1

- Throughput

Figure 177 *Throughput Graph*



For more information about the graphs in the network view and for monitoring procedures, see Table 38.

Table 38 *Network View — Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients	The Clients graph shows the number of clients associated with the network for the last 15 minutes. To see an enlarged view, click the graph. ● The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the Virtual Controller for the last 15 minutes. ● To see the exact number of clients in the Aruba Instant network at a particular time, hover the cursor over the graph line.	To check the number of clients associated with the network for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Networks** tab, click the network for which you want to check the client association. The Network view appears. 3. Study the Clients graph in the **Usage Trends** pane. For example, the graph shows that one client is associated with the selected network at 12:00 hours
Throughput	The Throughput graph shows the throughput of the selected network for the last 15 minutes. ● Outgoing traffic — Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. ● Incoming traffic — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. ● The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the network for the last 15 minutes. To see the exact throughput of the selected network at a particular time, hover the cursor over the graph line.	To check the throughput of the selected network for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Networks** tab, click the network for which you want to check the client association. The Network view appears. 3. Study the Throughput graph in the **Usage Trends** pane. For example, the graph shows 22.0 kbps incoming traffic throughput for the selected network at 12:03 hours.

Instant Access Point View

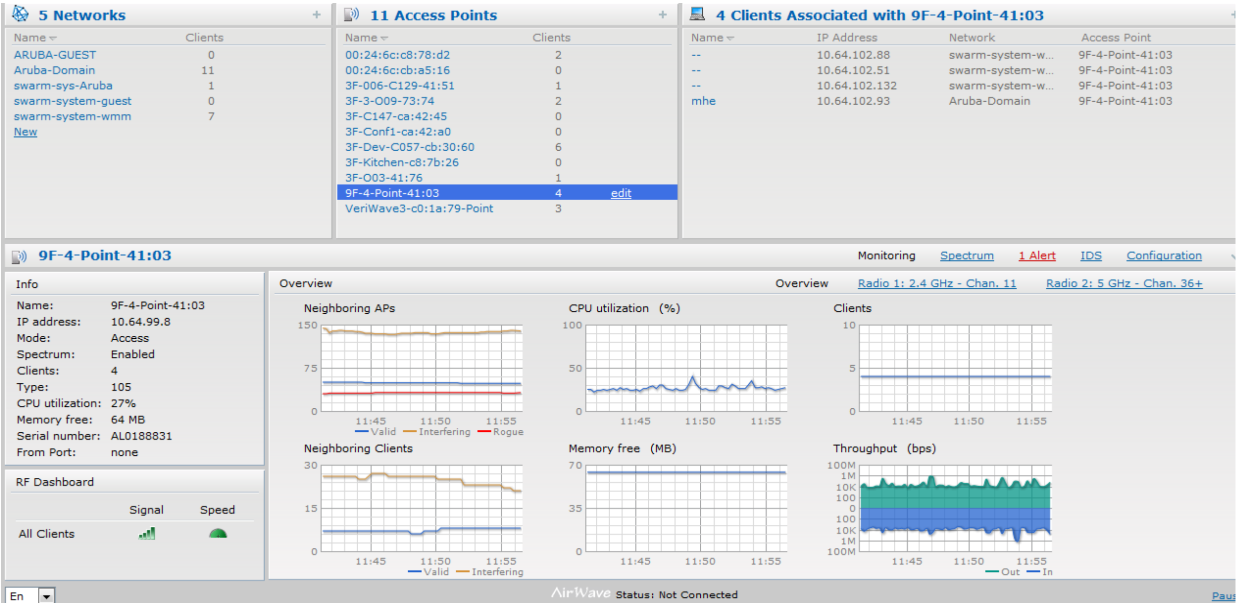
All IAPs in the Aruba Instant network are listed in the **Access Points** tab. Click the IAP that you want to monitor. Access Point view for that IAP appears.

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
- Overview

Figure 178 *Instant Access Point View*



5 Networks

Name	Clients
ARUBA-GUEST	0
Aruba-Domain	11
swarm-sys-Aruba	1
swarm-system-guest	0
swarm-system-wmm	7
New	

11 Access Points

Name	Clients	
00:24:6c:c8:78:d2	2	
00:24:6c:cb:a5:16	0	
3F-006-C129-41:51	1	
3F-3-O09-73:74	2	
3F-C147-ca:42:45	0	
3F-Conf1-ca:42:a0	0	
3F-Dev-C057-cb:30:60	6	
3F-Kitchen-c8:7b:26	0	
3F-O03-41:76	1	
9F-4-Point-41:03	4	edit
VeriWave3-c0:1a:79-Point	3	

4 Clients Associated with 9F-4-Point-41:03

Name	IP Address	Network	Access Point
--	10.64.102.88	swarm-system-w...	9F-4-Point-41:03
--	10.64.102.51	swarm-system-w...	9F-4-Point-41:03
--	10.64.102.132	swarm-system-w...	9F-4-Point-41:03
mhe	10.64.102.93	Aruba-Domain	9F-4-Point-41:03

9F-4-Point-41:03

Info

Name:	9F-4-Point-41:03
IP address:	10.64.99.8
Mode:	Access
Spectrum:	Enabled
Clients:	4
Type:	105
CPU utilization:	27%
Memory free:	64 MB
Serial number:	AL0188831
From Port:	none

RF Dashboard

	Signal	Speed
All Clients		

Status: Not Connected

Info

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

- **Name**— Displays the name of the selected IAP.
- **IP Address**— Displays the IP address of the IAP.
- **Mode**— Displays the mode type. In **Access** mode the IAP serves clients, while also monitoring for rogue APs in the background. In **Monitor** mode, the IAP acts as a dedicated monitor, scanning all channels for rogue APs and clients.
- **Spectrum**— Displays the status of the spectrum monitor.
- **Clients**— Number of clients associated with the IAP.
- **Type**— Displays the model number of the IAP.
- **CPU Utilization**— Displays the CPU utilization in percentage.
- **Memory Free**— Displays the memory availability of the IAP in Mega Bytes (MB).
- **Serial number**— Displays the serial number of the IAP.
- **From Port**— Displays the port from where the slave IAP is learned in hierarchy mode.

RF Dashboard

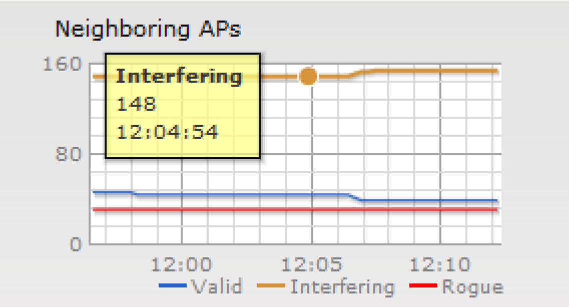
In the Instant Access Point view, the **RF Dashboard** section is moved below the **Info** section. It lists the IP address of the clients that are associated with the selected IAP if the signal strength or the data transfer speed of the client is low.

Overview

The **Overview** section displays the common RF metrics for the selected access point over the last 15 minutes. The following graphs are displayed for the selected IAP:

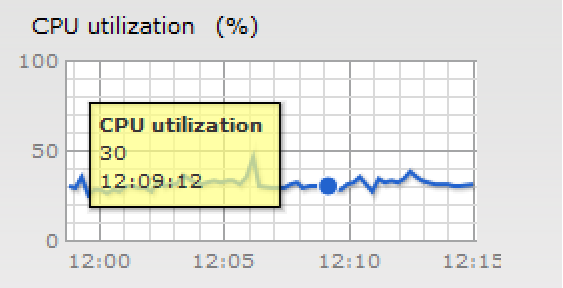
- Neighboring APs

Figure 179 *Neighboring APs Graph*



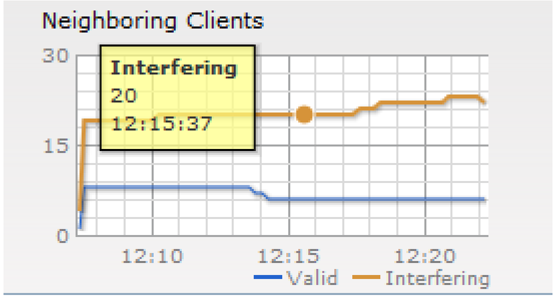
- CPU Utilization

Figure 180 *CPU Utilization Graph*



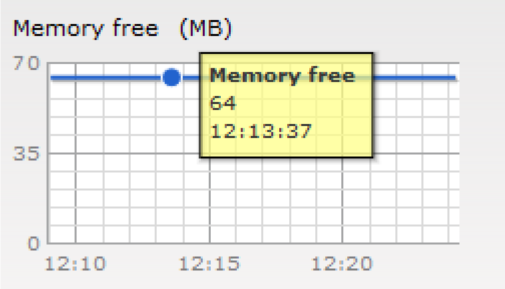
- Neighboring Clients

Figure 181 *Neighboring Clients Graph*



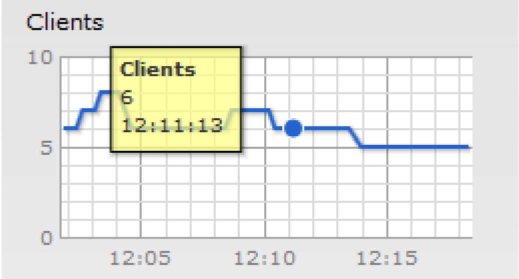
- Memory Free (MB)

Figure 182 *Memory free Graph*



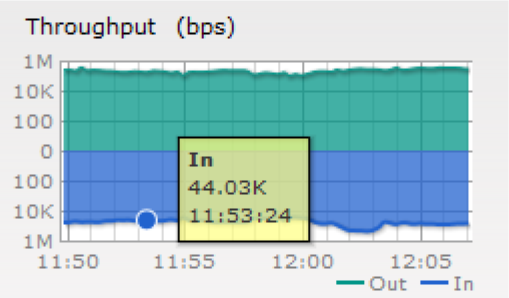
- Clients

Figure 183 *Clients Graph*



- Throughput (bps)

Figure 184 *Throughput Graph*



For more information about the graphs in the instant access point view and or monitoring procedures, see Table 39.

Table 39 *Instant Access Point View — Usage Trends and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Neighboring APs	The Neighboring APs graph shows the number of APs heard by the selected IAP: Valid APs: An AP that is part of the enterprise providing WLAN service. Interfering APs: An AP that is seen in the RF environment but is not connected to the network. Rogue APs: An unauthorized AP that is plugged into the wired side of the network. To see the number of different types of neighboring APs for the last 15 minutes, hover the cursor over the respective graph lines.	To check the neighboring APs detected by the IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the IAP for which you want to monitor the client association. The IAP view appears. 3. Study the Neighboring APs graph in the **Overview** section. For example, the graph shows that 148 interfering APs are detected by the IAP at 12:04 hours.
CPU Utilization	The CPU Utilization graph displays the utilization of CPU for the selected IAP. To see the CPU utilization of the IAP, hover the cursor over the graph line.	To check the CPU utilization of the IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the IAP for which you want to monitor the client association. The IAP view appears. 3. Study the CPU Utilization graph in the **Overview** pane. For example, the graph shows that the CPU utilization of the IAP is 30% at 12:09 hours.

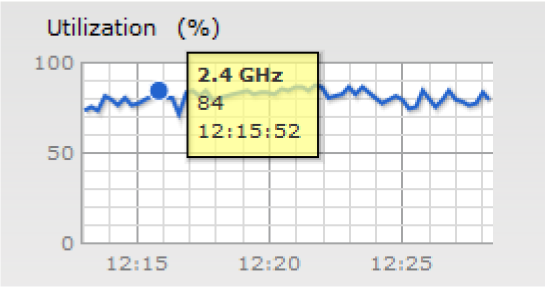
Table 39 *Instant Access Point View — Usage Trends and Monitoring Procedures (Continued)*

Graph Name	Description	Monitoring Procedure
Neighboring Clients	The Neighboring Clients graph shows the number of clients not connected to the selected AP, but heard by it: Valid: Any client that successfully authenticates with a valid AP and passes encrypted traffic is classified as a valid client. Interfering: A client associated to any AP and is not valid. To see the number of different types of neighboring clients for the last 15 minutes, hover the cursor over the respective graph lines.	To check the neighboring clients detected by the IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the IAP for which you want to monitor the client association. The IAP view appears. 3. Study the Neighboring Clients graph in the **Overview** pane. For example, the graph shows that 20 interfering clients were detected by the IAP at 12:15 hours.
Memory free (MB)	The memory free graph displays the memory availability of the IAP in Mega Bytes (MB). To see the free memory of the IAP, hover the cursor over the graph line.	To check the free memory of the IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the IAP for which you want to monitor the client association. The IAP view appears. 3. Study the Memory free graph in the **Overview** pane. For example, the graph shows that the free memory of the IAP is 64 MB at 12:13 hours.
Clients	The Clients graph shows the number of clients associated with the selected IAP for the last 15 minutes. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the IAP for the last 15 minutes. To see the exact number of clients associated with the selected IAP at a particular time, hover the cursor over the graph line.	To check the number of clients associated with the IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the IAP for which you want to monitor the client association. The IAP view appears. 3. Study the Clients graph. For example, the graph shows that six clients are associated with the IAP at 12:11 hours.
Throughput	The Throughput graph shows the throughput for the selected IAP for the last 15 minutes. • Outgoing traffic — Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown about the median line. • Incoming traffic — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. • The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the IAP for the last 15 minutes. To see the exact throughput of the selected IAP at a particular time, hover the cursor over the graph line.	To check the throughput of the selected IAP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the IAP for which you want to monitor the throughput. The IAP view appears. 3. Study the Throughput graph. For example, the graph shows 44.03 kbps incoming traffic throughput at 12:08 hours.

The **Overview** section also has two links— **2.4 GHz** and **5 GHz**. The following graphs are displayed for each band:

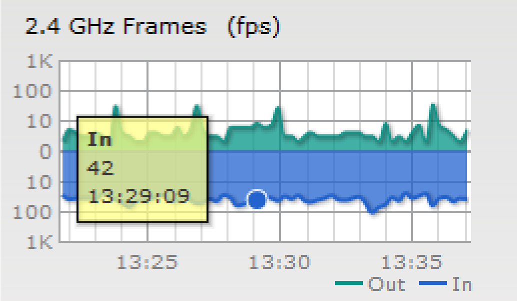
- Utilization

Figure 185 *Utilization Graph*



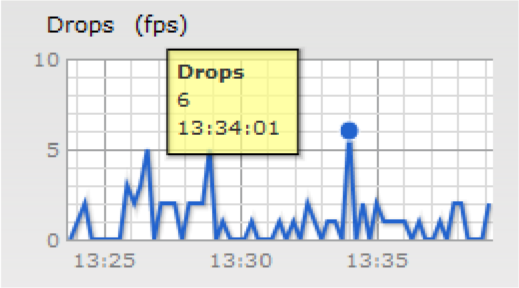
- 2.4 GHz Frames (fps)

Figure 186 *2.4 GHz Frames (fps) Graph*



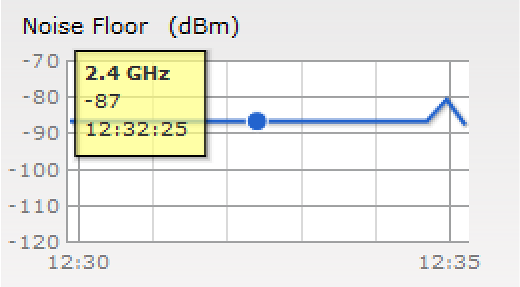
- Drops (fps)

Figure 187 *Drops (fps) Graph*



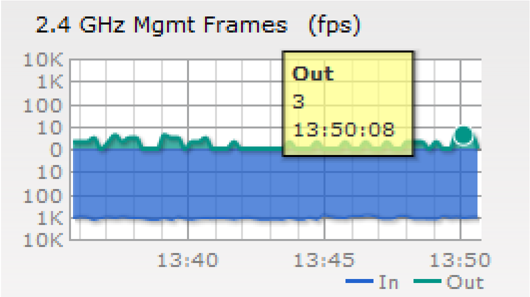
- Noise Floor (dBm)

Figure 188 *Noise Floor (dBm) Graph*



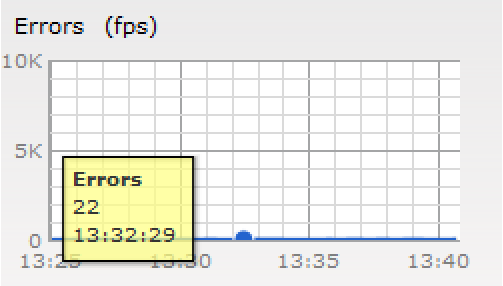
- 2.4 GHz Mgmt Frames

Figure 189 *2.4 GHz Mgmt Frames (fps) Graph*



- Errors (fps) Graph

Figure 190 *Errors (fps) Graph*



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

For more information about the graphs in the instant access point view and for monitoring procedures, see Table 40.

Table 40 *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 shows 84% IAP radio utilization for the 2.4 GHz band at 12:15 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. The rectangle icon is seen as follows: ▤

Table 40 *Instant Access Point View — RF Trends Graphs and Monitoring Procedures (Continued)*

Graph Name	Description	Monitoring Procedure
2.4 GHz Frames	The 2.4 GHz Frames graph shows the In and Out frame rate per second for the radio in 2.4 GHz band for the last 15 minutes. ● Outgoing frames — Outgoing frame traffic is displayed in green. It is shown above the median line. ● Incoming frames — Incoming frame traffic is displayed in blue. It is shown below the median line. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing frames. To see the exact utilization percent at a particular time, hover the cursor over the graph line.	To monitor the In and Out frame rate per second for the radio in 2.4 GHz band, for the last 15 minutes, 1. Log in to the Instant WebUI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the name link of the IAP for which you want to monitor the frame rate. The IAP view appears. 3. Study the 2.4 GHz Frames graph. For example, the graph shows 42 incoming frames at 13:29 hours.
Drops	The Drops graph shows dropped frames over the last 15 minutes. To see the number of frames dropped at a particular time, hover the cursor over the graph line.	To monitor the number of frames dropped for the last 15 minutes, 1. Log in to the Instant WebUI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the name link of the IAP for which you want to monitor the frame rate. The IAP view appears. 3. Study the Drops graph. For example, the graph shows that 6 frames per second were dropped at 13:34 hours.
Noise Floor	The Noise Floor graph shows the signals created by all the noise sources and unwanted signals in the network. Noise floor is measured in decibels/metre. Too many unwanted signals hamper the performance of the IAP. Monitor the noise floor regularly for optimal performance of the IAP. To see an enlarged view, click the graph.The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In and Out frames. To see the exact utilization percent at a particular time, hover the cursor over the graph line.	To monitor the noise floor for the IAP for the last 15 minutes, 1. Log in to the Instant WebUI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the name link of the IAP for which you want to monitor the noise floor. The IAP view appears. 3. Study the Noise Floor graph. For example, the graph shows that the noise floor for the IAP at 22:38 hours is —82.0 dBm. **NOTE:** You can also click the rectangle icon the Noise column in the **RF Dashboard** pane to see the Noise graph for the selected IAP. The rectangle icon is seen as follows: ≣

Table 40 *Instant Access Point View — RF Trends Graphs and Monitoring Procedures (Continued)*

Graph Name	Description	Monitoring Procedure
2.4 GHz Mgmt Frames	The 2.4 GHz Mgmt Frames graph shows the rate for management frames in and out of the radio in the 2.4 GHz band for the last 15 minutes. Note that the scale for the Y-axis is logarithmic. To see the exact number of management frames per second at a particular time, hover the cursor over the graph lines.	To monitor the rate of management frames in and out of the radio for the last 15 minutes, 1. Log in to the Instant WebUI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the name link of the IAP for which you want to monitor the noise floor. The IAP view appears. 3. Study the 2.4 GHz Mgmt Frames graph. For example, the graph shows that 3 management frames were out of the radio at 13:50 hours.
Errors	The Errors graph shows the errors that occurred while receiving the frames for the last 15 minutes. The errors are measured in frames per second. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In and Out frames. To see the exact utilization percent at a particular time, hover the cursor over the graph line.	To monitor the errors for the IAP for the last 15 minutes, 1. Log in to the Instant WebUI. The Virtual Controller view appears. This is the default view. 2. In the **Access Points** tab, click the name link of the IAP for which you want to monitor the errors. The IAP view appears. 3. Study the Errors graph. For example, the graph shows that the errors for the IAP at 13:32 hours is 22 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.

Client View

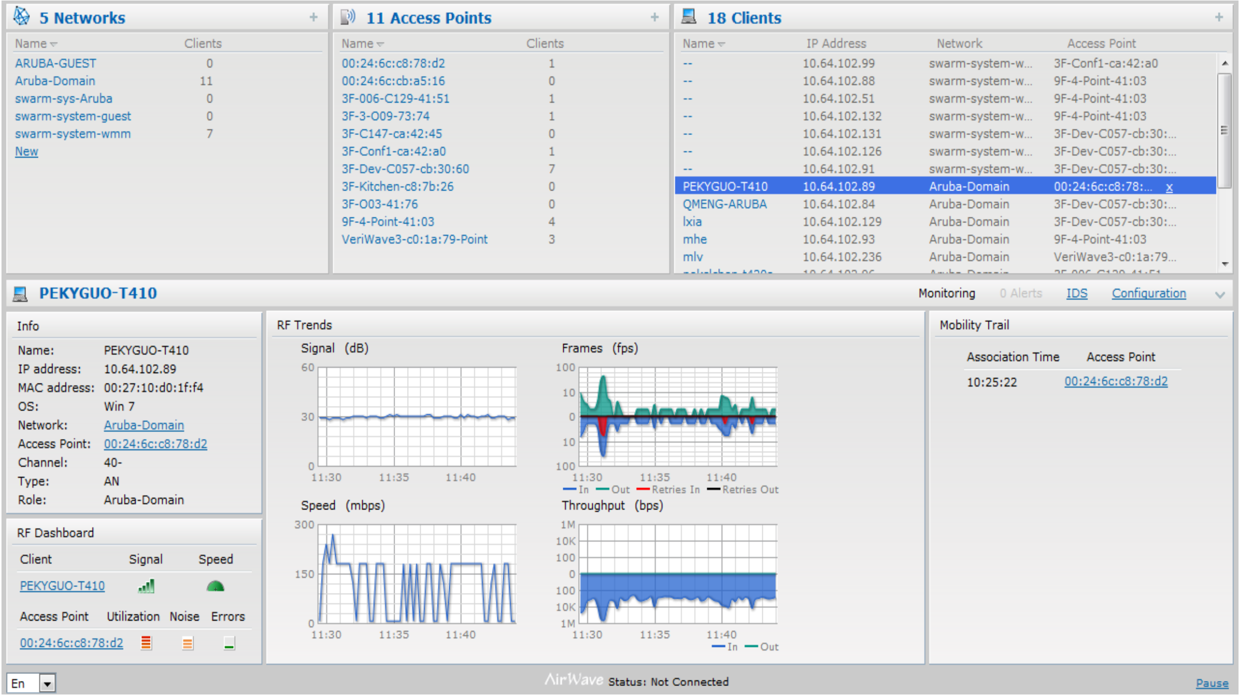
In the Virtual Controller view, all clients in the Aruba Instant network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor. Client view for that client appears.

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 191 *Client View*



5 Networks +

Name	Clients
ARUBA-GUEST	0
Aruba-Domain	11
swarm-sys-Aruba	0
swarm-system-guest	0
swarm-system-wmm	7
New	

11 Access Points +

Name	Clients
00:24:6c:c8:78:d2	1
00:24:6c:cb:a5:16	0
3F-006-C129-41:51	1
3F-3-O09-73:74	1
3F-C147-ca:42:45	0
3F-Conf1-ca:42:a0	1
3F-Dev-C057-cb:30:60	7
3F-Kitchen-c8:7b:26	0
3F-O03-41:76	0
9F-4-Point-41:03	4
VeriWave3-c0:1a:79-Point	3

18 Clients +

Name	IP Address	Network	Access Point
--	10.64.102.99	swarm-system-w...	3F-Conf1-ca:42:a0
--	10.64.102.88	swarm-system-w...	9F-4-Point-41:03
--	10.64.102.51	swarm-system-w...	9F-4-Point-41:03
--	10.64.102.132	swarm-system-w...	9F-4-Point-41:03
--	10.64.102.131	swarm-system-w...	3F-Dev-C057-cb:30:...
--	10.64.102.126	swarm-system-w...	3F-Dev-C057-cb:30:...
--	10.64.102.91	swarm-system-w...	3F-Dev-C057-cb:30:...
PEKYGUO-T410	10.64.102.89	Aruba-Domain	00:24:6c:c8:78:... x
QMENG-ARUBA	10.64.102.84	Aruba-Domain	3F-Dev-C057-cb:30:...
lxia	10.64.102.129	Aruba-Domain	3F-Dev-C057-cb:30:...
mhe	10.64.102.93	Aruba-Domain	9F-4-Point-41:03
mlv	10.64.102.236	Aruba-Domain	VeriWave3-c0:1a:79...

PEKYGUO-T410 Monitoring 0 Alerts IDS Configuration

Info

Name:	PEKYGUO-T410
IP address:	10.64.102.89
MAC address:	00:27:10:d0:1f:f4
OS:	Win 7
Network:	Aruba-Domain
Access Point:	00:24:6c:c8:78:d2
Channel:	40-
Type:	AN
Role:	Aruba-Domain

RF Dashboard

Client	Signal	Speed
PEKYGUO-T410		

Access Point	Utilization	Noise	Errors
00:24:6c:c8:78:d2			

Mobility Trail

Association Time	Access Point
10:25:22	00:24:6c:c8:78:d2

Info

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

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

RF Dashboard

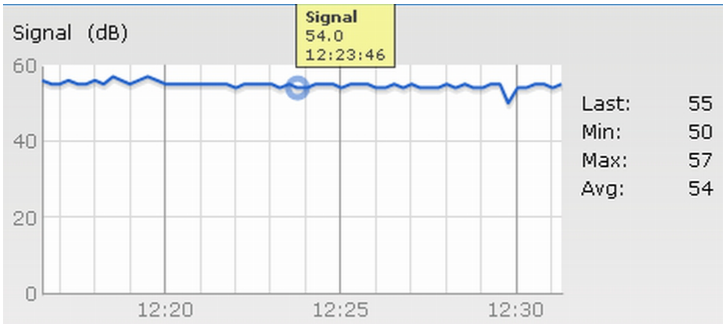
In the Client view, the **RF Dashboard** section is moved below the **Info** section. The **RF Dashboard** section in the client view shows the speed and the signal information for the client and the RF information for the IAP to which the client is connected to.

RF Trends

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

- Signal

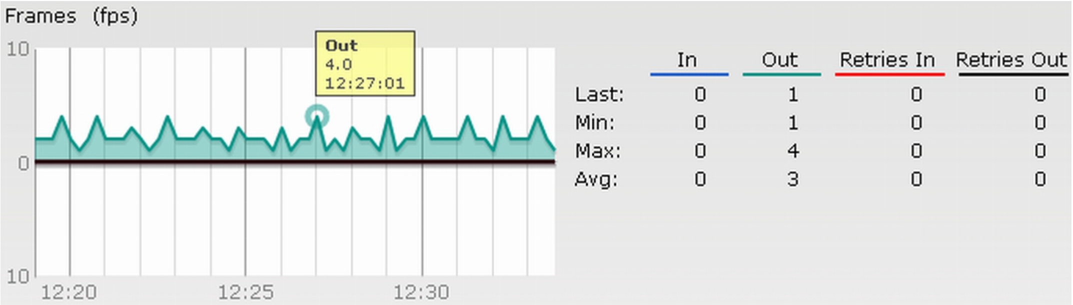
Figure 192 *Signal Graph*



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

- Frames

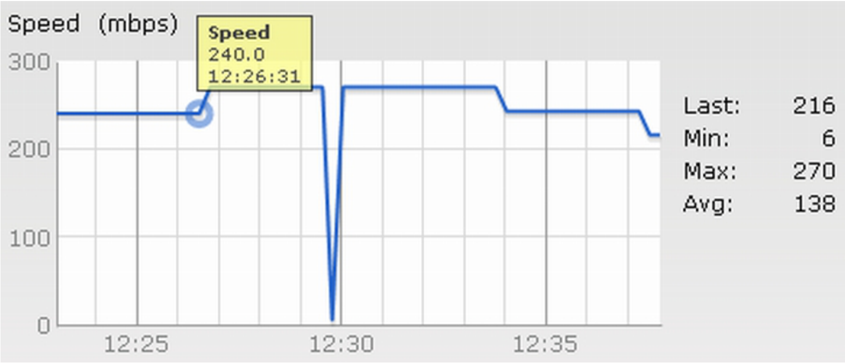
Figure 193 *Frames Graph*



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

- Speed

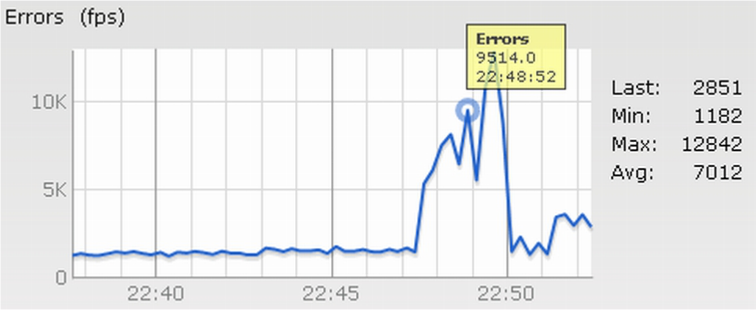
Figure 194 *Speed Graph*



Last:	216
Min:	6
Max:	270
Avg:	138

- Throughput

Figure 195 *Throughput Graph*



Last:	2851
Min:	1182
Max:	12842
Avg:	7012

For more information about RF trends graphs in the client view and for monitoring procedures, see Table 41.

Table 41 *Client View — RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Signal	The Signal graph shows the signal strength of the client for the last 15 minutes. It is measured in decibels. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average signal statistics for the client fr the last 15 minutes. To see the exact signal strength at a particular time, hover the cursor over the graph line.	To monitor the signal strength of the selected client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the signal strength. The client view appears. 3. Study the Signal graph in the RF Trends pane. For example, the graph shows that signal strength for the client is 54.0 dB at 12:23 hours.
Frames	The Frames Graph shows the In and Out frame rate per second for the client for the last 15 minutes. It also shows data for the Retry In and Retry Out frames. ● Outgoing frames — Outgoing frame traffic is displayed in green. It is shown above the median line. ● Incoming frames — Incoming frame traffic is displayed in blue. It is shown below the median line. ● Retry Out — Retries for the outgoing frames is displayed in black and is show above the median line. ● Retry In — Retries for the incoming frames is displayed in red and is shown below the median line. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In, Out, Retries In, and Retries Out frames. To see the exact frames at a particular time, hover the cursor over the graph line.	To monitor the In and Out frame rate per second and retry frames for the In and Out traffic, for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the frames. The client view appears. 3. Study the Frames graph in the RF Trends pane. For example, the graph 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 see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics for the client for the last 15 minutes. To see the exact speed at a particular time, hover the cursor over the graph line.	To monitor the speed for the client for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the speed. The client view appears. 3. Study the Speed graph in the RF Trends pane. For example, the graph shows that the data transfer speed at 12:26 hours is 240 mbps.

Table 41 *Client View — RF Trends Graphs and Monitoring Procedures* (Continued)

Graph Name	Description	Monitoring Procedure
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 shows 1.0 kbps outgoing traffic throughput for the client at 12:30 hours.

Mobility Trail

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

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

NOTE

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

Alert Types

Alerts are generated when a user encounters problems 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 time-out failure alerts.
- IP address related failure - Static IP address or DHCP related alerts.

Table 42 displays a list of alerts that are generated on the Aruba Instant network.

Table 42 *Alerts List*

Type Code	Description	Details	Corrective Actions
100101	Internal error	The IAP has encountered an internal error for this client.	Contact the Aruba customer support team.
100102	Unknown SSID in association request	The IAP cannot allow this client to associate because the association request received contains an unknown SSID.	Identify the client and check its Wi-Fi driver and manager software.
100103	Mismatched authentication/ encryption setting	The IAP cannot allow this client to associate because its authentication or encryption settings do not match IAP's configuration.	Ascertain the correct authentication or encryption settings and try to associate again.
100104	Unsupported 802.11 rate	The IAP cannot allow this client to associate because it does not support the 802.11 rate requested by this client.	Check the configuration on the IAP to see if the desired rate can be supported; if not, consider replacing the IAP with another model that can support the rate.
100105	Maximum capacity reached on IAP	The IAP has reached maximum capacity and cannot accommodate any more clients.	Consider expanding capacity by installing additional IAPs or balance load by relocating IAPs.
100206	Invalid MAC Address	The IAP cannot authenticate this client because the client's MAC address is not valid.	This condition may be indicative of a misbehaving client. Try to locate the client device and check its hardware and software.
100307	Client blocked due to repeated authentication failures	The IAP is temporarily blocking the 802.1X authentication request from this client because the credentials provided have been rejected by the RADIUS server too many times.	Identify the client and check its 802.1X credentials.

Table 42 *Alerts List (Continued)*

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.
100511	DHCP request timed out	This client did not receive a response to its DHCP request in time.	Check the status of the DHCP server in the network.

Chapter 28

Policy Enforcement Firewall

Aruba's Policy Enforcement Firewall (PEF) module for Aruba Instant provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks.

The PEF window displays the external/internal authentication servers, currently defined roles for all the networks, blacklisted clients and to enable or disable the protocols for ALG.

Navigate to the **PEF** link at the top right corner of the Instant WebUI to view the following features.

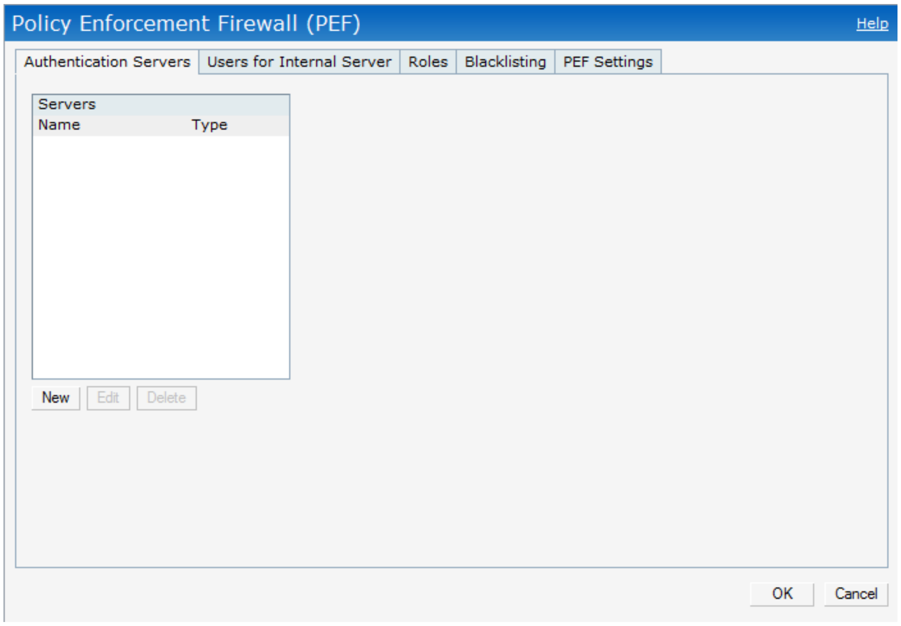
Authentication Servers

This section displays the currently defined external authentication servers.

- **Name**— Indicates the name of the external authentication server.
- **Type**— Indicates the type of the authentication server-RADIUS or LDAP.

1. Click **New** to configure an external RADIUS server for a wireless network. See "Configuring an External RADIUS Server" on page 125 for more information.
2. Click **OK** to apply the changes.

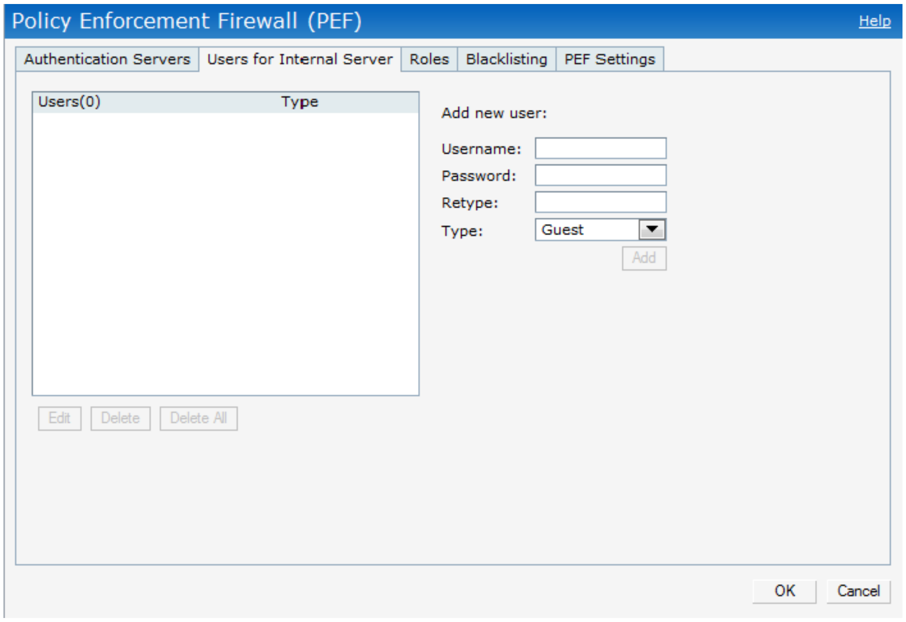
Figure 196 *Authentication Server*



Users for Internal Server

This section displays the currently defined users for the internal authentication server.

Figure 197 *Users for Internal Server*



To add a user:

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

See "User Database" on page 251 for more information.

Roles

This window consists of the following options:

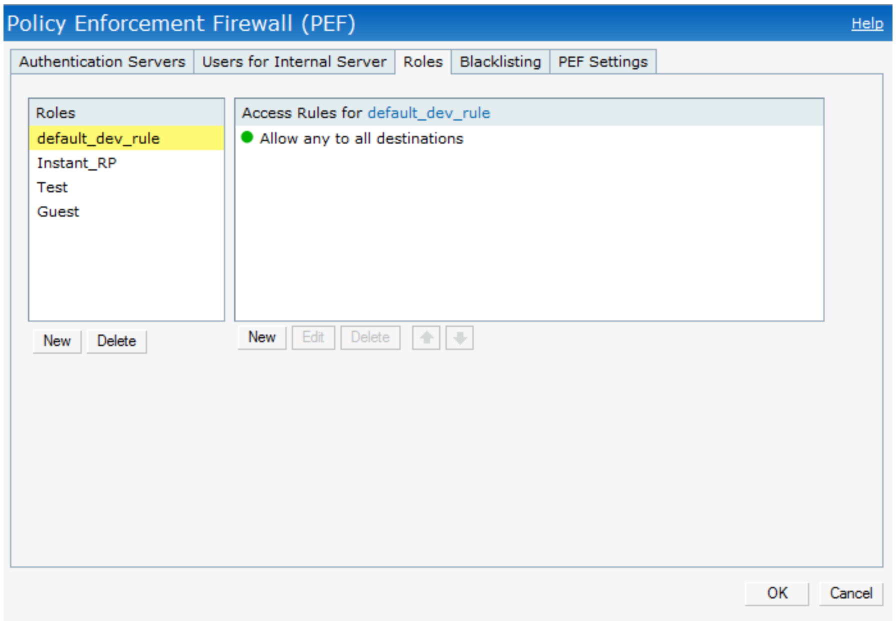
- **Roles—** This table displays all the roles defined for all the networks. See "User Role" on page 157 for more information.

NOTE

A special default role with the same name as the network is automatically defined for each network. These roles cannot be deleted or renamed.

- **Access Rules—** This table lists the permissions for each Role. See Chapter 14, "Role Derivation" for more information.

Figure 198 *Roles*



Roles

- default_dev_rule
- Instant_RP
- Test
- Guest

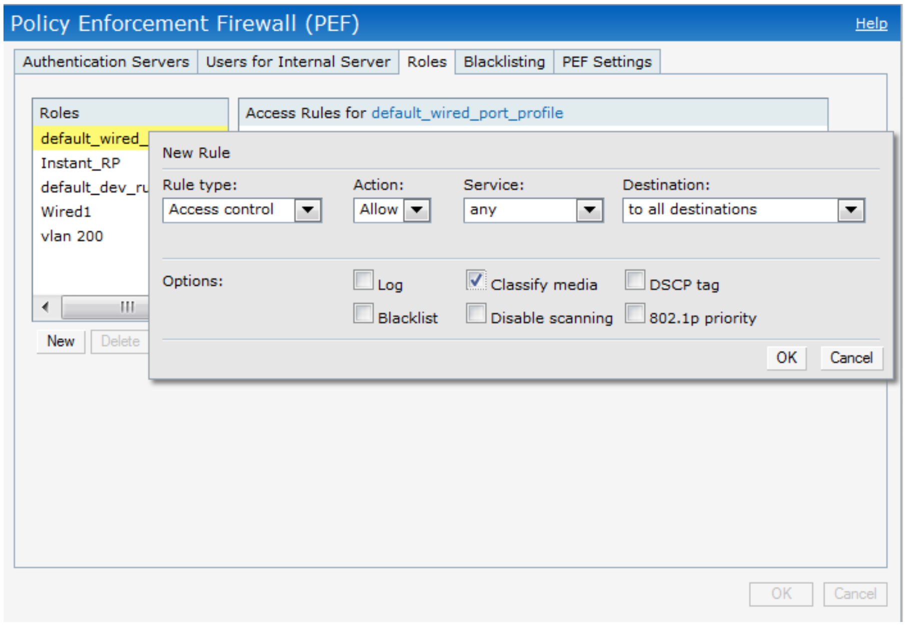
Access Rules for default_dev_rule

● Allow any to all destinations

Extended Voice and Video Functionalities

Instant has the added ability to identify and prioritize voice and video traffic from applications like Microsoft Office Communications Server (OCS) and Apple Facetime.

Figure 199 *Classify Media*



Roles

- default_wired_
- Instant_RP
- default_dev_ru
- Wired1
- vlan 200

Access Rules for default_wired_port_profile

New Rule

Rule type: Access control

Action: Allow

Service: any

Destination: to all destinations

Options: ☐ Log ☑ Classify media ☐ DSCP tag

☐ Blacklist ☐ Disable scanning ☐ 802.1p priority

QoS for Microsoft Office OCS and Apple Facetime

Voice and video devices use a signaling protocol to establish, control, and terminate voice and video calls.These control or signaling sessions are usually permitted using pre-defined ACLs. If, however, the control signaling packets are encrypted, the IAP cannot determine which dynamic ports are used for voice or video traffic. In these cases, the IAP has to use an ACL with the classify-media option enabled to identify the voice or video flow based on a deep packet inspection and analysis of the actual traffic.

Microsoft OCS

Microsoft Office Communications Server (OCS) uses Session Initiation Protocol (SIP) over TLS to establish, control, and terminate voice and video calls.

Apple Facetime

When an Apple device starts a Facetime video call, it initiates a TCP session to the Apple Facetime server over port 5223, then sends SIP signaling messages over a non-default port. When media traffic starts flowing, audio and video data are sent through that same port using RTP. (The audio and video packets are interleaved in the air, though individual the sessions can be uniquely identified using their payload type and sequence numbers.) The RTP header and payload also get encapsulated under the TURN ChannelData Messages. The Facetime call is terminated with a SIP BYE message that can be sent by either party.

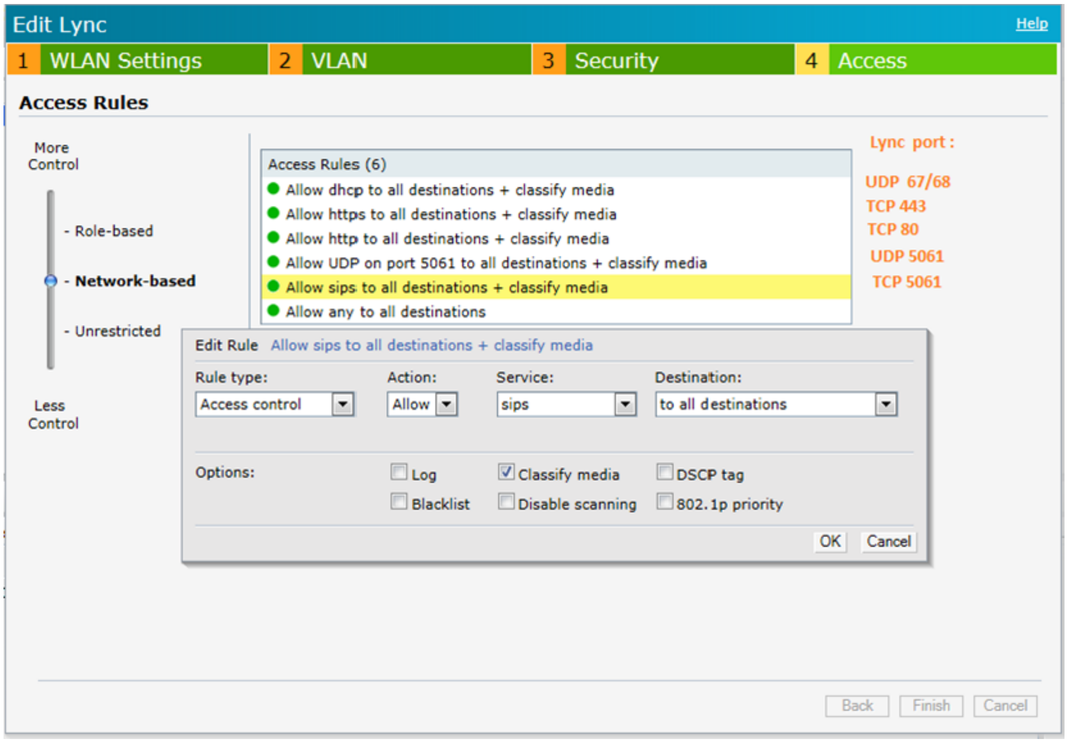
The following table lists the ports used by Apple Facetime. Facetime users need to be assigned a role where traffic is allowed on these ports.

Table 43 *Ports used by the Apple Facetime Application*

Port	Packet Type
53	TCP/UDP
443	TCP
3478-3497	UDP
5223	TCP
16384-16387	UDP
16393-16402	UDP

The following screenshots are configuration examples for Microsoft OCS and Apple Facetime applications.

Figure 200 *Classify Media —Microsoft OCS*



Access Rules

Access Rules (6)

- ● Allow dhcp to all destinations + classify media
- ● Allow https to all destinations + classify media
- ● Allow http to all destinations + classify media
- ● Allow UDP on port 5061 to all destinations + classify media
- ● Allow sips to all destinations + classify media
- ● Allow any to all destinations

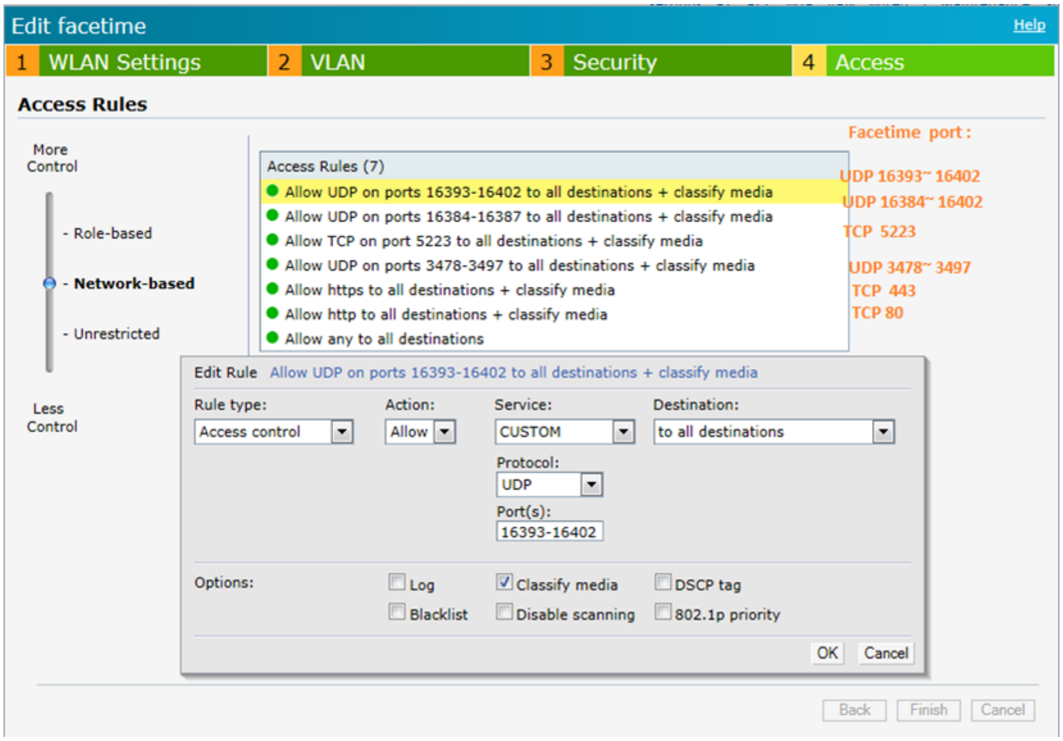
Lync port :
UDP 67/68
TCP 443
TCP 80
UDP 5061
TCP 5061

Edit Rule Allow sips to all destinations + classify media

Rule type: Access control
Action: Allow
Service: sips
Destination: to all destinations

Options: □ Log ☑ Classify media □ DSCP tag □ Blacklist □ Disable scanning □ 802.1p priority

Figure 201 *Classify Media —Apple Facetime*



Access Rules

Access Rules (7)

- ● Allow UDP on ports 16393-16402 to all destinations + classify media
- ● Allow UDP on ports 16384-16387 to all destinations + classify media
- ● Allow TCP on port 5223 to all destinations + classify media
- ● Allow UDP on ports 3478-3497 to all destinations + classify media
- ● Allow https to all destinations + classify media
- ● Allow http to all destinations + classify media
- ● Allow any to all destinations

Facetime port :
UDP 16393~ 16402
UDP 16384~ 16402
TCP 5223
UDP 3478~ 3497
TCP 443
TCP 80

Edit Rule Allow UDP on ports 16393-16402 to all destinations + classify media

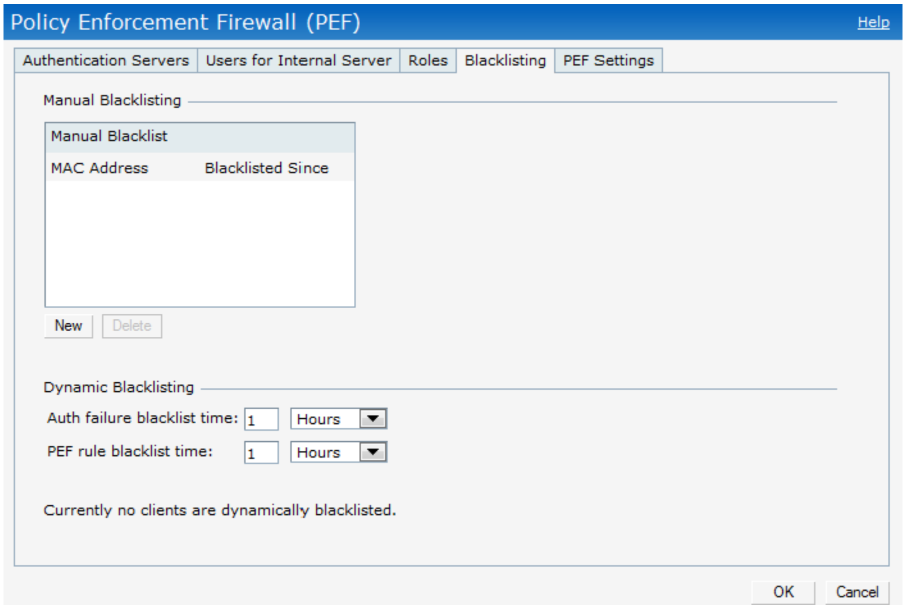
Rule type: Access control
Action: Allow
Service: CUSTOM
Destination: to all destinations
Protocol: UDP
Port(s): 16393-16402

Options: □ Log ☑ Classify media □ DSCP tag □ Blacklist □ Disable scanning □ 802.1p priority

Client Blacklisting

The client blacklisting denies connectivity to the blacklisted clients. When a client is blacklisted in an Aruba IAP, the client is not allowed to associate with the IAP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force the client to disconnect.

Figure 202 *Client Blacklisting*



Manual Blacklisting

Manual Blacklist

MAC Address	Blacklisted Since

Dynamic Blacklisting

Auth failure blacklist time: 1 Hours

PEF rule blacklist time: 1 Hours

Currently no clients are dynamically blacklisted.

Types of Client Blacklisting

The following types of client blacklisting can be generated in an Instant:

- Manual Blacklisting
- Dynamic Blacklisting
  - Authentication Failure Blacklisting
  - Session Firewall Based Blacklisting

Manual Blacklisting

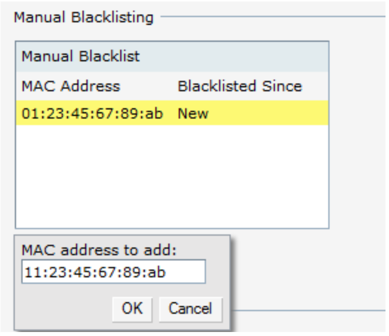
Manual blacklisting is the simplest way to add a client to the blacklist. In manual blacklisting, the MAC address of the client has to be known to the user. These clients would be added into a permanent blacklist. These clients are not allowed to connect to the network unless they are removed from the blacklist.

Adding a Client to the Manual Blacklist

To add a client to the blacklist manually using the MAC address of the client:

1. Click on the **PEF** link and then select **Blacklisting** tab.
2. Click on the **New** button under the **Manual Blacklisting** window.
3. Enter the MAC address of the client to be blacklisted in the **MAC address to add** text box.

Figure 203 *Manual Blacklisting*



Manual Blacklisting

Manual Blacklist

MAC Address	Blacklisted Since
01:23:45:67:89:ab	New

MAC address to add: 11:23:45:67:89:ab

4. Click **Ok**.

The **Blacklisted Since** tab displays the time at which the current blacklisting started for the client.

5. To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklisting** window and then click **Delete**.

Dynamic Blacklisting

The clients can be blacklisted dynamically when they exceed the authentication failure threshold or a blacklisting rule was triggered as part of the authentication process.

Authentication Failure Blacklisting

When the time taken by a client fails to authenticate exceeds the configured threshold, the client is automatically blacklisted by an IAP.

Session Firewall Based Blacklisting

In session firewall based blacklisting, an ACL rule is used to enable the option for automation blacklisting. when the ACL rule is hit, it would send out blacklist information and the client would be blacklisted.

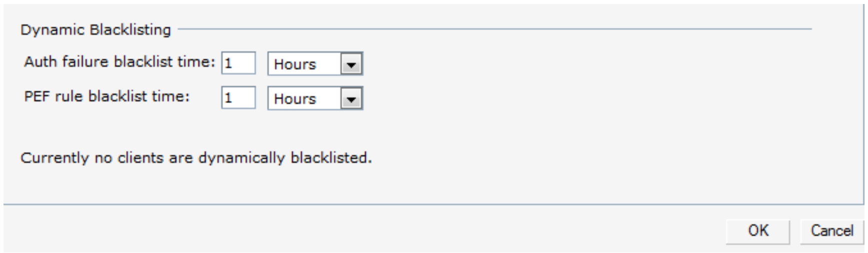
To set the blacklist duration:

1. Select the **PEF** link and then select **Blacklisting** tab.

- **Auth failure blacklist time**— Enter the duration since the blacklisting has been triggered when the authentication failure threshold is exceeded.
- **PEF rule blacklisted time**— Enter the duration since the blacklisting has been triggered when a blacklisting rule has been triggered.

> NOTE
>
> In the **Networks** tab, click the **New** link and navigate to **New WLAN > VLAN > Security** page to enable **Blacklisting**. Set a value between 1 to 10 in the **max authentication failures** field for the selected SSID.
> To enable session firewall based blacklisting, click **New** and navigate to **WLAN Settings > VLAN > Security > Access** window and enable the **Blacklist** option of the corresponding ACL rule.

Figure 204 *Dynamic Blacklisting*



Dynamic Blacklisting

Auth failure blacklist time: 1 Hours

PEF rule blacklist time: 1 Hours

Currently no clients are dynamically blacklisted.

PEF Settings

Firewall ALG Configuration

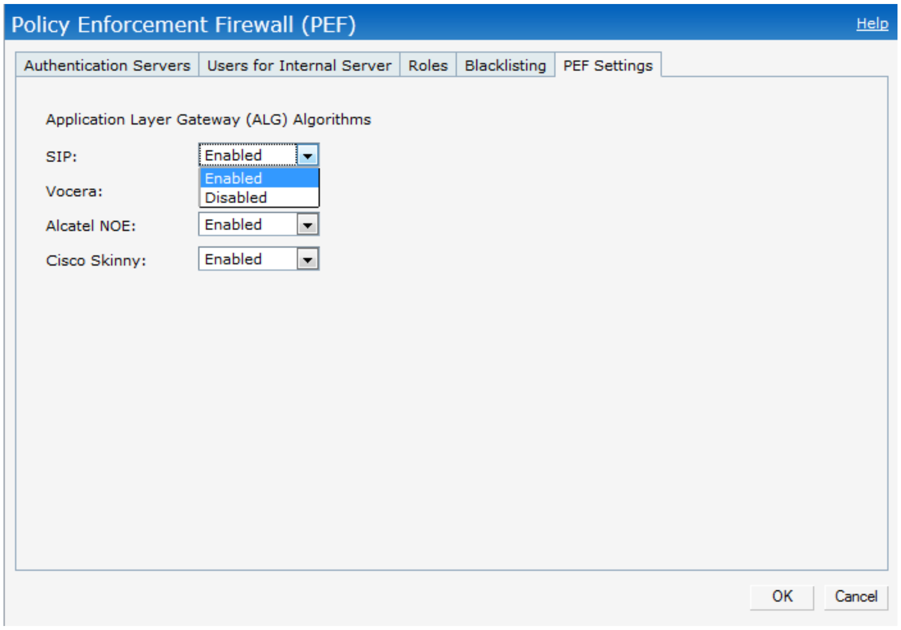
Instant firewall now supports the ALG (Application Layer Gateway) functions such as SIP, Vocera, Alcatel NOE, and Cisco Skinny protocols.

To enable or disable the protocols for ALG in Aruba Instant perform the following steps:

1. Select **PEF** from the top right of the Instant UI.

2. Select **PEF Settings** tab.
3. Select **Enabled** from the corresponding drop-down list to enable SIP, VOCERA, Alcatel NOE, and Cisco skinny protocols.

Figure 205 *Enabling ALG Protocols*



Policy Enforcement Firewall (PEF)

Application Layer Gateway (ALG) Algorithms

SIP: Enabled (Enabled / Disabled)

Vocera:

Alcatel NOE: Enabled

Cisco Skinny: Enabled

4. Click **OK.**

When the protocols for ALG are **Disabled** the changes do not take effect until the existing user sessions expire. Reboot the IAP and the client, or wait for few minutes to ensure the changes take effect.

Firewall-based Logging

Instant firewall now supports firewall based logging function. The firewall logs on the Instant APs are generated as syslog messages.

VPN Configuration

The IAP supports termination of a VPN tunnel on the Aruba controller.

VPN features are ideal for:

- enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
- branch offices that require multiple APs.
- individuals working from home, connecting to the VPN.

This new architecture and form factor seamlessly adds the survivability feature of Instant APs with the VPN connectivity of RAPs — providing corporate connectivity to non-corporates.

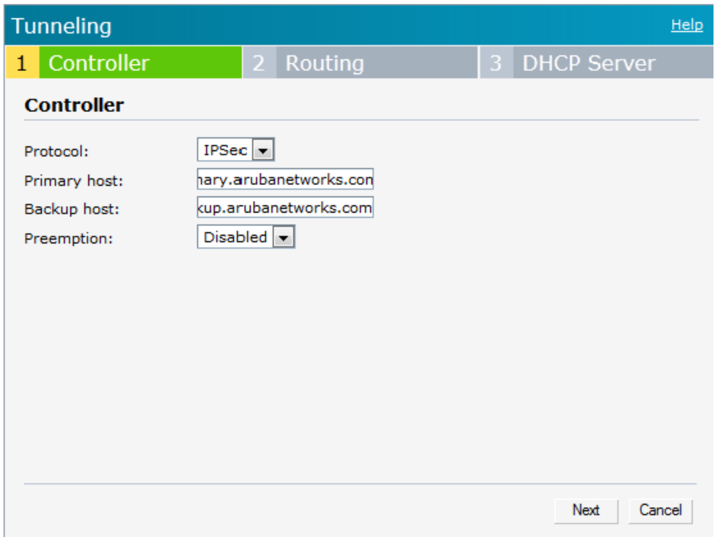
The following VPN features are briefly described:

VPN Configuration

The VPN configuration functionality enables the IAP to create a single VPN tunnel from the Virtual Controller to a Aruba Mobility Controller in your corporate office. Here, the VPN tunnels from the Instant APs terminate on the Aruba Mobility Controller. The controller solely acts as a VPN end-point and does not supply the Instant AP with any configuration.

To create a VPN tunnel from the Virtual Controller to an Aruba Mobility Controller:

Figure 206 *Tunneling— Controller*



Controller

Protocol: IPSec

Primary host: nary.arubanetworks.con

Backup host: kup.arubanetworks.com

Preemption: Disabled

1. Navigate to the **VPN** link at the top right corner of the Instant WebUI. The **Tunneling** window appears.
2. Select **IPSec** from the **Protocol** drop-down list.
3. If you select **GRE** from the **Protocol** drop-down list then the packets are sent and received without encryption.
   a. **GRE type** — Enter the value for GRE type parameter.
   b. **Per-AP tunnel** — Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. The user can create GRE tunnels from all of the APs instead of creating tunnels only from the AP that is acting

as the Virtual Controller. The traffic going to the corporate is send via L2 GRE tunnel from the AP itself and does not have to be forwarded through the Virtual Controller.

NOTE

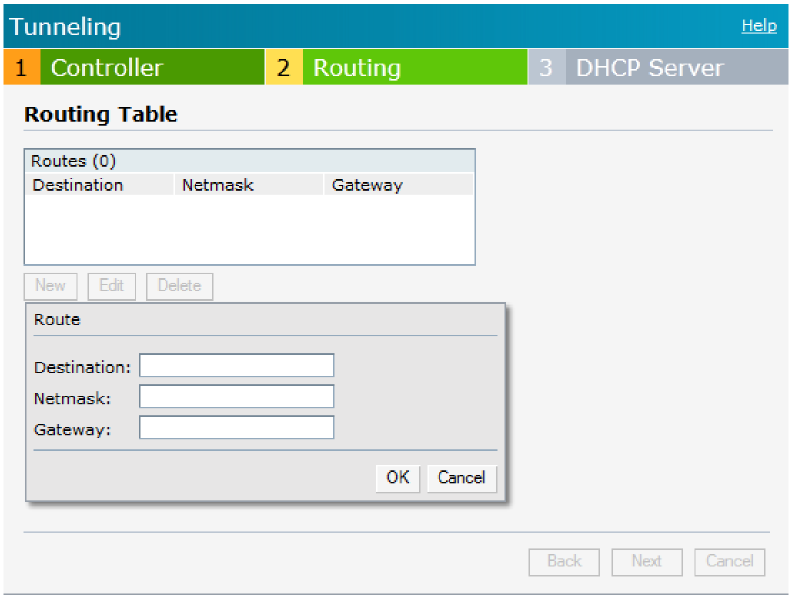
By default, the **Per-AP tunnel** option is disabled.

4. Enter the IP address or fully qualified domain name for the main VPN/GRE endpoint in the **Primary host** field.
5. Enter the IP address or fully qualified domain name for the backup VPN endpoint in the **Backup host** field. This entry is optional.
6. Select **Enabled** from the **Preemption** drop-down list to switch back to the primary host when and if it becomes available again. This step is optional.
7. Click **Next** to continue.

Routing Profile Configuration

Instant can terminate a single VPN connection on an Aruba Mobility Controller. The Routing profile defines the corporate subnets which need to be tunneled through the IPSec tunnel.

Figure 207 *Tunneling— Routing*



Use the **Routing Table** to specify policy based on routing into the VPN tunnel. Each routing table entry has a destination, network mask, and default gateway.

8. Click **New** and update the following parameters.
   - Destination— Specify the destination network to be routed into the VPN tunnel.
   - Netmask— Specify the network mask of the network to be routed into the VPN tunnel.
   - Gateway— Specify the default gateway to which traffic should be routed. This IP address should be the 'controller-ip' of the controller on which the VPN connection is terminated. See "Controller Configuration for VPN" on page 259 for more information.

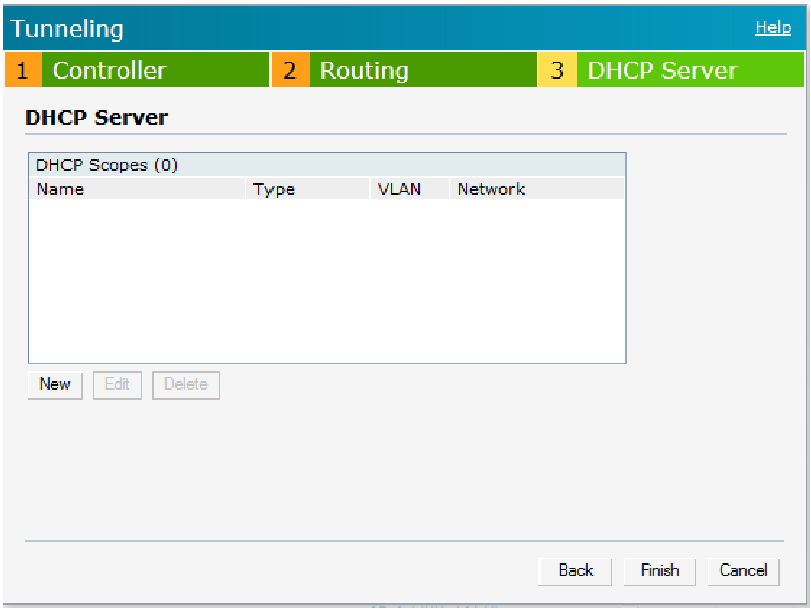
     In the example above, 10.0.0.0/8 network is configured as the corporate destination and is routed through the controller-ip of the primary controller.
9. Click **Next** to continue.
10. The **DHCP Server** window appears. Use this table to define DHCP pools of different types based on your deployment modes as described in the following section.

DHCP Server Configuration

The Virtual Controller (VC) on an Instant AP enables different DHCP pools (various deployment models) in addition to allocating IP subnets to each branch. The following modes of DHCP server are supported:

- Local Subnet— In this mode, the VC assigns an IP address from a configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. This is achieved by appropriately translating the network address (NAT) and forwarding the packet through the IPSec tunnel or through the uplink.
- L2 Switching Mode— In this mode, Instant supports the following two types to support L2 switching mode of connection to corporate:
  - Distributed L2— In this mode, the VC assigns an IP address from a configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The VC adds the VLAN configured in this subnet to the controller VLAN multicast table enabling the L2 subnet to act as an extension of the VLAN on the controller. Corporate traffic is sent on the IPSec tunnel and non-corporate traffic is sent on the uplink.
  - Centralized L2— In this mode, the VC does not assign an IP address to the client, but the DHCP traffic is directly forwarded to the controller over the IPSec tunnel and gets an IP address from either the controller or a DHCP server behind the controller serving the VLAN of the client. However, Instant AP does forward client traffic in the same way as the **Distributed L2** mode.
- L3 Routing Mode— In this mode, Instant supports L3 routing mode of connection to corporate. VC assigns an IP addresses from the configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. Instant AP takes care of routing on the subnet and also adds a route on the controller after the VPN tunnel is set up during the registration of the subnet.

Figure 208 *Tunneling— DHCP Server*



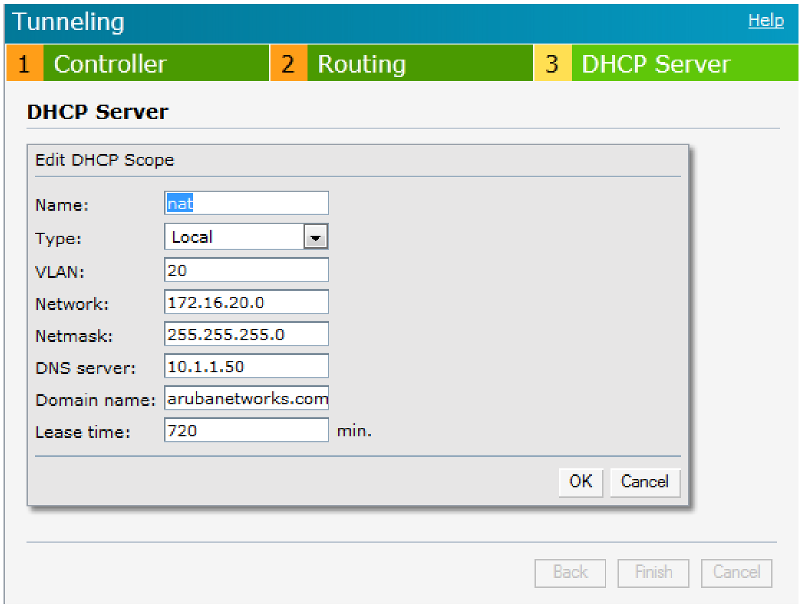
NAT DHCP Configuration

In NAT mode, the scope of the subnet is local to the IAP and forwards traffic through the IPSec tunnel or through the uplink.

1. Click **New** in the **DHCP Server** window and select **Local** to configure the following parameters for NAT mode DHCP pool.
   - Name— Name of the subnet (must be unique).
   - Type— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Local** implies that this is a NAT mode DHCP subnet.

- VLAN— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
- Network— Network to be used for this subnet.
- Netmask— Net mask of the subnet. This along with Network determines the size of the subnet.
- DNS server— An optional field which defines the DNS server.
- Domain name— An optional field which defines the domain name.
- Lease time— An optional field which defines the lease time for client.

Figure 209 *NAT DHCP Configuration*



Name:	nat
Type:	Local
VLAN:	20
Network:	172.16.20.0
Netmask:	255.255.255.0
DNS server:	10.1.1.50
Domain name:	arubanetworks.com
Lease time:	720 min.

2. Click **OK** to apply these changes.

Distributed L2 DHCP Configuration

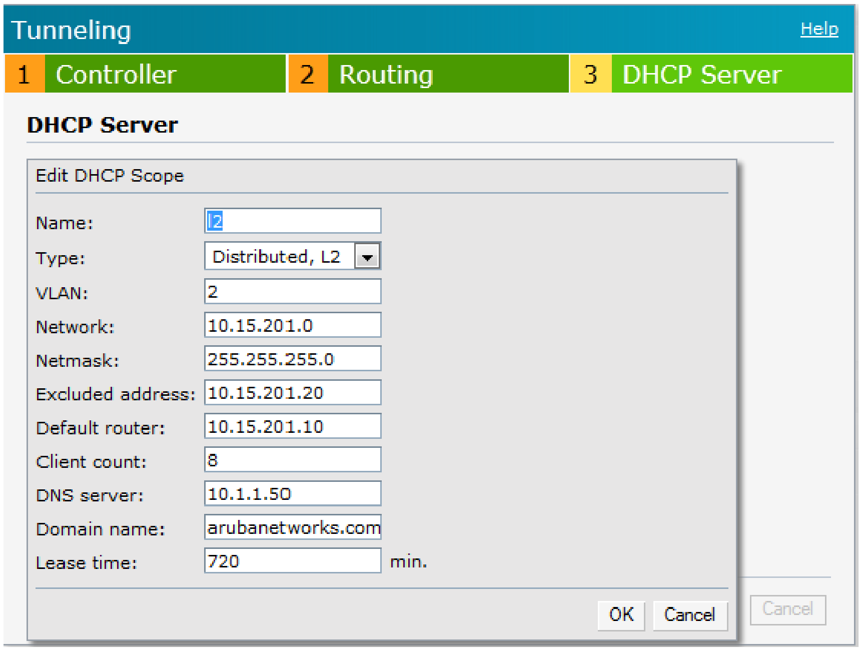
In Distributed L2 mode, the Virtual Controller acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel.

1. Click **New** in the **DHCP Server** window and select **Distributed, L2** to configure the following parameters for Distributed L2 mode DHCP pool:
   - Name— Name of the subnet (must be unique).
   - Type— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Distributed, L2** implies that this is a Distributed mode L2 DHCP subnet.
   - VLAN— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
   - Network— Network to be used for this subnet.
   - Netmask— Net mask of the subnet. This along with Network determines the size of the subnet.
   - Excluded address— This determines the exclusion range of the subnet. Based on the size of the subnet and value configured here (location within the subnet scope), this is used to either exclude IP addresses before this IP or after this IP. This is an optional field.
   - Default router— Default router for the subnet. This is an IP address on/behind the controller in the same subnet.
   - Client count— This along with network and mask determines how many branches can be supported. For the current phase of IAP, it is important that this value is configured consistent across all branches.

- DNS server— An optional field which defines the DNS server.
- Domain name— An optional field which defines the domain name.
- Lease time— An optional field which defines the lease time for client.

2. Click **OK** to apply these changes.

Figure 210 *Distributed L2 DHCP Configuration*



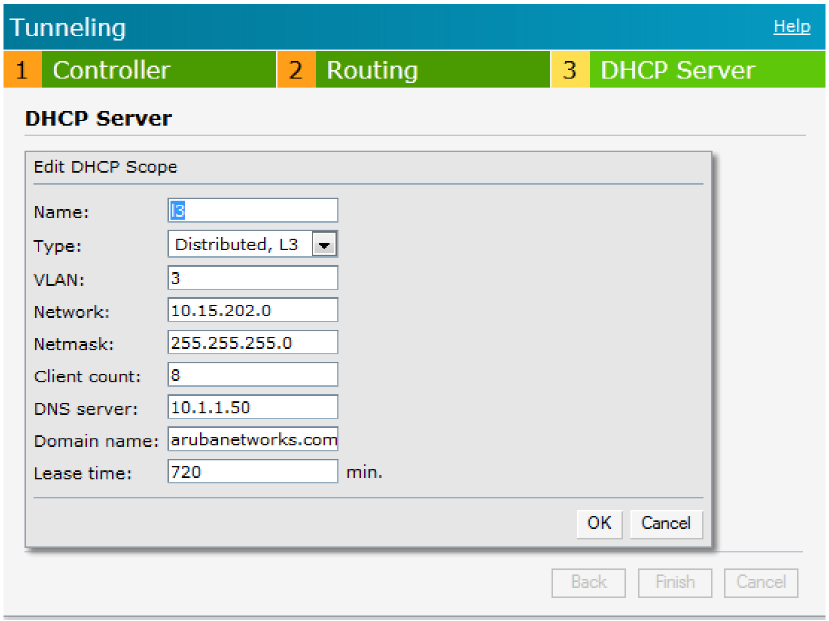
Name: L2
Type: Distributed, L2
VLAN: 2
Network: 10.15.201.0
Netmask: 255.255.255.0
Excluded address: 10.15.201.20
Default router: 10.15.201.10
Client count: 8
DNS server: 10.1.1.50
Domain name: arubanetworks.com
Lease time: 720 min.

Distributed L3 DHCP Configuration

In Distributed L3 mode, the Virtual Controller acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel.

1. Click **New** in the **DHCP Server** window and select **Distributed, L3** to configure the following parameters for Distributed L3 mode DHCP pool:
   - Name — Name of the subnet (must be unique).
   - Type— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Distributed, L3** implies that this is a Distributed mode L3 DHCP subnet.
   - VLAN— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
   - Network— Network to be used for this subnet.
   - Netmask— Net mask of the subnet. This along with Network determines the size of the subnet.
   - Client count— This along with network and mask determines how many branches can be supported. For the current phase of IAP, it is important that this value is configured consistent across all branches.
   - DNS server— An optional field which defines the DNS server.
   - Domain name— An optional field which defines the domain name.
   - Lease time— An optional field which defines the lease time for client
2. Click **OK** to apply these changes.

Figure 211 *Distributed L3 DHCP Configuration*



DHCP Server

Edit DHCP Scope

Name:	L3
Type:	Distributed, L3
VLAN:	3
Network:	10.15.202.0
Netmask:	255.255.255.0
Client count:	8
DNS server:	10.1.1.50
Domain name:	arubanetworks.com
Lease time:	720 min.

Centralized L2 DHCP Configuration

In Centralized L2 mode, both the DHCP server and default gateway are in the data center, on the other side of the VPN tunnel.

1. Click **New** in the **DHCP Server** window and select **Centralized, L2** to configure the following parameters for the Distributed L3 mode DHCP pool:
   - Name — Name of the subnet (must be unique).
   - Type— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Centralized, L2** implies that this is a Centralized mode L2 DHCP subnet.
   - VLAN— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
   - DHCP RelayDHCP Relay Agent and Option 82— Select to enable or disable these features.

     When a DHCP server is configured with a DHCP Relay agent, the client's Broadcast DHCP Discover packet is not sent to the corporate network, instead the Virtual Controller acts as the DHCP Relay and unicasts DHCP packets to the corporate DHCP server. Enable DHCP Option 82 to allow clients to send DHCP packets with the Option 82 string.

     The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following:
     - Remote Circuit ID¡X AP-MAC; SSID; SSID-Type
     - Remote Agent¡X IDUE-MAC

NOTE

The Option 82 is specific to Alcatel and is not configurable in this version of Instant.

The following table describes the behavior of DHCP Relay Agent and Option 82 in the IAP.

Table 44 *DHCP Relay and Option 82*

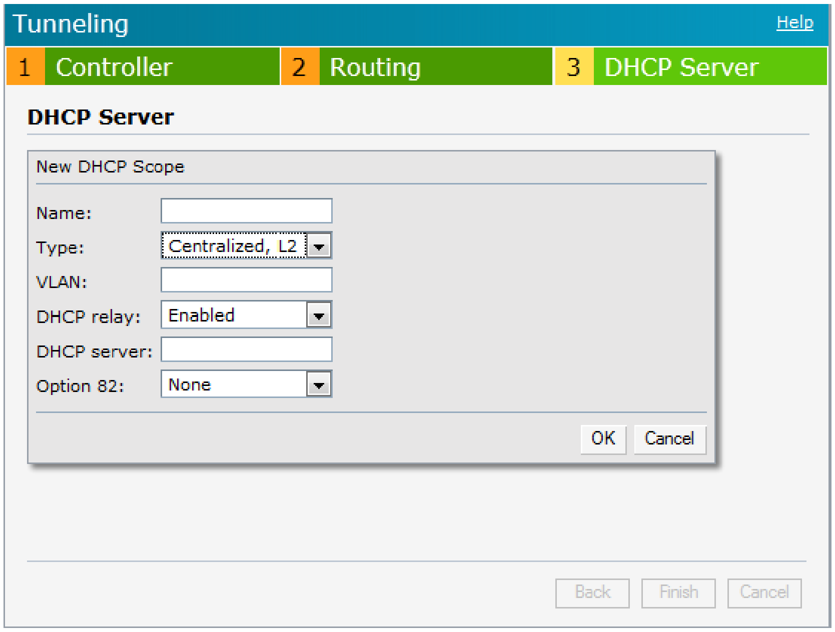
DHCP Relay	Option 82	Behavior
Enabled	Enabled	DHCP packet relayed with the ALU-specific Option 82 string

Table 44 *DHCP Relay and Option 82 (Continued)*

DHCP Relay	Option 82	Behavior
Enabled	Disabled	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	Enabled	DHCP packet not relayed, but broadcasted with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcasted without the ALU-specific Option 82 string

2. Click **OK** to apply these changes.

Figure 212 *Centralized L2 DHCP Configuration*



DHCP Server

New DHCP Scope

Name:

Type: Centralized, L2

VLAN:

DHCP relay: Enabled

DHCP server:

Option 82: None

Chapter 30

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 is temporarily using the enterprise network to access the internet. However, you may not want to share the internal network and the intranet with them. To segregate the guest traffic from the enterprise traffic, you can create a Guest WLAN, specify the required authentication, encryption, and access rules and allow the guest user to use the enterprise network.

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

NOTE

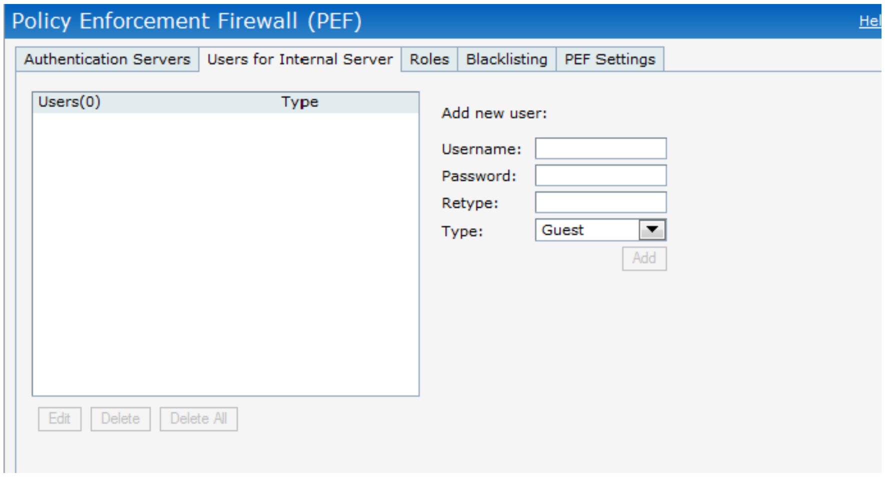
The User Database is also used when Instant is employed as an internal RADIUS server.

Adding a User

To add a user:

1. At the top right corner of the Instant UI, click the **PEF** link and click **Users for Internal Server**.

Figure 213 *Adding a User*



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

Editing User Settings

To edit user settings:

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

Deleting a User

To delete a user:

1. At the top right corner of the Instant UI, click the **Users** link. The **Users** window appears.
2. In the **Users** section, select the username that you want to delete and click **Delete.**
   To delete all users or multiple users at a time, select the usernames that you want to delete, and click **Delete All**.

NOTE

Deleting a user only removes the user record from the user database, and won't disconnect the online user associated with this username.

Chapter 31

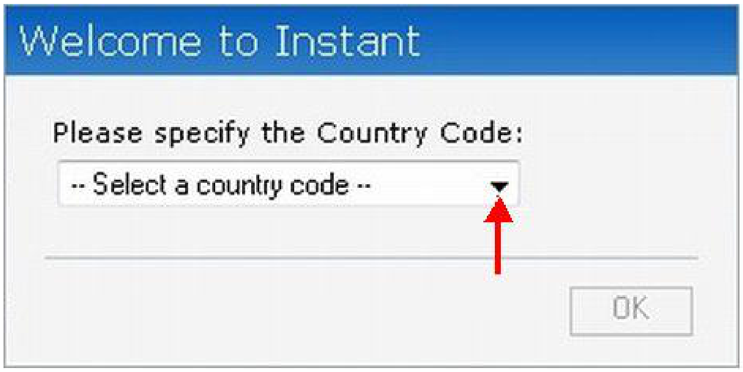
Regulatory Domain

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

The initial Wi-Fi setup requires you to specify the country code for the country in which the Aruba Instant operates. This configuration sets the regulatory domain for the radio frequencies that the IAPs use. Within the regulated transmission spectrum, a high-throughput 802.11a, 802.11b/g, or 802.11n radio setting can be configured. The available 20 MHz and 40 MHz channels are dependent on the specified country code.

You cannot change the country code for the IAPs designated for US, Japan, and Israel. Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions on operators of wireless networks with devices set to improper country codes. Table 45 shows the list of country codes.

Figure 214 *Specifying a Country Code*



Welcome to Instant

Please specify the Country Code:

Country Codes List

Table 45 *Country Codes List*

Code	Country Name
US	United States
CA	Canada
JP3	Japan
DE	Germany
NL	Netherlands
IT	Italy
PT	Portugal
LU	Luxembourg
NO	Norway
FI	Finland
DK	Denmark
CH	Switzerland
CZ	Czech Republic
ES	Spain
GB	United Kingdom
KR	Republic of Korea (South Korea)
CN	China
FR	France
HK	Hong Kong
SG	Singapore
TW	Taiwan
BR	Brazil
IL	Israel
SA	Saudi Arabia
LB	Lebanon
AE	United Arab Emirates
ZA	South Africa

Table 45 *Country Codes List (Continued)*

Code	Country Name
AR	Argentina
AU	Australia
AT	Austria
BO	Bolivia
CL	Chile
GR	Greece
IS	Iceland
IN	India
IE	Ireland
KW	Kuwait
LI	Liechtenstein
LT	Lithuania
MX	Mexico
MA	Morocco
NZ	New Zealand
PL	Poland
PR	Puerto Rico
SK	Slovak Republic
SI	Slovenia
TH	Thailand
UY	Uruguay
PA	Panama
RU	Russia
KW	Kuwait
LI	Liechtenstein
LT	Lithuania
MX	Mexico
MA	Morocco

Table 45 *Country Codes List (Continued)*

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

Table 45 *Country Codes List (Continued)*

Code	Country Name
BH	Bahrain
OM	Oman
JO	Jordan
BM	Bermuda
CO	Colombia
DO	Dominican Republic
GT	Guatemala
PH	Philippines
LK	Sri Lanka
SV	El Salvador
TN	Tunisia
PK	Islamic Republic of Pakistan
QA	Qatar
DZ	Algeria

Appendix A

Controller Configuration for VPN

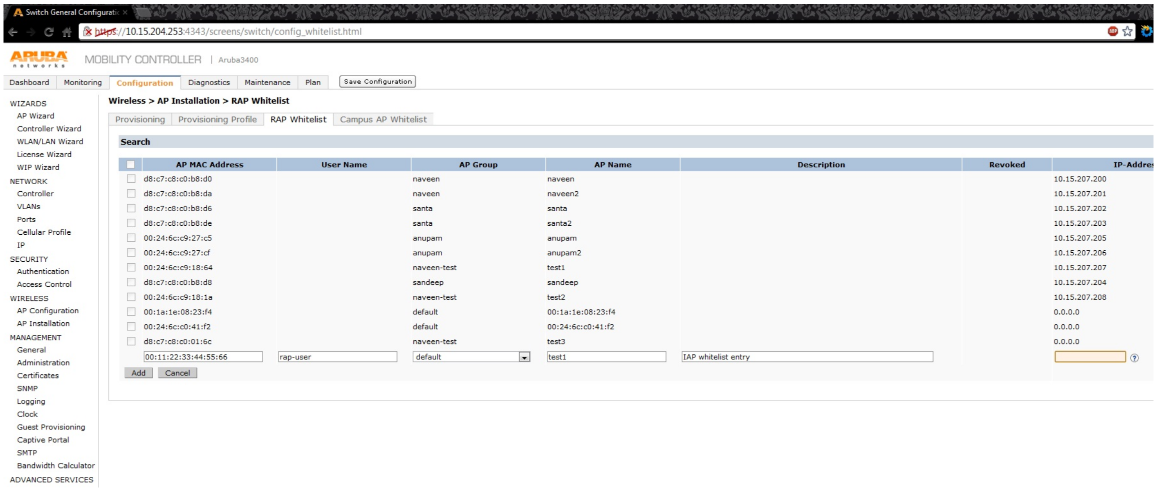
On the controller, the following configuration is needed to setup an IAP.

Whitelist DB Configuration

If you decide to use the Controller as the whitelist entry to configure the whitelist database, use the following CLI command:

```
(Aruba3400) #local-userdb-ap add mac-address 00:11:22:33 44:55 ap-group test
(Aruba3400) #
```

The ap-group parameter is not used for any configuration, but needs to be configured. The parameter can be any valid string. If an external whitelist is being used, the AP MAC address needs to be saved in the RADIUS server as a lower-case entry without any delimiter.



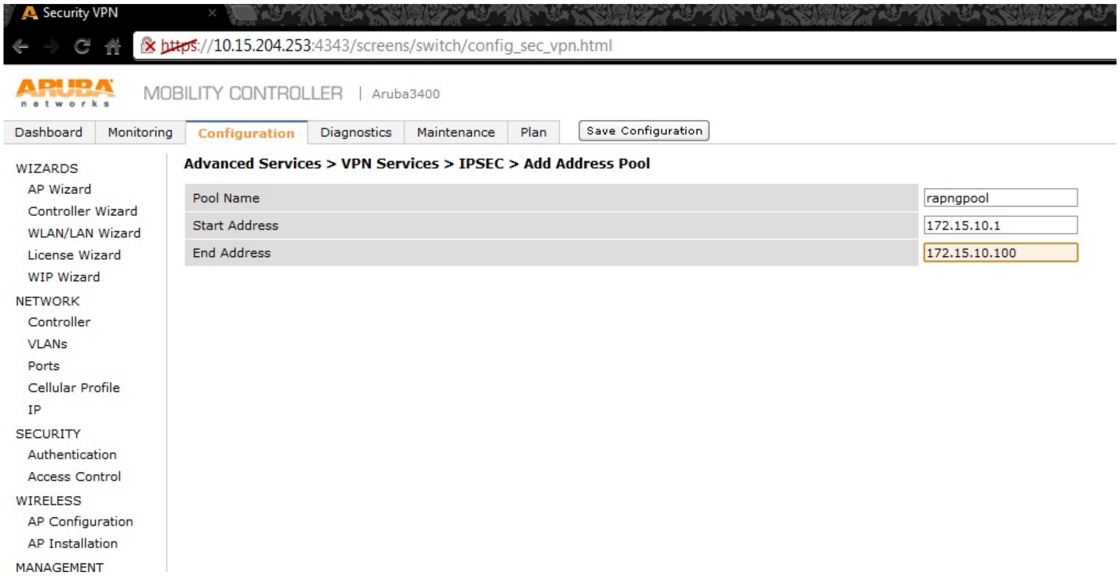
Wireless > AP Installation > RAP Whitelist

□	AP MAC Address	User Name	AP Group	AP Name	Description	Revoked	IP-Addres
□	d8:c7:c8:c0:b8:d0		naveen	naveen			10.15.207.200
□	d8:c7:c8:c0:b8:da		naveen	naveen2			10.15.207.201
□	d8:c7:c8:c0:b8:d6		santa	santa			10.15.207.202
□	d8:c7:c8:c0:b8:de		santa	santa2			10.15.207.203
□	00:24:6c:c9:27:c5		anupam	anupam			10.15.207.205
□	00:24:6c:c9:27:cf		anupam	anupam2			10.15.207.206
□	00:24:6c:c9:18:64		naveen-test	test1			10.15.207.207
□	d8:c7:c8:c0:b8:d8		sandeep	sandeep			10.15.207.204
□	00:24:6c:c9:18:1a		naveen-test	test2			10.15.207.208
□	00:1a:1e:08:23:f4		default	00:1a:1e:08:23:f4			0.0.0.0
□	00:24:6c:c0:41:f2		default	00:24:6c:c0:41:f2			0.0.0.0
□	d8:c7:c8:c0:01:6c		naveen-test	test3			0.0.0.0
	00:11:22:33:44:55:66	rap-user	default	test1	IAP whitelist entry		

VPN Local Pool Configuration

This pool is used to assign an IP Address to the IAP after successful VPN authentication.

```
(Aruba3400) # ip local pool "rapngpool" <startip> <endip>
(Aruba3400) #
```



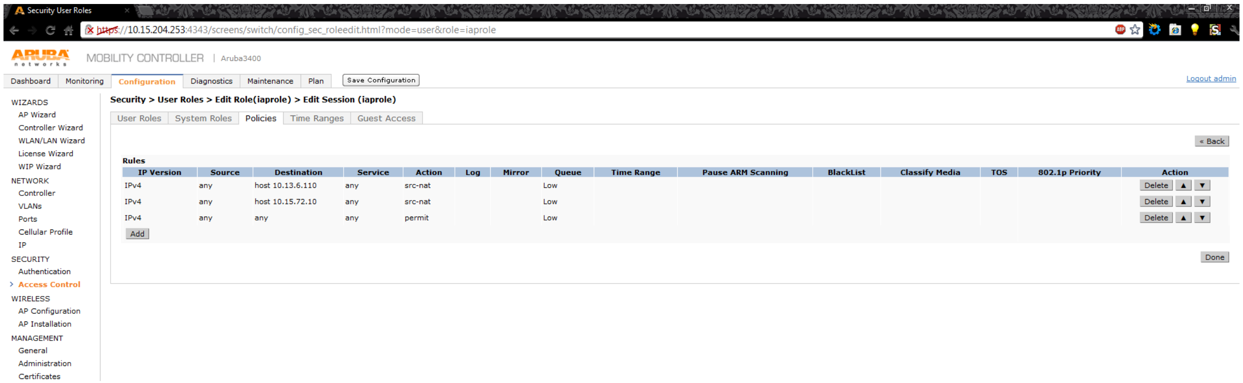
Advanced Services > VPN Services > IPSEC > Add Address Pool

Pool Name	rapngpool
Start Address	172.15.10.1
End Address	172.15.10.100

IAP VPN Profile Configuration

This defines the server used to authenticate the IAP (internal or an external server) and the role for IAP user. This role is used to define the src-nat rule to RADIUS server to allow Dynamic RADIUS proxy.

```
(Aruba3400) (config) #ip access-list session iaprole
(Aruba3400) (config-sess-iaprole)#any host <radius-server-ip> any src-nat
(Aruba3400) (config-sess-iaprole)#any any any permit
(Aruba3400) (config-sess-iaprole)#!
```

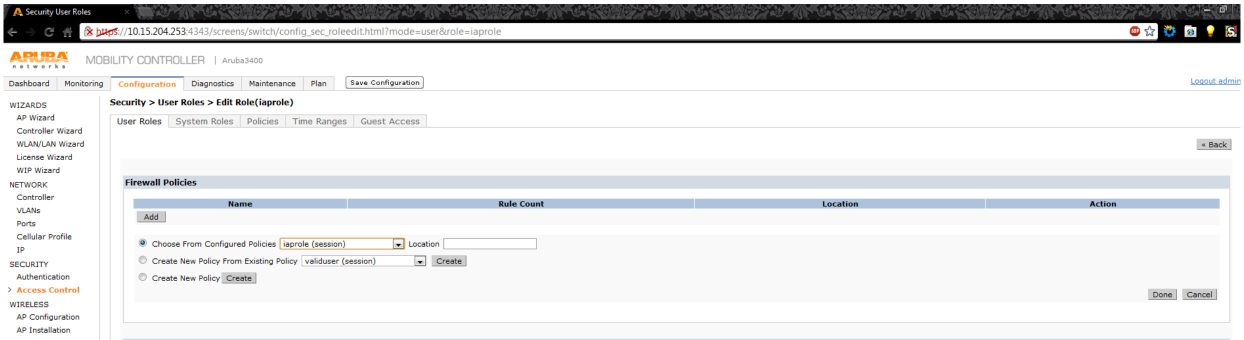


Security > User Roles > Edit Role(iaprole) > Edit Session (iaprole)

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	BlackList	Classify Media	TOS	802.1p Priority	Action
IPv4	any	host 10.13.6.110	any	src-nat			Low							Delete ▲ ▼
IPv4	any	host 10.15.72.10	any	src-nat			Low							Delete ▲ ▼
IPv4	any	any	any	permit			Low							Delete ▲ ▼

```
(Aruba3400) (config) #user-role iaprole
(Aruba3400) (config-role) #session-acl iaprole
(Aruba3400) (config-role) #
```



Security > User Roles > Edit Role(iaprole)

Firewall Policies

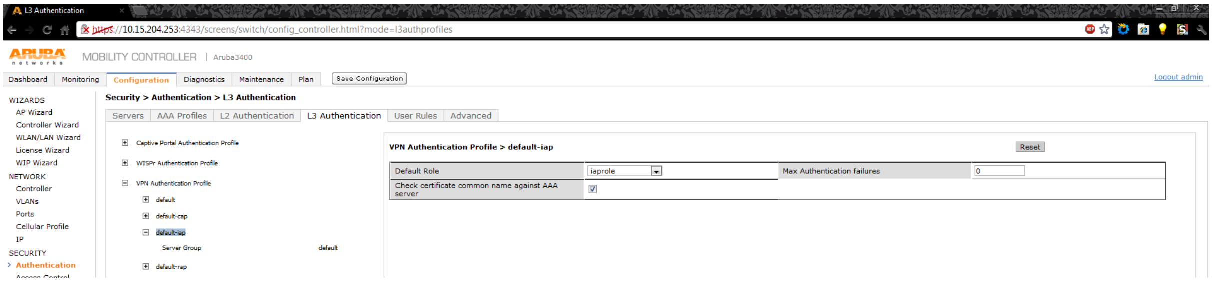
Name	Rule Count	Location	Action

● Choose From Configured Policies: iaprole (session) Location:

○ Create New Policy From Existing Policy: validuser (session)

○ Create New Policy

```
(Aruba3400) (config) #aaa authentication vpn default-iap
(Aruba3400) (VPN Authentication Profile "default-iap") #server-group default
(Aruba3400) (VPN Authentication Profile "default-iap") #default-role iaprole
(Aruba3400) (VPN Authentication Profile "default-iap") #!
(Aruba3400) (config) #
```



Security > Authentication > L3 Authentication

- Captive Portal Authentication Profile
- WISPr Authentication Profile
- VPN Authentication Profile
  - default
  - default-cap
  - default-iap
    - Server Group: default
  - default-rap

VPN Authentication Profile > default-iap

Default Role	iaprole	Max Authentication failures	0
Check certificate common name against AAA server	☑		

Appendix B

Abbreviations

Abbreviations

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

Table 46 *List of abbreviations*

Abbreviation	Expansion
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
BSS	Basic Server Set
BSSID	Basic Server Set Identifier
CA	Certification Authority
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
IAP	Instant Access Point
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
Instant WebUI	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

Table 46 *List of abbreviations (Continued)*

Abbreviation	Expansion
NTP	Network Time Protocol
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial In User Service
VC	Virtual Controller
VSA	Vendor-Specific Attributes
WLAN	Wireless Local Area Network