

# AOS-W Instant 5.0.3.0-1.1



User Guide

## Copyright

© 2011 Alcatel-Lucent. All rights reserved.  
Specifications in this manual are subject to change without notice.  
Originated in the USA.

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 are trademarks of Alcatel-Lucent in the United States and certain other countries.

Any other trademarks appearing in this manual are the property of their respective companies.

## Legal Notice

The use of Alcatel-Lucent switching platforms and software, by all individuals or corporations, to terminate Cisco or Nortel VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Alcatel-Lucent from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of Cisco Systems or Nortel Networks".



[www.alcatel-lucent.com](http://www.alcatel-lucent.com)  
26801 West Agoura Road  
Calabasas, CA 91301

<b>About this Guide</b> .....	<b>15</b>
Objective.....	15
Intended Audience.....	15
Conventions.....	15
Contacting Support .....	16
<b>Chapter 1</b> <b>OAW IAP Internal Antenna Patterns</b> .....	<b>17</b>
OAW IAP-92 and OAW IAP-93 Antenna Patterns .....	17
OAW IAP-105 Antenna Pattern .....	18
<b>Chapter 2</b> <b>Initial Configuration</b> .....	<b>21</b>
Initial Setup.....	21
Pre-Installation Checklist .....	21
Connecting the OAW IAP to a Power Source .....	22
Assigning an IP Address to the OAW IAP .....	22
Connecting to the Provisioning Wi-Fi network.....	22
Login into Instant User Interface .....	23
Specifying the Country Code .....	24
<b>Chapter 3</b> <b>Instant User Interface</b> .....	<b>25</b>
Understanding the Instant UI Layout.....	25
Banner.....	26
Search .....	26
Tabs .....	26
Networks Tab .....	26
Access Points Tab.....	27
Clients Tab.....	27
Links.....	28
New version available .....	28
Users.....	28
Settings.....	29
Servers.....	30
Roles.....	30
Maintenance .....	30
Support.....	30
Help .....	32
Logout.....	32
Monitoring.....	33
Client Alerts .....	35
IDS .....	36
Language.....	37
OmniVista 3600 Air Manager Setup .....	37
Pause/Resume .....	37
Views.....	38
<b>Chapter 4</b> <b>Wireless Network</b> .....	<b>39</b>
Network Types.....	39

	Employee Network.....	39
	Adding an Employee Network.....	39
	Voice Network.....	46
	Adding a Voice Network.....	46
	Guest Network.....	49
	Adding a Guest Network.....	49
	Editing a Network.....	52
	Deleting a Network.....	53
	Bandwidth Contracts.....	53
<b>Chapter 5</b>	<b>Mesh Network.....</b>	<b>55</b>
	Mesh Instant Access Points.....	55
	Mesh Portals.....	55
	Mesh Points.....	56
	Instant Mesh Setup.....	56
<b>Chapter 6</b>	<b>Managing OAW IAPs.....</b>	<b>59</b>
	Auto Join Mode.....	59
	Disabling Auto Join Mode.....	59
	LED Display.....	60
	Terminal Access.....	60
	Syslog Server.....	61
	Adding an OAW IAP to the Network.....	61
	Removing an OAW IAP from the Network.....	62
	Editing OAW IAP Settings.....	62
	Changing OAW IAP Name.....	62
	Changing IP Address of the OAW IAP.....	63
	Configuring Adaptive Radio Management.....	64
	Configuring an External Antenna.....	65
	Migrating from a Virtual Controller.....	65
	Rebooting the OAW IAP.....	67
	Firmware Image Server in Cloud Network.....	67
	Automatic Firmware Image Check and Upgrade.....	68
	Upgrading to the new OS version.....	68
	Manual Firmware Image Check and Upgrade.....	69
<b>Chapter 7</b>	<b>NTP Server.....</b>	<b>71</b>
	Configuring an NTP Server.....	71
<b>Chapter 8</b>	<b>Virtual Controller.....</b>	<b>73</b>
	Master Election Protocol.....	73
	Virtual Controller IP Address.....	73
	Specifying Name and IP Address for the Virtual Controller.....	73
	Configuring the DHCP Server.....	74
<b>Chapter 9</b>	<b>Authentication.....</b>	<b>75</b>
	Authentication Methods in Alcatel-Lucent Instant.....	75
	802.1X Authentication.....	75
	Internal RADIUS Server.....	75
	External RADIUS Server.....	76
	Configuring an External RADIUS Server.....	76
	Enabling Instant RADIUS.....	77
	RADIUS Server Authentication with VSA.....	78

	List of supported VSA's.....	78
	Management Authentication Settings .....	80
	Captive Portal .....	81
	Internal Captive Portal.....	81
	Configuring Internal Captive Portal Authentication when Adding a Guest Network .....	82
	Configuring Internal Captive Portal Authentication when Editing a Guest Network .....	82
	Configuring Internal Captive Portal with External Radius Server Authentication when Adding a Guest Network.....	83
	Customizing a Splash Page.....	84
	Disabling Captive Portal authentication .....	85
	External Captive Portal .....	85
	Configuring External Captive Portal Authentication when Adding a Guest Network .....	86
	Configuring External Captive Portal Authentication when editing a Guest Network .....	86
	MAC Authentication.....	87
	Configuring MAC Authentication .....	87
	Certificates.....	88
	Loading Certificates .....	88
<b>Chapter 10</b>	<b>Encryption .....</b>	<b>91</b>
	Encryption Types Supported in Alcatel-Lucent Instant.....	91
	WEP .....	91
	TKIP.....	91
	AES .....	91
	Encryption Recommendations .....	91
	Understanding WPA and WPA2 .....	91
	Recommended Authentication and Encryption Combinations.....	92
<b>Chapter 11</b>	<b>Role Derivation.....</b>	<b>93</b>
	User Roles .....	93
	Creating a New User Role.....	93
	Creating Role Assignment Rules .....	94
<b>Chapter 12</b>	<b>Guest DMZ .....</b>	<b>97</b>
<b>Chapter 13</b>	<b>Instant Firewall.....</b>	<b>99</b>
	Service Options .....	99
	Destination Options .....	101
	Example Access Rules .....	101
	Allow TCP service to a particular network .....	102
	Allow PoP3 service to a particular server .....	103
	Deny FTP service except to a particular server .....	103
	Deny bootp service except to a particular network .....	104
<b>Chapter 14</b>	<b>Content Filtering .....</b>	<b>107</b>
	Enabling Content Filtering .....	107
<b>Chapter 15</b>	<b>OS Fingerprinting.....</b>	<b>109</b>
<b>Chapter 16</b>	<b>Adaptive Radio Management .....</b>	<b>111</b>
	ARM Features .....	111

	Channel or Power Assignment.....	111
	Voice Aware Scanning .....	111
	Load Aware Scanning .....	111
	Band Steering Mode .....	111
	Air Time Fairness.....	112
	Air Time Fairness Modes .....	112
	Customize valid channels .....	112
	Min transmit power .....	112
	Max transmit power .....	112
	Monitoring the Network with ARM.....	113
	ARM Metrics .....	113
	Configuring Administrator Assigned Radio Settings for OAW-IAP .....	113
<b>Chapter 17</b>	<b>Intrusion Detection System .....</b>	<b>115</b>
	Rogue AP Detection and Classification.....	115
	Rogue Containment .....	115
	Containment Methods .....	116
<b>Chapter 18</b>	<b>SNMP .....</b>	<b>117</b>
	SNMP Parameters for OAW IAP.....	117
<b>Chapter 19</b>	<b>OmniVista 3600 Air Manager Integration and Management.....</b>	<b>121</b>
	OmniVista 3600 Air Manager Features.....	121
	Image Management .....	121
	OAW-IAP and Client Monitoring .....	121
	Template Based Configuration .....	121
	Trending Reports .....	122
	Intrusion Detection System .....	122
	Configuring OmniVista 3600 Air Manager .....	122
	Creating your Organization String.....	122
	The Shared Key.....	123
	Entering the Organization String and AMP Information into the OAW IAP	123
	OmniVista 3600 Air Manager Discovery through DHCP Option .....	123
<b>Chapter 20</b>	<b>Monitoring .....</b>	<b>125</b>
	Virtual Controller View .....	125
	Monitoring Link .....	125
	Info .....	126
	RF Dashboard .....	126
	Usage Trends.....	126
	Client Alerts Link .....	127
	IDS Link.....	127
	Network View.....	128
	Info .....	128
	Usage Trends.....	128
	Instant Access Point View .....	130
	Info .....	131
	RF Dashboard .....	131
	RF Trends.....	131
	Usage Trends.....	134
	Client View .....	134
	Info .....	135
	RF Dashboard .....	135
	RF Trends.....	135
	Mobility Trail.....	138

<b>Chapter 21</b>	<b>Alert Types and Management.....</b>	<b>139</b>
	Alert Types.....	139
<b>Chapter 22</b>	<b>User Database .....</b>	<b>141</b>
	Adding a User.....	141
	Editing User Settings .....	141
	Deleting a User.....	142
<b>Chapter 23</b>	<b>Regulatory Domain.....</b>	<b>143</b>
	Country Codes List.....	144
<b>Appendix A</b>	<b>Abbreviations .....</b>	<b>149</b>
	Abbreviations.....	149





Figure 1	OAW IAP93 Antenna Pattern .....	18
Figure 2	OAW IAP-105 Antenna Pattern .....	19
Figure 3	Connecting to Provisioning Wi-Fi network - Microsoft Windows.....	23
Figure 4	Connecting to Provisioning Wi-Fi network - MAC OS.....	23
Figure 5	Instant User Interface Login Screen .....	24
Figure 6	Specifying the Country Code .....	24
Figure 7	Basic Sections in the Instant UI .....	25
Figure 8	Networks Tab - Compressed View and Expanded View .....	26
Figure 9	Access Points Tab - Compressed View and Expanded View .....	27
Figure 10	Client Tab - Compressed View and Expanded View .....	28
Figure 11	Users Box .....	29
Figure 12	Settings Link - Default View .....	29
Figure 13	Maintenance Link - Default View .....	30
Figure 14	Support Box .....	32
Figure 15	Help Link.....	32
Figure 16	Monitoring on Instant UI .....	33
Figure 17	Info Section in the Monitoring Pane .....	33
Figure 18	RF Dashboard in the Monitoring Pane .....	33
Figure 19	Usage Trends Section in the Monitoring Pane .....	35
Figure 20	Client Alerts link on Instant UI .....	36
Figure 21	Client Alerts Link .....	36
Figure 22	Intrusion Detection on Instant UI .....	37
Figure 23	OmniVista 3600 Air Manager Setup Link.....	37
Figure 24	Adding an Employee Network - Basic Info Tab .....	40
Figure 25	Band and Hide SSID Settings .....	41
Figure 26	Security Tab - Enterprise .....	44
Figure 27	Security Tab - Personal .....	45
Figure 28	Security Tab - Open .....	45
Figure 29	Adding an Employee Network - Access Rules Tab - Network.....	46
Figure 30	Adding a Voice Network - Basic Info Tab .....	47
Figure 31	Adding a Guest Network - Basic Info Tab .....	50
Figure 32	Adding a Guest Network - Splash Page Settings .....	51
Figure 33	Configuring a Splash Page - Encryption Settings .....	52
Figure 34	Open Instant SSID .....	56
Figure 35	Untrusted Connection Window .....	56
Figure 36	Login Window .....	57
Figure 37	Mesh Portal .....	57
Figure 38	Disabling Auto Join Mode .....	59
Figure 39	LED Display .....	60
Figure 40	Terminal Access .....	60
Figure 41	Syslog Server.....	61
Figure 42	Adding an OAW IAP to the Instant Network .....	61
Figure 43	Entering the MAC Address for the New OAW IAP .....	62
Figure 44	Editing OAW IAP Settings .....	62

Figure 45	Changing OAW IAP Name .....	63
Figure 46	Configuring OAW IAP Settings - Connectivity Tab .....	63
Figure 47	Configuring OAW IAP Connectivity Settings - Specifying Static Settings .....	64
Figure 48	Configuring OAW IAP Radio Settings Mode - Access .....	64
Figure 49	Configuring OAW IAP External Antenna Settings .....	65
Figure 50	Maintenance Box .....	66
Figure 51	Maintenance - Convert Tab.....	66
Figure 52	Confirm Access Point Conversion Box .....	66
Figure 53	Rebooting the OAW IAP .....	67
Figure 54	Automatic Image Check - New Version Available Link .....	68
Figure 55	New Version Available Box.....	69
Figure 56	Manual Image Check .....	69
Figure 57	Configuring NTP Server .....	71
Figure 58	Specifying Virtual Controller Name and IP Address .....	73
Figure 59	Configuring the DHCP Server.....	74
Figure 60	Configuring External RADIUS Server .....	77
Figure 61	Enabling Instant RADIUS .....	77
Figure 62	Management Authentication Settings .....	81
Figure 63	Configuring Captive Portal when Adding A Guest Network .....	82
Figure 64	Configuring Captive Portal when Editing a Guest Network.....	83
Figure 65	Configuring Internal Captive Portal with External Radius Server Authentication	84
Figure 66	Customizing a Splash Page.....	85
Figure 67	Disabling Captive Portal Authentication .....	85
Figure 68	Configuring External Captive Portal when Adding a Guest Network .....	86
Figure 69	Configuring External Captive Portal Authentication when editing a Guest Network	87
Figure 70	Configuring MAC Authentication .....	88
Figure 71	Loading Certificates .....	89
Figure 72	Access Tab - Instant User Role Settings.....	93
Figure 73	Creating a New User Role .....	94
Figure 74	Creating Role Assignment Rules .....	95
Figure 75	Access Tab - Instant Firewall Settings .....	99
Figure 76	Defining Rule - Allow TCP Service to a Particular Network .....	102
Figure 77	Defining Rule - Allow POP3 Service to a Particular Server .....	103
Figure 78	Defining Rule - Deny FTP Service Except to a Particular Server .....	104
Figure 79	Defining Rule - Deny bootp Service Except to a Particular Network .....	105
Figure 80	Enabling Content Filtering .....	107
Figure 81	OS Fingerprinting .....	109
Figure 82	Air Time Fairness Mode.....	112
Figure 83	Configuring Administrator Assigned Radio Settings for OAW-IAP .....	113
Figure 84	Intrusion Detection .....	115
Figure 85	Rogue Containmen.....	116
Figure 86	Containment Methods.....	116
Figure 87	Creating Community Strings for SNMPV1 and SNMPV2.....	118
Figure 88	Creating Users for SNMPV3.....	119
Figure 89	Template Based Configuration.....	121
Figure 90	Configuring OmniVista 3600 Air Manager .....	123
Figure 91	Virtual Controller View .....	125
Figure 92	Clients Graph.....	126
Figure 93	Throughput Graph .....	127

Figure 94	Network View.....	128
Figure 95	Clients Graph.....	129
Figure 96	Throughput Graph .....	129
Figure 97	Instant Access Point View .....	131
Figure 98	2.4 GHz Frames Graph.....	132
Figure 99	Client View .....	135
Figure 100	Signal Graph.....	136
Figure 101	Frames Graph.....	136
Figure 102	Speed Graph .....	136
Figure 103	Throughput Graph .....	137
Figure 104	Adding a User .....	141
Figure 105	Specifying a Country Code .....	143



Table 1	Conventions.....	15
Table 2	RF Dashboard icons .....	33
Table 3	IEEE 802.11 Standards.....	39
Table 4	Conditions for Adding an Employee Network - Basic Info Tab.....	40
Table 5	Conditions for Adding an Employee Network - Security Tab.....	42
Table 6	Conditions for Adding a Voice Network - Basic Info Tab.....	47
Table 7	Conditions for Adding a Voice Network - Security Tab.....	48
Table 8	Conditions for Adding a Guest Network - Basic Info Tab .....	50
Table 9	WPA and WPA2 Features.....	92
Table 10	Recommended Authentication and Encryption Combinations .....	92
Table 11	Network Service Options.....	99
Table 12	Destination Options .....	101
Table 13	SNMP Parameters for IAP .....	117
Table 14	Virtual Controller View - Graphs and Monitoring Procedures .....	127
Table 15	Network View - Graphs and Monitoring Procedures.....	129
Table 16	Instant Access Point View - RF Trends Graphs and Monitoring Procedures ...	132
Table 17	Instant Access Point View - Usage Trends and Monitoring Procedures .....	134
Table 18	Client View - RF Trends Graphs and Monitoring Procedures .....	137
Table 19	Alerts List.....	139
Table 20	Country Codes List.....	144
Table 21	List of abbreviations .....	149



# About this Guide

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

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

## Objective

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

## Intended Audience

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

## Conventions

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

**Table 1** *Conventions*

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

The following informational icons are used throughout this guide:



---

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

---



---

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

---



---

Indicates a risk of personal injury or death.

---

## Contacting Support

Contact Center Online	
• Main Site	<a href="http://www.alcatel-lucent.com/enterprise">http://www.alcatel-lucent.com/enterprise</a>
• Support Site	<a href="https://service.esd.alcatel-lucent.com">https://service.esd.alcatel-lucent.com</a>
• Email	<a href="mailto:esd.support@alcatel-lucent.com">esd.support@alcatel-lucent.com</a>
Service & Support Contact Center Telephone	
• North America	1-800-995-2696
• Latin America	1-877-919-9526
• Europe	+33 (0) 38 855 6929
• Asia Pacific	+65 6240 8484
• Worldwide	1-818-878-4507



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

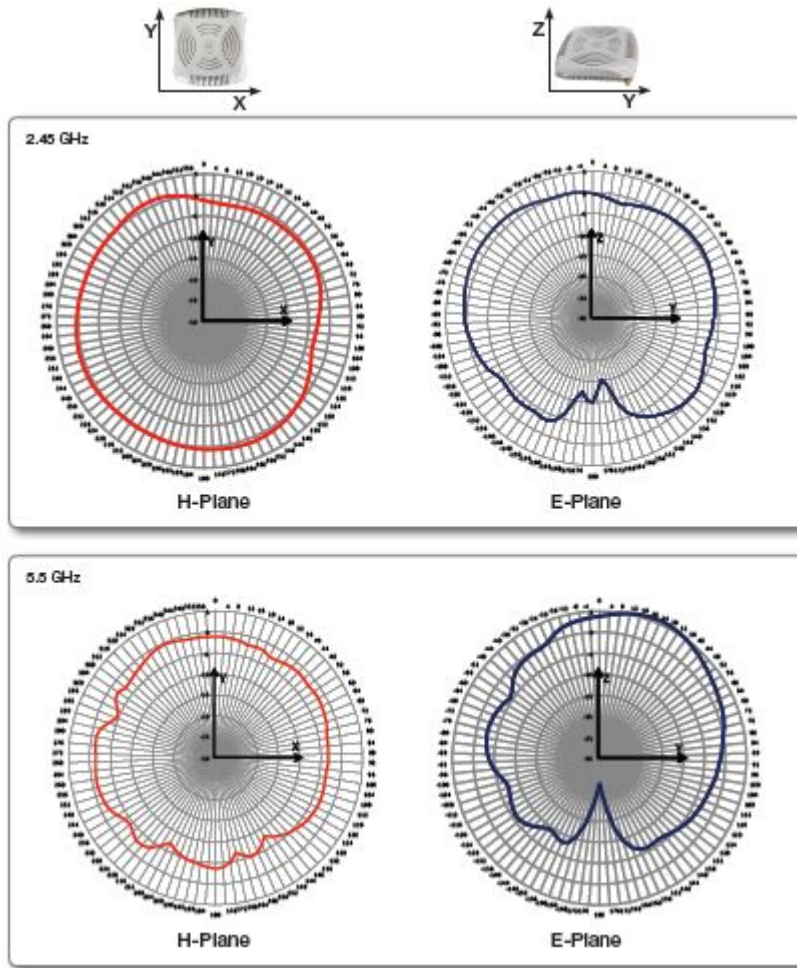
### OAW IAP-92 and OAW IAP-93 Antenna Patterns

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

- OAW IAP-92: Dual, RP-SMA interfaces for external antenna support (supporting up to 2x2 MIMO with spatial diversity). For information to configure an external antenna, see [“Configuring an External Antenna”](#) on page 65.
- OAW IAP-93: Integrated, omnidirectional antenna elements (supporting up to 2x2 MIMO with spatial diversity)
- Maximum antenna gain for OAW IAP-92 and OAW IAP-93:
  - 2.4 GHz/2.5 dBi
  - 5 GHz/5.8 dBi

[Figure 1](#) shows antenna patterns of OAW IAP-93 for 2.45 GHz and 5.5 GHz.

**Figure 1** OAW IAP93 Antenna Pattern



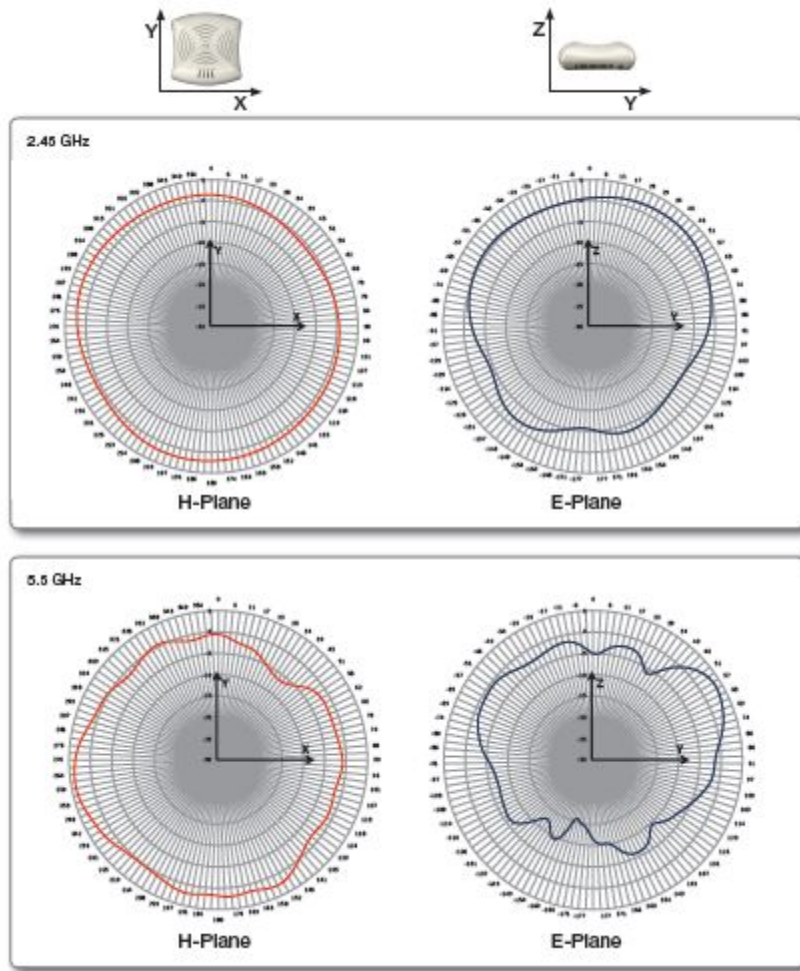
## OAW IAP-105 Antenna Pattern

The antenna specifications of OAW IAP-105 are as follows:

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

Figure 2 shows antenna patterns of OAW IAP-105 for 2.45 GHz and 5.5 GHz.

**Figure 2** OAW IAP-105 Antenna Pattern





This chapter provides information that is required to setup 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 Alcatel-Lucent 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.
  - Alcatel-Lucent IAP AC-DC adapter kit (this kit is sold separately).

---

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



Endspan: The switch that the AP is connected to can provide power.

Midspan: A device can sit between the switch and the AP.

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

---

---

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

---



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

---

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

1. “Connecting the OAW IAP to a Power Source” on page 22
2. “Assigning an IP Address to the OAW IAP” on page 22

3. “Connecting to the Provisioning Wi-Fi network” on page 22
4. “Login into Instant User Interface” on page 23
5. “Specifying the Country Code” on page 24 Skip this step, if you are installing the OAW IAP in United States, Japan or Israel.

## Connecting the OAW 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 OAW IAP to the power source:

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

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

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



---

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

---

## Connecting to the Provisioning Wi-Fi network

Connect a wireless enabled client to the provisioning Wi-Fi network. The provisioning network name is **instant**.

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



---

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

---

**Figure 3** Connecting to Provisioning Wi-Fi network - Microsoft Windows



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

**Figure 4** Connecting to Provisioning Wi-Fi network - MAC OS

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

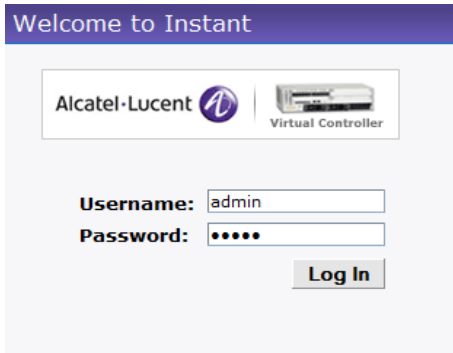


## Login into Instant User Interface

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

- Username - admin
- Password - admin

**Figure 5** Instant User Interface Login Screen



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

## Specifying the Country Code



---

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

---

Alcatel-Lucent Instant Access Points are shipped in four variants:

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

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

For the complete list of the countries that are supported in the IAP-ROW variant type, see “Regulatory Domain” on page 143.

**Figure 6** Specifying the Country Code





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

Supported browsers are:

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



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

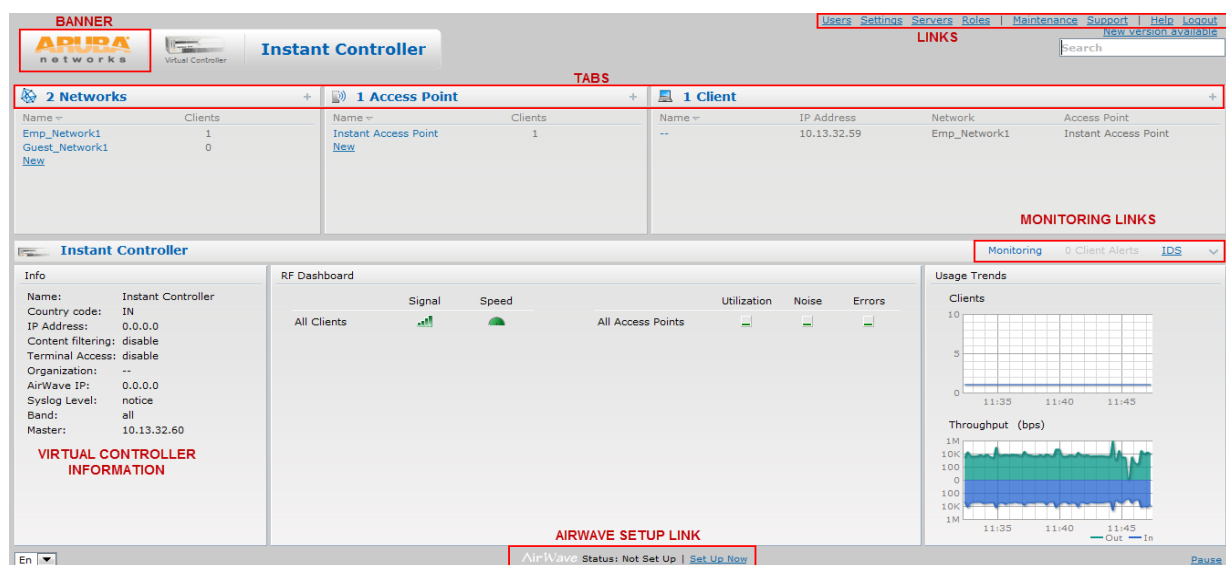
## Understanding the Instant UI Layout

The Instant UI consists of the following elements:

- Banner
- Search
- Tabs
- Links
- Views

These elements are explained in the following sections.

**Figure 7** Basic Sections in the Instant UI



## 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 OAW IAP, Client or a Network using a simple **Search** dialog box in the UI. This Search option helps fill in the blank when you type in a word and suggested matches will be automatically displayed in a dynamic list. The list will become 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 Alcatel-Lucent Instant network.
- **Access Points** - Provides information about the OAW 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, OAW IAPs, or clients in the network precedes the tab names. Click on the tabs to see the expanded view and click to compress the expanded view. Items in each tab are associated with a triangle icon. Click to sort the data in increasing or decreasing order. Each tab is explained in the following sections.

### Networks Tab

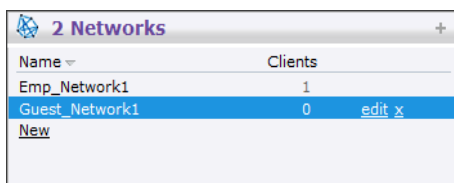
This tab displays a list of Wi-Fi networks that are configured in the Alcatel-Lucent Instant network. The network names appear as links. The expanded view displays the following information about each Wi-Fi network:

- **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 39](#).

An **edit** link appears on clicking the network name in the **Networks** tab. For information about editing a wireless network, see [“Editing a Network” on page 52](#). To delete a network, click **x** on the right side of the **edit** link.

**Figure 8** *Networks Tab - Compressed View and Expanded View*



Name	Clients
Emp_Network1	1
Guest_Network1	0

[New](#)

2 Networks						
Name ▾	Clients	Type	Band	Authentication Method	Key Management	IP Assignment
<a href="#">Emp_Network1</a>	0	Employee	All	None	WPA2-AES	Default VLAN
<a href="#">Guest_Network1</a>	0	Guest	All	None	None	NAT Mode
<a href="#">New</a>						

## Access Points Tab

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

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

The expanded view displays the following information about each OAW IAP:

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

An edit link appears on clicking the OAW IAP name. For details about editing OAW IAP settings see, “Editing OAW IAP Settings” on page 62.

**Figure 9** Access Points Tab - Compressed View and Expanded View

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

1 Access Point													
Name ▾	IP Address	Mode	Clients	Type	Mesh Role	2.4 GHz				5.0 GHz			
						Channel	Power (dB)	Utilization (%)	Noise (dBm)	Channel	Power (dB)	Utilization (%)	Noise (dBm)
<a href="#">Instant Access Point</a>	10.13.32.60	Access	0	105	Portal	11	23	48	-93	157+	20	3	-87

## Clients Tab

This tab displays a list of clients that are connected to the Alcatel-Lucent 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** - OAW 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 - Signal strength.**
- **Speed (mbps)** - Data transfer speed.

**Figure 10** *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 is explained in the subsequent sections.

- [New version available](#)
- [Users](#)
- [Settings](#)
- [Servers](#)
- [Roles](#)
- [Servers](#)
- [Support](#)
- [Help](#)
- [Logout](#)
- [Monitoring](#)
- [Client Alerts](#)
- [IDS](#)
- [Language](#)
- [OmniVista 3600 Air Manager Setup](#)
- [Pause/Resume](#)

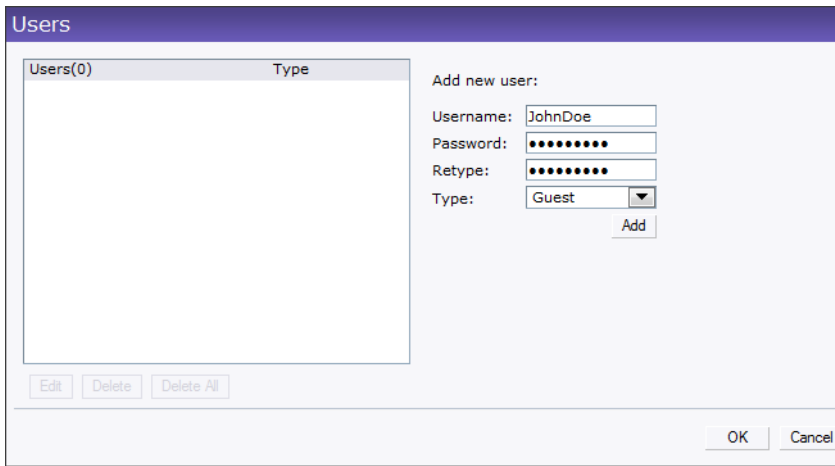
### New version available

This link appears in the Instant UI only if a new image version is available on the image server and OmniVista 3600 Air Manager is not configured. For more information about the **New version available** link and its functions, see “[Firmware Image Server in Cloud Network](#)” on page 67.

### Users

This link displays the **Users** box. This box contains fields that are required to add, edit, or delete a user or users. You can also specify the user type. Two types of users, employee and guest, will be using the Alcatel-Lucent Instant network. For more information about users, see [Chapter 22, “User Database”](#).

**Figure 11** *Users Box*

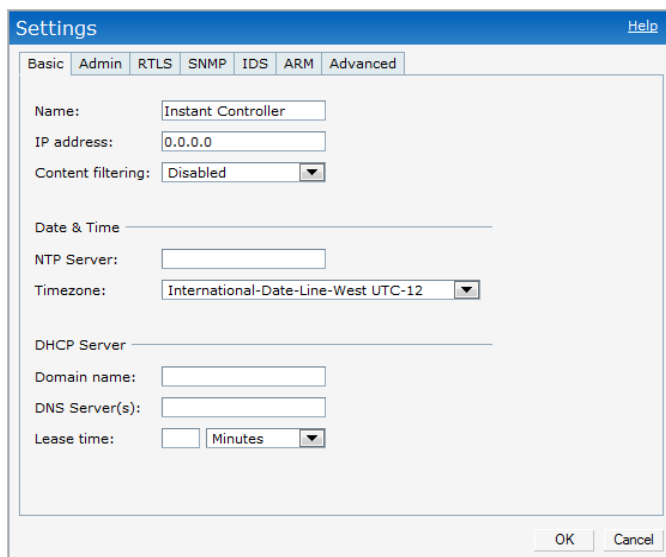


## Settings

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

- **Basic** - View or edit the virtual controller's name, IP address, and Content filtering setting. For information about virtual controller settings and content filtering, see [Chapter 8, “Virtual Controller”](#) and [Chapter 14, “Content Filtering”](#).
- **Admin** - View or edit the admin credentials.
- **RTLS** - View or edit the RTLS server settings.
- **SNMP** - View or specify SNMP agent settings. For information see [Chapter 18, “SNMP”](#).
- **IDS** - View or select the Rogue classification and Containment methods to monitor the network for the presence of unauthorized OAW IAP's and clients. For more information see [Chapter 17, “Intrusion Detection System”](#).
- **ARM** -View or assign channel and power settings for all the OAW IAP's in the network. For information about ARM, see [Chapter 16, “Adaptive Radio Management”](#).
- **Advanced** - View or edit the preferred band for the network, dynamic RADIUS Proxy, and Auto join mode settings. For information about dynamic RADIUS Proxy and Auto join mode, see [“External RADIUS Server”](#) on page 76 and [“Auto Join Mode”](#) on page 59.

**Figure 12** *Settings Link - Default View*



## Servers

This link displays the **RADIUS Server** box. This box allows you to add new server. To add a new radius server, see “Configuring an External RADIUS Server” on page 76.

## Roles

This link displays the **Roles** box. You can create new user roles and new rules for the user roles. For more information, see “User Roles” on page 93.

## Maintenance

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

- **About** - Displays the Build Time, OAW IAP model name, Alcatel-Lucent OS version, Web address of Alcatel-Lucent Networks, and Copyright information.
- **Configuration** - Displays the current configuration of the network. The Clear Configuration button allows you to delete or clear the current configuration of the network and reset to provisioning configuration.
- **Certificates** - Displays information about current certificate installed in the network. Provides interface to upload new certificates and to set passphrase for the certificates. For more information, see “Certificates” on page 88.
- **Firmware** - Displays the current firmware version and provides options to upgrade to a new firmware version. For more information, see “Manual Firmware Image Check and Upgrade” on page 69.
- **Reboot** - Displays the OAW IAPs in the network and provides an option to reboot the required access point or all access points. For more information, see “Rebooting the OAW IAP” on page 67.
- **Convert** - Provides an option to change the virtual controller managed network to an Alcatel-Lucent Mobility Controller managed network. For more information, see “Migrating from a Virtual Controller” on page 65.

**Figure 13** Maintenance Link - Default View



## Support

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

- **Command** drop-down list - Provides various options for which you can generate support logs.

- **Target** drop-down list - Provides a list of OAW IAPs in the network.
- **Run** button - Click this button to generate the support log for the selected option and OAW IAP.
- **Access point** tabs - Displays support log for the selected OAW IAPs.

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

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




---

For more information, use the support commands under the supervision of Alcatel-Lucent technical support.

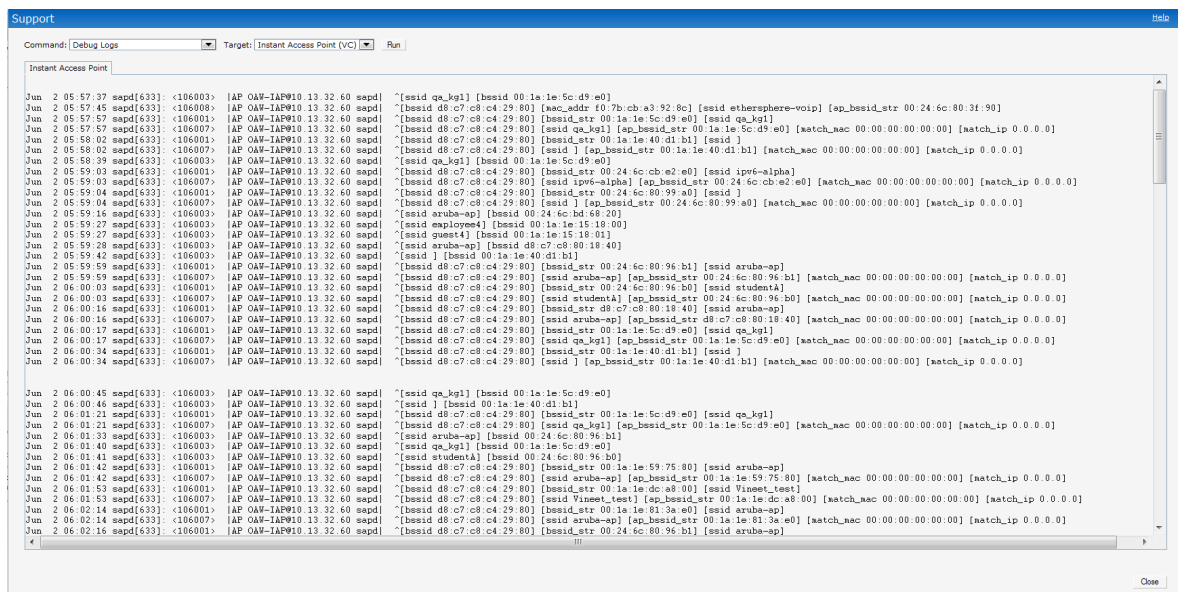
---

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

- **Summary** - Displays the OAW IAP configuration.
- **Debug Logs** - Displays debug logs of the selected OAW IAP.
- **Driver Logs** - Displays the driver logs of the selected OAW IAP.
- **Tech Support Dump** - Displays the technical support dump logs of the selected OAW IAP.
- **Active Configuration** - Displays the active configuration of virtual controller.
- **Saved Configuration** - Displays the saved configuration of virtual controller.
- **Management Frames** - Displays the traced 802.11 management frames of the selected OAW IAP.
- **Authentication Frames** - Displays the authentication trace buffer information of the selected OAW IAP.
- **System Status** - Displays detailed system status information for the selected OAW IAP.
- **Crash Info** - Displays crash log information (if it exists) for the selected OAW IAP. The stored information is cleared from the flash after the reboots.
- **802.1X Statistics** - Displays the 802.1X statistics of the selected OAW IAP.
- **RADIUS Statistics** - Displays the RADIUS statistics of the selected OAW IAP.
- **System Status** - Displays the system status of the selected OAW IAP.
- **Client Table** - Displays information of the client connected to the selected OAW IAP.
- **Association Table** - Displays information of the selected OAW IAP association.
- **Allowed Channels** - Displays information of the allowed channels for the selected OAW IAP.
- **Radio 0 Stats** - Displays aggregate debug statistics of the selected OAW IAP Radio 0.
- **Radio 1 Stats** - Displays aggregate debug statistics of the selected OAW IAP Radio 1.
- **Bridge Table** - Displays bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for the selected OAW 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 OAW IAP.
- **Session Table** - Displays the datapath session table statistics for the selected OAW IAP.
- **Route Table** - Displays datapath route table statistics for the selected OAW IAP.
- **Datapath Statistics** - Displays the hardware packet statistics for the selected OAW IAP.

- **VLAN Table** - Displays the VLAN table information such as VLAN memberships inside the datapath including L2 tunnels for the selected OAW IAP.
- **BSSID Table** - Displays the Basic Service Set (BSS) table of the selected OAW IAP.
- **IDS Status** - Displays WLAN Interface, Data Structures, WLAN Interface Switch Status and RTLS Configuration tables for the selected OAW IAP.
- **IDS Table** - Displays the Monitored OAW IAP Table, which lists all the OAW IAPs monitored by the selected OAW IAP.
- **ARM Bandwidth Management** - Displays bandwidth management information for the selected OAW IAP.
- **ARM History** - Displays the history of channel and power changes due to Adaptive Radio Management (ARM) for the selected OAW IAP.
- **ARM Neighbors** - Displays the ARM settings for the selected OAW IAP's neighbors.
- **ARM RF Summary** - Displays the state and statistics for all channels being monitored by the selected OAW IAP.
- **ARM Scan Times** - Displays AM channel scan times for the selected OAW IAP.

Figure 14 Support Box

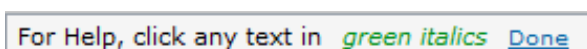


## Help

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

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

Figure 15 Help Link




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

## Logout

Use this link to logout of the Instant UI.

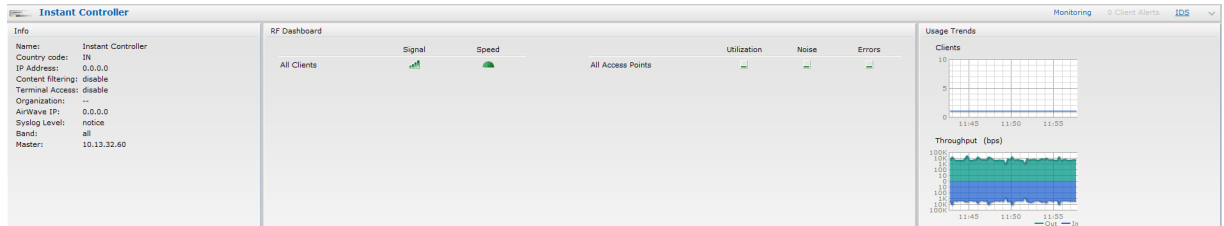


## Monitoring

This link displays the Monitoring pane. This pane can be used to monitor the Alcatel-Lucent 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

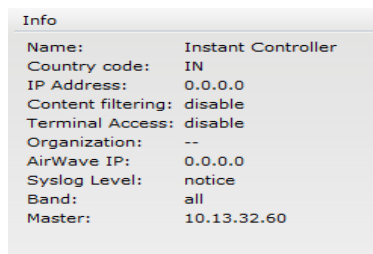
**Figure 16** Monitoring on Instant UI



### Info

Displays the configuration information of the virtual controller by default. In a [Network View](#), this section displays configuration information of the selected network. Similarly, in an [Instant Access Point View](#) or [Client View](#), this section displays the configuration information of the selected OAW IAP or the client.

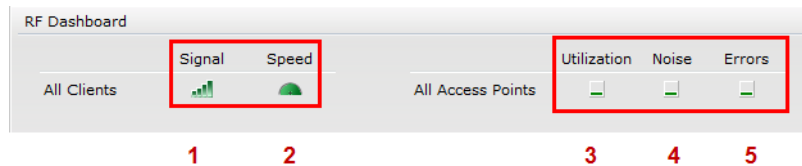
**Figure 17** Info Section in the Monitoring Pane



### RF Dashboard

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

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



The following table lists the icons in the RF Dashboard.

**Table 2** RF Dashboard icons

Icon	Name
1	Signal bar
2	Speed icon
3	Utilization icon

**Table 2** RF Dashboard icons

Icon	Name
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 OAW IAPs whose utilization, noise, or errors are not within the specified threshold. The OAW IAP names appear as links. When the OAW IAP is clicked, the OAW 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 20, "Monitoring"](#) .
  - Utilization - Displays the radio utilization rate of the OAW 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 OAW IAP, click on the Utilization icon against the OAW IAP in the Utilization column.

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

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

- Errors - Displays the errors for the OAW 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.

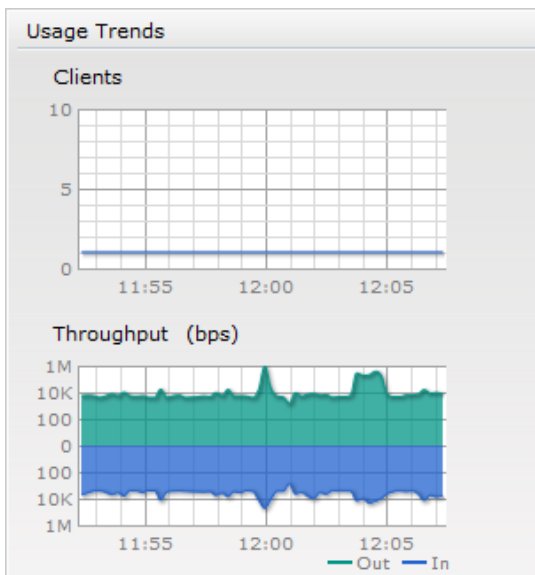
To view the errors graph of an OAW IAP, click on the Errors icon against the OAW IAP in the Errors column.

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

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



For more information about the graphs and monitoring procedures, see [Chapter 20, “Monitoring”](#) .

### Client Alerts

Alerts are generated when a user faces problems while accessing or connecting to the Wi-Fi network. The Client Alerts link appears in red only if there are any client alerts. Click this link to see the related alert. An alert consists of the following fields:

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

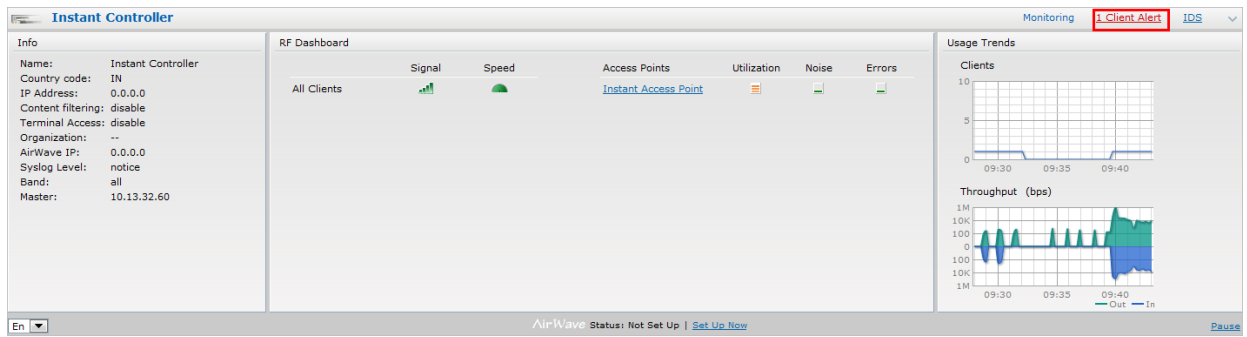



---

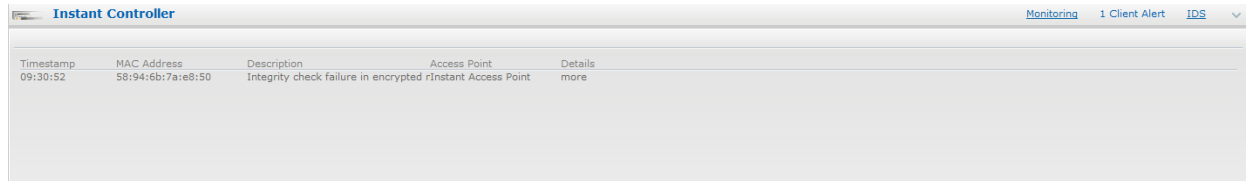
New alerts will be generated for an incomplete DHCP transaction of a client.

---

**Figure 20** Client Alerts link on Instant UI



**Figure 21** Client Alerts Link



For more information about alerts, see [Chapter 21, “Alert Types and Management”](#).

## IDS

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

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

For more information on the intrusion detection feature, see [Chapter 17, “Intrusion Detection System”](#).

**Figure 22** *Intrusion Detection on Instant UI*

Foreign Access Points Detected							Foreign Clients Detected						
MAC Address	Network	Classification	Chan.	Type	Last Seen	Where	MAC Address	Network	Classification	Chan.	Type	Last Seen	Where
00:24:6c:80:74:00	ethersphere-voip	Interfering	6	GN 20MZ	15:31:52		b4:07:f9:f2:06:eb	ethersphere-voip	Interfering	1	BN 20MZ	15:31:52	
00:24:6c:bd:56:a0	manoj-vap	Interfering	1	GN 20MZ	15:31:52		00:27:10:5c:78:24	ethersphere-voip	Interfering	36	AN 40MZ	15:31:52	
00:0b:86:50:47:48	vijay-ap	Interfering	64	A	15:31:52		58:94:6b:7a:40:c0	ethersphere-wpa2	Interfering	157	AN 40MZ	15:31:52	
00:24:6c:80:95:c8	ethersphere-wpa2	Interfering	161	AN 40MZ	15:31:52		f8:db:7f:9b:03:fb	ethersphere-voip	Interfering	1	BN 20MZ	15:31:52	
00:1c:b0:e0:d9:60	IBM	Interfering	6	G	15:31:52		00:27:10:5c:65:04	ethersphere-wpa2	Interfering	36	AN 40MZ	15:31:52	
00:24:6c:80:74:01	Aruba-India-Guest	Interfering	6	GN 20MZ	15:31:52		58:94:6b:58:6b:04	ethersphere-wpa2	Interfering	36	AN 40MZ	15:31:52	
00:1a:1e:40:7c:81	shobha-765-rt-bridge	Interfering	1	GN 20MZ	15:31:52		00:26:c6:bd:51:04	ethersphere-wpa2	Interfering	40	AN 40MZ	15:31:52	
00:24:6c:80:95:c9	ethersphere-voip	Interfering	161	AN 40MZ	15:31:52		00:26:c6:44:a9:b2	ethersphere-voip	Interfering	1	G	15:31:52	
00:1a:1e:9b:a9:f0	ipv6-alpha	Interfering	149	AN 40MZ	15:31:52		f0:7b:cb:a3:92:8c	ethersphere-voip	Interfering	1	BN 20MZ	15:31:52	
00:1a:1e:17:dc:60	ipv6-alpha	Interfering	1	GN 20MZ	15:31:52		00:1e:65:71:49:2c	shobha-765-rt-bridge	Interfering	1	BN 20MZ	15:31:52	
00:24:6c:80:4f:88	ethersphere-wpa2	Interfering	149	AN 40MZ	15:31:52		00:26:c6:be:59:e2	ipv6-alpha	Interfering	48	AN 40MZ	15:31:52	
00:24:6c:80:6f:28	ethersphere-wpa2	Interfering	157	AN 40MZ	15:31:52		58:94:6b:79:ce:f0	ethersphere-wpa2	Interfering	40	AN 40MZ	15:31:52	
00:24:6c:80:95:ca	Aruba-India-Guest	Interfering	161	AN 40MZ	15:31:52		00:27:10:5c:74:64	ethersphere-wpa2	Interfering	149	A	15:31:52	
00:24:6c:80:4b:f0	ethersphere-voip	Interfering	1	GN 20MZ	15:31:52		80:50:1b:b9:0c:3d	ethersphere-voip	Interfering	1	B	15:31:52	
00:1a:1e:89:c2:00	aruba-ap	Interfering	6	GN 20MZ	15:31:52		00:27:10:5c:02:64	ethersphere-wpa2	Interfering	157	AN 40MZ	15:31:52	
00:24:6c:80:03:42	sw-byadav-swathc	Interfering	1	GN 20MZ	15:31:52		00:26:c6:71:e9:36	ethersphere-wpa2	Interfering	48	AN 40MZ	15:31:52	
00:24:6c:80:ec:60	ethersphere-voip	Interfering	1	GN 20MZ	15:31:52		58:94:6b:bd:2c:ac	ethersphere-wpa2	Interfering	149	A	15:31:52	
00:24:6c:80:6f:29	ethersphere-voip	Interfering	157	AN 40MZ	15:31:52		00:27:10:2a:c6:ac	ipv6-alpha	Interfering	6	B	15:31:52	
00:24:6c:80:99:a8	ethersphere-wpa2	Interfering	153	AN 40MZ	15:31:52		00:1e:65:71:11:de	arunsp	Interfering	44	A	15:31:52	
00:24:6c:80:4f:89	ethersphere-voip	Interfering	149	AN 40MZ	15:31:52		00:27:10:5c:23:78	ethersphere-wpa2	Interfering	48	AN 40MZ	15:31:52	
00:24:6c:80:4h:f1	Aruba-India-Guest	Interfering	1	GN 20MZ	15:31:52		00:1c:26:5b:a5:43	ethersphere-wpa2	Interfering	157	A	15:31:52	

## Language

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

## OmniVista 3600 Air Manager Setup

OmniVista 3600 Air Manager is a solution for managing rapidly changing wireless networks. When enabled, OmniVista 3600 Air Manager allows you to manage the Instant network. For more information on OmniVista 3600 Air Manager, see [Chapter 19, “OmniVista 3600 Air Manager Integration and Management”](#). The OmniVista 3600 Air Manager status is displayed on the right side of the language links in the Instant UI. If the OmniVista 3600 Air Manager status is Not Set Up, click the **Set Up Now** link to set up the OmniVista 3600 Air Manager. The Settings box appears with **Admin** tab selected. For information to configure OmniVista 3600 Air Manager, see [“Configuring OmniVista 3600 Air Manager”](#) on page 122.

**Figure 23** *OmniVista 3600 Air Manager Setup Link*

The screenshot shows the 'Settings' dialog box with the 'Admin' tab selected. The 'AirWave' section is highlighted with a red box and contains the following fields:

- Organization: Aruba Networks
- AirWave IP: 192.1.0.0
- Shared key: [Redacted]
- Retype: [Redacted]

Buttons for 'OK' and 'Cancel' are visible at the bottom of the dialog.

## 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, OAW 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 Alcatel-Lucent Instant network.
- Network view - The Network view provides information that is necessary to monitor a selected wireless network. All Wi-Fi networks in the Alcatel-Lucent 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 OAW IAP. All OAW IAPs in the Alcatel-Lucent Instant network are listed in the Access Points tab. Click the name of the OAW IAP that you want to monitor. Access Point view for that OAW IAP appears.
- Client view - The Client view provides information that is necessary to monitor a selected client. In the Virtual Controller view, all clients in the Alcatel-Lucent 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 20, “Monitoring”](#) .

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 3](#).

**Table 3** 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 OAW IAP. After locating the OAW IAP, the following transactions take place between the client and the OAW IAP:

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

## Network Types

Alcatel-Lucent Instant wireless networks are categorized as:

- Employee Network
- Voice Network
- Guest Network

### Employee Network

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

#### Adding an Employee Network

This section provides the procedure to add an employee network.

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

**Figure 24** Adding an Employee Network - Basic Info Tab

The screenshot shows the 'New Network' configuration window with the 'Basic Info' tab active. The 'Name (SSID)' field contains 'Emp\_Network1'. Under 'Primary usage', the 'Employee' radio button is selected. Under 'Client IP assignment', the 'Network assigned' option is selected, with 'Default' as the sub-option. The 'Band' is set to 'All'. The 'Hide SSID' checkbox is unchecked. 'Next' and 'Cancel' buttons are at the bottom right.

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

**Table 4** Conditions for Adding an Employee Network - Basic Info Tab

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

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



**Figure 25** Band and Hide SSID Settings

The screenshot shows the 'New Network' configuration interface. At the top, there are three tabs: '1 Basic Info' (highlighted in green), '2 Security', and '3 Access'. A 'Help' link is in the top right corner. Below the tabs is the 'Basic Information' section. It contains the following fields and options:

- Name (SSID):  [< Less](#)
- Primary usage:  Employee,  Voice,  Guest
- Band:  ▼
- Hide SSID:
- Client IP assignment:  Network assigned,  Virtual Controller assigned
- Under 'Network assigned':  Default,  VLAN ID:
- Bandwidth Limits:  Percentage of Airtime,  Each user,  Each radio

At the bottom right, there are 'Next' and 'Cancel' buttons.

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

**Table 5** Conditions for Adding an Employee Network - Security Tab

If	then,
You select the <b>Enterprise</b> security level	<p>Perform the following steps:</p> <ol style="list-style-type: none"><li>1. Select the required key options from the <b>Key management</b> drop-down list. Available options are:<ul style="list-style-type: none"><li>● WPA-2 Enterprise</li><li>● WPA Enterprise</li><li>● Both (WPA-2 &amp; WPA)</li><li>● Dynamic WEP with 802.1x</li></ul>For more information on encryption and recommended encryption type, see <a href="#">Chapter 10, “Encryption”</a> .</li><li>2. Select the required Authentication server option from the <b>Authentication server 1</b> drop-down list. Available options are:<ul style="list-style-type: none"><li>● External - If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see <a href="#">Chapter 9, “Authentication”</a> .</li><li>● 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.</li></ul>For information on adding a user, see <a href="#">“Adding a User” on page 141</a>.</li></ol>

**Table 5** Conditions for Adding an Employee Network - Security Tab

If	then,
<p>You want to use the default security level, <b>Personal</b></p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Select the required key options from the <b>Key management</b> drop-down list. Available options are: <ul style="list-style-type: none"> <li>● WPA-2 Personal</li> <li>● WPA Personal</li> <li>● Both (WPA-2 &amp; WPA)</li> <li>● Static WEP</li> </ul> <p>If you have selected <b>Static WEP</b>, then do the following:</p> <ul style="list-style-type: none"> <li>● Select appropriate <b>WEP key size</b> from the WEP key size drop-down list. Available options are 64-bit and 128-bit.</li> <li>● Select appropriate Tx key from the <b>Tx Key</b> drop-down list. Available options are 1, 2, 3, and 4.</li> <li>● Enter an appropriate WEP key and reconfirm.</li> </ul> <p>For more information on encryption and recommended encryption type, see <a href="#">Chapter 10, “Encryption”</a> .</p> </li> <li>2. Select a passphrase format from the Passphrase format drop-down list. Available options are: <ul style="list-style-type: none"> <li>● 8-63 alphanumeric chars</li> <li>● 64 hexadecimal chars</li> </ul> </li> <li>3. Enter a passphrase in the Passphrase text box and reconfirm.</li> <li>4. Select the required option from the MAC authentication drop-down list. Available options are <ul style="list-style-type: none"> <li>● None - This option provides open authentication. Any client that requests association is allowed to connect to the network. Open authentication is not recommended unless you want users to gain quick access to the network.</li> <li>● External RADIUS Server - If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring external RADIUS server, see <a href="#">“Configuring an External RADIUS Server”</a> on page 76.</li> </ul> </li> </ol>
<p>You select the <b>Open</b> security level</p>	<p>Select the required MAC authentication from the <b>MAC authentication</b> drop-down list. Available options are:</p> <ul style="list-style-type: none"> <li>● None -This option provides open authentication. Any client that requests association is allowed to connect to the network. Open authentication is not recommended unless you want users to gain quick access to the network.</li> <li>● External RADIUS Server - If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see <a href="#">“Configuring an External RADIUS Server”</a> on page 76.</li> </ul>

Figure 26 Security Tab - Enterprise

The screenshot shows the 'New Network' configuration window with the 'Security' tab selected. The window has a blue header with 'New Network' and a 'Help' link. Below the header are three tabs: '1 Basic Info', '2 Security', and '3 Access'. The 'Security' tab is active and displays the 'Security Level' section. On the left, a vertical slider indicates the security level, with 'Enterprise' selected at the top, 'Personal' in the middle, and 'Open' at the bottom. The 'Enterprise' level is associated with 'More Secure' at the top and 'Less Secure' at the bottom. To the right of the slider, the 'Key management' dropdown is set to 'WPA-2 Enterprise'. Below it, 'Authentication server 1' is set to 'InternalServer' and 'Authentication server 2' is set to '-- Select Server --'. Underneath, there are links for 'Users' and 'Certificates' under the heading 'For internal server:'. At the bottom right of the window are three buttons: 'Back', 'Next', and 'Cancel'.

**Figure 27** Security Tab - Personal

The screenshot shows the 'New Network' configuration window with the 'Security' tab selected. The 'Security Level' is set to 'Personal'. The 'Key management' dropdown is set to 'WPA-2 Personal'. The 'Passphrase' field is empty, with a note '8-63 chars' to its right. The 'Retype' field is also empty. The 'MAC authentication' dropdown is set to 'None'. A vertical slider on the left indicates the security level, with 'Personal' selected between 'Enterprise' and 'Open'. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

**Figure 28** Security Tab - Open

The screenshot shows the 'New Network' configuration window with the 'Security' tab selected. The 'Security Level' is set to 'Open'. The 'Encryption' dropdown is set to 'None'. The 'MAC authentication' dropdown is set to 'Enabled'. The 'Authentication server 1' dropdown is set to 'InternalServer'. The 'Authentication server 2' dropdown is set to '-- Select Server --'. Below these, there are links for 'Users' and 'Certificates' under the heading 'For internal server:'. A vertical slider on the left indicates the security level, with 'Open' selected between 'Personal' and 'Enterprise'. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. InstantFirewall treats packets based on the first rule matched. For more information, see [Chapter 13, “Instant Firewall”](#) .

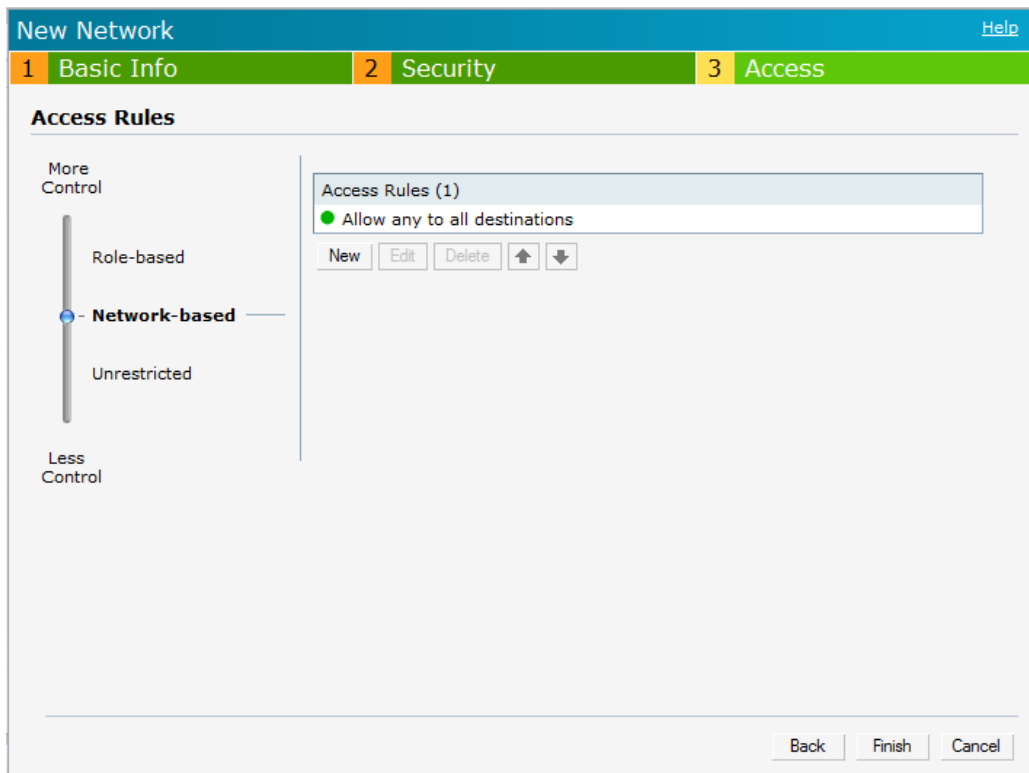
To edit the default rule, perform the following steps:

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

To define an access rule, perform the following steps:

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

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



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

## Voice Network

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

### Adding a Voice Network

This section provides the procedure to add a voice network.

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

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

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

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

**Table 6** Conditions for Adding a Voice Network - Basic Info Tab

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

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

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

**Table 7** Conditions for Adding a Voice Network - Security Tab

If	then,
<p>You select the Enterprise security level</p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>Select the required key options from the Key management drop-down list. Available options are: <ul style="list-style-type: none"> <li>WPA-2 Enterprise</li> <li>WPA Enterprise</li> <li>Both (WPA-2 &amp; WPA)</li> <li>Dynamic WEP with 802.1x</li> </ul> </li> </ol> <p>For more information on encryption and recommended encryption type, see <a href="#">Chapter 10, "Encryption"</a> .</p> <ol style="list-style-type: none"> <li>Select the required RADIUS server option from the RADIUS Server drop-down list. Available options are: <ul style="list-style-type: none"> <li>External - If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see <a href="#">"Configuring an External RADIUS Server"</a> on page 76.</li> <li>Internal - If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the Users link to add the users.</li> </ul> </li> </ol> <p>For information about adding a user, see <a href="#">"Adding a User"</a> on page 141.</p>
<p>You want to use the default security level, Personal,</p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>Select the required key options from the Key management drop-down list. Available options are: <ul style="list-style-type: none"> <li>WPA-2 Personal</li> <li>WPA Personal</li> <li>Both (WPA-2 &amp; WPA)</li> <li>Static WEP</li> </ul> </li> </ol> <p>If you selected Static WEP, then do the following:</p> <ul style="list-style-type: none"> <li>Select appropriate WEP key size from the WEP key size drop-down list. Available options are 64-bit and 128-bit.</li> <li>Select appropriate Tx key from the Tx Key drop-down list. Available options are 1, 2, 3, and 4.</li> <li>Enter an appropriate WEP key in the WEP Key text box and reconfirm.</li> </ul> <p>For more information on encryption and recommended encryption type, see <a href="#">Chapter 10, "Encryption"</a> .</p> <ol style="list-style-type: none"> <li>Enter a passphrase in the Passphrase text box and reconfirm.</li> <li>Select the required option from the MAC authentication drop-down list. Available options are: <ul style="list-style-type: none"> <li>None - This option provides open authentication. Any client that requests association is allowed to connect to the network. Open authentication is not recommended unless you want users to gain quick access to the network.</li> <li>External RADIUS Server - For information on configuring an external RADIUS server, see <a href="#">"Configuring an External RADIUS Server"</a> on page 76.</li> </ul> </li> </ol>



**Table 7** Conditions for Adding a Voice Network - Security Tab

If	then,
You select the Open security level	Select the required MAC authentication from the MAC authentication drop-down list. Available options are: <ul style="list-style-type: none"><li>• None - This option provides open authentication. Any client that requests association is allowed to connect to the network. Open authentication is not recommended unless you want users to gain quick access to the network.</li><li>• External RADIUS Server - For information on configuring an external RADIUS server, see <a href="#">“Configuring an External RADIUS Server”</a> on page 76.</li></ul>

4. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. InstantFirewall treats packets based on the first rule matched. For more information, see [Chapter 13, “Instant Firewall”](#) .

To edit the default rule, perform the following steps:

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

To define an access rule, perform the following steps:

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

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

## Guest Network

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

### Adding a Guest Network

This section provides the procedure to add a guest network.

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

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

2. In the **Basic Info** tab, perform the following steps:
  - a. Type a name for the network in the **Name (SSID)** text box.
  - b. Select the **Guest** radio button from the **Primary usage** options. This selection determines the primary usage of the network being added.  
The **Client IP assignment** selection automatically changes to **Virtual Controller assigned**. The virtual controller creates a private subnet and VLAN for the OAW IAPs and the wireless clients. The virtual controller NATs all traffic out of this interface. For more information, see [Chapter 12, “Guest DMZ”](#).
3. Click the **More** link and perform the following steps (These steps are optional).
  - a. **Band** - Set the band at which the network will transmit radio signals. Available options are **All**, **2.4 GHz**, and **5 GHz**. The **All** option is selected by default. It is also the recommended option.
  - b. **Hide SSID** - Select this check box if you want to hide the SSID (network name) from the users.
4. Click **Next**. The **Security** tab appears. This tab allows you to configure the captive portal page for the Guest network. Select one of the following splash page type:

**Table 8** Conditions for Adding a Guest Network - Basic Info Tab

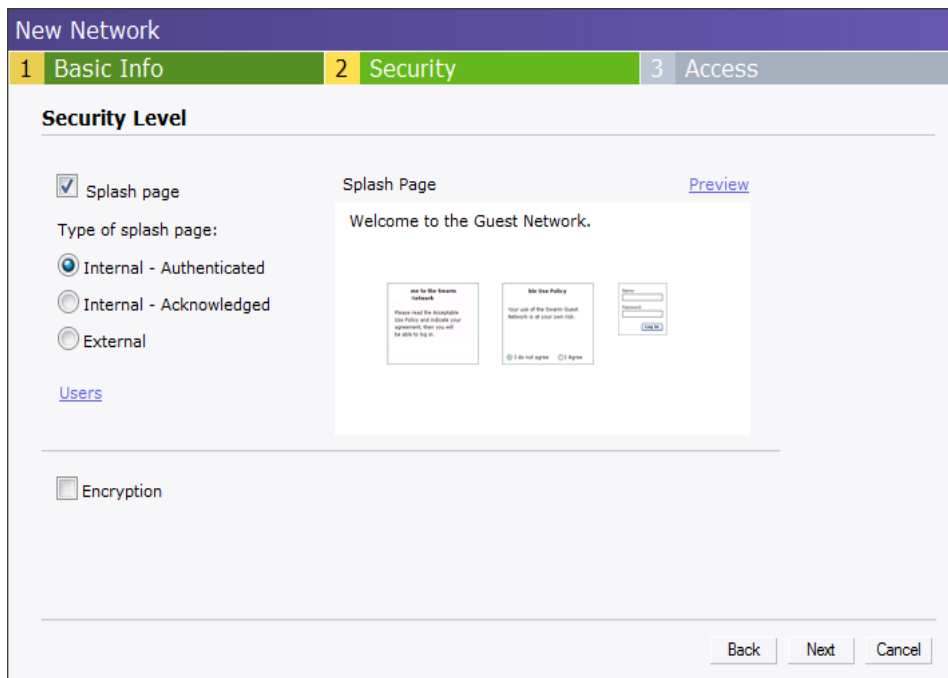
Splash Page Type	Description and steps to set up
Internal - Authenticated	A user has to accept the terms and conditions and enter a username and password on the captive portal page. If this option is selected, then add the users who are required to use the captive portal authentication to the user database. Click the Users link to add the users. For information about adding a user, see <a href="#">“Adding a User” on page 141</a> . For information on customizing the splash page, see <a href="#">“Customizing a Splash Page” on page 84</a> .

**Table 8** Conditions for Adding a Guest Network - Basic Info Tab

Splash Page Type	Description and steps to set up
Internal - Acknowledged	A user has to accept the terms and conditions for this splash page type. For information on customizing the splash page, see “Customizing a Splash Page” on page 84.
External	An external server will be used to display the splash page to the user. If this option is selected, then do the following: <ol style="list-style-type: none"> <li>1. Enter the IP or hostname of the external server in the IP or hostname text box.</li> <li>2. Enter the URL of the captive portal page in the URL text box.</li> <li>3. Enter the number of the port to be used for communicating with the external server in the Port text box.</li> <li>4. In the Authentication text box, enter the unique signature that the external server will return in the response after a successful user authentication.</li> </ol>

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

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



5. Select the **Encryption** check box and perform the following steps (These steps are optional):
  - a. Select the required key management option from the **Key management** drop-down list. Available options are:
    - WPA-2 Personal
    - WPA Personal
    - Both (WPA-2 & WPA)
    - Static WEP. If you selected Static WEP, then do the following:

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

**Figure 33** Configuring a Splash Page - Encryption Settings

6. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. InstantFirewall treats packets based on the first rule matched. For more information, see [Chapter 13, “Instant Firewall”](#).

To edit the default rule, perform the following steps:

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

To define an access rule, perform the following steps:

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

7. Click **Finish**.

## Editing a Network

To edit a network, perform the following steps:

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

## Deleting a Network

To delete a network, perform the following steps:

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

## Bandwidth Contracts

The OAW IAP supports three types of bandwidth limits:

- **Percentage of Airtime:** % Air Time allocated to SSID
- **Each user:** Per User per SSID contract specified in kbps
- **Each radio:** Per radio per SSID contract specified in kbps



The Alcatel-Lucent Instant secure enterprise mesh solution is an effective way to expand network coverage for outdoor and indoor enterprise environments without any wires. Using mesh, you can bridge multiple Ethernet LANs or you can extend your wireless coverage. As traffic traverses across mesh OAW 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 OAW IAP stops functioning or a connection fails.



---

A mesh network can be configured only on OAW IAP-105. By default, the 5Ghz radio is always enabled on the mesh.

---

This chapter describes the Alcatel-Lucent Instant secure enterprise mesh architecture, in the following topics:

## Mesh Instant Access Points

Mesh OAW IAPs learn about their environment when they boot up. Mesh OAW IAPs are either configured as a mesh portal (MPP), an OAW IAP that uses its wired interface to reach the controller, or a mesh point (MP), an OAW IAP that establishes an all-wireless path to the mesh portal. Mesh OAW 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 OAW IAPs configured for mesh.

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

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

## Mesh Portals

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

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

## Mesh Points

The mesh point (MP) is an OAW IAP configured for mesh and assigned the mesh point role. Depending on the OAW IAP model, configuration parameters, and how it was provisioned, the mesh point can perform multiple tasks. The mesh point provides traditional WLAN services (such as client connectivity, intrusion detection system (IDS) capabilities, user role association, and Quality of Service (QoS) for LAN-to-mesh communication) to clients and performs mesh backhaul/network connectivity. A mesh radio can be configured to carry mesh-backhaul traffic only. Mesh points use one of their wireless interfaces to carry traffic and reach the controller.



---

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

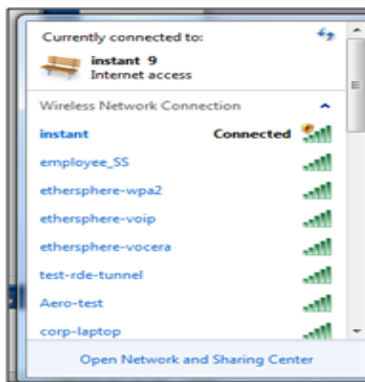
---

## Instant Mesh Setup

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

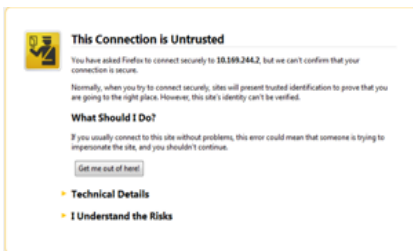
1. Wire all the OAW IAPs to a DHCP server so the OAW IAPs get their IP addresses in the same subnet.
2. An open SSID, **instant** will be listed. Connect a laptop to the default, open **instant** SSID.

**Figure 34** Open Instant SSID



3. Type [instant.alcatel-lucent.com](http://instant.alcatel-lucent.com) in the browser.
4. Click **I understand the risks and Add exception** to ignore the certificate warnings that the client does not recognize the certificate authority.

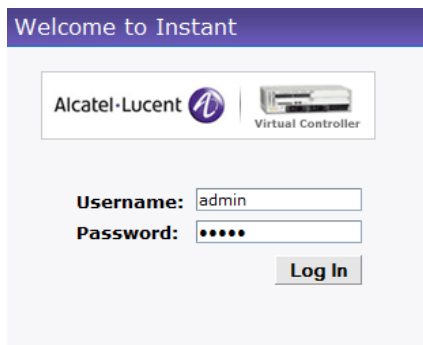
**Figure 35** Untrusted Connection Window



5. In the login screen as shown in [Figure 36](#), enter the following credentials:
  - Username - admin
  - Password - admin

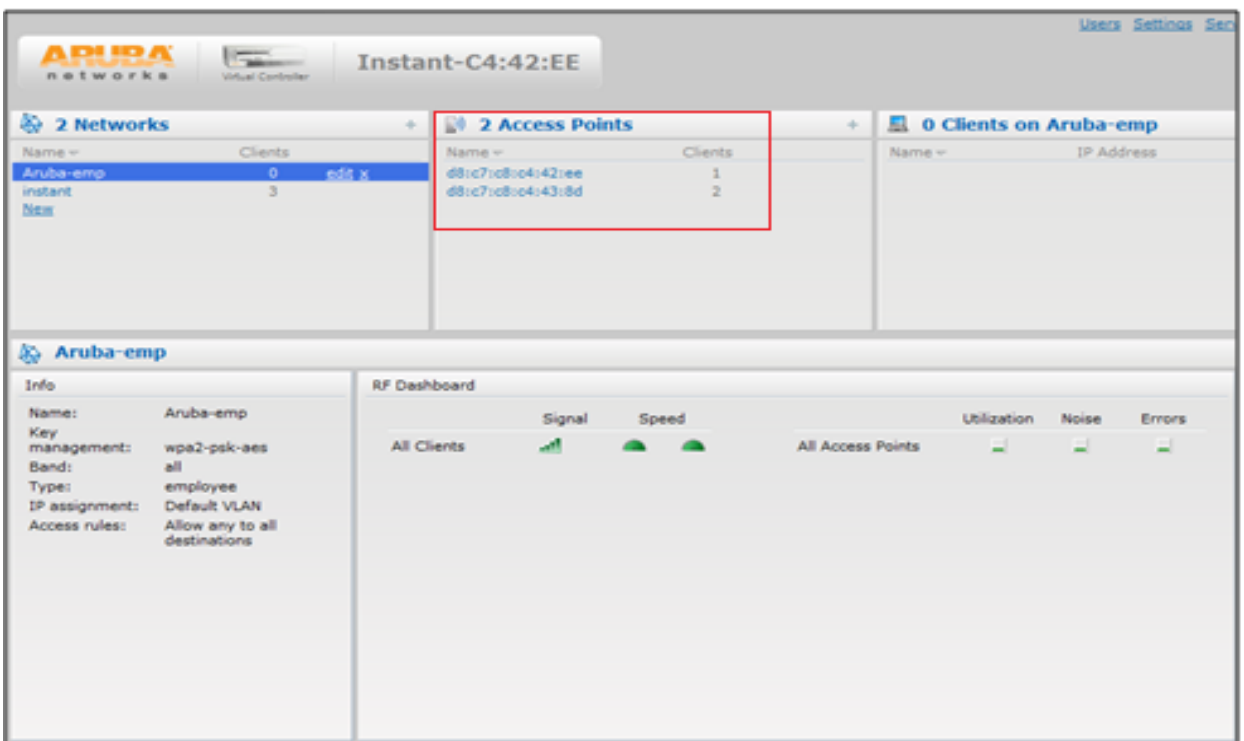


**Figure 36** Login Window



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

**Figure 37** Mesh Portal



The OAW IAPs in US, JP, or IL regulatory domain which are in factory default state will scan for several minutes after booting. These OAW IAPs will automatically join the mesh if only a single provisioned Instant mesh network is available.



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

## Auto Join Mode

The Auto Join Mode feature allows the OAW 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 OAW IAPs to the network. For more information, see [“Adding an OAW IAP to the Network” on page 61](#). Also, when this feature is disabled, OAW IAPs that are configured but not active appear in red.

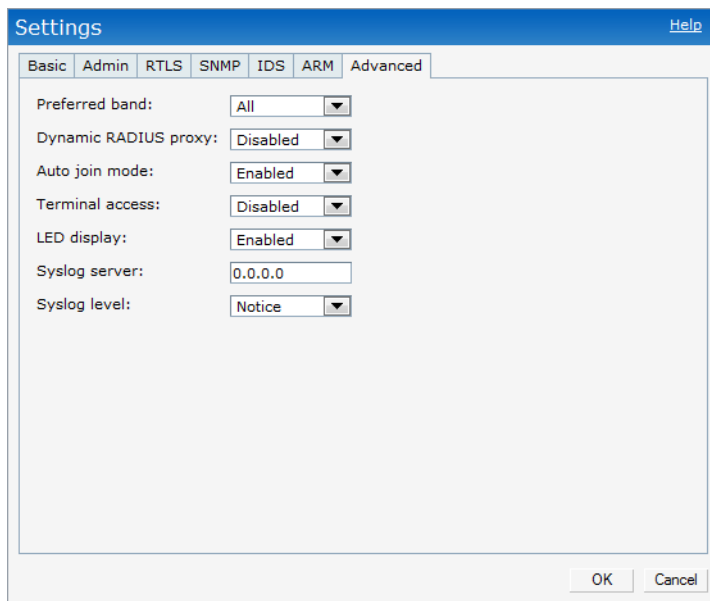
## Disabling Auto Join Mode

To disable Auto Join Mode, perform the following steps:

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

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

**Figure 38** *Disabling Auto Join Mode*

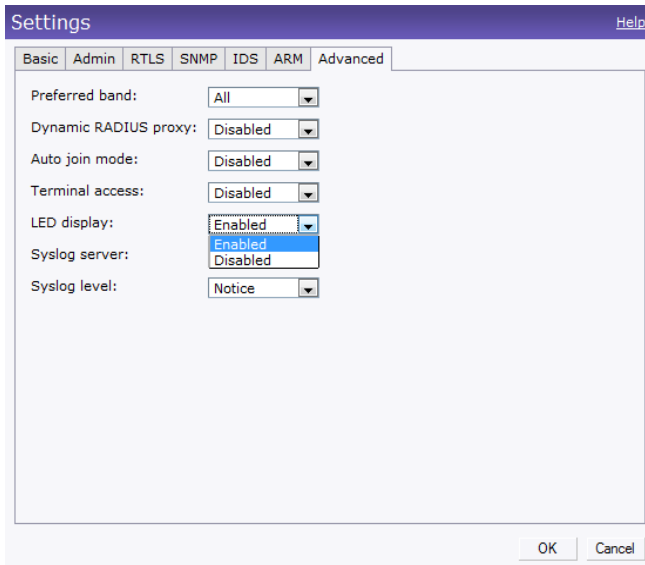


3. Click **OK**.

## LED Display

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

**Figure 39** *LED Display*



---

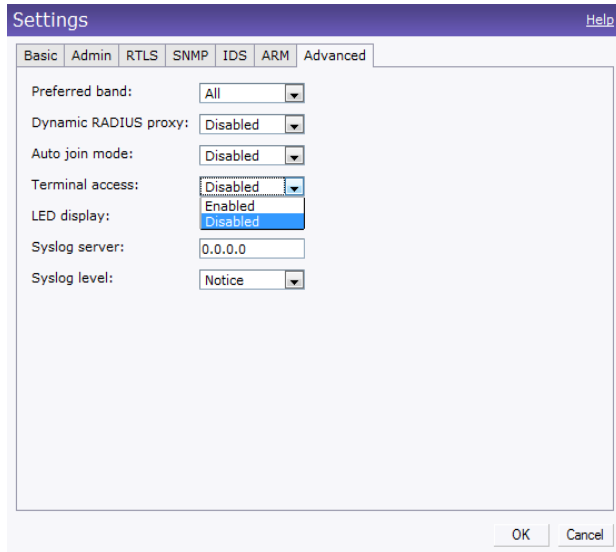
The LED display will be always in Enabled mode while rebooting the IAP.

---

## Terminal Access

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

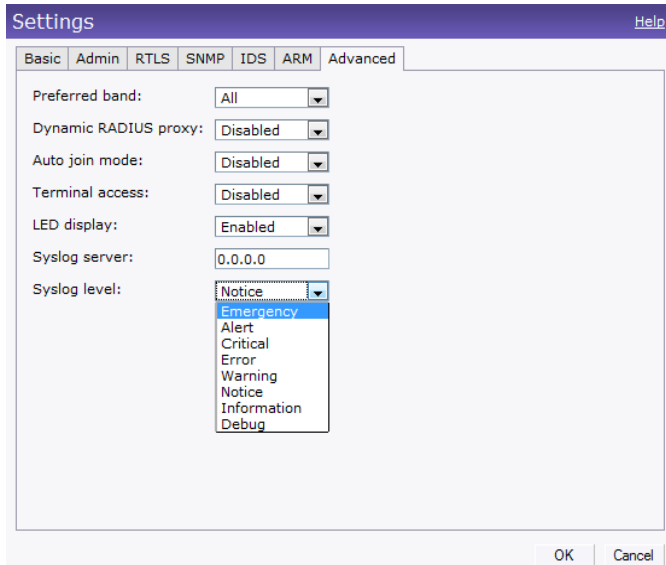
**Figure 40** *Terminal Access*



## Syslog Server

Go to **Settings > Advanced > Syslog Server** to specify a Syslog Server for sending all syslog messages to the external servers.

**Figure 41** Syslog Server



## Adding an OAW IAP to the Network

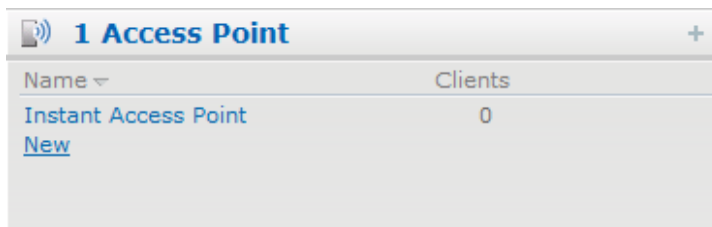
To add an OAW IAP to the Alcatel-Lucent Instant network, assign an IP address. For more information, see “Assigning an IP Address to the OAW IAP” on page 22.

After an OAW 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 OAW 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 OAW IAP to the network:

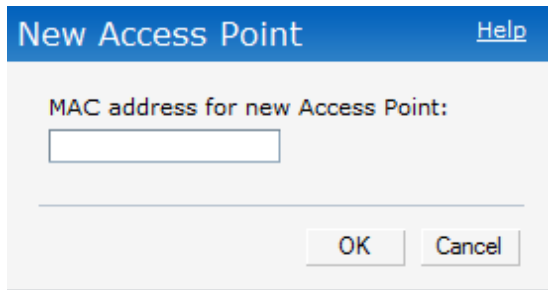
1. In the **Access Points** tab, click the **New** link.

**Figure 42** Adding an OAW IAP to the Instant Network



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

**Figure 43** Entering the MAC Address for the New OAW IAP



3. Click **OK**.

## Removing an OAW IAP from the Network

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

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



---

The deleted OAW IAP(s) cannot join the Instant anymore.

---

## Editing OAW IAP Settings

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

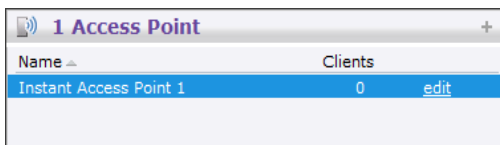
- Name
- IP Address
- Adaptive Radio Management (ARM) Configuration
- External Antenna Configuration
- Migrating from a Virtual Controller Managed Network to Mobility Controller Managed Network

### Changing OAW IAP Name

To change the OAW IAP name, perform the following steps:

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

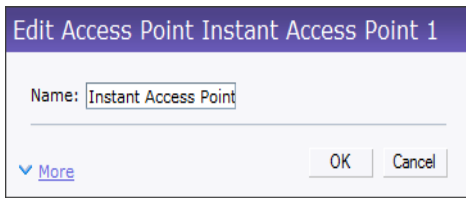
**Figure 44** Editing OAW IAP Settings



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

2. Click the **edit** link.

**Figure 45** Changing OAW IAP Name



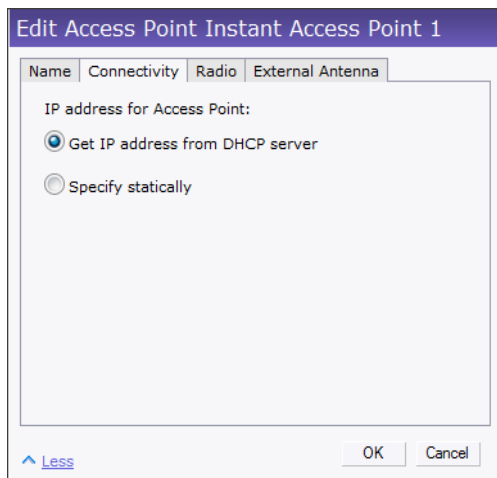
3. Edit the OAW IAP name in the **Name** text box.
4. Click **OK**.

## Changing IP Address of the OAW IAP

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

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

**Figure 46** Configuring OAW IAP Settings - Connectivity Tab



4. Select the **Get IP address from DHCP server** or **Specify statically** option. If you selected the **Specify statically** option, perform the following steps:
  1. Enter the new IP address for the OAW 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 47** Configuring OAW IAP Connectivity Settings - Specifying Static Settings

The screenshot shows a dialog box titled "Edit Access Point Instant Access Point 1". It has four tabs: "Name", "Connectivity", "Radio", and "External Antenna". The "Connectivity" tab is active. Under "IP address for Access Point:", there are two radio buttons: "Get IP address from DHCP server" (unselected) and "Specify statically" (selected). Below are five text input fields: "IP address:" (1.1.1.1), "Netmask:" (255.255.255.255), "Default gateway:" (1.1.1.1), "DNS server:" (1.1.1.1), and "Domain name:" (www.example.com). At the bottom, there is a "Less" link, "OK", and "Cancel" buttons.

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

## Configuring Adaptive Radio Management

Adaptive Radio Management (ARM) is enabled in Alcatel-Lucent Instant by default. However, if ARM is disabled, perform the following steps to enable it. For more information about ARM, see “[Adaptive Radio Management](#)” on page 111.

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

**Figure 48** Configuring OAW IAP Radio Settings Mode - Access

The screenshot shows a dialog box titled "Edit Access Point OAW-IAP". It has four tabs: "Name", "Connectivity", "Radio", and "External Antenna". The "Radio" tab is active. There are two sections: "2.4 GHz band" and "5 GHz band". Each section has two radio buttons: "Adaptive radio management assigned" (selected) and "Administrator assigned" (unselected). Below each section are two text input fields: "Channel:" (1) and "Transmit power:" (0). At the bottom, there is a "Less" link, "OK", and "Cancel" buttons.

5. Click **OK**.



## Configuring an External Antenna

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



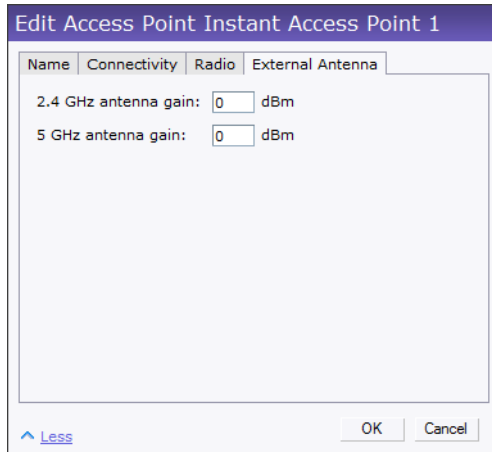
---

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

---

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

**Figure 49** Configuring OAW IAP External Antenna Settings



The screenshot shows a dialog box titled "Edit Access Point Instant Access Point 1". It has four tabs: "Name", "Connectivity", "Radio", and "External Antenna". The "External Antenna" tab is selected. Inside the dialog, there are two input fields: "2.4 GHz antenna gain: 0 dBm" and "5 GHz antenna gain: 0 dBm". At the bottom left, there is a link "< Less". At the bottom right, there are "OK" and "Cancel" buttons.

4. Click **OK**.

## Migrating from a Virtual Controller

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



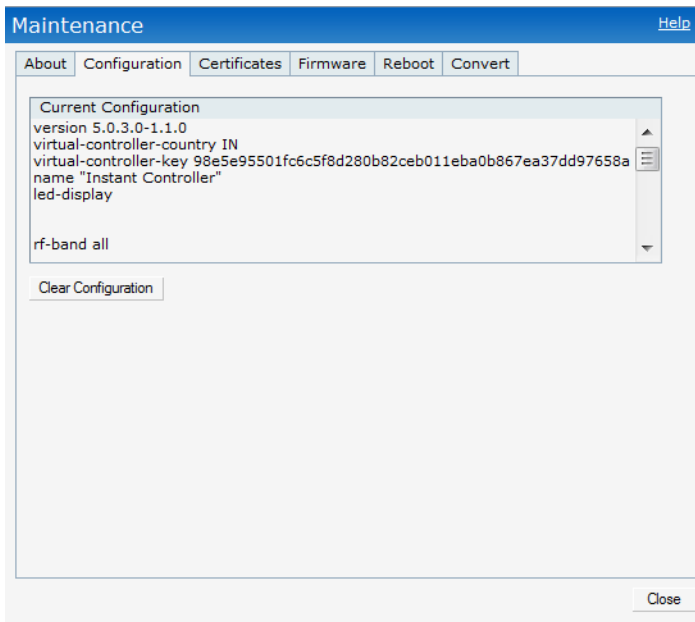
---

Migrating from a virtual controller managed network to mobility controller managed network is a one way transition. An Alcatel-Lucent OS Campus AP cannot be converted to an OAW IAP.

---

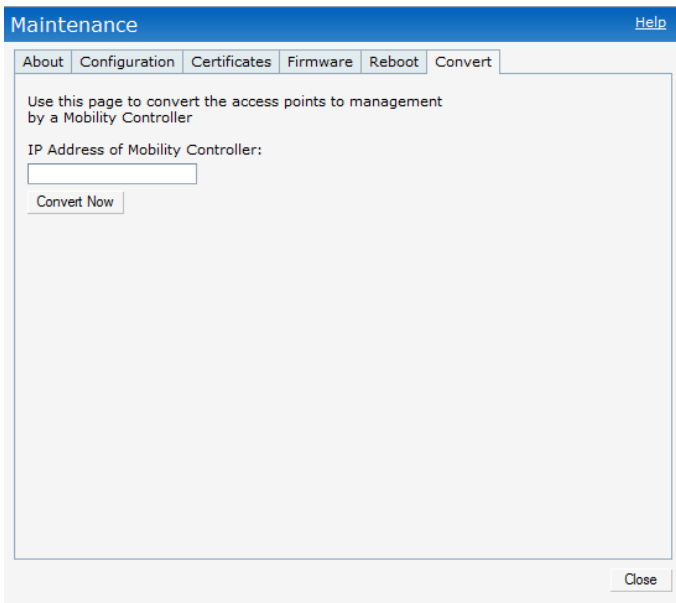
1. At the top right corner of Instant UI, click the **Maintenance** link. The **Maintenance** box appears.

**Figure 50** Maintenance Box



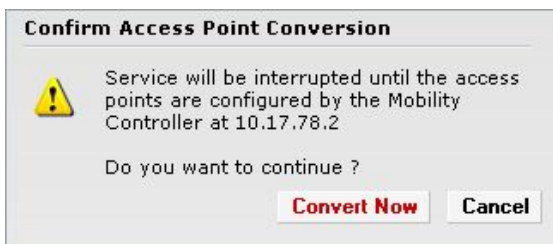
2. Click the **Convert** tab.

**Figure 51** Maintenance - Convert Tab



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

**Figure 52** Confirm Access Point Conversion Box



5. Click **Close**.



---

An OAW IAP can be converted to an AOS-W Campus AP only if the controller is running AOS-W 6.1 or later.

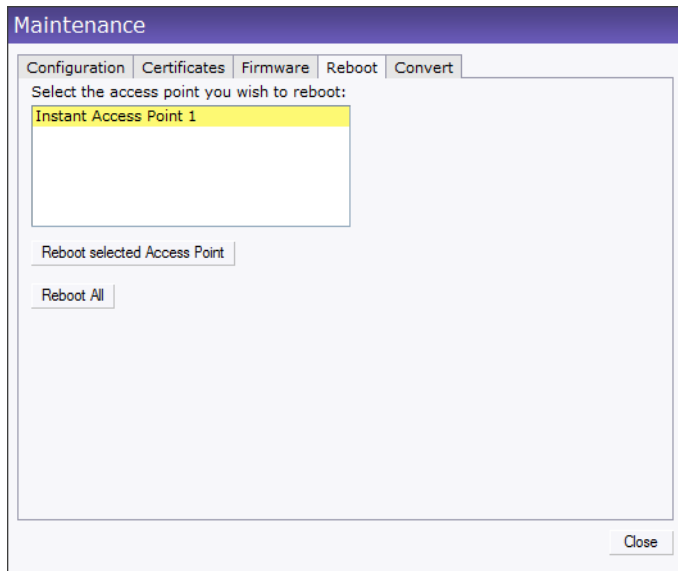
---

## Rebooting the OAW IAP

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

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

**Figure 53** Rebooting the OAW IAP



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

## Firmware Image Server in Cloud Network

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

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

- Current software version
- Type Code
- Globally Unique ID (GUID)
- OEM-Tag
- Organization (if available)

- Access Point Information (for each AP attached to the VC)
  - AP type
  - AP serial number

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

## Automatic Firmware Image Check and Upgrade

Automatic image check is enabled by default. If AirWave is configured, then the automatic image check is automatically disabled. You have to use the manual image check option. For more information, see “Manual Firmware Image Check and Upgrade” on page 69.

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

**Figure 54** Automatic Image Check - New Version Available Link

The screenshot shows the Instant UI for an OmniVista 3600 access point. At the top right, a red box highlights a link labeled "New version available". Below this, the interface is divided into several sections:
 

- Network:** Shows "Emp\_Network1" with 0 clients.
- Access Point:** Shows "Instant Access Point 1" with 0 clients.
- Info Panel:** Lists configuration details such as Name (Instant-C4:42:98), Country code (IN), IP Address (0.0.0.0), and Auto join mode (enable).
- RF Dashboard:** Displays signal strength and speed indicators for "All Clients".
- Usage Trends:** Contains two line graphs: "Clients" and "Throughput (Kbps)", both showing zero activity over the time period 16:10 to 16:20.

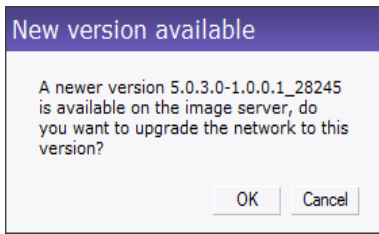
 At the bottom, the status "OmniVista 3600 Status: Not Set Up" and "Last Updated 16:25:24" are visible.

## Upgrading to the new OS version

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

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

**Figure 55** *New Version Available Box*



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

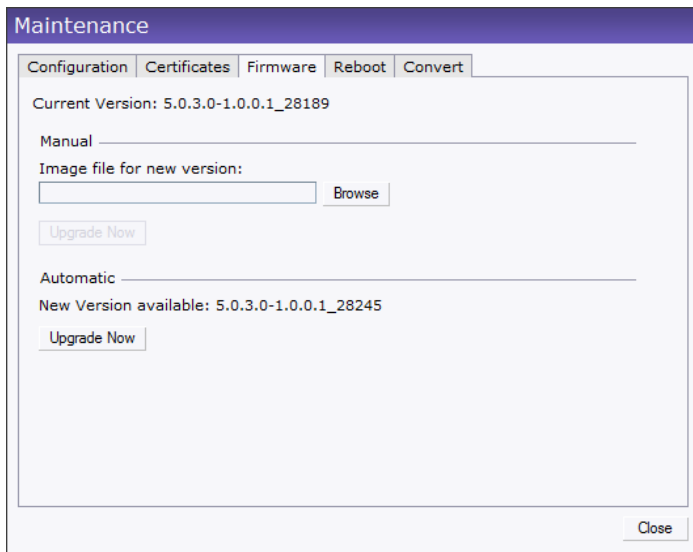
- Upgrading - While image upgrading is in progress.
- Upgrade successful -When the upgrading is successful.
- Upgrade fail -When the upgrading fails.

## Manual Firmware Image Check and Upgrade

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

1. At the top right corner of the Instant UI, click the **Maintenance** link.
2. In the **Maintenance** box, click the **Firmware** tab.
3. In the **Firmware** tab, click the **Check for New Version** button.

**Figure 56** *Manual Image Check*



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

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

4. If a new version is found, the **Upgrade Now** button appears and the **New version available** message and the version number are displayed.

5. Click the **Upgrade Now** button.

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

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

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 Alcatel-Lucent Instant network, an OAW 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 Alcatel-Lucent Instant, perform the following steps.

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

**Figure 57** Configuring NTP Server

The screenshot shows the 'Settings' dialog box with the 'Basic' tab selected. The configuration fields are as follows:

- Name:** Instant-C4:42:8D
- IP address:** 10.13.32.75
- Content filtering:** Disabled
- Date & Time:**
  - NTP Server:** (empty text box)
  - Timezone:** International-Date-Line-West UTC-12
- DHCP Server:**
  - Domain name:** test
  - DNS Server(s):** 10.100.11.153,10.100.1
  - Lease time:** 5 Minutes

Buttons for 'OK' and 'Cancel' are located at the bottom right of the dialog box.





Alcatel-Lucent Instant does not require an external controller to regulate and manage the Wi-Fi network. Any OAW IAP in the Alcatel-Lucent 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 OAW IAPs.

## Master Election Protocol

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

## Virtual Controller IP Address

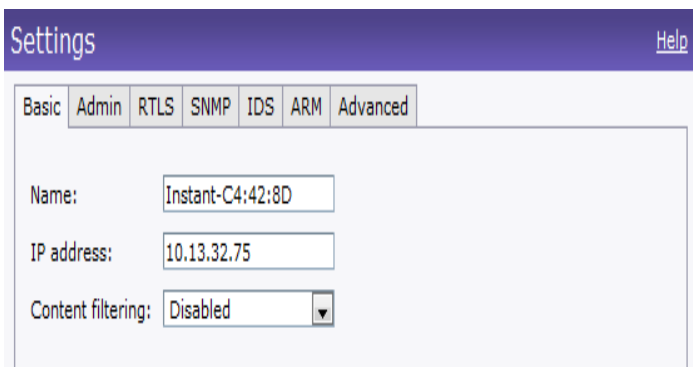
You can specify a single static IP address that can be used to manage a multi-AP Alcatel-Lucent Instant network. This IP address is automatically provisioned on a shadow interface on the OAW IAP that takes the role of a virtual controller. When an OAW IAP becomes a virtual controller, it sends three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

## Specifying Name and IP Address for the Virtual Controller

To specify name and IP address for the virtual controller, perform the following steps:

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

**Figure 58** Specifying Virtual Controller Name and IP Address



The screenshot shows the 'Settings' interface with the following fields:

- Name:** Instant-C4:42:8D
- IP address:** 10.13.32.75
- Content filtering:** Disabled

2. Enter a name for virtual controller in the **Name** text box.

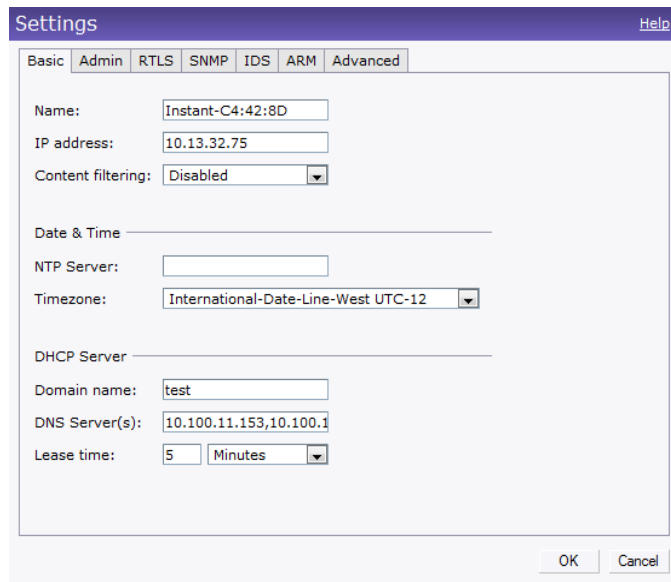
3. Enter the appropriate IP address in the **IP address** text box.
4. Click **OK**.

## Configuring the DHCP Server

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

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

**Figure 59** *Configuring the DHCP Server*



The screenshot shows a 'Settings' dialog box with a purple title bar and a 'Help' link. The 'Basic' tab is selected, and other tabs include 'Admin', 'RTLS', 'SNMP', 'IDS', 'ARM', and 'Advanced'. The configuration fields are as follows:

- Name: Instant-C4:42:8D
- IP address: 10.13.32.75
- Content filtering: Disabled
- Date & Time section:
  - NTP Server: (empty)
  - Timezone: International-Date-Line-West UTC-12
- DHCP Server section:
  - Domain name: test
  - DNS Server(s): 10.100.11.153,10.100.1
  - Lease time: 5 Minutes

At the bottom right, there are 'OK' and 'Cancel' buttons.

7. click Ok.

## Authentication Methods in Alcatel-Lucent 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 Alcatel-Lucent 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 OAW 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.



---

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

### Internal RADIUS Server

Each OAW IAP has an instance of FreeRADIUS server operating locally. When you enable the Internal RADIUS server option for the network, the authenticator on the OAW 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 Alcatel-Lucent 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 OAW IAP. The client certificate is verified on the 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.



---

Alcatel-Lucent Instant does not ship with any 802.1x server certificate. EAP-TTLS and EAP-PEAP support is not available until the administrator uploads a valid 802.1x server certificate to the Alcatel-Lucent Instant network. By default, the 802.1x authentication is limited to LEAP only.

---



---

Alcatel-Lucent does not recommend the use of LEAP authentication method because it does not provide any resistance to network attacks.

---

## External RADIUS Server

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

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

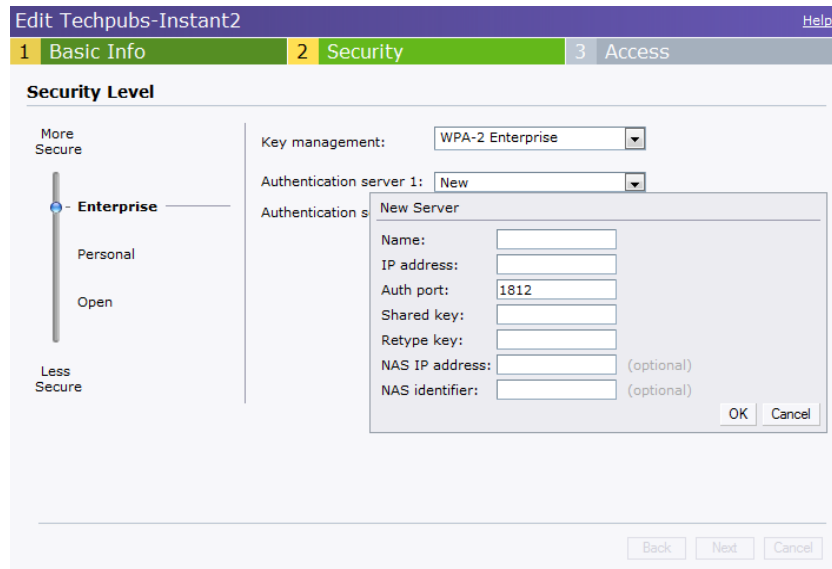
### Configuring an External RADIUS Server

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

1. In the **Network** tab, click the network for which you want to configure the external RADIUS Server. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** box for the network appears.
3. Click **Next** and perform the following tasks in the **Security** tab:
  1. For a network with **Personal** or **Open** security level, select **External Radius Server** from the **MAC Authentication** drop-down list.
  2. Click the **Primary** link and perform the following steps:
    - a. Enter the IP address of the external RADIUS server in the **IP address** text box.
    - b. Enter the authorization port number of the external RADIUS server in the **Auth Port** text box. The port number is set to 1812 by default.
    - c. Enter a shared key for communicating with the external RADIUS server in the **Shared key** text box.
    - d. Enter the virtual controller IP address in the **NAS IP address** text box. The NAS IP address is the virtual controller IP address that is sent in the data packets.

3. Click the **Backup** link and set appropriate values for the backup RADIUS server.

**Figure 60** *Configuring External RADIUS Server*



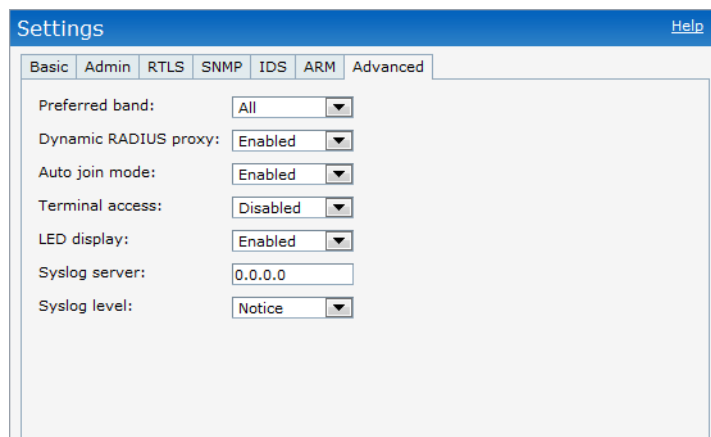
4. Click **Next** and click **Finish**.

### Enabling Instant RADIUS

To enable Instant RADIUS, perform the following steps:

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

**Figure 61** *Enabling Instant RADIUS*



4. Click **OK**.

## RADIUS Server Authentication with VSA

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

### List of supported VSA's

Instant supports the following types of VSA's:

- AP-Group
- AP-Name
- ARAP-Features
- ARAP-Security
- ARAP-Security-Data
- ARAP-Zone-Access
- Acct-Authentic
- Acct-Delay-Time
- Acct-Input-Gigawords
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Link-Count
- Acct-Multi-Session-Id
- Acct-Output-Gigawords
- Acct-Output-Octets
- Acct-Output-Packets
- Acct-Session-Id
- Acct-Session-Time
- Acct-Status-Type
- Acct-Terminate-Cause
- Acct-Tunnel-Packets-Lost
- Add-Port-To-IP-Address
- Alcatel-Lucent-AP-Group
- Alcatel-Lucent-Admin-Role
- Alcatel-Lucent-Essid-Name
- Alcatel-Lucent-Location-Id
- Alcatel-Lucent-Named-User-Vlan
- Alcatel-Lucent-Port-Id
- Alcatel-Lucent-Priv-Admin-User
- Alcatel-Lucent-Template-User
- Alcatel-Lucent-User-Role
- Alcatel-Lucent-User-Vlan
- CHAP-Challenge
- Callback-Id
- Callback-Number

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

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

## Management Authentication Settings

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

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



- **Internal** - Select the **Username** and **Password** specified in the respective text boxes to access the Virtual Controller Management UI.
- **RADIUS Server** - Specify one or two radius servers to authenticate UI. If two servers are configured users can use them in primary/backup mode or load-balancing mode, this is identical to the radius server configuration for SSIDs. For information on configuring external RADIUS server, see “[External RADIUS Server](#)” on page 76.
- **RADIUS server w/ fallback to internal** - Specify the radius servers as well as a Username and Password.

**Figure 62** *Management Authentication Settings*

4. Click **OK**.

## Captive Portal

Alcatel-Lucent 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 Alcatel-Lucent 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:

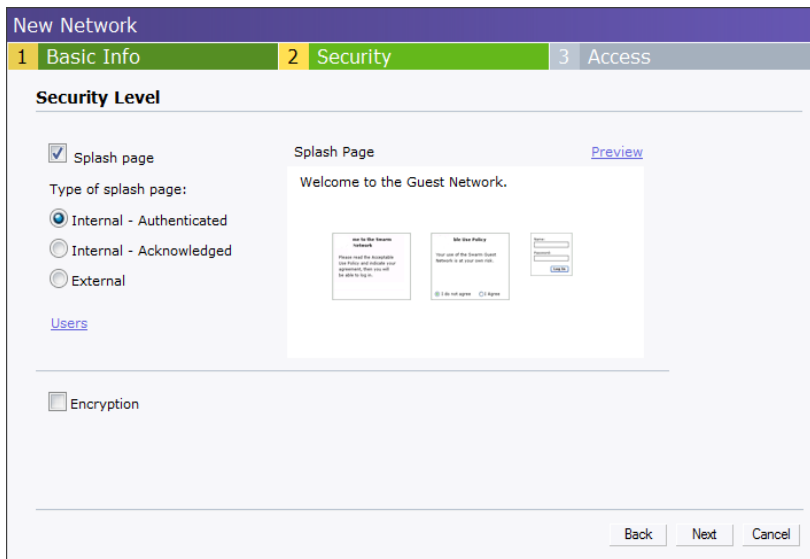
- **Internal Authenticated** - To gain access to the wireless network, a user must authenticate in the captive portal page. If this option is selected, then users who are required to authenticate have to be added to the user database. Click the **Users** link to add the users. For information about adding users, see “[Adding a User](#)” on page 141.
- **Internal Acknowledged** - To gain access to the wireless network, a user must accept the terms and conditions.

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

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

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

**Figure 63** Configuring Captive Portal when Adding A Guest Network



The screenshot shows the 'New Network' configuration window with the 'Security' tab selected. The 'Security Level' section is active, showing a 'Splash page' checkbox that is checked. Below it, the 'Type of splash page:' section has three radio button options: 'Internal - Authenticated' (selected), 'Internal - Acknowledged', and 'External'. A 'Preview' link is visible next to the selected option. The preview window displays a 'Welcome to the Guest Network.' message and a form with fields for 'User Name' and 'Password', along with 'OK' and 'Cancel' buttons. At the bottom of the main window, there are 'Back', 'Next', and 'Cancel' buttons.

The appearance of a splash page can be customized as required. For information on customizing a splash page, see “Customizing a Splash Page” on page 84.

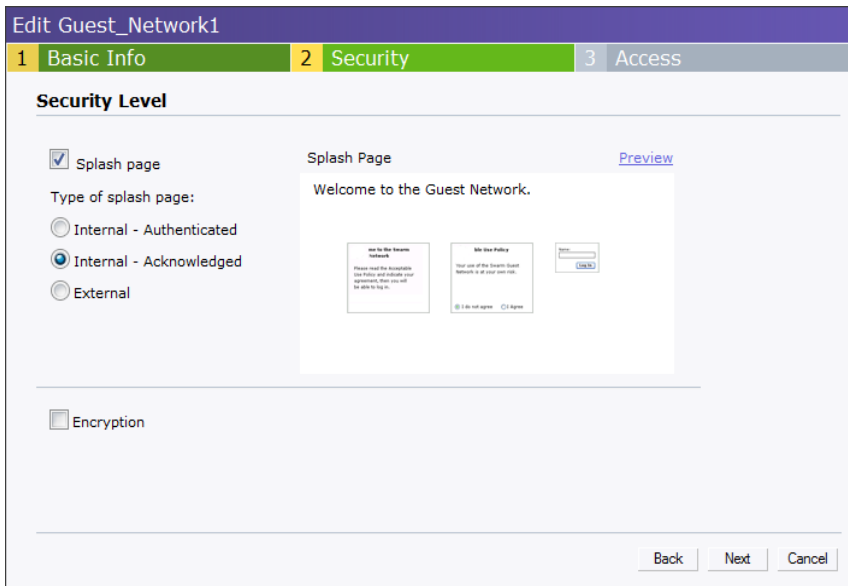
4. Click **Next** and click **Finish**.

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

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

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

**Figure 64** Configuring Captive Portal when Editing a Guest Network



The appearance of a splash page can be customized as required. For information on customizing a splash page, see “Customizing a Splash Page” on page 84.

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

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

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

1. In the **Network** tab, click the **New** link. The **New Network** box opens.
2. In the **Basic Info** tab, perform the following:
  1. Enter a name for the network in the **Name (SSID)** text box.
  2. Click the **Guest** radio button and click **Next**.
3. In the **Security** tab, select **External** for the splash page type.
4. Enter the following details for the External Splash Page:
  - a. **IP or hostname** - IP address of the external splash page server.
  - b. **URL** - URL of the external splash page server.
  - c. **Port** - Port used for communicating with the external splash page server.
  - d. **Authentication text** - Text string returned by the external server after successful authentication.
5. Click **Next**. Associate to the new SSID and access any URL.

**Figure 65** Configuring Internal Captive Portal with External Radius Server Authentication

The screenshot shows the 'New Network' configuration wizard with the 'Security' tab selected. The 'Security Level' section is expanded, showing the following configuration:

- Splash page
- External splash page:
  - Type of splash page:
    - Internal - Authenticated
    - Internal - Acknowledged
    - External
  - IP or hostname: 10.65.18.222
  - URL: port=80&gw\_id=default
  - Port: 80
  - Authentication text: Auth:1
- Encryption

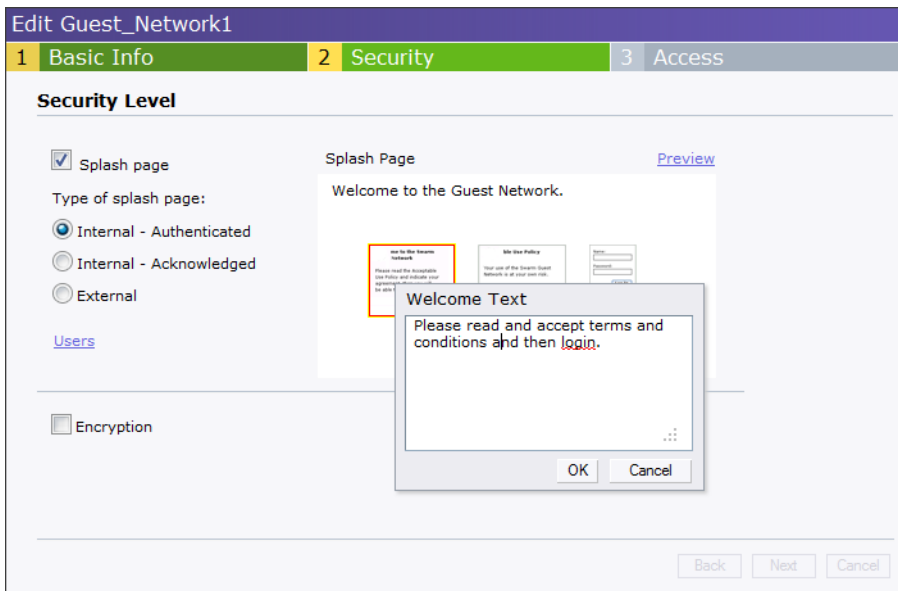
Navigation buttons at the bottom: Back, Next, Cancel.

### Customizing a Splash Page

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

1. In the **Network** tab, click the network for which you want to customize the splash page. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** box for the network appears.
3. Click **Next** and perform the following steps in the **Security** tab:
  1. To change the color of the splash page, click the Splash page rectangle and select the required color from the Background Color palette.
  2. To change the welcome text, click the first square in the splash page, type the required text in the **Welcome** text box, and click **OK**. The welcome text should not exceed 127 characters.
  3. To change the policy text, click the second square in the splash page, type the required text in the **Policy** text box, and click **OK**. The policy text should not exceed 255 characters.

**Figure 66** Customizing a Splash Page



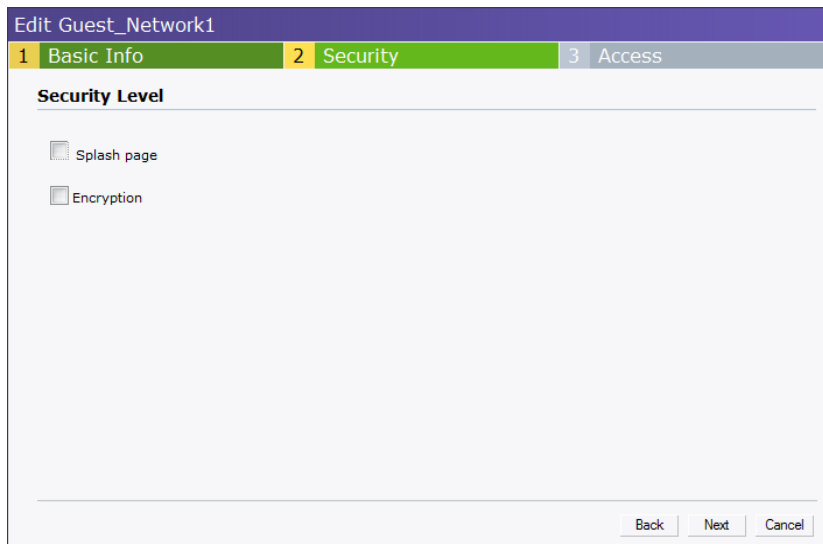
4. Click **Next** and then click **Finish**.

### Disabling Captive Portal authentication

To disable captive portal authentication, perform the following steps:

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

**Figure 67** Disabling Captive Portal Authentication



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

### External Captive Portal

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

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

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

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

**Figure 68** Configuring External Captive Portal when Adding a Guest Network

The screenshot shows the 'New Network' configuration window with the 'Security' tab selected. The 'Security Level' section is expanded, showing the 'External' option selected. The 'External splash page' section includes the following fields:

Field	Value
IP or hostname	localhost
URL	/
Port	80
Authentication text	Authenticated

The 'Encryption' checkbox is unchecked. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

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

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

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

1. In the **Network** tab, click the network for which you want to configure the external captive portal authentication. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** box for the network appears.
3. Click **Next**, and click the **External** button and perform the following steps in the **Security** tab:
  1. Enter the IP address or the hostname in the **IP or hostname** text box.
  2. Enter the URL for the splash page in the **URL** text box.

3. Enter the number of the port to be used for communicating with the external server in the **Port** text box.
4. In the **Authentication** text box, enter the unique signature that the external server will return in the response after a successful authentication.

**Figure 69** Configuring External Captive Portal Authentication when editing a Guest Network

The screenshot shows the 'Edit Guest\_Network1' configuration interface. At the top, there are three tabs: '1 Basic Info', '2 Security' (which is active), and '3 Access'. Below the tabs, the 'Security Level' section is visible. It contains a checked checkbox for 'Splash page'. Underneath, there are three radio button options for 'Type of splash page': 'Internal - Authenticated', 'Internal - Acknowledged', and 'External' (which is selected). To the right of these options are four input fields: 'External splash page:' with a value of 'localhost', 'URL:' with a value of '/', 'Port:' with a value of '80', and 'Authentication text:' with a value of 'Authenticated'. Below this section is an unchecked checkbox for 'Encryption'. At the bottom right of the form, there are three buttons: 'Back', 'Next', and 'Cancel'.

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

## MAC Authentication

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

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

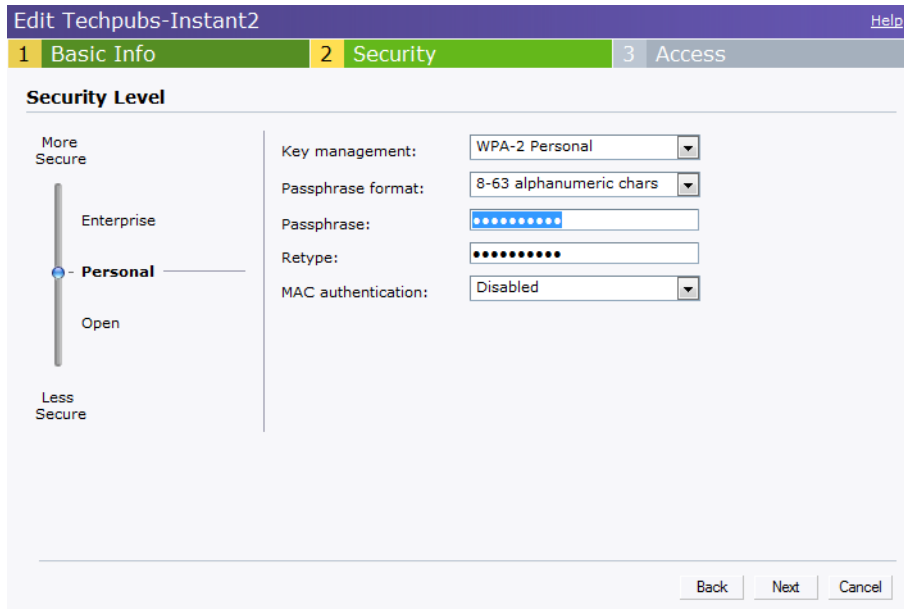
## Configuring MAC Authentication

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

1. In the **Network** tab, click the network for which you want to enable MAC authentication. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** box for the network appears.
3. Click **Next** and perform the following tasks in the **Security** tab:
  1. For a network with **Personal** or **Open** security level, select **External Radius Server** from the **MAC Authentication** drop-down list.

2. Click the **Primary** link and perform the following steps:
  3. Enter the IP address of the external RADIUS server in the **IP address** text box.
  4. Enter the authorization port number of the external RADIUS server in the **Auth Port** text box. The port number is set to **1812** by default.
  5. Enter a shared key for communicating with the external RADIUS server in the **Shared key** text box.
  6. Enter the virtual controller IP address in the **NAS IP address** text box. The NAS IP is the virtual controller IP address that is sent in the data packets.
4. Click the **Backup** link and set appropriate values for the backup RADIUS server.

**Figure 70** *Configuring MAC Authentication*



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

## Certificates

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

### Loading Certificates

To load a certificate, perform the following steps:

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



**Figure 71** *Loading Certificates*

The screenshot shows a web interface titled "Maintenance" with a sub-tab "Certificates". The interface includes a navigation bar with "Configuration", "Certificates", "Firmware", "Reboot", and "Convert". The main content area displays "Current certificate:" followed by "-- No certificate uploaded --". Below this is a "Certificate file to upload:" section with a text input field and a "Browse" button. An "Upload Certificate" button is positioned below the input field. The "Passphrase:" section contains two text input fields for entering and reconfirming the passphrase. A "Close" button is located in the bottom right corner of the form.

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



## Encryption Types Supported in Alcatel-Lucent 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 Alcatel-Lucent 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. Alcatel-Lucent 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. Alcatel-Lucent 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. Alcatel-Lucent recommends that all devices be upgraded or replaced so that they are capable of AES encryption.



---

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

---

## Encryption Recommendations

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

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

## Understanding WPA and WPA2

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

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

**Table 9** WPA and WPA2 Features

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

## Recommended Authentication and Encryption Combinations

Table 10 summarizes the recommendations for authentication and encryption combinations that should be used in Wi-Fi networks.

**Table 10** Recommended Authentication and Encryption Combinations

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

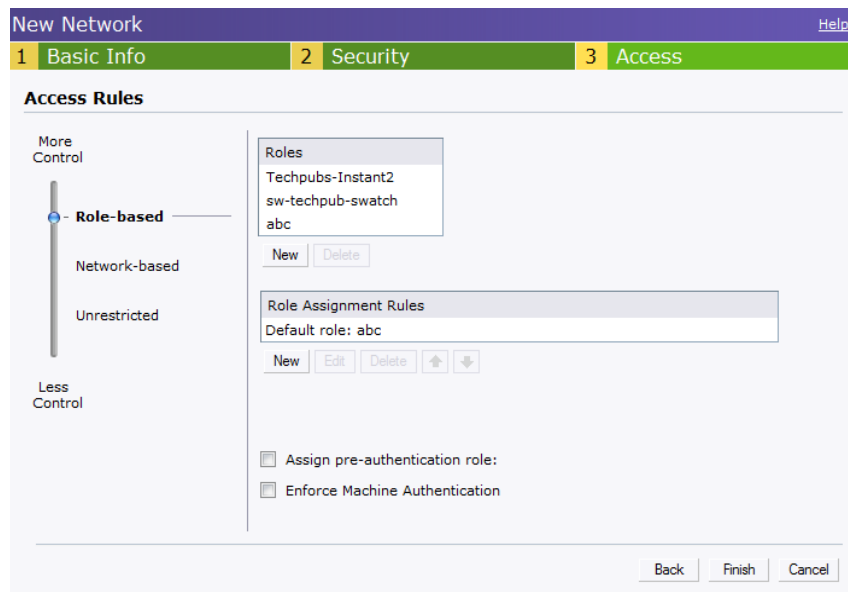
Every client in an Alcatel-Lucent Instant network is associated with a user role, which determines the client's network privileges, how often it must re-authenticate, and which bandwidth contracts are applicable.

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

## User Roles

This section describes how to create a new user role.

**Figure 72** Access Tab - Instant User Role Settings

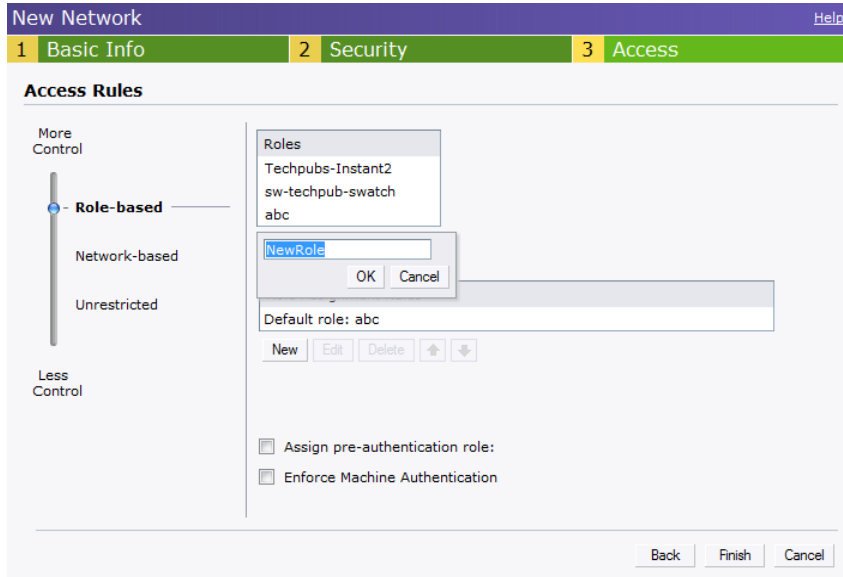


### Creating a New User Role

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

1. Click the **New** link in the **Networks** tab.  
To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate values in the **Security** tab.
4. Click **Next**. The **Access** tab appears.
5. Select **Role-based** from the scroll bar in the left.
6. Click the **New** button. The **New Rule** box appears. Enter the name of the new user role in this box.

**Figure 73** *Creating a New User Role*



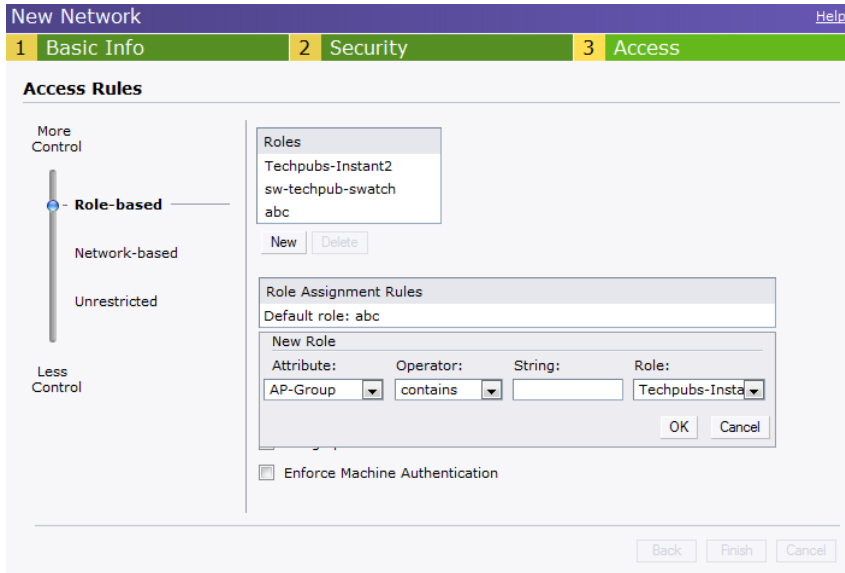
7. Click **OK**. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To create new access rules, see [“Example Access Rules” on page 101](#).
8. To delete a user role, select the user role and click the **Delete** button.

## Creating Role Assignment Rules

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

1. Click **New** button in the Role Assignment Rules table. The default user role is the newly created user role.
2. Select the attribute from the **Attribute** drop-down list. To view the list of supported attributes, see [“List of supported VSA’s” on page 78](#).
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 74** *Creating Role Assignment Rules*







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

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



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

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

**Figure 75** Access Tab - Instant Firewall Settings

The screenshot shows the 'New Network' configuration interface. At the top, there are three tabs: '1 Basic Info', '2 Security', and '3 Access'. The 'Access' tab is selected. Below the tabs, the section is titled 'Advanced Access Rules'. Under this section, there is a list of 'Access Rules (1)' containing one rule: 'Allow any to all destinations'. Below the list is a 'New Rule' dialog box. The dialog box has three fields: 'Action' (set to 'Allow'), 'Service' (set to 'any'), and 'Destination' (set to 'to all destinations'). There are 'OK' and 'Cancel' buttons at the bottom of the dialog box. At the bottom of the main window, there are 'Back', 'Finish', and 'Cancel' buttons.

## Service Options

Table 11 lists a sample set of service options available in the Instant UI. You can allow or deny access to any or all of these services depending on your requirements.

**Table 11** Network Service Options

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

**Table 11** *Network Service Options*

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

**Table 11** *Network Service Options*

Service	Description
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
svp	Software Validation Protocol
tftp	Trivial file transfer protocol

## Destination Options

Table 12 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 12** *Destination Options*

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

## Example Access Rules

This section provides procedures to create the following access rules.

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

## Allow TCP service to a particular network

1. Click the **New** link in the **Networks** tab.  
To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate values in the **Security** tab.
4. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define allow TCP service access rule to a particular network, perform the following steps:
  - a. Click the **New** button. The **New Rule** box appears.
  - b. Select **Allow** from the **Action** drop-down list.
  - c. Select **custom** from the **Service** drop-down list.
    - 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 76** Defining Rule - Allow TCP Service to a Particular Network

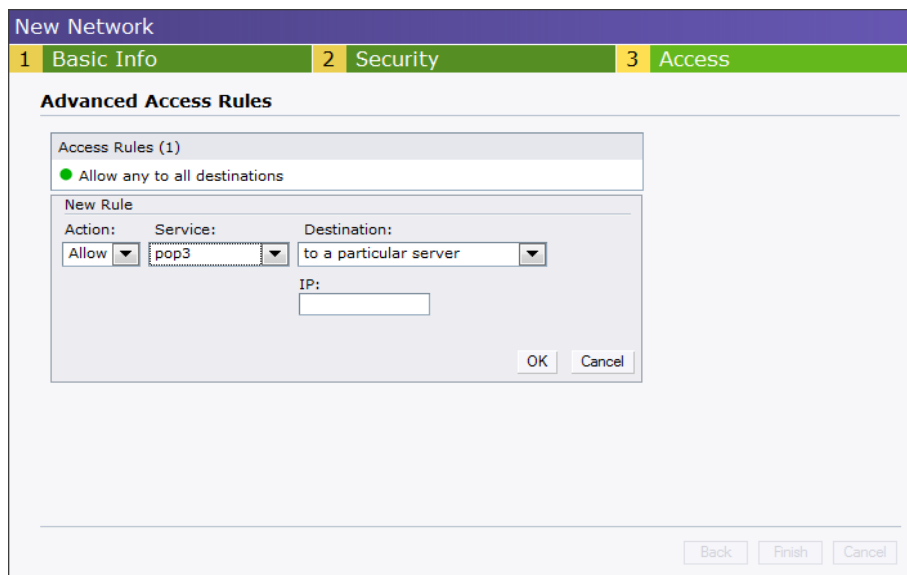
The screenshot shows the 'New Network' configuration interface. At the top, there are three tabs: '1 Basic Info', '2 Security', and '3 Access'. The 'Access' tab is active. Below the tabs, the 'Advanced Access Rules' section is visible. It contains a list of rules, with 'Allow any to all destinations' selected. A 'New Rule' dialog box is open, showing the following configuration: Action: Allow, Service: custom, Destination: to a network, Protocol: TCP. There are empty text boxes for Port(s), IP, and Netmask. The dialog has 'OK' and 'Cancel' buttons. At the bottom of the main window, there are 'Back', 'Finish', and 'Cancel' buttons.

- e. Click **OK**.
5. Click **Finish**.

## Allow POP3 service to a particular server

1. Click the **New** link in the **Networks** tab.  
To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate security levels using the slider button in the **Security** tab.
4. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define allow POP3 service access rule to a particular server, perform the following steps:
  1. Click the **New** button. The **New Rule** box appears.
  2. Select **Allow** from the **Action** drop-down list.
  3. Select **pop3** from the **Service** drop-down list.
  4. Select **to a particular server** from the **Destination** drop-down list and enter appropriate IP address in the IP text box.
  5. Click **OK**.
5. Click **Finish**.

**Figure 77** Defining Rule - Allow POP3 Service to a Particular Server

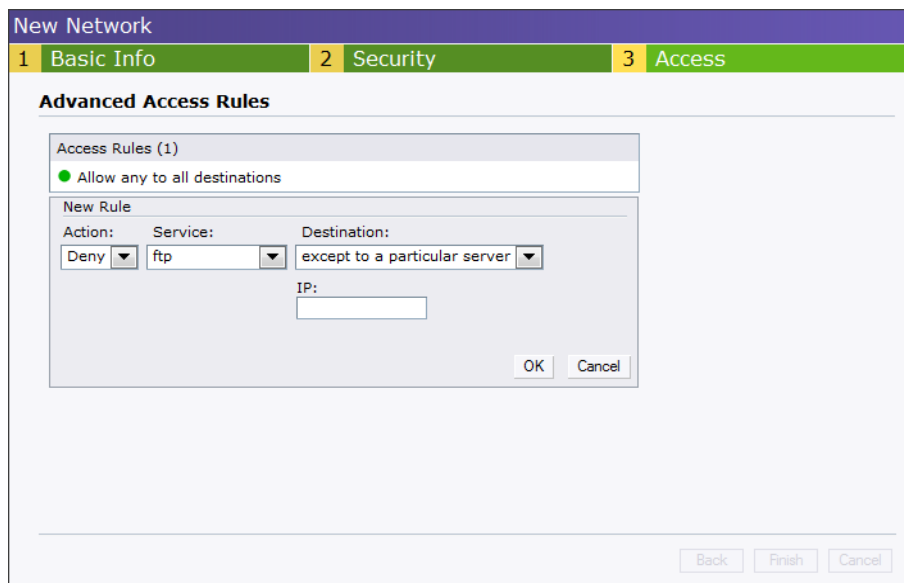


## Deny FTP service except to a particular server

1. Click the **New** link in the **Networks** tab.  
To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate security levels using the slider button in the **Security** tab.

4. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define deny FTP service access rule except to a particular server, perform the following steps:
  1. Click the **New** button. The **New Rule** box appears.
  2. Select **Deny** from the **Action** drop-down list.
  3. Select **ftp** from the **Service** drop-down list.
  4. Select **except to a particular server** from the **Destination** drop-down list and enter appropriate IP address in the **IP** text box.
  5. Click **OK**
5. Click **Finish**

**Figure 78** Defining Rule - Deny FTP Service Except to a Particular Server



## Deny bootp service except to a particular network

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

To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **Basic Info** tab, enter the appropriate information.
3. Click **Next** and set appropriate security levels using the slider button in the **Security** tab.
4. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define deny bootp service access rule except to a network, perform the following steps:
  1. Click the **New** button. The **New Rule** box appears.
  2. Select **Deny** from the **Action** drop-down list.
  3. Select **bootp** from the **Service** drop-down list.
  4. Select **except to a network** from the **Destination** drop-down list.
    - Enter appropriate IP address in the IP text box.
    - Enter appropriate netmask in the Netmask text box.
  5. Click **OK**.
5. Click **Finish**.



**Figure 79** *Defining Rule - Deny bootp Service Except to a Particular Network*

The screenshot shows the 'New Network' configuration wizard with three tabs: '1 Basic Info', '2 Security', and '3 Access'. The 'Advanced Access Rules' section is active. It contains a list of 'Access Rules (1)' with one rule selected: 'Allow any to all destinations'. A 'New Rule' dialog box is open, showing the following configuration:

Action:	Service:	Destination:
Deny	bootp	except to a network

Below the 'Destination' dropdown, there are two empty text input fields labeled 'IP:' and 'Netmask:'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons. At the bottom right of the main window are 'Back', 'Finish', and 'Cancel' buttons.



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

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

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

When this feature is enabled on Alcatel-Lucent Instant, all external DNS requests are forwarded to OpenDNS servers. A user is allowed or denied access to a website depending on the blacklist and whitelist entries in these servers. Internal DNS requests are forwarded to the internal DNS server.

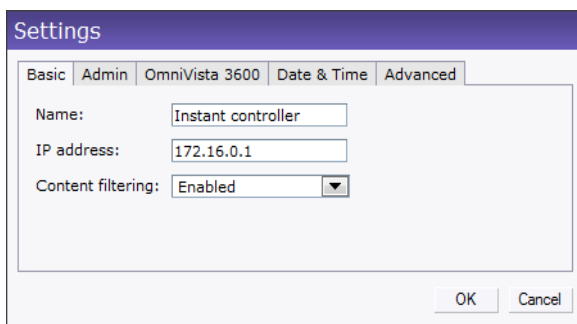
This feature also enables the OAW IAP to store or cache the responses from the OpenDNS servers. When the IAP receives an access request, it searches the cache memory. If a suitable record is found, the OAW IAP responds accordingly instead of contacting the DNS server again.

## Enabling Content Filtering

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

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

**Figure 80** *Enabling Content Filtering*



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



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

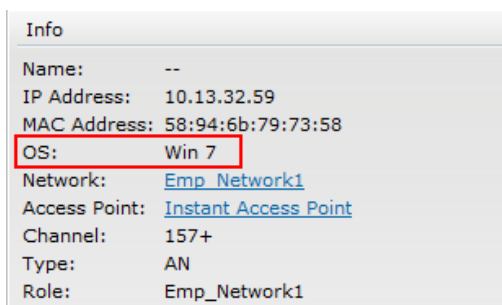
- Identifying rogue clients - Helps to identify clients that are running on forbidden operating systems.
- Identifying outdated operating systems - Helps to locate outdated and unexpected OS in the company network.
- Locating and patching vulnerable operating systems - Assists in locating and patching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

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

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

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

**Figure 81** OS Fingerprinting



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



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 OAW-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 Alcatel-Lucent Instant.

### Channel or Power Assignment

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

### Voice Aware Scanning

This feature stops the OAW-IAP that is supporting an active voice call from scanning for other channels in the RF spectrum. The OAW-IAP resumes scanning when no more active voice calls are present on that OAW-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 OAW-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 OAW-IAPs. This feature reduces co-channel interference and increases available bandwidth for dual-band clients because there are more channels on the 5 GHz band than on the 2.4 GHz band.

Band steering supports the following three different band steering modes:

- **Prefer 5Ghz** - If you configure the OAW-IAP to use prefer-5GHz band steering mode, the OAW-IAP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts.
- **Force 5Ghz** - When the OAW-IAP is configured in force-5GHz band steering mode, the OAW-IAP will try to force 5Ghz-capable OAW-IAPs to use that radio band.
- **Balance Bands** - In this band steering mode, the OAW-IAP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that

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

## Air Time Fairness

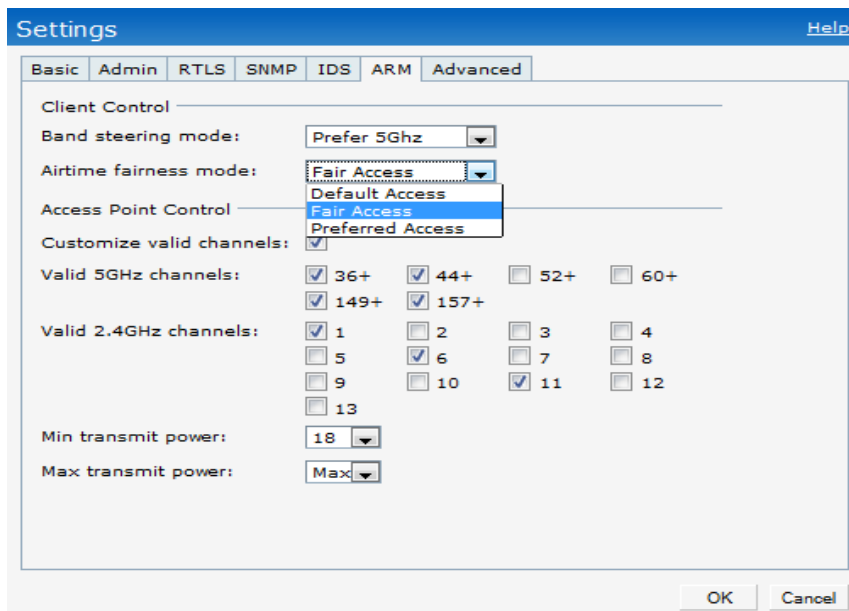
This feature provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system, thus delivering uniform performance to all clients. This feature prevents some clients from monopolizing resources at the expense of other clients.

### Air Time Fairness Modes

The Air Time Fairness consists of the following modes:

- Default Access - Provides access based on the client request. When Air Time Fairness is set to default access, per user and per SSID bandwidth contracts are not enforced
- Fair Access - Allocates Airtime evenly across all the clients
- Preferred Access - Allocates Airtime to all the clients but preference is for higher performing clients

**Figure 82** Air Time Fairness Mode



### Customize valid channels

You can customize the valid 5GHz channels and the valid 2.4 GHz channels for the IAP.

### Min transmit power

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

Default: 18 dBm

### Max transmit power

Maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. Higher power level settings may be constrained by local regulatory requirements and AP capabilities. In the event that an



AP is configured for a Max Tx EIRP setting it cannot support, this value will be reduced to the highest supported power setting.

Default: 127 dBm

## Monitoring the Network with ARM

When ARM is enabled, an OAW-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 OAW-IAP RF environment. Each OAW-IAP gathers other metrics on their ARM-assigned channel to provide a snapshot of the current RF health state.

## Configuring Administrator Assigned Radio Settings for OAW-IAP

ARM is enabled on Alcatel-Lucent Instant by default. It automatically assigns appropriate channel and power for the OAW-IAPs.

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

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

**Figure 83** Configuring Administrator Assigned Radio Settings for OAW-IAP

The screenshot shows a dialog box titled "Edit Access Point Instant Access Point 1" with four tabs: "Name", "Connectivity", "Radio", and "External Antenna". The "Radio" tab is active. It is divided into two sections: "2.4 GHz band" and "5 GHz band". Each section has two radio buttons: "Adaptive radio management assigned" and "Administrator assigned". In both sections, "Administrator assigned" is selected. Below each radio button are fields for "Channel" and "Transmit power". For the 2.4 GHz band, the Channel is set to "1" and Transmit power is "0". For the 5 GHz band, the Channel is set to "36+" and Transmit power is "0". At the bottom of the dialog, there are "OK" and "Cancel" buttons, and a "Less" link on the left.

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



Select the **Monitor** Mode to configure the specific OAW IAP in the Instant network in Monitor Mode and click **OK**.

5. Select the **Administrator assigned** radio button in **2.4 GHz** and **5 GHz** band sections.

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

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

## Rogue AP Detection and Classification

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

**Figure 84** *Intrusion Detection*

Foreign Access Points Detected							Foreign Clients Detected						
MAC Address	Network	Classification	Chan.	Type	Last Seen	Where	MAC Address	Network	Classification	Chan.	Type	Last Seen	Where
00:24:6c:80:74:00	ethersphere-voip	Interfering	6	GN 20MZ	15:31:52		b4:07:f9:f2:06:eb	ethersphere-voip	Interfering	1	BN 20MZ	15:31:52	
00:24:6c:bd:66:a0	manoj-vap	Interfering	1	GN 20MZ	15:31:52		00:27:10:5c:78:24	ethersphere-voip	Interfering	36	AN 40MZ	15:31:52	
00:0b:86:50:47:48	vijay-ap	Interfering	64	A	15:31:52		58:94:6b:7a:40:c0	ethersphere-wpa2	Interfering	157	AN 40MZ	15:31:52	
00:24:6c:80:95:c8	ethersphere-wpa2	Interfering	161	AN 40MZ	15:31:52		f8:db:7f:9b:03:fb	ethersphere-voip	Interfering	1	BN 20MZ	15:31:52	
00:1c:b0:eb:d9:60	IBM	Interfering	6	G	15:31:52		00:27:10:5c:65:04	ethersphere-wpa2	Interfering	36	AN 40MZ	15:31:52	
00:24:6c:80:74:01	Aruba-India-Guest	Interfering	6	GN 20MZ	15:31:52		58:94:6b:58:6b:04	ethersphere-wpa2	Interfering	36	AN 40MZ	15:31:52	
00:1a:1e:40:7c:81	shobha-765-rt-bridge	Interfering	1	GN 20MZ	15:31:52		00:26:c6:bd:51:d4	ethersphere-wpa2	Interfering	40	AN 40MZ	15:31:52	
00:24:6c:80:95:c9	ethersphere-voip	Interfering	161	AN 40MZ	15:31:52		00:26:c6:be:59:e2	ethersphere-voip	Interfering	1	G	15:31:52	
00:1a:1e:8b:a9:f0	ipv6-alpha	Interfering	149	AN 40MZ	15:31:52		f0:7b:cb:a3:92:8c	ethersphere-voip	Interfering	1	BN 20MZ	15:31:52	
00:1a:1e:17:dc:60	ipv6-alpha	Interfering	1	GN 20MZ	15:31:52		00:1e:65:71:49:2c	shobha-765-rt-bridge	Interfering	1	BN 20MZ	15:31:52	
00:24:6c:80:4f:88	ethersphere-wpa2	Interfering	149	AN 40MZ	15:31:52		00:26:c6:be:59:e2	ipv6-alpha	Interfering	48	AN 40MZ	15:31:52	
00:24:6c:80:6f:28	ethersphere-wpa2	Interfering	157	AN 40MZ	15:31:52		58:94:6b:79:ce:f0	ethersphere-wpa2	Interfering	40	AN 40MZ	15:31:52	
00:24:6c:80:95:ca	Aruba-India-Guest	Interfering	161	AN 40MZ	15:31:52		00:27:10:5c:74:64	ethersphere-wpa2	Interfering	149	A	15:31:52	
00:24:6c:80:4b:f0	ethersphere-voip	Interfering	1	GN 20MZ	15:31:52		80:50:1b:b9:0c:3d	ethersphere-voip	Interfering	1	B	15:31:52	
00:1a:1e:89:c2:00	aruba-ap	Interfering	6	GN 20MZ	15:31:52		00:27:10:5c:02:64	ethersphere-wpa2	Interfering	157	AN 40MZ	15:31:52	
00:24:6c:80:03:42	sw-byadav-swatch	Interfering	1	GN 20MZ	15:31:52		00:26:c6:71:e9:36	ethersphere-wpa2	Interfering	48	AN 40MZ	15:31:52	
00:24:6c:80:6c:60	ethersphere-voip	Interfering	1	GN 20MZ	15:31:52		58:94:6b:b2:cd:ac	ethersphere-wpa2	Interfering	149	A	15:31:52	
00:24:6c:80:6f:29	ethersphere-voip	Interfering	157	AN 40MZ	15:31:52		00:27:10:2a:c6:ac	ipv6-alpha	Interfering	6	B	15:31:52	
00:24:6c:80:99:a8	ethersphere-wpa2	Interfering	153	AN 40MZ	15:31:52		00:1e:65:71:18:de	arunsp	Interfering	44	A	15:31:52	
00:24:6c:80:4f:89	ethersphere-voip	Interfering	149	AN 40MZ	15:31:52		00:27:10:5c:23:78	ethersphere-wpa2	Interfering	48	AN 40MZ	15:31:52	
00:24:6c:80:4b:f1	Aruba-India-Guest	Interfering	1	GN 20MZ	15:31:52		00:1c:26:5b:a5:43	ethersphere-wpa2	Interfering	157	A	15:31:52	

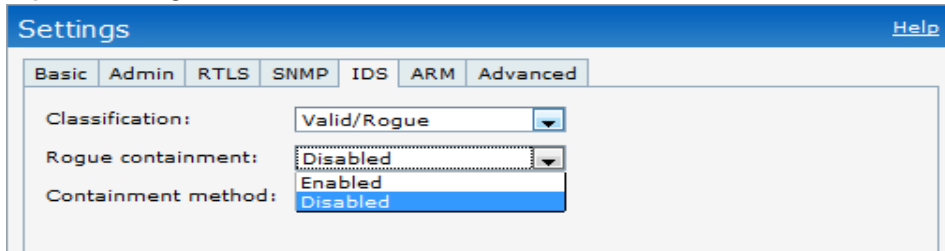
## Rogue Containment

Enable or disable rogue containment on the Instant network. By default, this is disabled.



The rogue containment is supported only when the OAW IAPs are in the monitor mode.

**Figure 85** Rogue Containmen



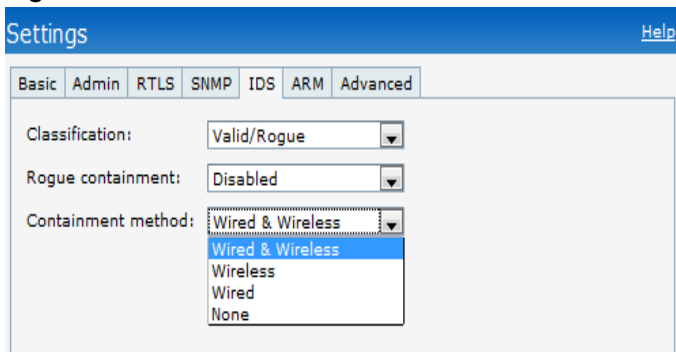
## Containment Methods

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 & Wireless - An OAW IAP or client is contained by disrupting its connection on the wired and wireless interfaces.
- Wired - An OAW IAP or client is contained by disrupting its connection on the wired interface.
- Wireless - An OAW IAP or client is contained by disrupting its association on the wireless interface.
- None - Disables all the containment mechanisms.

**Figure 86** Containment Methods



---

Wireless containment is the recommended containment method.

---

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

## SNMP Parameters for OAW IAP

You can configure the following parameters for OAW IAP.

**Table 13** *SNMP Parameters for IAP*

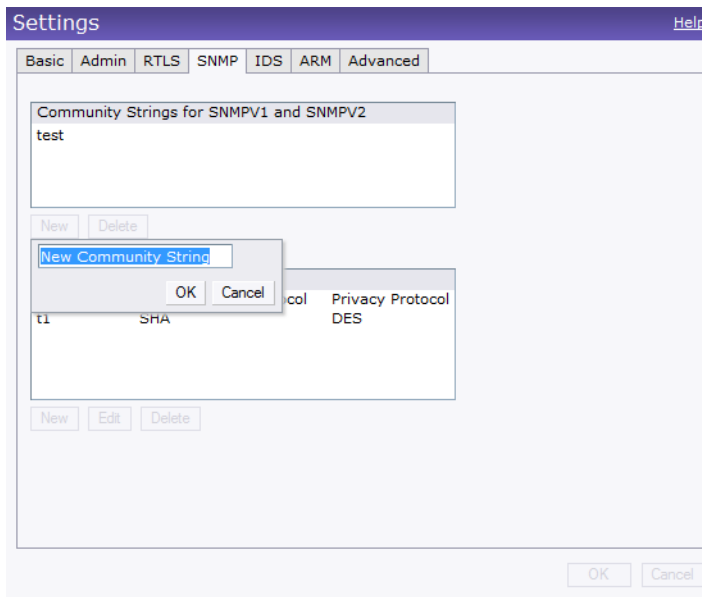
Field	Description
Community Strings for SNMPV1 and SNMPV2	Community strings used to authenticate requests for SNMP versions before version 3. NOTE: This is needed only if using SNMP v2c and is not needed if using version 3.
If you are using SNMPv3 to obtain values from the Alcatel-Lucent switch, then you can configure the following parameters	
Name	A string representing the name of the user.
Authentication Protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: <ul style="list-style-type: none"> <li>MD5: HMAC-MD5-96 Digest Authentication Protocol</li> <li>SHA: HMAC-SHA-96 Digest Authentication Protocol</li> </ul>
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption).
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol.

Follow the steps below to create community strings for SNMPV1 and SNMPV2

1. In the Settings tab click the **SNMP** tab.
2. Click the **New** button 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 the **Delete** button.

**Figure 87** *Creating Community Strings for SNMPV1 and SNMPV2*



Follow the steps below to create, edit, and delete users for SNMPV3

1. In the Settings tab click the **SNMP** tab.
2. Click the **New** button in the Users for SNMPV3 box.
3. Enter the name of the user in the **Name** text box.
4. Select the type of authentication protocol from the **Auth protocol** drop-down list.
5. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box.
6. Select the type of privacy protocol from the **Privacy protocol** drop-down list.
7. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box.
8. click **OK**.
9. To edit the details for a particular user, select the user and click the **Edit** button.
10. To delete a particular user, select the user and click the **Delete** button.

**Figure 88** *Creating Users for SNMPV3*

The screenshot shows a 'Settings' window with a purple title bar and a 'Help' button. Below the title bar are tabs for 'Basic', 'Admin', 'RTLS', 'SNMP', 'IDS', 'ARM', and 'Advanced'. The 'SNMP' tab is selected. The main content area is divided into two sections. The top section, titled 'Community Strings for SNMPV1 and SNMPV2', contains a text box with the word 'test' and 'New' and 'Delete' buttons below it. The bottom section, titled 'New SNMPV3 User', is a dialog box with the following fields: 'Name:' (text box), 'Auth protocol:' (dropdown menu with 'SHA' selected), 'Privacy protocol:' (dropdown menu with 'DES' selected), 'Password:' (text box), 'Retype:' (text box), and another 'Password:' (text box) and 'Retype:' (text box) pair. 'OK' and 'Cancel' buttons are at the bottom right of the dialog box. At the bottom of the main window, there are also 'OK' and 'Cancel' buttons.





OmniVista 3600 Air Manager is a solution for managing rapidly changing wireless networks. The easy-to-use interface and user-centric approach lets you to easily solve any connectivity issues. It allows you to efficiently and remotely manage and monitor enterprise wireless LAN. It allows you to monitor and change wireless LAN settings, generate compliance reports, locate users and OAW-IAPs, and diagnose problems from any Internet connection. Alcatel-Lucent OAW-IAPs communicate with OmniVista 3600 Air Manager using the HTTPS protocol. This allows an OmniVista 3600 Air Manager server to be deployed in the cloud across a NAT device such as a router.

### OmniVista 3600 Air Manager Features

This section describes the OmniVista 3600 Air Manager features that are available in the Alcatel-Lucent Instant network.

#### Image Management

OmniVista 3600 Air Manager allows updating the firmware on WLAN devices by defining a minimum acceptable firmware version for each make and model of a device. It remotely distributes the firmware image to the WLAN devices that require updates, and also schedules the firmware updates such that updating is completed without the necessity to manually monitor the devices.

The following models can be used to upgrade the firmware:

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

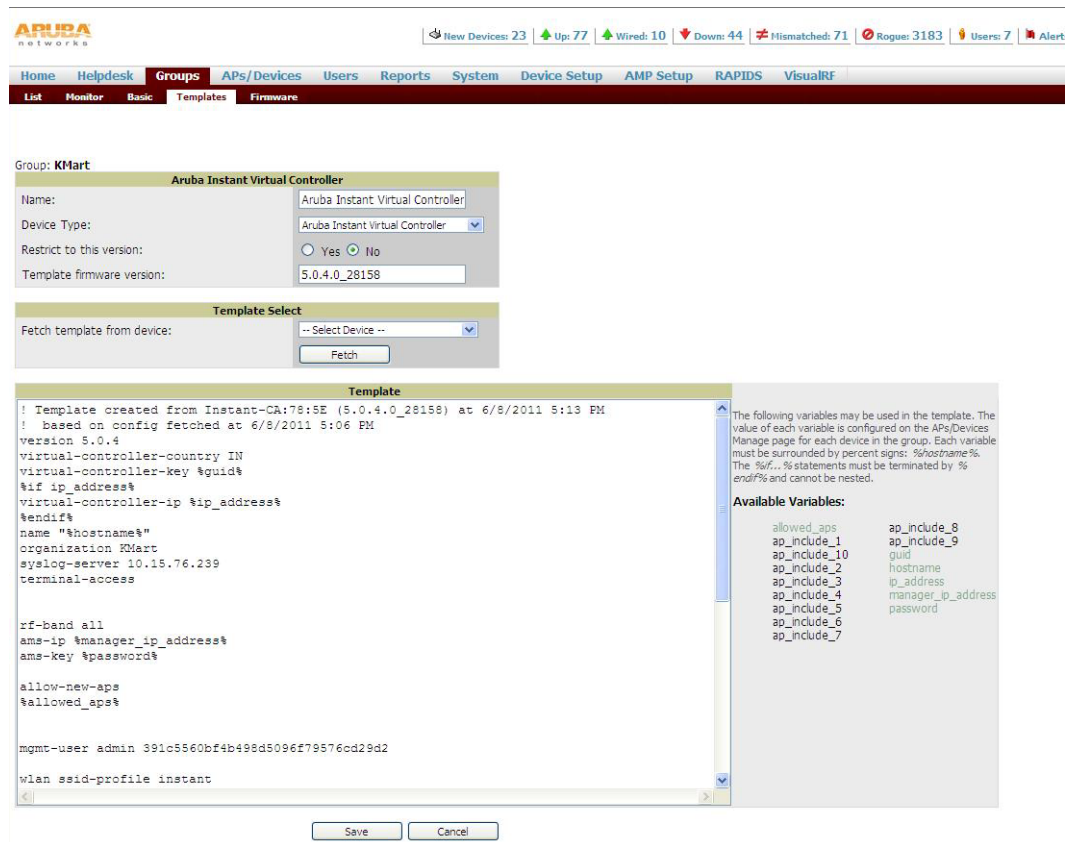
#### OAW-IAP and Client Monitoring

OmniVista 3600 Air Manager allows you to find any OAW-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

OmniVista 3600 Air Manager automatically creates a configuration template based on any of the existing OAW-IAPs, and it applies that template across the network as shown in [Figure 89](#). 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 89** *Template Based Configuration*



## Trending Reports

OmniVista 3600 Air Manager saves up to two years of actionable information, including network performance data and user roaming patterns so you can analyze how network usage and performance trends have changed over time. It also provides the detailed capacity reports with which you can plan the capacity and plan right strategies for your organization.

## Intrusion Detection System

OmniVista 3600 Air Manager provides advanced, rules-based rogue classification. It automatically detects rogue OAW-IAPs irrespective of their location in the network. It prevents authorized OAW-IAPs from being detected as rogue OAW-IAPs. It tracks and correlates the IDS events to provide a complete picture of network security.

## Configuring OmniVista 3600 Air Manager

This section describes how to configure OmniVista 3600 Air Manager. Before configuring the OmniVista 3600 Air Manager, you need the following:

- IP address of the OmniVista 3600 Air Manager server.
- Shared key for service authorization - This is assigned by the OmniVista 3600 Air Manager administrator.

## Creating your Organization String

The Organization String is a set of colon-separated strings created by the OmniVista 3600 Air Manager administrator to accurately represent the deployment of each Alcatel-Lucent Instant system. This string is entered into the Alcatel-Lucent 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 subfolders under the folder named "Org":

- subfolder1 would be a folder under the "Org" folder
- subfolder2 would be a folder under subfolder1

## The 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 OAW IAP

1. Click the **OmniVista 3600 Air Manager Set Up Now** link in the bottom-middle region of the Instant UI. The **Settings** box with the **OmniVista 3600 Air Manager** tab selected appears.

**Figure 90** *Configuring OmniVista 3600 Air Manager*

The screenshot shows a 'Settings' dialog box with a purple title bar and a 'Help' button. The 'Basic' tab is selected, and the 'OmniVista 3600' section is active. The 'Local' section includes a dropdown for 'Authentication' set to 'Internal', and text boxes for 'Username' (containing 'admin'), 'Password', and 'Retype'. The 'OmniVista 3600' section includes text boxes for 'Organization', 'OmniVista 3600 IP', 'Shared key', and 'Retype'. 'OK' and 'Cancel' buttons are at the bottom right.

2. Enter the name of your organization in the **Organization** name text box.
3. Enter the IP address of the OmniVista 3600 Air Manager server in the **OmniVista 3600 Air Manager IP** text box.
4. Enter the shared key in the **Shared key** text box and reconfirm. This shared key is used for configuring the first AP in the Alcatel-Lucent Instant network.
5. Click **OK**.

## OmniVista 3600 Air Manager Discovery through DHCP Option

The OmniVista 3600 Air Manager configuration can also be performed on the DHCP option that is configured on the DHCP server. You can configure this only if the OmniVista 3600 Air Manager is not configured earlier or have deleted the precedent configuration.

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



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

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

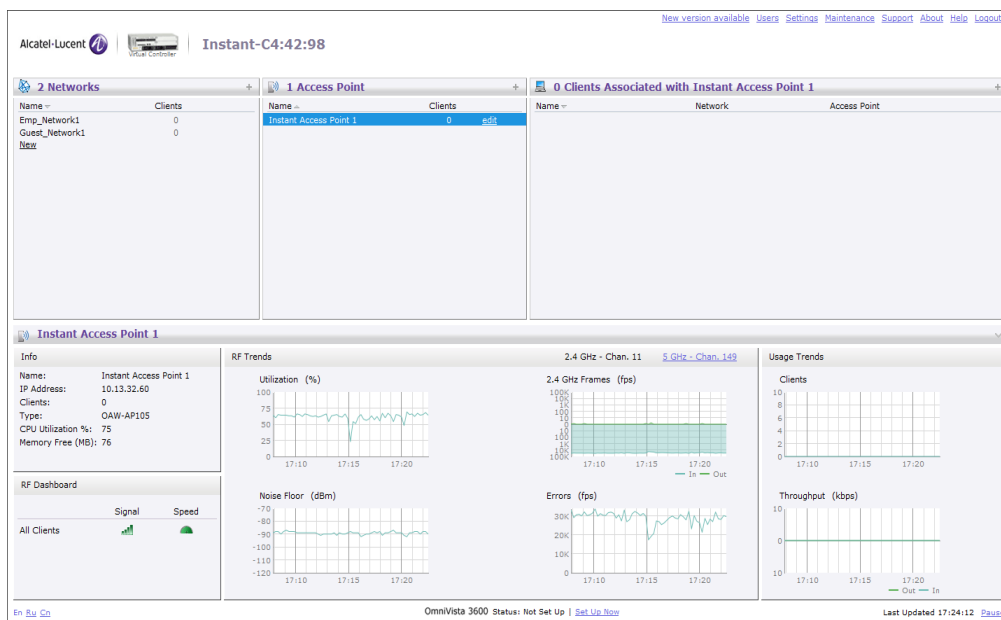
This chapter provides information about the parameters that can be monitored using these views. It also provides procedures to monitor these parameters.

## Virtual Controller View

The Virtual Controller view is the default view. This view allows you to monitor the Alcatel-Lucent 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. These links allow you to monitor the Alcatel-Lucent Instant network. For detailed information about the sections in these links and how they can be used to monitor the network, see [Monitoring Link](#), [IDS Link](#), [Client Alerts Link](#) sections.

**Figure 91** Virtual Controller View



## Monitoring Link

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

- Info
- RF Dashboard
- Usage Trends

## Info

The **Info** section displays the following information about the Virtual Controller:

- **Name** - Virtual Controller name.
- **Country Code** - Country in which the Virtual Controller is operating.
- **IP address** - IP address of the Virtual Controller.
- **Content filtering** - Status of the Content Filtering feature: Enabled or Disabled.
- **Organization** - Name of the organization.
- **AirWave IP** - IP address of the AirWave server.
- **Band** - Band in which the virtual controller is operating: 2.4 GHz band, 5.4 GHz band, or both.
- **NTP server** - IP address of the NTP server.

## RF Dashboard

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

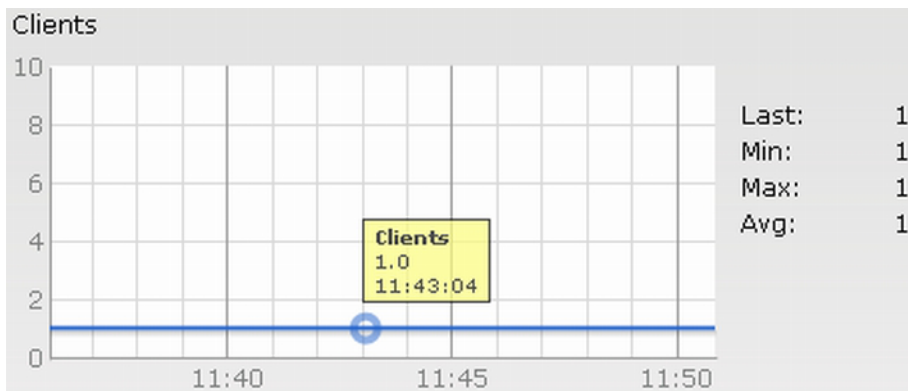
- IP address, Signal, and Speed information about the clients in the Alcatel-Lucent Instant network. If the speed or signal strength of a client is low, IP address of the client appears as a link. Click the link to monitor the client. For more information, see “[Client View](#)” on page 134.
- Instant Access Points, Utilization, Noise, and Errors information about the OAW-IAPs in the Alcatel-Lucent Instant network. If utilization, noise or errors of an OAW-IAP are not within the specified threshold, the OAW-IAP name appears as a link. Click the link to monitor the OAW-IAP. For more information, see “[Instant Access Point View](#)” on page 130.

## Usage Trends

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

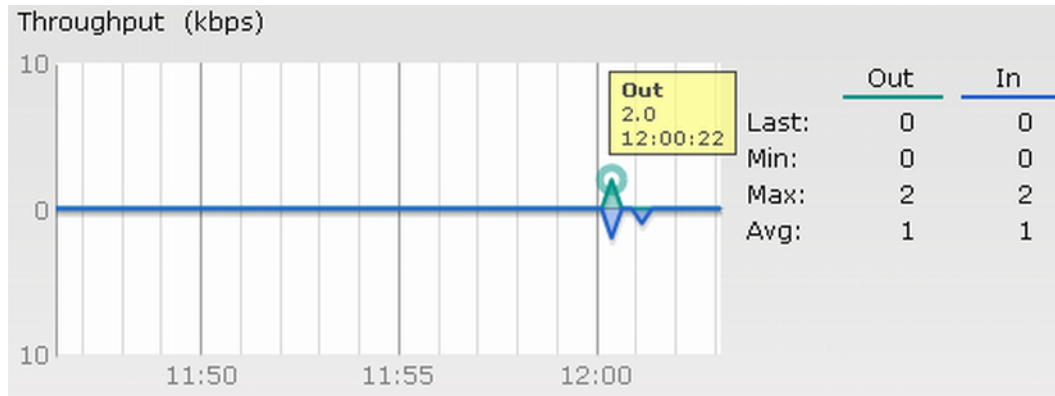
- Clients Graph

**Figure 92** *Clients Graph*



- Throughput Graph

**Figure 93** *Throughput Graph*



For more information about the graphs in the virtual controller view and for monitoring procedures, see [Table 14](#).

**Table 14** *Virtual Controller View - Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients	<p>The Clients graph shows the number of clients associated with the virtual controller for the last 15 minutes.</p> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the Virtual Controller for the last 15 minutes.</li> <li>To see the exact number of clients in the Alcatel-Lucent Instant network at a particular time, hover the cursor over the graph line.</li> </ul>	<p>To check the number of clients associated with the virtual controller for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>Study the Clients graph in the <b>Usage Trends</b> pane. For example, the graph on the left shows that one client is associated with the virtual controller at 11:43 hours.</li> </ol>
Throughput	<p>The Throughput graph shows the throughput of all networks and OAW IAPs associated with the virtual controller for the last 15 minutes.</p> <ul style="list-style-type: none"> <li>Outgoing traffic - Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line.</li> <li>Incoming traffic - Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line.</li> </ul> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the virtual controller for the last 15 minutes.</li> </ul> <p>To see the exact throughput of the Alcatel-Lucent Instant network at a particular time, hover the cursor over the graph line.</p>	<p>To check the throughput of the networks and OAW IAPs associated with the virtual controller for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>Study the Throughput graph in the <b>Usage Trends</b> pane. For example, the graph on the left shows 2.0 kbps outgoing traffic throughput at 12:00 hours. It also shows some incoming traffic throughput at the same time.</li> </ol>

### Client Alerts Link

For information about the Client Alerts link, see [Chapter 3, “Instant User Interface”](#) and [Chapter 21, “Alert Types and Management”](#) chapters.

### IDS Link

For information about the IDS link, see [Chapter 3, “Instant User Interface”](#).

## Network View

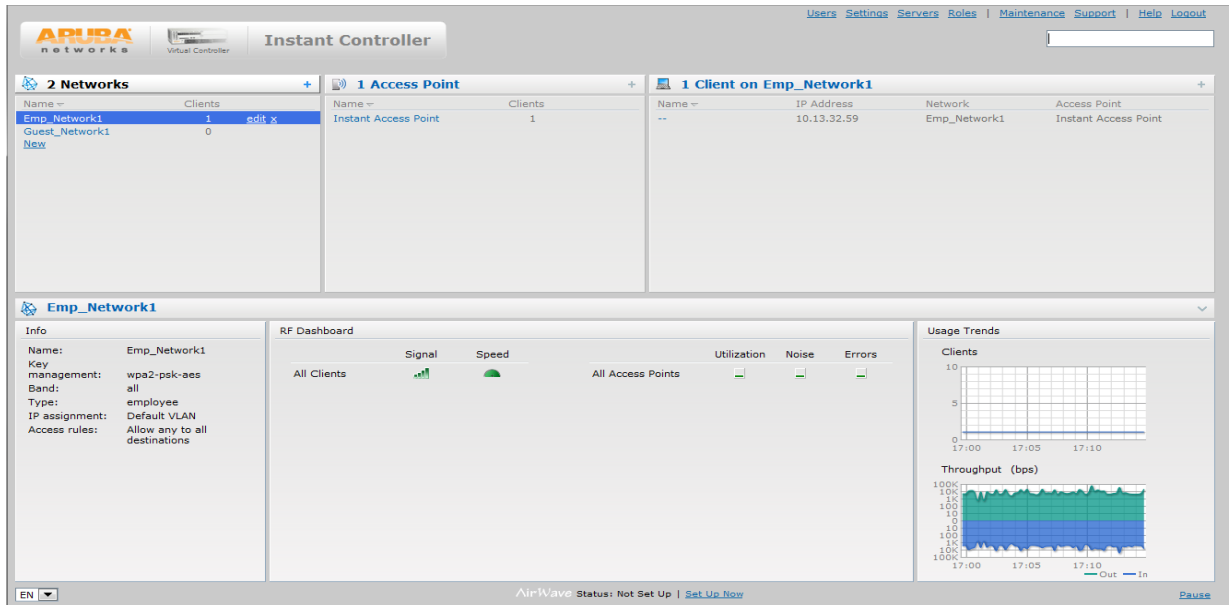
All Wi-Fi networks in the Alcatel-Lucent Instant network are listed in the **Networks** tab. Click the network that you want to monitor. Network View for the selected network appears.

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 94** Network View



### Info

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

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

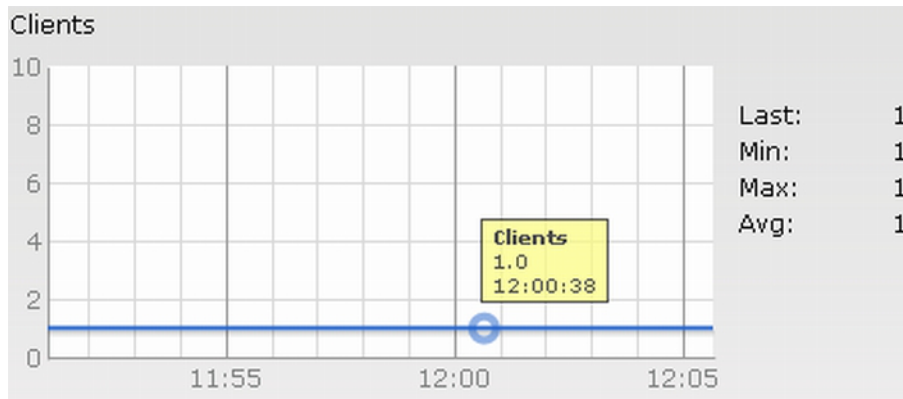
### Usage Trends

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

- Clients

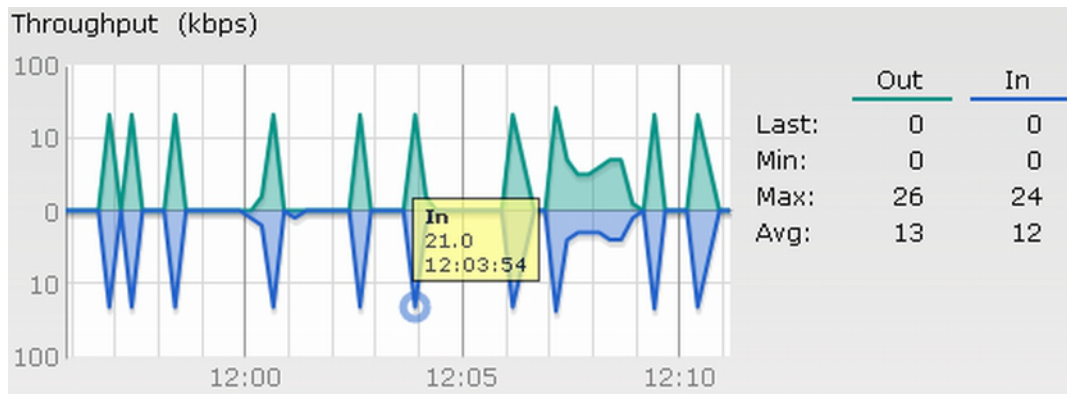


**Figure 95** Clients Graph



- Throughput

**Figure 96** Throughput Graph



For more information about the graphs in the network view and for monitoring procedures, see [Table 15](#).

**Table 15** Network View - Graphs and Monitoring Procedures

Graph Name	Description	Monitoring Procedure
Clients	<p>The Clients graph shows the number of clients associated with the network for the last 15 minutes.</p> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>• The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the Virtual Controller for the last 15 minutes.</li> <li>• To see the exact number of clients in the Alcatel-Lucent Instant network at a particular time, hover the cursor over the graph line.</li> </ul>	<p>To check the number of clients associated with the network for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the <b>Networks</b> tab, click the network for which you want to check the client association. The Network view appears.</li> <li>3. Study the Clients graph in the <b>Usage Trends</b> pane. For example, the graph on the left shows that one client is associated with the selected network at 12:00 hours</li> </ol>

**Table 15** Network View - Graphs and Monitoring Procedures

Graph Name	Description	Monitoring Procedure
Throughput	<p>The Throughput graph shows the throughput of the selected network for the last 15 minutes.</p> <ul style="list-style-type: none"><li>Outgoing traffic - Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line.</li><li>Incoming traffic - Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line.</li></ul> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"><li>The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the network for the last 15 minutes.</li></ul> <p>To see the exact throughput of the selected network at a particular time, hover the cursor over the graph line.</p>	<p>To check the throughput of the selected network for the last 15 minutes,</p> <ol style="list-style-type: none"><li>Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li><li>In the <b>Networks</b> tab, click the network for which you want to check the client association. The Network view appears.</li><li>Study the Throughput graph in the <b>Usage Trends</b> pane. For example, the graph on the left shows 22.0 kbps incoming traffic throughput for the selected network at 12:03 hours.</li></ol>

## Instant Access Point View

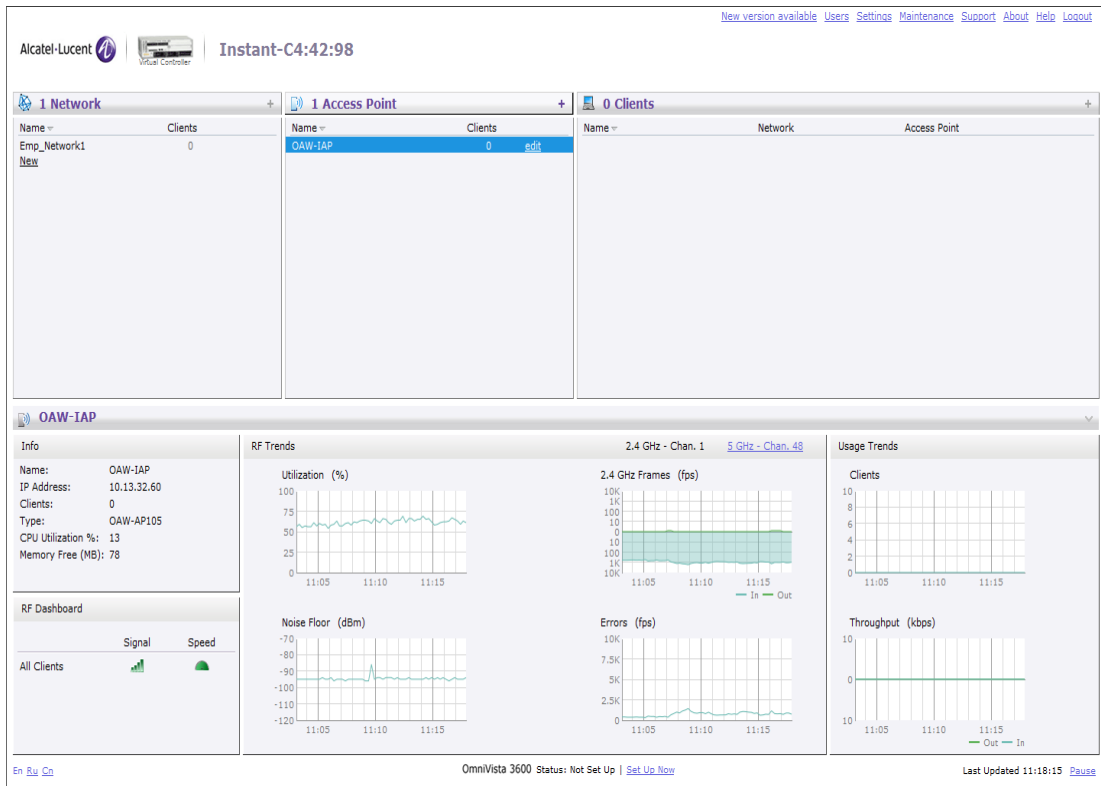
All OAW IAPs in the Alcatel-Lucent Instant network are listed in the **Access Points** tab. Click the OAW IAP that you want to monitor. Access Point view for that OAW IAP appears.

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 OAW IAP:

- Info
- RF Dashboard
- RF Trends
- Usage Trends

**Figure 97** Instant Access Point View



## Info

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

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

## RF Dashboard

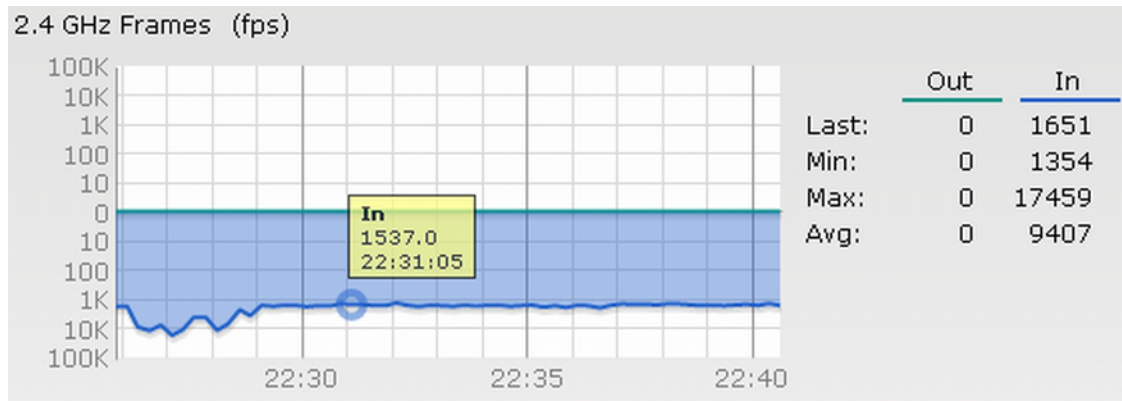
In the Instant Access Point view, the **RF Dashboard** section is moved below the **Info** section. It lists the IP address of the clients that are associated with the selected OAW IAP if the signal strength or the data transfer speed of the client is low.

## RF Trends

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

- Utilization
- 2.4 GHz Frames

**Figure 98** 2.4 GHz Frames Graph




- Noise Floor
- Errors



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

For more information about the graphs in the instant access point view and for monitoring procedures, see [Table 16](#).

**Table 16** Instant Access Point View - RF Trends Graphs and Monitoring Procedures

Graph Name	Description	Monitoring Procedure
Utilization	<p>The Utilization graph shows the radio utilization percentage of the access point for the last 15 minutes.</p> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>• The enlarged view provides Last, Minimum, Maximum, and Average radio utilization statistics for the OAW IAP for the last 15 minutes.</li> </ul> <p>To see the exact utilization percent at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the utilization of the selected OAW IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>2. In the Access Points tab, click the OAW IAP for which you want to monitor the utilization. The IAP view appears.</li> <li>3. Study the Utilization graph in the RF Trends pane. For example, the graph on the left shows 62% OAW IAP radio utilization for the 2.4 GHz band at 22:28 hours.</li> </ol> <p><b>NOTE:</b> You can also click the rectangle icon under the Utilization column in the <b>RF</b></p> <div style="text-align: center;">  </div> <p><b>Dashboard</b> pane to see the Utilization graph for the selected OAW IAP.</p>

**Table 16** Instant Access Point View - RF Trends Graphs and Monitoring Procedures

Graph Name	Description	Monitoring Procedure
2.4 GHz Frames	<p>The 2.4 GHz Frames graph shows the In and Out frame rate per second for the radio in 2.4 GHz band for the last 15 minutes.</p> <ul style="list-style-type: none"> <li>Outgoing frames - Outgoing frame traffic is displayed in green. It is shown above the median line.</li> <li>Incoming frames - Incoming frame traffic is displayed in blue. It is shown below the median line.</li> </ul> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing frames.</li> </ul> <p>To see the exact utilization percent at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the In and Out frame rate per second for the radio in 2.4 GHz band, for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the WebUI. The Virtual Controller view appears. This is the default view.</li> <li>In the Access Points tab, click the name link of the OAW IAP for which you want to monitor the frame rate. The OAW IAP view appears.</li> <li>Study the 2.4 GHz Frames graph in the RF Trends pane. For example, the graph on the left shows 1537.0 incoming frames at 22:31 hours.</li> </ol>
Noise Floor	<p>The Noise Floor graph shows the signals created by all the noise sources and unwanted signals in the network. Noise floor is measured in decibels/metre. Too many unwanted signals hamper the performance of the OAW IAP. Monitor the noise floor regularly for optimal performance of the OAW IAP.</p> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In and Out frames.</li> </ul> <p>To see the exact utilization percent at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the noise floor for the OAW IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the WebUI. The Virtual Controller view appears. This is the default view.</li> <li>In the Access Points tab, click the name link of the OAW IAP for which you want to monitor the noise floor. The OAW IAP view appears.</li> <li>Study the Noise Floor graph in the RF Trends pane. For example, the graph on the left shows that the noise floor for the OAW IAP at 22:38 hours is -82.0 dBm.</li> </ol> <p><b>NOTE:</b> You can also click the rectangle icon under the Noise column in the <b>RF</b></p>  <p><b>Dashboard</b> pane to see the Noise graph for the selected OAW IAP.</p>
Errors	<p>The Errors graph shows the errors that occurred while receiving the frames for the last 15 minutes. The errors are measured in frames per second.</p> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In and Out frames.</li> </ul> <p>To see the exact utilization percent at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the errors for the OAW IAP for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the WebUI. The Virtual Controller view appears. This is the default view.</li> <li>In the Access Points tab, click the name link of the OAW IAP for which you want to monitor the errors. The OAW IAP view appears.</li> <li>Study the Errors graph in the RF Trends pane. For example, the graph on the left shows that the errors for the OAW IAP at 22:48 hours is 9514.0 frames per second.</li> </ol> <p><b>NOTE:</b> You can also click the rectangle icon under the Errors column in the <b>RF</b></p>  <p><b>Dashboard</b> pane to see the Errors graph for the selected OAW IAP.</p>

## Usage Trends

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

- Clients Graph
- Throughput Graph

For more information about the usage trends graphs in the instant access point view and or monitoring procedures, see [Table 17](#).

**Table 17** *Instant Access Point View - Usage Trends and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients	<p>The Clients graph shows the number of clients associated with the selected OAW IAP for the last 15 minutes.</p> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"><li>• The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the OAW IAP for the last 15 minutes.</li></ul> <p>To see the exact number of clients associated with the selected OAW IAP at a particular time, hover the cursor over the graph line.</p>	<p>To check the number of clients associated with the OAW IAP for the last 15 minutes,</p> <ol style="list-style-type: none"><li>1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li><li>2. In the Access Points tab, click the OAW IAP for which you want to monitor the client association. The OAW IAP view appears.</li><li>3. Study the Clients graph in the Usage Trends pane. For example, the graph on the left shows that one client is associated with the OAW IAP at 12:12 hours.</li></ol>
Throughput	<p>The Throughput graph shows the throughput for the selected OAW IAP for the last 15 minutes.</p> <ul style="list-style-type: none"><li>• Outgoing traffic - Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown about the median line.</li><li>• Incoming traffic - Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line.</li></ul> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"><li>• The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the OAW IAP for the last 15 minutes.</li></ul> <p>To see the exact throughput of the selected OAW IAP at a particular time, hover the cursor over the graph line.</p>	<p>To check the throughput of the selected OAW IAP for the last 15 minutes,</p> <ol style="list-style-type: none"><li>1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li><li>2. In the Access Points tab, click the OAW IAP for which you want to monitor the throughput. The OAW IAP view appears.</li><li>3. Study the Throughput graph in the Usage Trends pane. For example, the graph on the left shows 4.0 kbps incoming traffic throughput at 12:08 hours.</li></ol>

## Client View

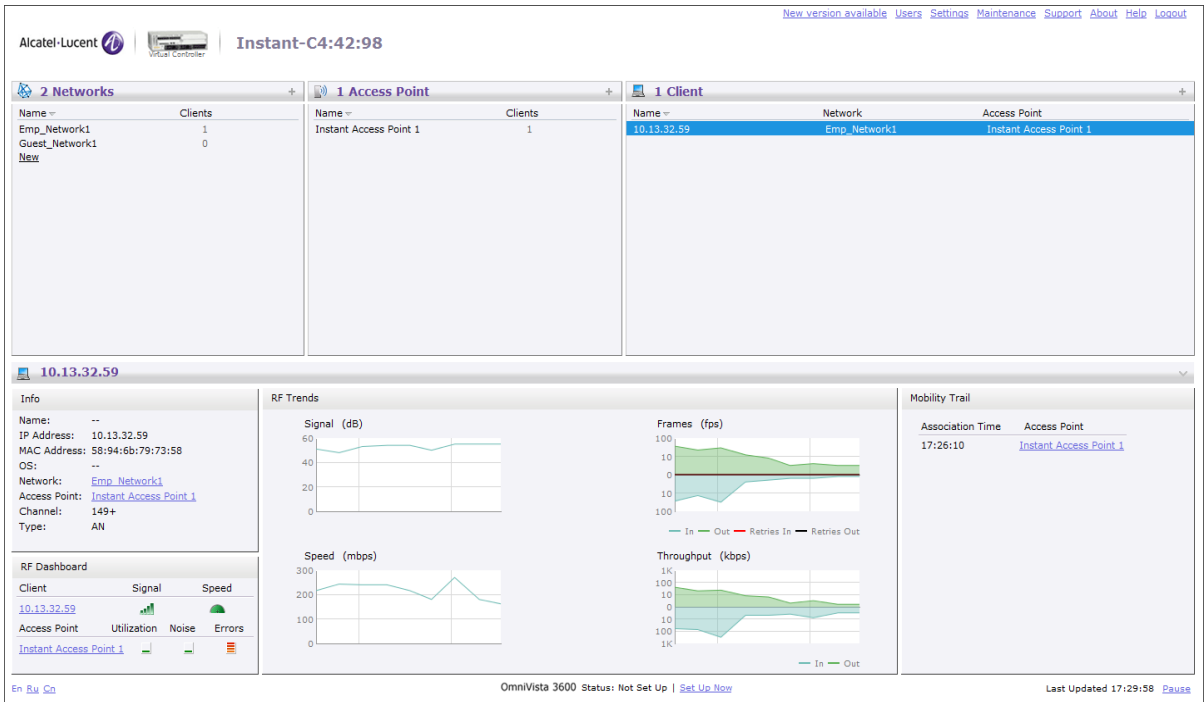
In the Virtual Controller view, all clients in the Alcatel-Lucent Instant network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor. Client view for that client appears.

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 99 Client View**



## Info

The **Info** section provides the following information about the selected OAW-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** - OAW-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

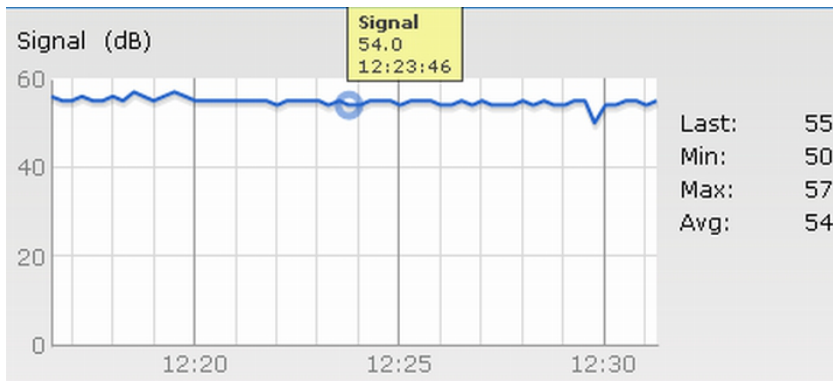
In the Client view, the **RF Dashboard** section is moved below the **Info** section. The **RF Dashboard** section in the client view shows the speed and the signal information for the client and the RF information for the OAW-IAP to which the client is connected to.

## RF Trends

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

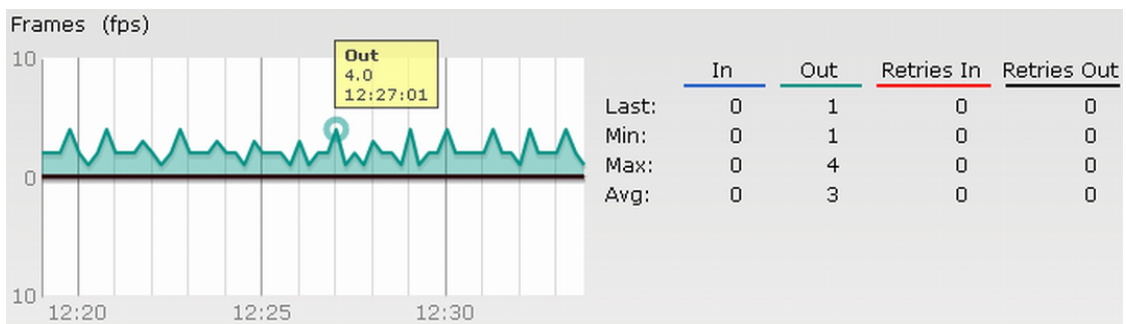
- Signal

**Figure 100** *Signal Graph*



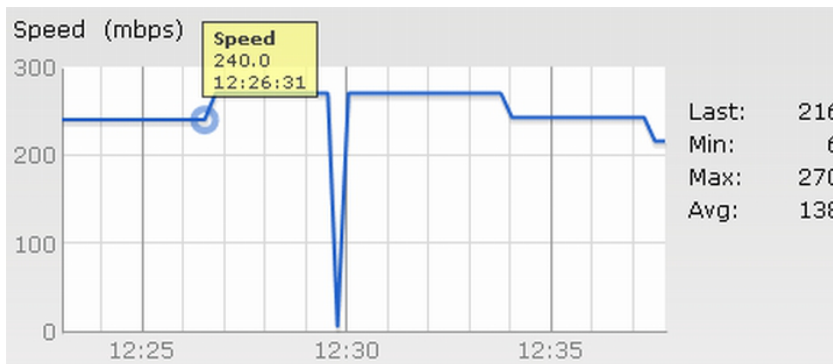
- Frames

**Figure 101** *Frames Graph*



- Speed

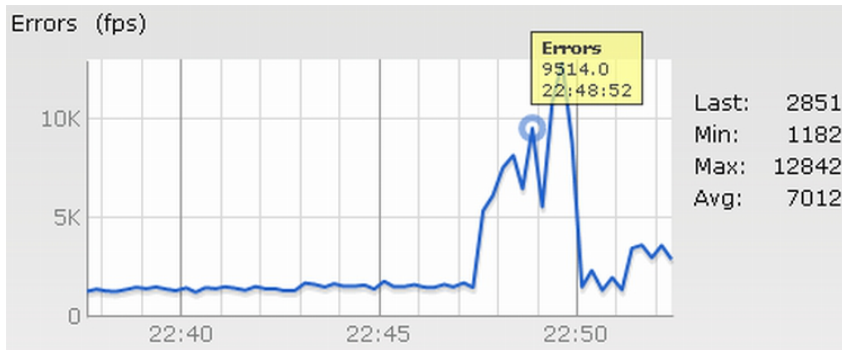
**Figure 102** *Speed Graph*



- Throughput



**Figure 103** Throughput Graph



For more information about RF trends graphs in the client view and for monitoring procedures, see [Table 18](#).

**Table 18** Client View - RF Trends Graphs and Monitoring Procedures

Graph Name	Description	Monitoring Procedure
Signal	<p>The Signal graph shows the signal strength of the client for the last 15 minutes. It is measured in decibels.</p> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view provides Last, Minimum, Maximum, and Average signal statistics for the client for the last 15 minutes.</li> </ul> <p>To see the exact signal strength at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the signal strength of the selected client for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the Clients tab, click the IP address of the client for which you want to monitor the signal strength. The client view appears.</li> <li>Study the Signal graph in the RF Trends pane. For example, the graph on the left shows that signal strength for the client is 54.0 dB at 12:23 hours.</li> </ol>
Frames	<p>The Frames Graph shows the In and Out frame rate per second for the client for the last 15 minutes. It also shows data for the Retry In and Retry Out frames.</p> <ul style="list-style-type: none"> <li>Outgoing frames - Outgoing frame traffic is displayed in green. It is shown above the median line.</li> <li>Incoming frames - Incoming frame traffic is displayed in blue. It is shown below the median line.</li> <li>Retry Out - Retries for the outgoing frames is displayed in black and is shown above the median line.</li> <li>Retry In - Retries for the incoming frames is displayed in red and is shown below the median line.</li> </ul> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In, Out, Retries In, and Retries Out frames.</li> </ul> <p>To see the exact frames at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the In and Out frame rate per second and retry frames for the In and Out traffic, for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the Clients tab, click the IP address of the client for which you want to monitor the frames. The client view appears.</li> <li>Study the Frames graph in the RF Trends pane. For example, the graph on the left shows 4.0 frames per second for the client at 12:27 hours.</li> </ol>

**Table 18** *Client View - RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Speed	<p>The Speed graph shows the data transfer speed for the client. Data transfer is measured in Mega bits per second (mbps).</p> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view shows Last, Minimum, Maximum, and Average statistics for the client for the last 15 minutes.</li> </ul> <p>To see the exact speed at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the speed for the client for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the Clients tab, click the IP address of the client for which you want to monitor the speed. The client view appears.</li> <li>Study the Speed graph in the RF Trends pane. For example, the graph on the left shows that the data transfer speed at 12:26 hours is 240 mbps.</li> </ol>
Throughput	<p>The Throughput Graph shows the throughput for the selected client for the last 15 minutes.</p> <ul style="list-style-type: none"> <li>Outgoing traffic - Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line.</li> <li>Incoming traffic - Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line.</li> </ul> <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> <li>The enlarged view shows Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the client for the last 15 minutes.</li> </ul> <p>To see the exact throughput at a particular time, hover the cursor over the graph line.</p>	<p>To monitor the errors for the client for the last 15 minutes,</p> <ol style="list-style-type: none"> <li>Log in to the Instant UI. The Virtual Controller view appears. This is the default view.</li> <li>In the Clients tab, click the IP address of the client for which you want to monitor the throughput. The client view appears.</li> <li>Study the Throughput graph in the RF Trends pane. For example, the graph on the left shows 1.0 kbps outgoing traffic throughput for the client at 12:30 hours.</li> </ol>

## Mobility Trail

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

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




---

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

---

## Alert Types

Alerts are generated when a user encounters problems while accessing or connecting to the Wi-Fi network. These alerts enable you to troubleshoot the problems. The alerts that are generated on Alcatel-Lucent 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 19 displays a list of alerts that are generated on the Alcatel-Lucent Instant network.

**Table 19** Alerts List

Type Code	Description	Details	Corrective Actions
100101	Internal error	The OAW IAP has encountered an internal error for this client.	Contact the Alcatel-Lucent customer support team.
100102	Unknown SSID in association request	The OAW 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 OAW IAP cannot allow this client to associate because its authentication or encryption settings do not match OAW IAP's configuration.	Ascertain the correct authentication or encryption settings and try to associate again.
100104	Unsupported 802.11 rate	The OAW 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 OAW IAP to see if the desired rate can be supported; if not, consider replacing the OAW IAP with another model that can support the rate.
100105	Maximum capacity reached on OAW IAP	The OAW IAP has reached maximum capacity and cannot accommodate any more clients.	Consider expanding capacity by installing additional OAW IAPs or balance load by relocating OAW IAPs.
100206	Invalid MAC Address	The OAW 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 OAW 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 19 Alerts List**

Type Code	Description	Details	Corrective Actions
100308	RADIUS server connection failure	The OAW IAP cannot authenticate this client using 802.1X because the RADIUS server did not respond to the authentication request.	<p>If the OAW IAP is using the internal RADIUS server, recommend checking the related configuration as well as the installed certificate and passphrase.</p> <p>If the OAW IAP is using an external RADIUS server, check if there are any issues with the RADIUS server and try connecting again.</p>
100309	RADIUS server authentication failure	The OAW 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 OAW 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 OAW 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.

In Alcatel-Lucent 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 Alcatel-Lucent Instant system.

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

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

## Adding a User

To add a user, perform the following steps:

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

**Figure 104** Adding a User

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

## Editing User Settings

To edit user settings, perform the following steps:

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

## Deleting a User

To delete a user, perform the following steps:

1. At the top right corner of the Instant UI, click the **Users** link. The **Users** box appears.
2. In the **Users** section, select the username that you want to delete and click **Delete**.  
To delete all users or multiple users at a time, select the usernames that you want to delete, and click **Delete All**.



---

Deleting a user only removes the user record from the user database, and won't disconnect the online user under this username.

---

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

The initial Wi-Fi setup requires you to specify the country code for the country in which the Alcatel-Lucent Instant will operate. This configuration sets the regulatory domain for the radio frequencies that the OAW-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 OAW-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 20](#) shows the list of country codes.

**Figure 105** *Specifying a Country Code*



## Country Codes List

**Table 20** *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 20** *Country Codes List*

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 20** *Country Codes List*

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 20** *Country Codes List*

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



## Abbreviations

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

**Table 21** *List of abbreviations*

Abbreviation	Expansion
ABR	Adaptive Radio Management
ARP	Address Resolution Protocol
BSS	Basic Server Set
BSSID	Basic Server Set Identifier
CA	Certification Authority
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
IAP	Instant Access Point
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
Instant UI	Instant User Interface
LEAP	Lightweight Extensible Authentication Protocol
MX	Mail Exchanger
MAC	Media Access Control
NAS	Network Access Server
NAT	Network Address Translation
NS	Name Server

**Table 21** *List of abbreviations*

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