

AOS-W Instant

6.1.3.1-3.0.0.0



User Guide

Copyright

© 2012 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

26801 West Agoura Road
Calabasas, CA 91301

About this Guide	15
Alcatel-Lucent Instant Overview.....	15
Supported Devices.....	15
Objective.....	15
Intended Audience.....	15
Conventions.....	16
Contacting Support	16
Chapter 1 Initial Configuration	19
Initial Setup.....	19
Pre-Installation Checklist	19
Connecting the OAW-IAP to a Power Source	20
Assigning an IP Address to the OAW-IAP.....	20
Connecting to a Provisioning Wi-Fi Network	20
Login into Instant User Interface	21
Specifying the Country Code	22
OAW-IAP Cluster	23
Chapter 2 Instant User Interface	25
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
Settings.....	28
RF	31
PEF	31
WIP	32
VPN.....	33
Maintenance	33
Support.....	35
Help	38
Logout.....	38
Monitoring.....	38
Alerts.....	41
IDS	43
Configuration	44
Language.....	45
OmniVista Setup.....	45
Pause/Resume	46
Views.....	46
Chapter 3 Wireless Network	47

	Network Types.....	47
	Employee Network.....	47
	Adding an Employee Network.....	48
	Voice Network.....	56
	Adding a Voice Network.....	56
	Guest Network.....	63
	Adding a Guest Network.....	63
	Editing a Network.....	70
	Deleting a Network.....	70
Chapter 4	Mesh Network.....	71
	Mesh Instant Access Points.....	71
	Mesh Portals.....	71
	Mesh Points.....	72
	Instant Mesh Setup.....	72
Chapter 5	Managing OAW-IAPs.....	75
	Preferred Band.....	75
	Auto Join Mode.....	75
	Disabling Auto Join Mode.....	75
	LED Display.....	76
	Terminal Access.....	77
	TFTP Dump Server.....	77
	Syslog Server.....	78
	Syslog Facility Levels.....	79
	Adding an OAW-IAP to the Network.....	79
	Removing an OAW-IAP from the Network.....	80
	Editing OAW-IAP Settings.....	80
	Changing OAW-IAP Name.....	80
	Changing IP Address of the OAW-IAP.....	81
	Configuring Adaptive Radio Management.....	82
	Migrating from a Virtual Controller Managed Network to OmniAccess WLAN Switch Managed Network.....	83
	Converting an OAW-IAP to RAP Mode.....	83
	Converting an OAW-IAP to CAP.....	86
	Converting an OAW-IAP to Standalone Mode.....	87
	Converting back to an OAW-IAP.....	87
	Rebooting the OAW-IAP.....	88
	Firmware Image Server in Cloud Network.....	89
	Upgrade using OmniVista and Image Server.....	89
	Image management using Cloud Server.....	89
	Image management using OmniVista.....	89
	Automatic Firmware Image Check and Upgrade.....	89
	Upgrading to New Version.....	91
	Manual.....	91
	Automatic.....	91
Chapter 6	NTP Server.....	93
	Configuring an NTP Server.....	93
Chapter 7	Virtual Controller.....	95
	Master Election Protocol.....	95
	Virtual Controller IP Address.....	95
	Specifying Name and IP Address for the Virtual Controller.....	95

	Configuring the DHCP Server	96
Chapter 8	Authentication	99
	Authentication Methods in Alcatel-Lucent Instant	99
	802.1X Authentication	99
	Internal RADIUS Server	99
	External RADIUS Server	100
	Authentication Terminated on OAW-IAP	100
	Configuring an External RADIUS Server	101
	Enabling Instant RADIUS	103
	RADIUS Server Authentication with VSA	103
	List of supported VSA	103
	Management Authentication Settings	106
	Captive Portal	107
	Internal Captive Portal	107
	Configuring Internal Captive Portal Authentication when Adding a Guest Network	107
	Configuring Internal Captive Portal Authentication when Editing a Guest Network	108
	Configuring Internal Captive Portal with External Radius Server Authentication when Adding a Guest Network	109
	Customizing a Splash Page	110
	Disabling Captive Portal Authentication	111
	External Captive Portal	112
	Configuring External Captive Portal Authentication when Adding a Guest Network	112
	Configuring External Captive Portal Authentication when Editing a Guest Network	113
	External Captive Portal Authentication using Amigopod	114
	Creating a Web Login page in the Amigopod	114
	Configuring the RADIUS Server in Instant	115
	MAC Authentication	115
	Configuring MAC Authentication	115
	Walled Garden Access	117
	Creating a Walled Garden Access	117
	Certificates	118
	Loading Certificates using Instant WebUI	118
	Loading Certificates using OmniVista	119
Chapter 9	Encryption	123
	Encryption Types Supported in Alcatel-Lucent Instant	123
	WEP	123
	TKIP	123
	AES	123
	Encryption Recommendations	123
	Understanding WPA and WPA2	123
	Recommended Authentication and Encryption Combinations	124
Chapter 10	Role Derivation	125
	User Roles	125
	Creating a New User Role	125
	Creating Role Assignment Rules	126
Chapter 11	User VLAN Derivation	129
	User VLAN Derivation	129

	Vendor Specific Attributes (VSA).....	129
	VLAN Derivation Rule.....	130
	Configuring VLAN Derivation Rules on an OAW-IAP.....	130
	User Role.....	131
	Configuring a User Role	131
	SSID Profile.....	132
	Configuring VLAN Derivation Rules Using SSID Profile	133
Chapter 12	Instant Firewall.....	135
	Service Options	136
	Destination Options	137
	Examples for Access Rules	138
	Allow TCP Service to a Particular Network.....	138
	Allow PoP3 Service to a Particular Server	139
	Deny FTP Service except to a Particular Server	140
	Deny bootp Service except to a Particular Network.....	141
Chapter 13	Content Filtering	143
	Enabling Content Filtering	143
	Enterprise Domains	144
Chapter 14	OS Fingerprinting.....	147
Chapter 15	Adaptive Radio Management	149
	ARM Features.....	149
	Channel or Power Assignment.....	149
	Voice Aware Scanning	149
	Load Aware Scanning	149
	Band Steering Mode	149
	Airtime Fairness Mode	150
	Airtime Fairness Modes	150
	Access Point Control	150
	Customize Valid Channels.....	150
	Min Transmit Power.....	151
	Max Transmit Power.....	151
	Client Aware	151
	Scanning.....	151
	Wide Channel Bands	151
	Monitoring the Network with ARM	151
	ARM Metrics	151
	Configuring Administrator Assigned Radio Settings for OAW-IAP	152
	Configuring Radio Profiles in Instant	153
Chapter 16	Intrusion Detection System	155
	Rogue AP Detection and Classification.....	155
	Wireless Intrusion Protection (WIP).....	155
	Containment Methods	158
Chapter 17	SNMP	161
	SNMP Parameters for OAW-IAP	161
	SNMP Traps.....	163
Chapter 18	Ethernet Downlink	165
	Ethernet Downlink Overview.....	165
	Ethernet Downlink Profile Parameters	165

	Assigning a Profile to the Ethernet Port	166
Chapter 19	Uplink Configuration.....	169
	Uplink Configuration Overview	169
	Ethernet	169
	3G Uplink	169
	Types of Modems	169
	Uplink Switchover	172
	Uplink Preemption.....	173
	Uplink Preference.....	173
Chapter 20	OmniVista Integration and Management.....	175
	OmniVista Features	175
	Image Management	175
	OAW-IAP and Client Monitoring	175
	Template-based Configuration	175
	Trending Reports	176
	Intrusion Detection System	176
	Wireless Intrusion Detection System (WIDS) Event Reporting to OmniVista....	176
	RF Visualization Support for Alcatel-Lucent Instant	176
	Configuring OmniVista.....	177
	Creating your Organization String.....	177
	About Shared Key	177
	Entering the Organization String and AMP Information into the OAW-IAP	178
	OmniVista Discovery through DHCP Option.....	178
	Standard DHCP option 60 and 43 on Windows Server 2008 for Alcatel-	178
	Lucent Instant APs	178
	Alternate method for defining Vendor Specific DHCP options	181
Chapter 21	Monitoring	185
	Virtual Controller View	185
	Monitoring Link	185
	Info	186
	RF Dashboard	186
	Usage Trends.....	186
	Client Alerts Link	187
	IDS Link.....	187
	Network View.....	188
	Info	188
	Usage Trends.....	188
	Instant Access Point View	190
	Info	190
	RF Dashboard	191
	RF Trends.....	191
	Usage Trends.....	193
	Client View	194
	Info	195
	RF Dashboard	195
	RF Trends.....	195
	Mobility Trail.....	199
Chapter 22	Alert Types and Management.....	201
	Alert Types.....	201

Chapter 23	Policy Enforcement Firewall	203
	Authentication Servers	203
	Users for Internal Server	203
	Roles	204
	Client Blacklisting	205
	Types of Client Blacklisting	205
	Manual Blacklisting	206
	Adding a Client to the Manual Blacklist	206
	Dynamic Blacklisting	206
	Authentication Failure Blacklisting	206
	Session Firewall Based Blacklisting	206
	PEF Settings	207
	Firewall ALG Configuration	207
	Firewall-based Logging	208
Chapter 24	VPN Configuration	209
	VPN Configuration	209
	Routing Profile Configuration	210
	DHCP Server Configuration	210
	NAT DHCP Configuration	211
	Distributed L2 DHCP Configuration	212
	Distributed L3 DHCP Configuration	213
	Centralized L2 DHCP Configuration	214
Chapter 25	User Database	217
	Adding a User	217
	Editing User Settings	218
	Deleting a User	218
Chapter 26	Regulatory Domain	219
	Country Codes List	220
Appendix A	Switch Configuration for VPN	225
	Whitelist DB Configuration if the Switch is acting as the Whitelist Entry	225
	VPN Local Pool Configuration	226
	OAW-IAP VPN Profile Configuration	226
Appendix B	Abbreviations	229
	Abbreviations	229

Figure 1	Connecting to a provisioning Wi-Fi Network — Microsoft Windows	21
Figure 2	Connecting to a provisioning Wi-Fi Network — Mac OS	21
Figure 3	Instant User Interface Login Screen	22
Figure 4	Specifying the Country Code	22
Figure 5	Instant UI Interface	25
Figure 6	Networks Tab— Compressed View and Expanded View	26
Figure 7	Access Points Tab— Compressed View and Expanded View	27
Figure 8	Client Tab— Compressed View and Expanded View	28
Figure 9	Settings Link	29
Figure 10	RTLS	30
Figure 11	OpenDNS.....	30
Figure 12	RF	31
Figure 13	PEF	32
Figure 14	WIP	33
Figure 15	VPN.....	33
Figure 16	Maintenance Link — Default View	34
Figure 17	Support Window.....	35
Figure 18	Support commands.....	38
Figure 19	Help Link.....	38
Figure 20	Monitoring on Instant UI	39
Figure 21	Info Section in the Monitoring Pane	39
Figure 22	RF Dashboard in the Monitoring Pane	39
Figure 23	Usage Trends Section in the Monitoring Pane	41
Figure 24	Alerts Link	42
Figure 25	Client Alerts	42
Figure 26	Fault History	43
Figure 27	Active Faults	43
Figure 28	Intrusion Detection on Instant UI	44
Figure 29	Configuration	45
Figure 30	OmniVista Setup Link – OmniVista Configuration	46
Figure 31	Adding an Employee Network — Basic Info Tab	48
Figure 32	Adding an Employee Network— VLAN Tab	49
Figure 33	Employee Security Tab— Enterprise.....	50
Figure 34	Employee Security Tab— Personal	53
Figure 35	Employee Security Tab — Open	55
Figure 36	Adding an Employee Network— Access Rules Tab.....	56
Figure 37	Adding a Voice Network— Basic Info Tab	57
Figure 38	Voice Security Tab— Enterprise.....	59
Figure 39	Adding a Voice Network— Access Rules Tab.....	63
Figure 40	Adding a Guest Network— Basic Info Tab	64
Figure 41	Adding a Guest Network — Splash Page Settings	68
Figure 42	Configuring a Splash Page — Encryption Settings	69
Figure 43	Adding a Guest Network — Access Rules Tab.....	70
Figure 44	Open Instant SSID.....	72

Figure 45	Untrusted Connection Window	73
Figure 46	Login Window	73
Figure 47	Mesh Portal	74
Figure 48	Disabling Auto Join Mode	76
Figure 49	LED Display	76
Figure 50	Terminal Access	77
Figure 51	TFTP Dump Server	78
Figure 52	Syslog Server.....	78
Figure 53	Adding an OAW-IAP to the Instant Network	80
Figure 54	Entering the MAC Address for the New OAW-IAP	80
Figure 55	Editing OAW-IAP Settings	81
Figure 56	Changing OAW-IAP Name	81
Figure 57	Configuring OAW-IAP Settings — Connectivity Tab	81
Figure 58	Configuring OAW-IAP Connectivity Settings — Specifying Static Settings	82
Figure 59	Configuring OAW-IAP Radio Settings Mode — Access.....	83
Figure 60	Maintenance — Convert Tab.....	85
Figure 61	Convert options	85
Figure 62	Confirm Access Point Conversion	86
Figure 63	Converting an OAW-IAP to CAP	86
Figure 64	Standalone AP Conversion.....	87
Figure 65	Rebooting the OAW-IAP	88
Figure 66	Confirm Reboot message.....	88
Figure 67	Reboot In Progress.....	88
Figure 68	Reboot Successful	89
Figure 69	Automatic Image Check — New Version Available Link	90
Figure 70	New Version Available	90
Figure 71	Upgrading single class or multi-class AP Networks.....	91
Figure 72	Configuring NTP Server	93
Figure 73	Specifying Virtual Controller Name and IP Address	96
Figure 74	Configuring the DHCP Server.....	97
Figure 75	Configuring an External RADIUS Server	102
Figure 76	Enabling Instant RADIUS	103
Figure 77	Management Authentication Settings	106
Figure 78	Configuring Captive Portal when Adding A Guest Network	108
Figure 79	Configuring Captive Portal when Editing a Guest Network.....	109
Figure 80	Configuring Internal Captive Portal with External Radius Server Authentication ... 110	
Figure 81	Customizing a Splash Page.....	111
Figure 82	Disabling Captive Portal Authentication	111
Figure 83	Configuring External Captive Portal when Adding a Guest Network	112
Figure 84	Configuring External Captive Portal Authentication when Editing a Guest Network 114	
Figure 85	Configuring MAC Authentication	116
Figure 86	Walled Garden	117
Figure 87	Loading Certificates	118
Figure 88	New Certificate	119
Figure 89	Loading Certificate via OmniVista	120
Figure 90	CA Certificate	120
Figure 91	Server Certificate	120
Figure 92	Selecting the Group.....	121

Figure 93	Virtual Controller Certificate.....	121
Figure 94	Access Tab - Instant User Role Settings.....	125
Figure 95	Creating a New User Role	126
Figure 96	Creating Role Assignment Rules	127
Figure 97	Radius Access—Accept packets with VSA.....	129
Figure 98	Configure VSA on a Radius Server.....	130
Figure 99	Configuring Radius Attributes on the Radius Server.....	130
Figure 100	Configuring VLAN Derivation Rules on an OAW-IAP	131
Figure 101	Configuring VLAN Derivation using the User Role	132
Figure 102	To Use a Defined User VLAN Role	132
Figure 103	Configuring VLAN Derivation Rules Using SSID Profile	133
Figure 104	Access Tab - Instant Firewall Settings	135
Figure 105	Defining Rule — Allow TCP Service to a Particular Network	139
Figure 106	Defining Rule — Allow POP3 Service to a Particular Server	140
Figure 107	Defining Rule — Deny FTP Service Except to a Particular Server	141
Figure 108	Defining Rule — Deny bootp Service Except to a Network	142
Figure 109	Enabling Content Filtering	144
Figure 110	Enterprise Domains	144
Figure 111	OS Fingerprinting	147
Figure 112	Airtime fairness mode.....	150
Figure 113	Configuring Administrator Assigned Radio Settings for OAW-IAP	152
Figure 114	Radio Profile	153
Figure 115	Intrusion Detection	155
Figure 116	Wireless Intrusion Protection— Detection.....	156
Figure 117	Wireless Intrusion Protection— Protection.....	158
Figure 118	Containment Methods.....	159
Figure 119	Creating Community Strings for SNMPV1 and SNMPV2.....	162
Figure 120	Creating Users for SNMPV3.....	163
Figure 121	SNMP Traps	163
Figure 122	Ethernet Profile Configuration	166
Figure 123	Assigning a Profile to the Ethernet Port.....	167
Figure 124	Uplink Status	169
Figure 125	Provisioning 3G Uplink— Manually	172
Figure 126	Provisioning 3G Uplink— Automatically.....	172
Figure 127	Uplink Preference	173
Figure 128	Template-based Configuration.....	176
Figure 129	Adding an OAW-IAP in VisualRF	177
Figure 130	Configuring OmniVista	178
Figure 131	Instant and DHCP options for OmniVista— Set Predefined Options.....	179
Figure 132	Instant and DHCP options for OmniVista— Predefined Options and Values....	179
Figure 133	Instant and DHCP options for OmniVista— Server Options	180
Figure 134	Instant and DHCP options for OmniVista— 060 Alcatel-Lucent Instant AP in Server Options180	
Figure 135	Instant and DHCP options for OmniVista— 043 Vendor Specific Info	181
Figure 136	Instant and DHCP options for OmniVista— Scope Options	181
Figure 137	Vendor Specific DHCP options	182
Figure 138	OmniVista — New Group	183
Figure 139	OmniVista — Monitor	183
Figure 140	Virtual Controller View	185
Figure 141	Clients Graph.....	186

Figure 142	Throughput Graph	187
Figure 143	Network View	188
Figure 144	Clients Graph	189
Figure 145	Throughput Graph	189
Figure 146	Instant Access Point View	190
Figure 147	2.4 GHz Frames Graph	191
Figure 148	Client View	195
Figure 149	Signal Graph	195
Figure 150	Frames Graph	196
Figure 151	Speed Graph	196
Figure 152	Throughput Graph	196
Figure 153	Authentication Server	203
Figure 154	Users for Internal Server	204
Figure 155	Roles	205
Figure 156	Client Blacklisting	205
Figure 157	Manual Blacklisting	206
Figure 158	Dynamic Blacklisting	207
Figure 159	Enabling ALG Protocols	207
Figure 160	Corporate Access— Controller	209
Figure 161	Corporate Access— Routing	210
Figure 162	Corporate Access— DHCP Server	211
Figure 163	NAT DHCP Configuration	212
Figure 164	Distributed L2 DHCP Configuration	213
Figure 165	Distributed L3 DHCP Configuration	214
Figure 166	Centralized L2 DHCP Configuration	215
Figure 167	Adding a User	217
Figure 168	Specifying a Country Code	219

Table 1	Conventions.....	16
Table 2	Contacting Support	16
Table 3	RF Dashboard icons	39
Table 4	IEEE 802.11 Standards.....	47
Table 5	Conditions for Client IP and VLAN assignment.....	49
Table 6	Conditions for Adding an Employee Network— Security Tab	51
Table 7	Conditions for Adding an Employee Network— Security Tab	54
Table 8	Conditions for Client IP and VLAN Assignment	58
Table 9	Conditions for Adding a Voice Network— Security Tab	60
Table 10	Conditions for Client IP and VLAN assignment.....	65
Table 11	Conditions for Adding a Guest Network— Security Tab.....	66
Table 12	Logging Levels	79
Table 13	Supported OAW-IAP Platforms and Minimal AOS Version for OAW-IAP to CAP Conversion ⁸⁴	
Table 14	Supported OAW-IAP platforms and minimal AOS version for OAW-IAP to RAP Conversion ⁸⁴	
Table 15	WPA and WPA2 Features.....	124
Table 16	Recommended Authentication and Encryption Combinations	124
Table 17	Network Service Options.....	136
Table 18	Destination Options	137
Table 19	Radio Profile Configuration Parameters	153
Table 20	Infrastructure Detection Policies	156
Table 21	Client Detection Policies.....	157
Table 22	Infrastructure Protection Policies	158
Table 23	Client Protection Policies.....	158
Table 24	SNMP Parameters for OAW-IAP	161
Table 25	Ethernet Downlink Profile Parameters.....	165
Table 26	List of Supported 3G Modems	170
Table 27	Virtual Controller View — Graphs and Monitoring Procedures	187
Table 28	Network View — Graphs and Monitoring Procedures	189
Table 29	Instant Access Point View — RF Trends Graphs and Monitoring Procedures .	192
Table 30	Instant Access Point View — Usage Trends and Monitoring Procedures	194
Table 31	Client View — RF Trends Graphs and Monitoring Procedures	197
Table 32	Alerts List.....	201
Table 33	Country Codes List.....	220
Table 34	List of abbreviations	229

Alcatel-Lucent Instant Overview

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

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

Alcatel-Lucent Instant consists of an Instant Access Point (OAW-IAP) and a Virtual Controller (VC). The Virtual Controller resides within one of the access points. In an 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 the required information from the Virtual Controller.

Supported Devices

The following is a list of Instant devices supported by Alcatel-Lucent:

- OAW-IAP-92
- OAW-IAP-93
- OAW-IAP-104
- OAW-IAP-105
- OAW-IAP-134
- OAW-IAP-135
- OAW-IAP-175P/175AC
- OAW-RAP3WN/3WN-US/3WNP/3WNP-US



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

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.

Conventions

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

Table 1 *Conventions*

Type Style	Description
<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">• Screen output• On screen system prompt• Filenames, software devices, and specific commands
Bold	This style is used to emphasize Instant UI elements. For example, name of a text box or the name of a drop-down list.

The following informational icons are used throughout this guide:



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

Table 2 *Contacting Support*

Contact Center Online	
• Main Site	http://www.alcatel-lucent.com/enterprise
• Support Site	https://service.esd.alcatel-lucent.com
• Email	esd.support@alcatel-lucent.com
Service & Support Contact Center Telephone	
• North America	1-800-995-2696
• Latin America	1-877-919-9526

Contact Center Online	
● Europe	+33 (0) 38 855 6929
● Asia Pacific	+65 6240 8484
● Worldwide	1-818-878-4507

This chapter provides information that is required to setup Alcatel-Lucent 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 (OAW-IAP), make sure that you have the following:

- Ethernet cable of required length to connect the OAW-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 power 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 the following two ways:



Endspan— The switch that the OAW-IAP is connected to can provide power.

Midspan— A device can sit between the switch and the OAW-IAP.

The choice of endspan or midspan depends on the capabilities of the switch that the OAW-IAP is 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 an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server because it provides the required IP address for a network peripheral or element.



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

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

1. [“Connecting the OAW-IAP to a Power Source” on page 20](#)

2. “Assigning an IP Address to the OAW-IAP” on page 20
3. “Connecting to a Provisioning Wi-Fi Network” on page 20
4. “Login into Instant User Interface” on page 21
5. “Specifying the Country Code” on page 22 — 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, the OAW-IAP tries to connect to the DHCP server if the static IP configuration is not available. If DHCP times out, a default IP within 169.254.x.y/16 subnet is configured on the OAW-IAP. The DHCP client still continues to run so that when the DHCP service recovers, the OAW-IAP gets a valid IP address and reboots.



In addition, you can manually assign a static IP without the support of DHCP after it comes up with the 169.254.x.y/16 subnet.

Connecting to a Provisioning Wi-Fi Network

To connect to a provisioning Wi-Fi network:

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



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

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



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

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

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

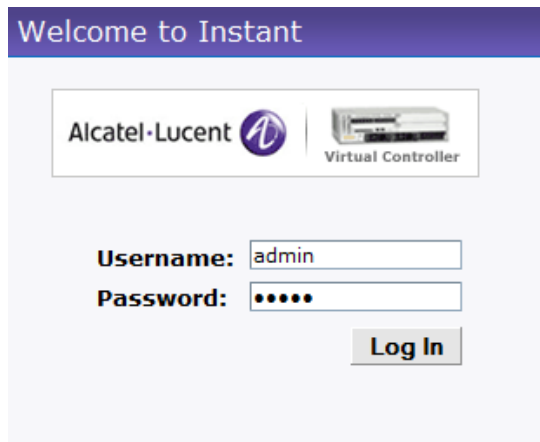


Login into Instant User Interface

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

- Username— admin
- Password— admin

Figure 3 Instant User Interface Login Screen



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

Specifying the Country Code



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

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

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

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

For the complete list of the countries that are supported in the OAW-IAP-ROW variant type, see [“Regulatory Domain”](#) on page 219.

Figure 4 Specifying the Country Code



OAW-IAP Cluster

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



Moving an OAW-IAP from one cluster to another requires a factory reset of the OAW-IAP that is being moved. See Chapter 5, “Managing OAW-IAPs” on page 75 for more information.

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

Supported browsers are:

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



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

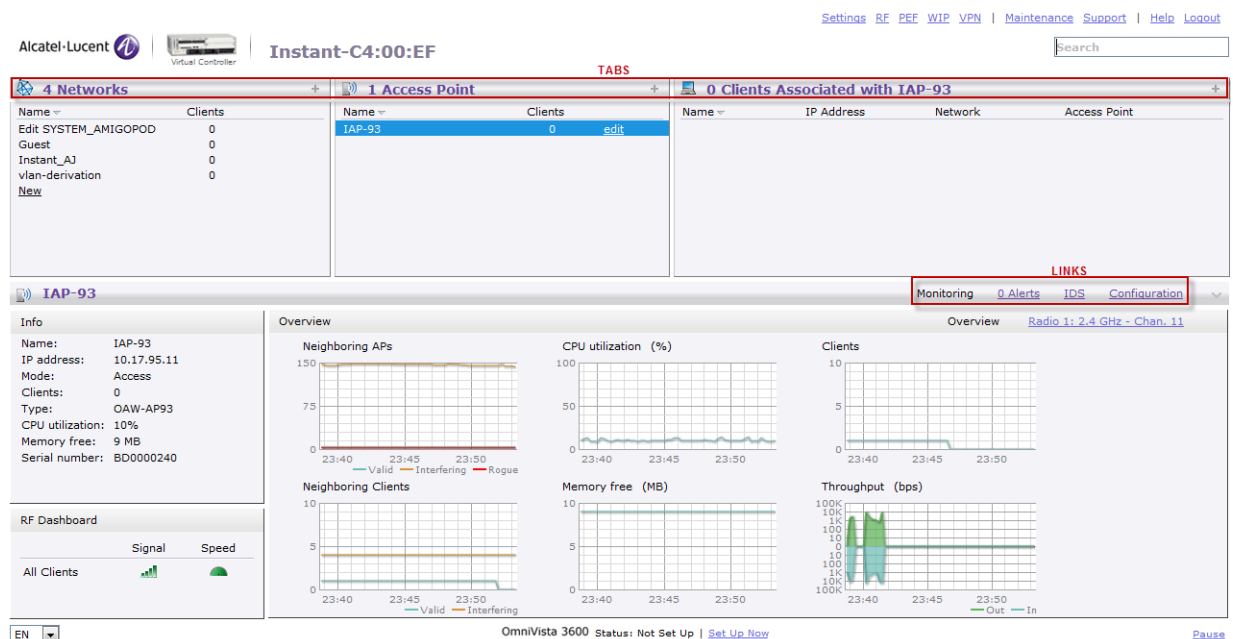
Understanding the Instant UI Layout

The Instant UI consists of the following elements:

- Banner
- Search
- Tabs
- Links
- Views

These elements are explained in the following sections.

Figure 5 *Instant UI Interface*



Banner

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

Search

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

Tabs

The Instant UI consists of the following tabs:

- **Networks**— Provides information about the Wi-Fi networks in the 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 again to compress the expanded view. Items in each tab are associated with a triangle icon. Click on the triangle icon to sort the data in increasing or decreasing order. Each tab is explained in the following sections.

Networks Tab

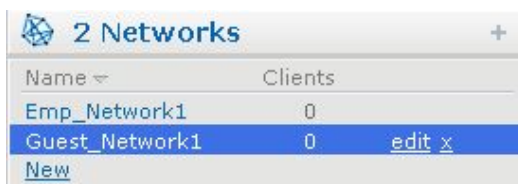
This tab displays a list of Wi-Fi networks that are configured in the Alcatel-Lucent Instant network. The network names appear as links. The expanded view displays the following information about each Wi-Fi network:

- **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 3, “Wireless Network” on page 47](#).

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 70](#). To delete a network, click on the link **x** located next to the **edit** link.

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



Name	Clients
Emp_Network1	0
Guest_Network1	0
New	

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

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, a **New** link appears. Click on this link to add a new OAW-IAP to the network. 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 the 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 80.

Figure 7 Access Points Tab— Compressed View and Expanded View

1 Access Point		
Name ▾	Clients	
Instant Access Point	0	edit

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)
Instant Access Point	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**— Indicates Signal strength.
- **Speed (mbps)**— Data transfer speed.

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

1 Client Associated with Instant Access Point			
Name	IP Address	Network	Access Point
--	10.13.32.59	Emp_Network1	Instant Access Point

1 Client										
Name	IP Address	MAC Address	OS	Network	Access Point	Channel	Type	Role	Signal	Speed (mbps)
--	10.13.32.59	58:94:6b:79:73:58	--	Emp_Network1	Instant Access Point	157+	AN	Emp_Network1	55	8

Links

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

- [New Version Available](#)
- [Settings](#)
- [RF](#)
- [PEF](#)
- [WIP](#)
- [VPN](#)
- [Maintenance](#)
- [Support](#)
- [Help](#)
- [Logout](#)
- [Monitoring](#)
- [Alerts](#)
- [IDS](#)
- [Configuration](#)
- [Language](#)
- [OmniVista Setup](#)
- [Pause/Resume](#)

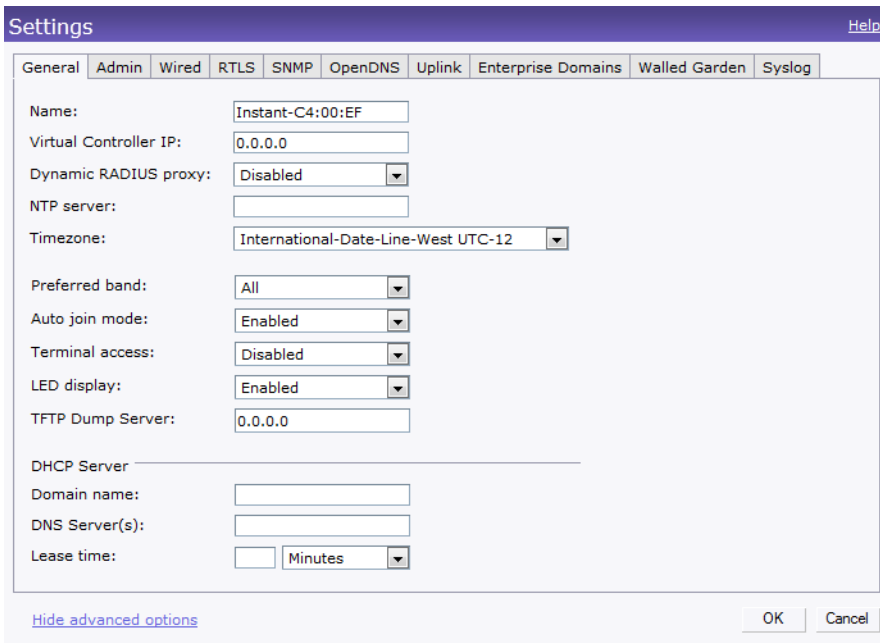
New Version Available

This link appears in the top right corner of Instant UI only if a new image version is available on the image server and OmniVista is not configured. For more information about the **New version available** link and its functions, see “Firmware Image Server in Cloud Network” on page 89.

Settings

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

Figure 9 *Settings Link*



The screenshot shows a 'Settings' window with a purple header and a 'Help' link. Below the header are tabs for 'General', 'Admin', 'Wired', 'RTLS', 'SNMP', 'OpenDNS', 'Uplink', 'Enterprise Domains', 'Walled Garden', and 'Syslog'. The 'General' tab is active, displaying the following settings:

- Name: Instant-C4:00:EF
- Virtual Controller IP: 0.0.0.0
- Dynamic RADIUS proxy: Disabled
- NTP server: (empty)
- Timezone: International-Date-Line-West UTC-12
- Preferred band: All
- Auto join mode: Enabled
- Terminal access: Disabled
- LED display: Enabled
- TFTP Dump Server: 0.0.0.0
- DHCP Server section:
 - Domain name: (empty)
 - DNS Server(s): (empty)
 - Lease time: (empty) Minutes

At the bottom left, there is a link 'Hide advanced options'. At the bottom right, there are 'OK' and 'Cancel' buttons.



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

- **General**— View or edit the Name, IP address, NTP Server, and DHCP server settings of the Virtual Controller. For information about Virtual Controller settings and NTP Server, see [Chapter 7, “Virtual Controller”](#) and [Chapter 6, “NTP Server”](#). For information about Auto join mode, Terminal Access, and LED display see [Chapter 5, “Managing OAW-IAPs”](#).
- **Admin**— View or edit the admin credentials for access to the Virtual Controller Management User Interface. See [“Management Authentication Settings” on page 106](#) for more information. You can also configure OmniVista in this tab. See [“Configuring OmniVista” on page 177](#) for more information.
- **Wired**— Specify the desired profile for each port of the OAW-IAP. See [Chapter 18, “Ethernet Downlink”](#) for more information.
- **RTLS**— View or edit the RTLS server settings.
 - **Alcatel-Lucent RTLS**— Enable this to integrate with OmniVista Management platform, Ekahau Real Time Location Server and Nearbuy Real Time Location Server. Specify the IP address and port number of the server to which location reports are sent, a shared secret key, and the frequency at which packets are sent to the server.
 - Update— This indicates how frequently the Virtual Controller updates the RTLS server.
 - **Aeroscout**— Enables the AP to send RFID tag information to an AeroScout real-time asset location (RTLS) server. Specify the IP address and port number of the AeroScout server to which location reports should be sent.

Figure 10 *RTLS*

The screenshot shows the 'Settings' window with the 'RTLS' tab selected. The 'Aruba RTLS' section is checked, and the 'Aeroscout' section is also checked. The 'IP address' for both is set to '0.0.0.0'. The 'Update' interval is set to 'Every 30 seconds'. The 'Port' fields are empty. The 'Passphrase' and 'Retype' fields are also empty. The window has a 'Hide advanced options' link and 'OK' and 'Cancel' buttons at the bottom.

- **SNMP**— View or specify SNMP agent settings. See [Chapter 17, “SNMP”](#) for more information.
- **OpenDNS**— Instant supports OpenDNS business solutions which requires an OpenDNS (<http://www.opendns.com>) account comprising a username and a password. These credentials will be used by Instant to access OpenDNS to provide enterprise-level content filtering.

Figure 11 *OpenDNS*

The screenshot shows the 'Settings' window with the 'OpenDNS' tab selected. The 'Credentials for Connecting to OpenDNS' section is visible, with 'Username' and 'Password' input fields. The window has a 'Hide advanced options' link and 'OK' and 'Cancel' buttons at the bottom.



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

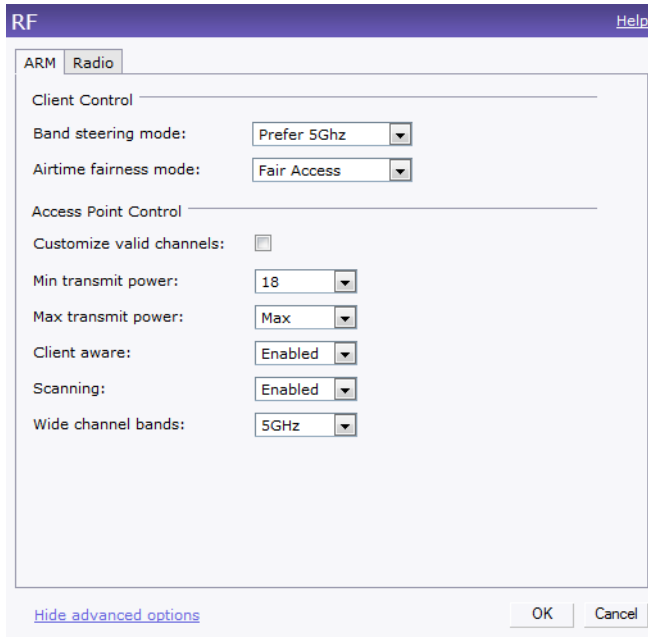
- **Uplink**— View or configure uplink settings. See [Chapter 19, “Uplink Configuration”](#) for more information.

- **Enterprise Domains**— This tab indicates all the DNS domain names valid on the enterprise network which is used to determine how client DNS requests should be routed. When **Content Filtering** is enabled for the wireless network, the names that do not match this list are sent to OpenDNS server.
- **Walled Garden**— The Walled Garden directs the user’s navigation within particular areas to allow access to a selection of websites and/or prevent access to other websites. For more information, see “Walled Garden Access” on page 117.
- **Syslog**— View or specify a Syslog Server for sending syslog messages to the external servers. See “Syslog Server” on page 78 for more information.

RF

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

Figure 12 *RF*



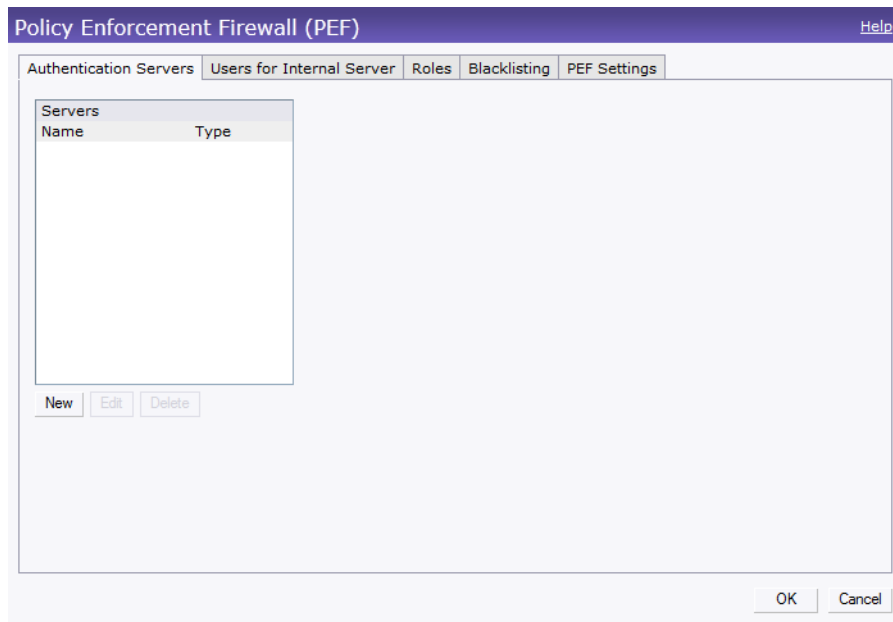
ARM — View or assign channel and power settings for all the OAW-IAPs in the network. For information about ARM (Adaptive Radio Management), see “ARM Features” on page 149.

Radio — View or configure radio settings for 2.4GHz and the 5GHz radio profiles. For information about Radio, see “Configuring Radio Profiles in Instant” on page 153.

PEF

This link displays the following features.

Figure 13 PEF



Authentication Servers— Use this window to configure an external RADIUS server for a wireless network. See [“Configuring an External RADIUS Server”](#) on page 101 for more information.

Users for Internal Server— Use this window to populate the system’s internal authentication server with users. This list will be used by networks for which per-user authorization is specified using the Virtual Controller’s internal authentication server. For more information about users, see [Chapter 25, “User Database”](#).

Roles— This window displays all the roles defined for all the Networks and the **Access Rules** lists the permissions for each role. For more information, see [“User Roles”](#) on page 125.

Blacklisting— Use this window to manually blacklist clients. See [“Client Blacklisting”](#) on page 205 for more information.

PEF Settings— Use this window to enable/disable gateway filters supporting address and port translation for various protocols. See [Chapter 23, “Policy Enforcement Firewall”](#) on page 203 for more information.

WIP

WIP offers a wide selection of intrusion detection and protection features to protect the network against wireless threats. Use this window to specify standard levels of threat detection. See [“Wireless Intrusion Protection \(WIP\)”](#) on page 155 for more information.

Figure 14 WIP

Wireless Intrusion Protection (WIP) Help

1 Detection 2 Protection

Specify What Threats to Detect

Infrastructure:

- High
- Medium
- Low
- Off

Custom settings

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

Clients:

- High
- Medium
- Low
- Off

Custom settings

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

Next Cancel

VPN

Use this window to define how to communicate with the remote switch. See [Chapter 24, “VPN Configuration”](#) on page 209 for more information.

Figure 15 VPN

Corporate Access Help

1 Controller 2 Routing 3 DHCP Server

Controller

Protocol:

Primary host:

Backup host:

Preemption:

NOTE: Secure VPN/GRE access requires Aruba Mobility controller and a special ArubaOS build.
Contact your Aruba SE for details.

Next Cancel

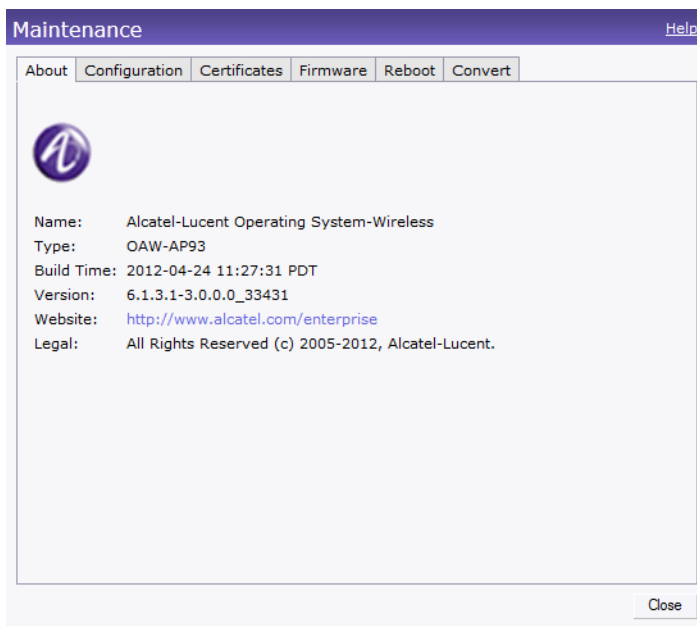
Maintenance

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

- **About**— Displays the Build Time, OAW-IAP model name, Alcatel-Lucent OS version, Web address of Alcatel-Lucent, and Copyright information.
- **Configuration**— Displays the current configuration of the network.
 - **Clear Configuration**— Click to delete or clear the current configuration of the network and reset to provisioning configuration.

- **Backup Configuration**— Use this feature to create local Instant configuration backup. Click **Backup Configuration** to save the configuration file named **instant.cfg**.
- **Restore Configuration**— Click **Restore Configuration** to browse and locate the backup file to restore. Reboot the OAW-IAP for the changes to take effect.
- **Certificates** — Displays information about the current certificate installed in the network. Provides an interface to upload new certificates and to set a passphrase for the certificates. For more information, see “Certificates” on page 118.
- **Firmware** — Displays the current firmware version and provides options to upgrade to a new firmware version. For more information, see “Upgrading to New Version” on page 91.
- **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 88.
- **Convert** — Provides an option to change the network from a Virtual Controller managed network to an Alcatel-Lucent OmniAccess WLAN Switch managed network. For more information, see “Migrating from a Virtual Controller Managed Network to OmniAccess WLAN Switch Managed Network” on page 83.

Figure 16 *Maintenance Link — Default View*

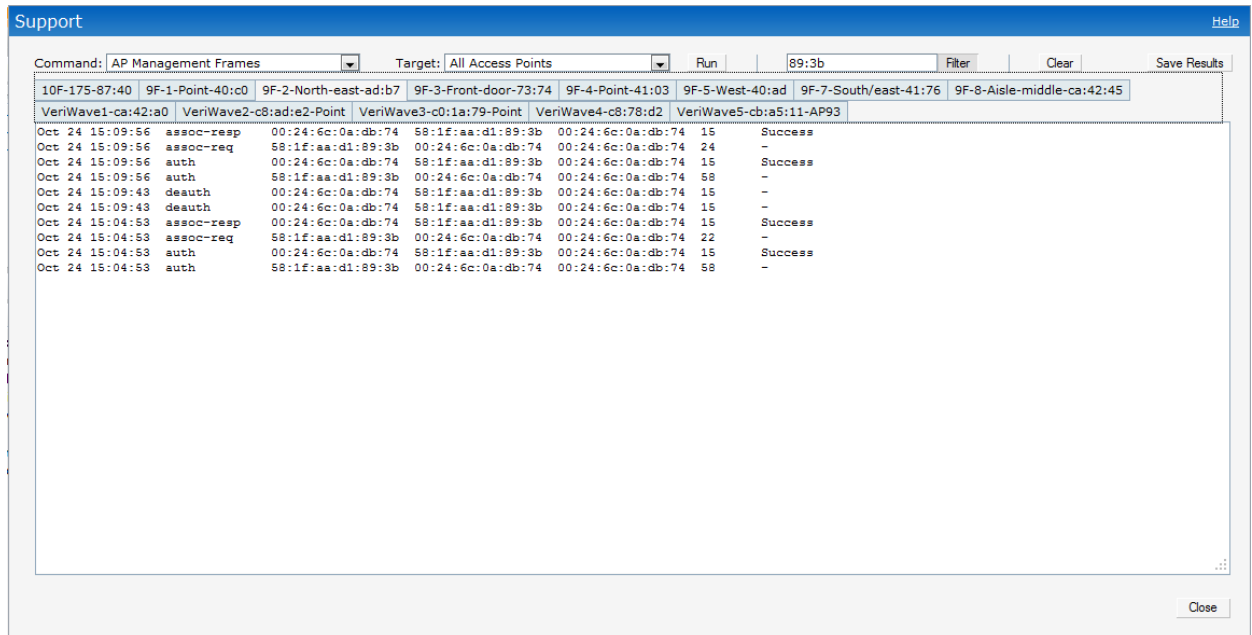


Support

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

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

Figure 17 Support Window



To view the log information, perform the following steps:

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



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 window:

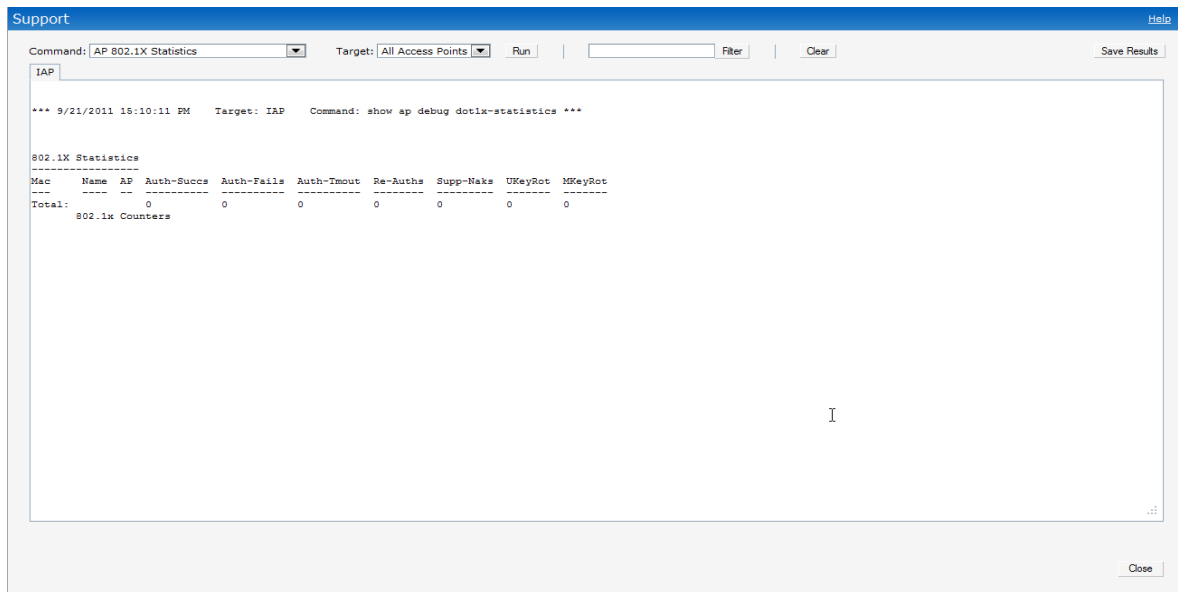
- **AP Access Rule Table**— Displays all the ACL rules of the selected OAW-IAP.
- **AP Active**— Displays all the APs of Instant.
- **AP All Supported Timezones**— Displays all the supported time zones of Instant.
- **AP ARM Channels**— Displays channels of ARM in the selected OAW-IAP.
- **AP ARM Configuration**—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

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

- **VC Application Services**— Displays the details of application services of the selected OAW-IAP, which includes protocol number, port number.
- **VC Global Alerts**— Displays all the alerts about client of the selected OAW-IAP.
- **VC Global Statistics**— Displays the flow information and signal strength of the selected **OAW-IAP**.
- **VC Local User Database**— Displays the user configuration of the selected **OAW-IAP**.
- **VC Radius Attributes**— Displays the radius attributes of the selected **OAW-IAP**.
- **VC Radius Servers**— Displays the radius servers' configuration of the selected **OAW-IAP**.
- **VC Saved Configuration**— Displays the saved configuration information of the selected **OAW-IAP**.
- **VC SNMP Configuration**— Displays the SNMP configuration of the selected **OAW-IAP**.
- **AP 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.
- **AP Management Frames**— Displays the traced 802.11 management frames of the selected OAW-IAP.
- **AP Authentication Frames**— Displays the authentication trace buffer information of the selected OAW-IAP.
- **AP System Status**— Displays detailed system status information for the selected OAW-IAP.
- **AP Crash Info**— Displays crash log information (if it exists) for the selected OAW-IAP. The stored information is cleared from the flash after the AP reboots.
- **AP 802.1X Statistics**— Displays the 802.1X statistics of the selected OAW-IAP.
- **AP RADIUS Statistics**— Displays the RADIUS statistics of the selected OAW-IAP.
- **AP System Status**— Displays the system status of the selected OAW-IAP.
- **AP Client Table**— Displays information of the client connected to the selected OAW-IAP.
- **AP Association Table**— Displays information of the selected OAW-IAP association.
- **AP Allowed Channels**— Displays information of the allowed channels for the selected OAW-IAP.
- **AP Radio 0 Stats**— Displays aggregate debug statistics of the selected OAW-IAP Radio 0.
- **AP 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 AP 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 channel history 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.
- **OpenDNS Configuration and Status**— Displays configuration and status about open dns server.

Figure 18 Support commands

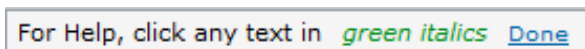


Help

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

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

Figure 19 Help Link




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

Logout

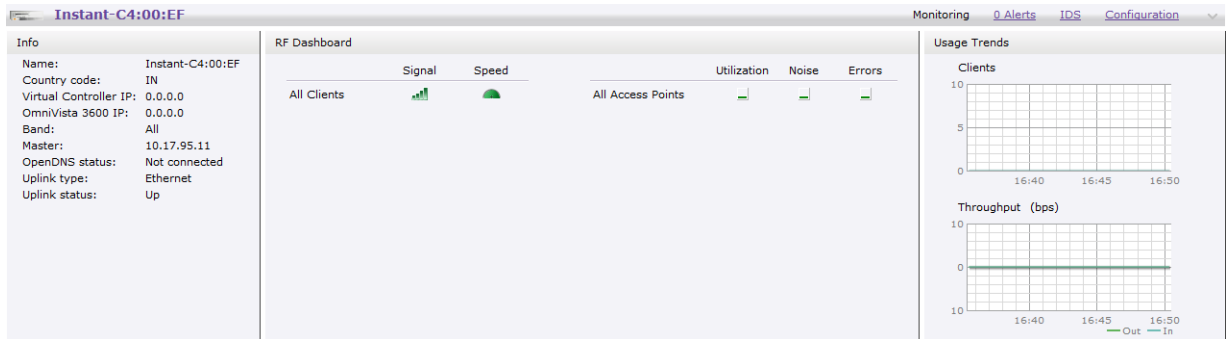
Use this link to logout of the Instant UI.

Monitoring

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

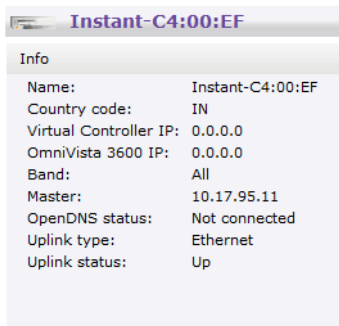
Figure 20 Monitoring on Instant UI



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.

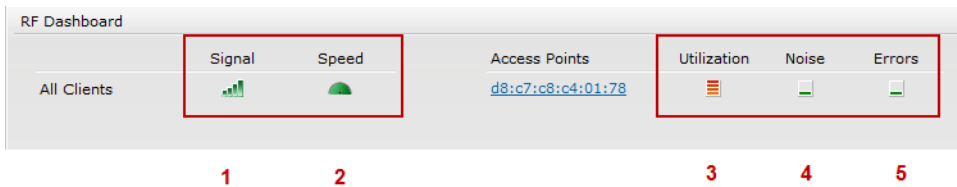
Figure 21 Info Section in the Monitoring Pane



RF Dashboard

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

Figure 22 RF Dashboard in the Monitoring Pane



The following table lists the icons in the RF Dashboard.

Table 3 RF Dashboard icons

Icon	Name
1	Signal bar
2	Speed icon

Table 3 RF Dashboard icons

Icon	Name
3	Utilization icon
4	Noise icon
5	Errors icon

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

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

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

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

- Access Points— Lists the 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 21, “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 80dBm-87dBm.
 - Red— Noise floor is less than 80dBm.

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.

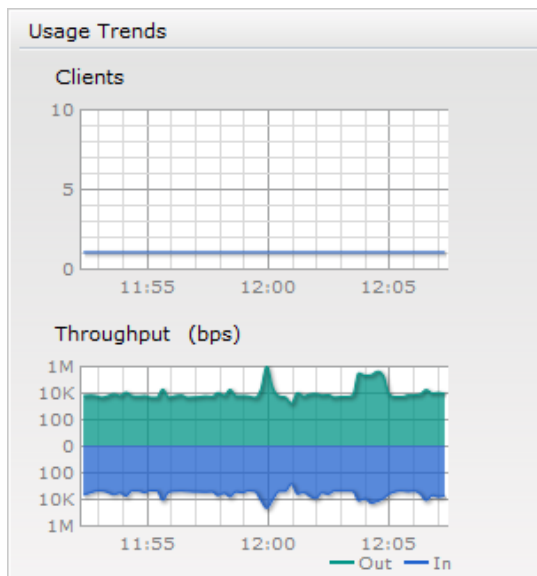
To view the errors graph of an OAW-IAP, click on the Errors icon against the OAW-IAP in the Errors column.

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 in 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 in the last 15 minutes.
- Throughput— In the default Virtual Controller view, the Throughput graph displays the incoming and outgoing throughput traffic for the Virtual Controller in the last 15 minutes. In the Network or OAW-IAP view, this graph displays the incoming and outgoing throughput traffic for the selected network or OAW-IAP in the last 15 minutes.

Figure 23 Usage Trends Section in the Monitoring Pane



For more information about the graphs and monitoring procedures, see [Chapter 21, “Monitoring”](#) .

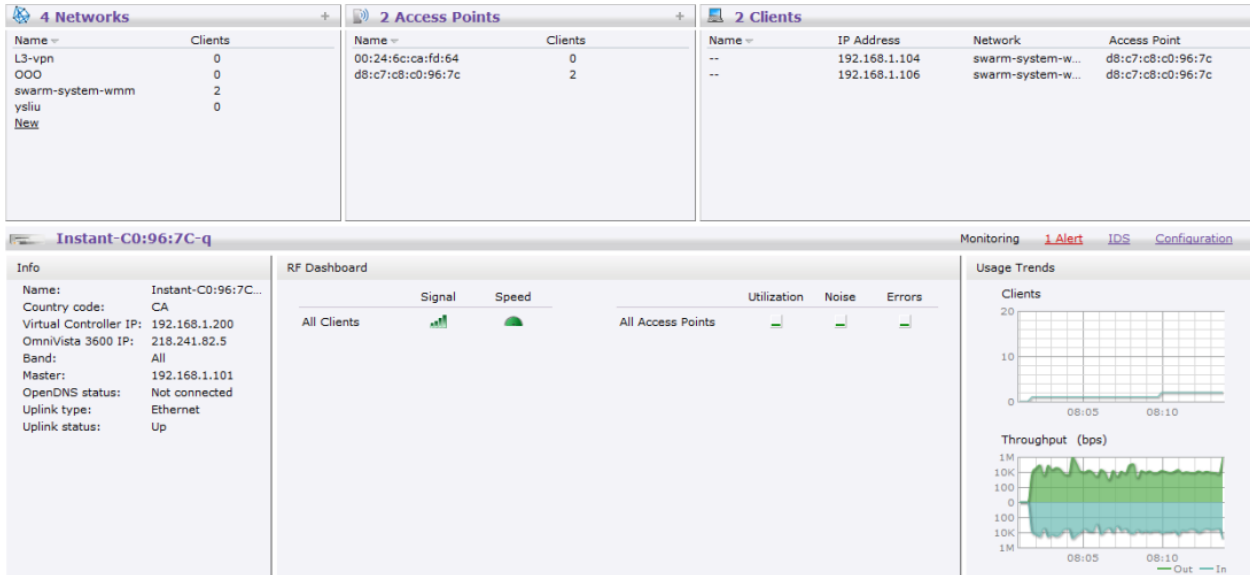
Alerts

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



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

Figure 24 Alerts Link

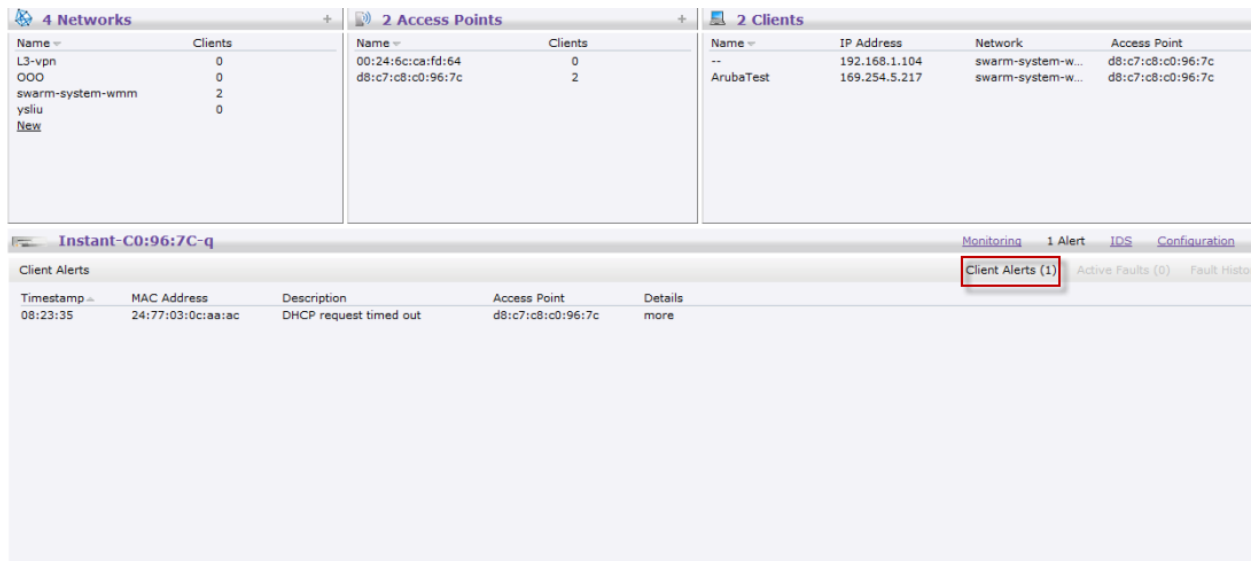


Client Alerts

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

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

Figure 25 Client Alerts



Fault History

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

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

- Description— Displays the event details.

Figure 26 *Fault History*

Active Faults

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

- Time— Displays the system time when an event occurs.
- Number— Indicates the number of sequence.
- Description— Displays the event details.

Figure 27 *Active Faults*

For more information about alerts, see [Chapter 22, “Alert Types and Management”](#).

IDS

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

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

- Classification— Displays the classification of the foreign AP: Interfering OAW-IAP or Rogue OAW-IAP.
- Channel— Displays the channel in which the foreign AP is operating.
- Type— Displays the Wi-Fi type of the foreign AP.
- Last seen— Displays the time when the foreign AP was last detected in the network.
- Where— Provides information about the OAW-IAP that detected the foreign AP. Click the pushpin icon to view the information.
- Foreign Clients Detected— Lists the clients that are not controlled by the Virtual Controller. The following information is displayed for each foreign client:
 - Mac address— Displays the Mac address of the foreign client.
 - Network— Displays the name of the network to which the foreign client is connected.
 - Classification— Displays the classification of the foreign client: Interfering client.
 - Channel— Displays the channel in which the foreign client is operating.
 - Type— Displays the Wi-Fi type of the foreign client.
 - Last seen— Displays the time when the foreign client was last detected in the network.
 - Where— Provides information about the 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 16, “Intrusion Detection System” .

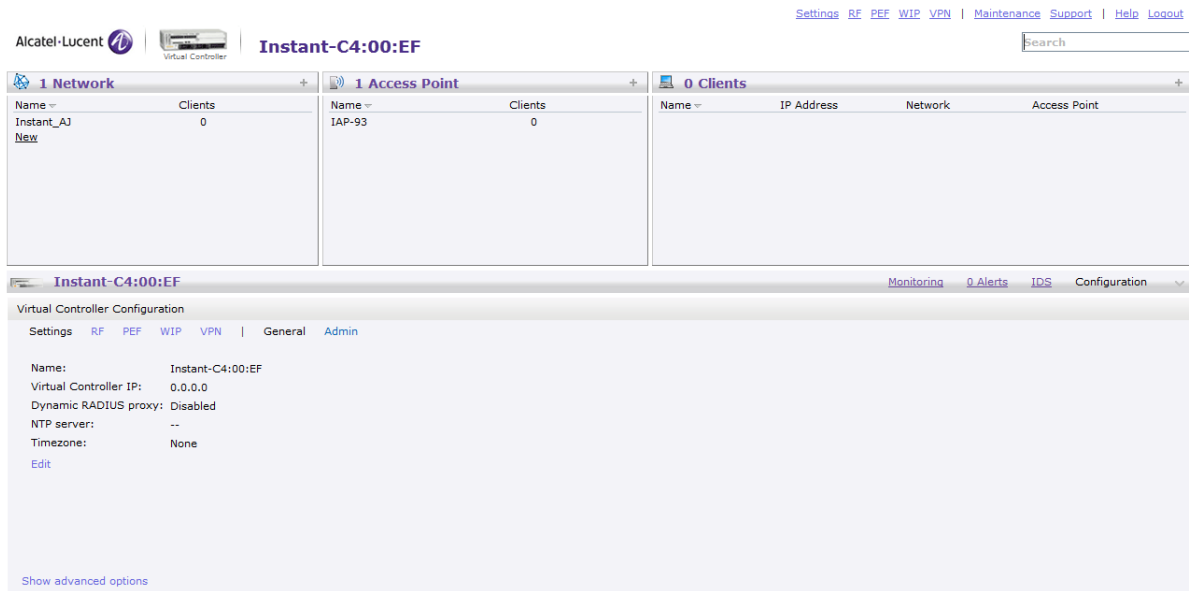
Figure 28 *Intrusion Detection on Instant UI*

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:bd:5f:70	lab_open	Interfering	161	AN 40MZ	11:52:40		00:22:41:0c:a9:fc	ethersphere-voip	Interfering	1	B	11:52:40	
00:24:6c:80:74:00	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40		00:27:10:5c:78:24	ethersphere-voip	Interfering	48	AN 40MZ	11:52:40	
00:0b:86:50:47:48	vjan-test	Interfering	64	A	11:52:40		00:1e:65:79:8c:c6	IBM	Interfering	1	B	11:52:40	
00:0b:86:21:8a:40	aruba-ap	Interfering	1	G	11:52:40		00:26:c6:b7:af:1c	IBM	Interfering	6	B	11:52:40	
00:0b:86:43:d3:a0	UIlab	Interfering	11	G	11:52:40		60:33:4b:15:85:f1	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40	
00:24:6c:07:2b:59	cp-radius	Interfering	149	AN 40MZ	11:52:40		58:94:6b:cc:be:84	IBM	Interfering	6	B	11:52:40	
00:1a:1e:17:da:c0	aruba-ap	Rogue	11	GN 20MZ	11:52:40		00:1e:65:71:49:2c	shobha-bridge-65	Interfering	1	GN 20MZ	11:52:40	
00:24:6c:80:74:01	ARUBA-VISITOR	Interfering	1	GN 20MZ	11:52:40		08:11:96:76:1d:1c	IBM	Interfering	6	B	11:52:40	
00:24:6c:84:25:e1	msbrcm	Interfering	1	GN 20MZ	11:52:40		00:26:b0:48:46:20	ARUBA-VISITOR	Interfering	1	B	11:52:40	
00:24:6c:07:2b:5a	cp-radius1	Interfering	149	AN 40MZ	11:52:40		a0:88:b4:84:b8:04	IBM	Interfering	1	B	11:52:40	
00:24:6c:80:74:02	indiamdns	Interfering	1	GN 20MZ	11:52:40		58:94:6b:b3:b7:5c	IBM	Interfering	6	B	11:52:40	
00:0b:86:70:4b:60	aruba-ap	Interfering	1	GN 20MZ	11:52:40		00:27:10:8e:4c:60	IBM	Interfering	6	B	11:52:40	
00:24:6c:80:8f:28	ethersphere-wpa2	Interfering	48	AN 40MZ	11:52:40		78:d6:f0:ca:f8:07	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40	
00:24:6c:84:21:08	rjji-aaa	Interfering	36	AN 40MZ	11:52:40		30:7c:30:5eb:cc:e2	ethersphere-voip	Interfering	1	B	11:52:40	
00:24:6c:80:4b:f0	ethersphere-voip	Interfering	6	GN 20MZ	11:52:40		58:94:6b:31:cc:48	ethersphere-wpa2	Interfering	48	AN 40MZ	11:52:40	
00:24:6c:80:4f:88	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40		a0:88:b4:b9:5e:f4	IBM	Interfering	1	G	11:52:40	
00:1a:1e:17:da:c2	Armol CP	Interfering	157	AN 40MZ	11:52:40		08:11:96:76:5b:b8	IBM	Interfering	6	B	11:52:40	
00:1a:1e:17:da:c2	WPA2	Interfering	11	GN 20MZ	11:52:40		00:26:c6:4a:aa:e8	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40	
00:24:6c:80:8c:60	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40		00:27:10:45:4a:34	IBM	Interfering	1	B	11:52:40	
00:0b:86:70:4b:61	Sandlin wlan zone	Interfering	1	GN 20MZ	11:52:40		18:3d:a7:77:ac:3c	IBM	Interfering	6	B	11:52:40	

Configuration

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

Figure 29 Configuration



Language

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

OmniVista Setup

OmniVista is a solution for managing rapidly changing wireless networks. When enabled, OmniVista allows you to manage the Instant network. For more information on OmniVista, see [Chapter 20, “OmniVista Integration and Management”](#). The OmniVista status is displayed on the right side of the language links in the Instant UI. If the OmniVista status is **Not Set Up**, click the **Set Up Now** link to set up the OmniVista. The Settings window appears with **Admin** tab selected. For information to configure OmniVista, see [“Configuring OmniVista” on page 177](#).

Figure 30 *OmniVista Setup Link – OmniVista Configuration*

The screenshot shows the 'Settings' window for OmniVista. The 'Local' section is expanded, showing 'Authentication' set to 'Internal', 'Username' as 'admin', and 'Password' and 'Retype' fields with masked characters. Below this, the 'OmniVista 3600' section is highlighted with a red box, containing 'Organization' set to 'Aruba', and empty fields for 'OmniVista 3600 IP', 'Shared key', and 'Retype'. At the bottom, there are 'OK' and 'Cancel' buttons and a link for 'Hide advanced options'.

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 Client view, all the 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 21, “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 4](#).

Table 4 IEEE 802.11 Standards

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

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



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

Employee Network

An Employee network is a classic Wi-Fi network. This network type is supported with full customization on 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** window appears.

Figure 31 Adding an Employee Network — Basic Info Tab

The screenshot shows the 'New Network' configuration window with the 'Basic Info' tab selected. The window has a purple header with 'New Network' and a 'Help' link. Below the header are four tabs: '1 Basic Info' (highlighted), '2 VLAN', '3 Security', and '4 Access'. The 'Basic Information' section contains the following fields and options:

- Name (SSID):** A text input field.
- Primary usage:** Radio buttons for 'Employee' (selected), 'Voice', and 'Guest'.
- Content filtering:** A dropdown menu set to 'Disabled'.
- Hide SSID:** A checkbox that is unchecked.
- Band:** A dropdown menu set to 'All'.
- Inactivity timeout:** A text input field with '1000' and 'secs'.
- Bandwidth Limits:** Three checked checkboxes: 'Percentage of Airtime' (with a percentage input field), 'Each user' (with a kbps input field), and 'Each radio' (with a kbps input field).
- Broadcast/Multicast:** A section with three dropdown menus: 'Multicast optimization' (set to 'Disabled'), 'Broadcast filtering' (set to 'Disabled'), and 'DTIM interval' (set to '1 beacon').
- Transmit Rates:** Two rows of dropdown menus: '2.4GHz' (Min: 1, Max: 54) and '5GHz' (Min: 6, Max: 54).

At the bottom, there is a link 'Hide advanced options' and two buttons: 'Next' and 'Cancel'.

2. In the **Basic Info** tab, perform the following steps:
 - a. **Name (SSID)**— Enter a name that uniquely identifies a wireless network.
 - b. **Primary usage**— Select **Employee** (this is selected by default) from the **Primary usage** options. This selection determines whether the network is primarily intended to be used for employee data, guest data, or voice traffic.
 - c. **Content filtering**— When enabled, all DNS requests to non-corporate domains on this wireless network are sent to OpenDNS.
 - d. **Hide SSID**— Select this check box if you do not want the SSID (network name) to be visible to users.
 - e. **Band**— Set the band at which the network will transmit radio signals. Available options are 2.4 GHz, 5 GHz and All. The All option is selected by default. It is also the recommended option.
 - f. **Inactivity timeout**— Indicates the time in seconds after which an idle client ages out. The minimum value is 60 seconds and the default value is 1000 seconds.
3. Click the **Show advanced options** link and perform the following steps.
 - a. **Bandwidth Limits**— You can specify three types of bandwidth limits.
 - **Percentage of Airtime**— Indicates the aggregate amount of airtime that all clients on this Network can use to send/receive data.
 - **Each user**— Indicates the throughput for any single user on this Network. The throughput value is specified in kbps.
 - **Each radio**— Indicates the aggregate amount of throughput each radio (some AP models have multiple radios) is allowed to provide for all clients connected to that radio.

b. Broadcast/Multicast

- **Multicast optimization**— When **Enabled**, the OAW-IAP will choose the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. The default values are 1 mbps for 2.4GHz and 6 mbps for 5.0GHz bands. Multicast traffic can be sent at up to 24 mbps when this option is enabled. This option is disabled by default.
 - **Broadcast filtering**— When set to **All**, the OAW-IAP will drop all broadcast and multicast frames except for DHCP and ARP. When set to **ARP**, in addition to the above, the OAW-IAP will convert ARP requests to unicast and send frames directly to the associated client. When **Disabled**, all broadcast and multicast traffic is forwarded.
 - **DTIM interval**— Indicates the DTIM (delivery traffic indication message) period in beacons. You can configure this option for every WLAN SSID profile. The default value is 1, which means the client will check for buffered data on the OAW-IAP at every beacon. You may choose to configure a larger DTIM value for power saving.
- c. **Transmit Rates**— Indicates the ability to configure the basic and supported rates per SSID for Alcatel-Lucent Instant. Select to set the minimum and maximum legacy (non-802.11n) transmit rates for each band — 2.4GHz and 5GHz.

4. Click **Next** to continue.

Figure 32 Adding an Employee Network— VLAN Tab

The screenshot shows the 'New Network' configuration wizard with the 'VLAN' tab selected. The 'Client IP & VLAN Assignment' section contains the following options:

- Client IP assignment:
 - Virtual Controller assigned
 - Network assigned
- Client VLAN assignment:
 - Default
 - Static
 - Dynamic

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

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

Table 5 Conditions for Client IP and VLAN assignment

If	then
You select Virtual Controller assigned	The client gets the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the OAW-IAP for the wireless clients. The Virtual Controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi site wireless network. See Chapter 7, “Virtual Controller” on page 95 for configuring the DHCP server.

Table 5 Conditions for Client IP and VLAN assignment (Continued)

If	then
You select Network assigned	<p>By default, the client VLAN is assigned to the native VLAN on the wired network.</p> <ul style="list-style-type: none"> • Default— The client gets the IP address in the same subnet as the OAW-IAPs. • Static— Select to specify a VLAN for all clients on this network. • Dynamic— Select to create rules for per-user VLAN assignment. See “VLAN Derivation Rule” on page 130 for more information.

6. Click **Next** to continue.

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

Figure 33 Employee Security Tab— Enterprise

The screenshot shows the 'New Network' configuration interface with the 'Security' tab selected. On the left, a vertical slider labeled 'Security Level' ranges from 'More Secure' at the top to 'Less Secure' at the bottom, with 'Enterprise', 'Personal', and 'Open' marked. The slider is positioned at the 'Enterprise' level. To the right, several configuration fields are visible: 'Key management' is set to 'WPA-2 Enterprise', 'Termination' is 'Disabled', 'Authentication server 1' is 'InternalServer', 'Reauth interval' is '0 min', 'Blacklisting' is 'Enabled', and 'Max authentication failures' is '0'. Below these, there are two 'Internal server' options: 'No users' with a link to 'Users' and 'No certificate' with a link to 'Upload certificate'. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

Table 6 Conditions for Adding an Employee 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"> 1. Select the required key options from the Key management drop-down list. Available options are: <ul style="list-style-type: none"> • WPA-2 Enterprise • WPA Enterprise • Both (WPA-2 & WPA) • Dynamic WEP with 802.1x • Use Session Key for LEAP— Use the Session Key for LEAP instead of using Session Key from the RADIUS Server to derive pair wise unicast keys. This is required for old printers that use dynamic WEP via LEAP authentication. This is Disabled by default. <p>For more information on encryption and recommended encryption type, see Chapter 9, “Encryption” .</p> 2. Termination— Enable this option to terminate the EAP portion of 802.1x authentication on the OAW-IAP instead of the RADIUS server. For more information, see “External RADIUS Server” on page 100. 3. Authentication server 1 and 2— Select the required Authentication server option from the drop-down list. Available options are: <ul style="list-style-type: none"> • New— If you select this option, an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 8, “Authentication” . • InternalServer— If you select this option, users who are required to authenticate with the internal RADIUS server must be added. Click the Users link to add the users. For information on adding a user, see “Adding a User” on page 217. 4. Reauth interval— When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients. 5. Blacklisting— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures. 6. Max authentication failures— Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10. <p>NOTE: Navigate to PEF > Blacklisting in the WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.</p> <ol style="list-style-type: none"> 7. Click Upload Certificate and browse to upload a certificate file for the internal server. See “Certificates” on page 118 for more information.

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

If	then,
<p>You want to use the default security level, Personal</p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> 1. Select the required key options from the Key management drop-down list. Available options are: <ul style="list-style-type: none"> ● WPA-2 Personal ● WPA Personal ● Both (WPA-2 & WPA) ● Static WEP <p>If you have selected Static WEP, do the following:</p> <ul style="list-style-type: none"> ● Select appropriate WEP key size from the WEP key size drop-down list. Available options are 64-bit and 128-bit. ● Select appropriate Tx key from the Tx Key drop-down list. Available options are 1, 2, 3, and 4. ● Enter an appropriate WEP key and reconfirm. <p>For more information on encryption and recommended encryption type, see Chapter 9, “Encryption”.</p> 2. Select a passphrase format from the Passphrase format drop-down list. Available options are: <ul style="list-style-type: none"> ● 8-63 alphanumeric chars ● 64 hexadecimal chars 3. Enter a passphrase in the Passphrase text box and reconfirm. 4. Select the required option from the MAC authentication drop-down list. Available options are <ul style="list-style-type: none"> ● Enabled and Disabled <p>When Enabled, user must configure at least one RADIUS server for authentication server. See “MAC Authentication” on page 115 for further details.</p> 5. Authentication server 1— Select the required Authentication server option from the drop-down list. Available options are: <ul style="list-style-type: none"> ● New— If you select this option, an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 8, “Authentication”. ● InternalServer— If you select this option, users who are required to authenticate with the internal RADIUS server must be added. Click the Users link to add the users. For information on adding a user, see “Adding a User” on page 217. 6. Reauth interval— When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients. 7. Blacklisting— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures. 8. Max authentication failures— Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10. <p>NOTE: Navigate to PEF > Blacklisting in the WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.</p>

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

If	then,
	<p>9. For Internal users— Click Users to populate the system’s internal authentication server with users. For information about adding a user, see “Adding a User” on page 217.</p> <p>10. Click Upload Certificate and browse to upload a certificate file for the internal server. See “Certificates” on page 118 for more information.</p>

Figure 34 Employee Security Tab— Personal

The screenshot shows the 'New Network' configuration interface. At the top, there are four tabs: '1 Basic Info', '2 VLAN', '3 Security', and '4 Access'. The 'Security' tab is active. Below the tabs, the 'Security Level' section features a vertical slider ranging from 'More Secure' at the top to 'Less Secure' at the bottom. The slider is positioned at 'Personal', with 'Enterprise' above it and 'Open' below it. To the right of the slider, there are several configuration options: 'Key management' is set to 'WPA-2 Personal', 'Passphrase format' is '8-63 chars', 'Passphrase' and 'Retype' are empty text boxes, and 'MAC authentication' is set to 'Disabled'. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

Table 7 Conditions for Adding an Employee Network— Security Tab

If	then,
You select the Open security level	<ol style="list-style-type: none">1. Select the required MAC authentication from the MAC authentication drop-down list. Available options are— Enabled and Disabled<ul style="list-style-type: none">● When Enabled, user must configure at least one RADIUS server for authentication server. See “MAC Authentication” on page 115 for further details.2. Authentication server 1— Select the required Authentication server option from the drop-down list. Available options are:<ul style="list-style-type: none">● New— If you select this option, an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 8, “Authentication” .● InternalServer— If you select this option, users who are required to authenticate with the internal RADIUS server must be added. Click the Users link to add the users. For information on adding a user, see “Adding a User” on page 217.3. Reauth interval— When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients.4. Blacklisting— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures.5. Max authentication failures— Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10. NOTE: Navigate to PEF > Blacklisting in the WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.6. For Internal users— Click Users to populate the system’s internal authentication server with users. For information about adding a user, see “Adding a User” on page 217.7. Click Upload Certificate and browse to upload a certificate file for the internal server. See “Certificates” on page 118 for more information.

Figure 35 *Employee Security Tab — Open*

The screenshot shows the 'New Network' configuration wizard with the 'Security' tab selected. The 'Security Level' section features a vertical slider ranging from 'More Secure' at the top to 'Less Secure' at the bottom. The slider is positioned at 'Open', with 'Enterprise' and 'Personal' also visible. To the right of the slider, the following configuration options are displayed:

- Encryption: None
- MAC authentication: Enabled
- Authentication server 1: InternalServer
- Reauth interval: 0 min.
- Blacklisting: Enabled
- Max authentication failures: 0
- Internal server: No users [Users](#)
- Internal server: No certificate [Upload certificate](#)

At the bottom of the wizard, there are 'Back', 'Next', and 'Cancel' buttons.

8. Click **Next** to continue.
9. Use the Access Rules page to specify optional access rules for this network.
 1. **Network-based**— Set the slider to **Network-based** if you want the same rules to apply to all users. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. Instant Firewall treats packets based on the first rule matched. For more information, see [Chapter 12, “Instant Firewall”](#).

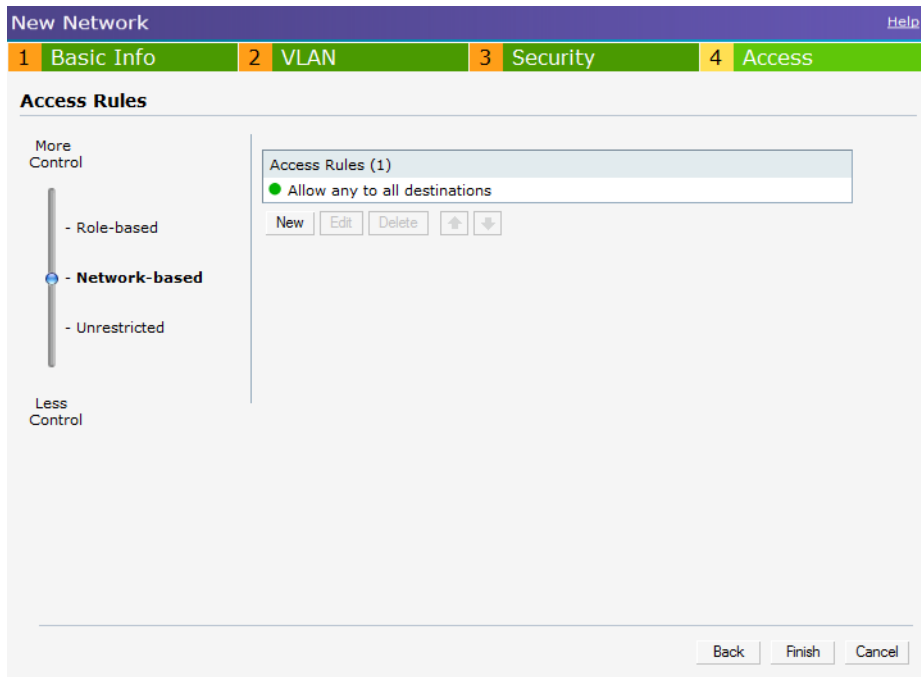
To edit the default rule, perform the following steps:

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

To define an access rule, perform the following steps:

- a. Click **New**.
 - b. Select appropriate options in the **New Rule** window.
 - c. Click **OK**.
 2. **Role-based**— Select **Role-based** if you want to specify per-user access rules. See [“Creating a New User Role” on page 125](#) for more information.
 3. **Unrestricted**— Select this to set no restrictions on access based on destination or type of traffic.
10. Click **Finish**. The network is added and listed in the **Networks** tab.

Figure 36 Adding an Employee Network— Access Rules Tab



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

Voice Network

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

Adding a Voice Network

This section provides the procedure to add a voice network.

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

Figure 37 Adding a Voice Network— Basic Info Tab

The screenshot shows the 'New Network' configuration interface with the 'Basic Info' tab selected. The interface includes a navigation bar with tabs for 'Basic Info', 'VLAN', 'Security', and 'Access'. The 'Basic Information' section contains the following fields and options:

- Name (SSID):** A text input field.
- Primary usage:** Radio buttons for Employee, Voice (selected), and Guest.
- Content filtering:** A dropdown menu set to 'Disabled'.
- Hide SSID:** A checkbox that is unchecked.
- Band:** A dropdown menu set to 'All'.
- Inactivity timeout:** A text input field with '1000' and 'secs'.
- Bandwidth Limits:** A section with three checkboxes: 'Percentage of Airtime', 'Each user', and 'Each radio', all of which are unchecked.
- Broadcast/Multicast:** A section with three dropdown menus: 'Multicast optimization' (set to 'Disabled'), 'Broadcast filtering' (set to 'Disabled'), and 'DTIM interval' (set to '1 beacon').
- Transmit Rates:** A section with two rows of dropdown menus: '2.4GHz: Min: 1, Max: 54' and '5GHz: Min: 6, Max: 54'.

At the bottom of the form, there is a link for 'Hide advanced options' and two buttons: 'Next' and 'Cancel'.

2. In the **Basic Info** tab, perform the following steps:
 - a. **Name (SSID)**— Enter a name that uniquely identifies a wireless network.
 - b. **Primary usage**— Select **Voice** from the **Primary usage** options. This selection determines whether the network is primarily intended to be used for employee data, guest data, or voice traffic.
 - c. **Content filtering**— When enabled, all DNS requests to non-corporate domains on this wireless network are sent to OpenDNS.
 - d. **Hide SSID**— Select this check box if you do not want the SSID (network name) to be visible to users.
 - e. **Band**— Set the band at which the network will transmit radio signals. Available options are 2.4 GHz, 5 GHz and All. The All option is selected by default. It is also the recommended option.
 - f. **Inactivity timeout**— Indicates the time in seconds after which an idle client ages out. The minimum value is 60 seconds and the default value is 1000 seconds.
3. Click the **Show advanced options** link and perform the following steps.
 - a. **Bandwidth Limits**— You can specify three types of bandwidth limits.
 - **Percentage of Airtime**— Indicates the aggregate amount of airtime that all clients on this Network can use to send/receive data.
 - **Each user**— Indicates the throughput for any single user on this Network. The throughput value is specified in kbps.
 - **Each radio**— Indicates the aggregate amount of throughput each radio (some AP models have multiple radios) is allowed to provide for all clients connected to that radio.
 - b. **Broadcast/Multicast**
 - **Multicast optimization**— When **Enabled**, the OAW-IAP will choose the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. The default values are 1 mbps for 2.4GHz and 6 mbps for 5.0GHz bands. Multicast traffic can be sent at up to 24 mbps when this option is enabled. This option is disabled by default.
 - **Broadcast filtering**— When set to **All**, the OAW-IAP will drop all broadcast and multicast frames except for DHCP and ARP. When set to **ARP**, in addition to the above, the OAW-IAP will

convert ARP requests to unicast and send frames directly to the associated client. When **Disabled**, all broadcast and multicast traffic is forwarded.

- **DTIM interval**— Indicates the DTIM (delivery traffic indication message) period in number of beacons. You can configure this option for every WLAN SSID profile. The default value is 1, which means the client will check for buffered data on the OAW-IAP at every beacon. You may choose to configure a larger DTIM value for power saving.
- c. **Transmit Rates**— Indicates the ability to configure the basic and supported rates per SSID for Alcatel-Lucent Instant. Select to set the minimum and maximum legacy (non-802.11n) transmit rates for each band —2.4GHz and 5GHz.



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

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

Table 8 *Conditions for Client IP and VLAN Assignment*

If	then
You select Virtual Controller assigned	<p>The client gets the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the OAW-IAP for the wireless clients.</p> <p>The Virtual Controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi site wireless network. See Chapter 7, “Virtual Controller” on page 95 for configuring the DHCP server.</p>
You select Network assigned	<p>By default, the client VLAN is assigned to the native VLAN on the wired network.</p> <ul style="list-style-type: none"> • Default— The client gets the IP address in the same subnet as the OAW-IAPs. • Static— Select to specify a VLAN for all clients on this network. • Dynamic— Select to create rules for per-user VLAN assignment. See “VLAN Derivation Rule” on page 130 for more information.

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

Figure 38 Voice Security Tab— Enterprise

New Network [Help](#)

1 Basic Info 2 VLAN 3 Security 4 Access

Security Level

More Secure

Enterprise

Personal

Open

Less Secure

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: InternalServer

Reauth interval: 0 min.

Blacklisting: Enabled

Max authentication failures: 0

Internal server: No users [Users](#)

Internal server: No certificate [Upload certificate](#)

[Back](#) [Next](#) [Cancel](#)

Table 9 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"> 1. Select the required key options from the Key management drop-down list. Available options are: <ul style="list-style-type: none"> ● WPA-2 Enterprise ● WPA Enterprise ● Both (WPA-2 & WPA) ● Dynamic WEP with 802.1x ● Use Session Key for LEAP: Use the Session Key for LEAP instead of using Session Key from the RADIUS Server to derive pair wise unicast keys. This is required for old printers that use dynamic WEP via LEAP authentication. This is Disabled by default. <p>For more information on encryption and recommended encryption type, see Chapter 9, “Encryption” .</p> 2. Termination— Enable this option to terminate the EAP portion of 802.1x authentication on the OAW-IAP instead of the RADIUS server. For more information, see “External RADIUS Server” on page 100. 3. Authentication server 1 and 2— Select the required Authentication server option from the drop-down list. Available options are: <ul style="list-style-type: none"> ● New— If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 8, “Authentication” . ● InternalServer— If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the Users link to add the users. <p>For information on adding a user, see “Adding a User” on page 217.</p> 4. Reauth interval— When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients. 5. Blacklisting— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures. 6. Max authentication failures— Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10. <p>NOTE: Navigate to PEF > Blacklisting in the WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.</p> <ol style="list-style-type: none"> 7. For Internal users— Click Users to populate the system’s internal authentication server with users. For information about adding a user, see “Adding a User” on page 217. 8. Click Upload Certificate and browse to upload a certificate file for the internal server. See “Certificates” on page 118 for more information

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

If	then,
<p>You want to use the default security level, Personal</p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> 1. Select the required key options from the Key management drop-down list. Available options are: <ul style="list-style-type: none"> ● WPA-2 Personal ● WPA Personal ● Both (WPA-2 & WPA) ● Static WEP <p>If you have selected Static WEP, then do the following:</p> <ul style="list-style-type: none"> ● Select appropriate WEP key size from the WEP key size drop-down list. Available options are 64-bit and 128-bit. ● Select appropriate Tx key from the Tx Key drop-down list. Available options are 1, 2, 3, and 4. ● Enter an appropriate WEP key and reconfirm. <p>For more information on encryption and recommended encryption type, see Chapter 9, “Encryption”.</p> 2. Select a passphrase format from the Passphrase format drop-down list. Available options are: <ul style="list-style-type: none"> ● 8-63 alphanumeric chars ● 64 hexadecimal chars 3. Enter a passphrase in the Passphrase text box and reconfirm. 4. Select the required option from the MAC authentication drop-down list. Available options are: Enabled and Disabled <p>When Enabled, user must configure at least one RADIUS server for authentication server. See “MAC Authentication” on page 115 for further details.</p> <ol style="list-style-type: none"> 5. Authentication server 1— Select the required Authentication server option from the drop-down list. Available options are: <ul style="list-style-type: none"> ● New— If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 8, “Authentication”. ● InternalServer— If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the Users link to add the users. <p>For information on adding a user, see “Adding a User” on page 217.</p> 6. Reauth interval— When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients. 7. Blacklisting— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures. 8. Max authentication failures— Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10. <p>NOTE: Navigate to PEF > Blacklisting in the WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.</p>

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

If	then,
	<p>NOTE: Navigate to PEF > Blacklisting in the WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.</p> <p>9. For Internal users— Click Users to populate the system’s internal authentication server with users. For information about adding a user, see “Adding a User” on page 217.</p> <p>10. Click Upload Certificate and browse to upload a certificate file for the internal server. See “Certificates” on page 118 for more information.</p>
<p>You select the Open security level</p>	<ol style="list-style-type: none"> 1. Select the required MAC authentication from the MAC authentication drop-down list. Available options are— Enabled and Disabled <ul style="list-style-type: none"> ● When Enabled, user must configure at least one RADIUS server for authentication server. See “MAC Authentication” on page 115 for further details. 2. Authentication server 1— Select the required Authentication server option from the drop-down list. Available options are: <ul style="list-style-type: none"> ● New— If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see Chapter 8, “Authentication” . ● InternalServer— If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the Users link to add the users. <p>For information on adding a user, see “Adding a User” on page 217.</p> 3. Reauth interval— When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients. 4. Blacklisting— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures. 5. Max authentication failures— Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10. <p>NOTE: Navigate to PEF > Blacklisting in the WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.</p> <p>6. For Internal users— Click Users to populate the system’s internal authentication server with users. For information about adding a user, see “Adding a User” on page 217.</p> <p>7. Click Upload Certificate and browse to upload a certificate file for the internal server. See “Certificates” on page 118 for more information.</p>

8. Use the Access Rules page to specify optional access rules for this network.
 - **Network-based**— Set the slider to **Network-based** if you want the same rules to apply to all users. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. Instant Firewall treats packets based on the first rule matched. For more information, see [Chapter 12, “Instant Firewall”](#) .

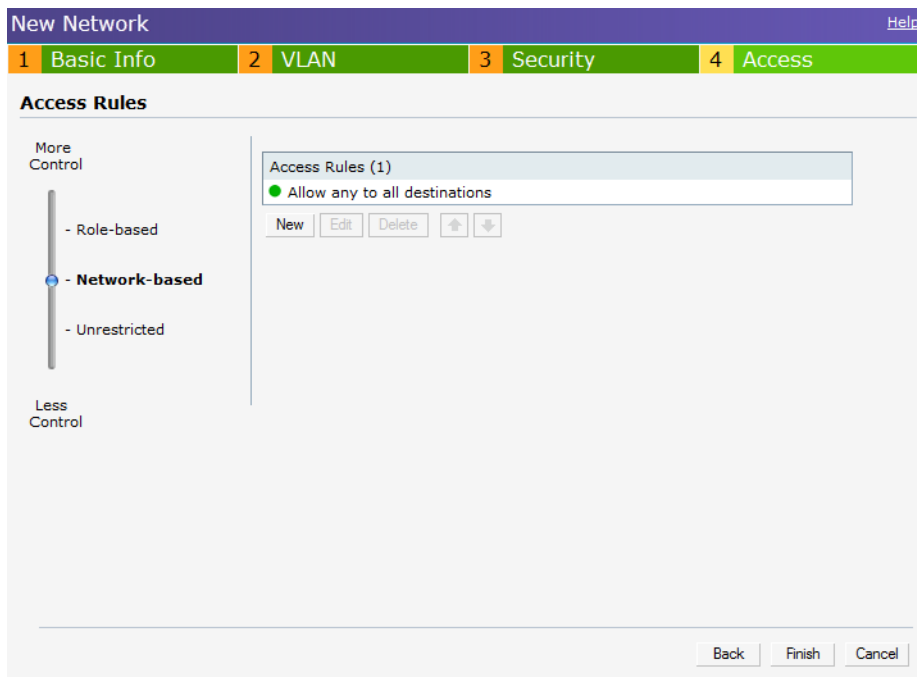
To edit the default rule, perform the following steps:

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

To define an access rule, perform the following steps:

- a. Click **New**.
 - b. Select appropriate options in the **New Rule** window.
 - c. Click **OK**.
- **Role-based**— Select **Role-based** if you want to specify per-user access rules. See “[Creating a New User Role](#)” on page 125 for more information.
 - **Unrestricted**— Select this to set no restrictions on access based on destination or type of traffic.

Figure 39 Adding a Voice Network— Access Rules Tab



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

Guest Network

The Guest wireless network is created for guests, visitors, contractors, and any non-employee users who 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 (see [step 10](#) of the following procedure).

Adding a Guest Network

This section provides the procedure to add a guest network.

Figure 40 Adding a Guest Network— Basic Info Tab

1. In the **Networks** tab, click the **New** link. The **New Network** window appears.
2. In the **Basic Info** tab, perform the following steps:
 - a. **Name (SSID)**— Enter a name that uniquely identifies a wireless network.
 - b. **Primary usage**— Select **Guest** from the **Primary usage** options. This selection determines whether the network is primarily intended to be used for employee data, guest data, or voice traffic.
 - c. **Content filtering**— When enabled, all DNS requests to non-corporate domains on this wireless network are sent to OpenDNS.
 - d. **Hide SSID**— Select this check box if you do not want the SSID (network name) to be visible to users.
 - e. **Band**— Set the band at which the network will transmit radio signals. Available options are 2.4 GHz, 5 GHz and All. The All option is selected by default. It is also the recommended option.
 - f. **Inactivity timeout**— Indicates the time in seconds after which an idle client ages out. The minimum value is 60 seconds and the default value is 1000 seconds.
3. Click the **Show advanced options** link and perform the following steps.
 - a. **Bandwidth Limits**— You can specify three types of bandwidth limits.
 - **Percentage of Airtime**— Indicates the aggregate amount of airtime that all clients on this Network can use to send/receive data.
 - **Each user**— Indicates the throughput for any single user on this Network. The throughput value is specified in kbps.
 - **Each radio**— Indicates the aggregate amount of throughput each radio (some AP models have multiple radios) is allowed to provide for all clients connected to that radio.
 - b. **Broadcast/Multicast**
 - **Multicast optimization**— When **Enabled**, the OAW-IAP will choose the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. The default values are 1 mbps for 2.4GHz and 6 mbps for 5.0GHz bands. Multicast traffic can be sent at up to 24 mbps when this option is enabled. This option is disabled by default.

- **Broadcast filtering**— When set to **All**, the OAW-IAP will drop all broadcast and multicast frames except for DHCP and ARP. When set to **ARP**, in addition to the above, the OAW-IAP will convert ARP requests to unicast and send frames directly to the associated client. When **Disabled**, all broadcast and multicast traffic is forwarded.
 - **DTIM interval**— Indicates the DTIM (delivery traffic indication message) period in number of beacons. You can configure this option for every WLAN SSID profile. The default value is 1, which means the client will check for buffered data on the OAW-IAP at every beacon. You may choose to configure a larger DTIM value for power saving.
- c. **Transmit Rates**— Indicates the ability to configure the basic and supported rates per SSID for Alcatel-Lucent Instant. Select to set the minimum and maximum legacy (non-802.11n) transmit rates for each band -2.4GHz and 5GHz.
4. Click **Next** to continue.
 5. Select the required Client IP assignment option — Virtual Controller assigned and Network assigned.

Table 10 *Conditions for Client IP and VLAN assignment*

If	then
You select Virtual Controller assigned	<p>The client gets the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the OAW-IAP for the wireless clients.</p> <p>The Virtual Controller NATs all traffic that passes out of this interface. This setup eliminates the need for complex VLAN and IP address management for a multi site wireless network. See Chapter 7, “Virtual Controller” on page 95 for configuring the DHCP server.</p>
You select Network assigned	<p>By default, the client VLAN is assigned to the native VLAN on the wired network.</p> <ul style="list-style-type: none"> ● Default— The client gets the IP address in the same subnet as the OAW-IAPs. ● Static— Select to specify a VLAN for all clients on this network. ● Dynamic— Select to create rules for per-user VLAN assignment. See “VLAN Derivation Rule” on page 130 for more information.

6. Click **Next** to continue.

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

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

Splash Page Type	Description and steps to set up
Internal — Authenticated	<p>The user has to accept the terms and conditions and enter a username and password on the captive portal page. If this option is selected, then add the users who are required to use the captive portal authentication to the user database. Click the Users link to add the users. For information about adding a user, see “Adding a User” on page 217. For information on customizing the splash page, see “Customizing a Splash Page” on page 110.</p> <ol style="list-style-type: none"> 1. Select the required Authentication server 1 option from the drop-down list. Available options are: <ul style="list-style-type: none"> ● New — If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see “Configuring an External RADIUS Server” on page 101. ● Internal Server — If you select this option, then users who are required to authenticate with the internal RADIUS server must be added. Click the Users link to add the users. For information on adding a user, see “Adding a User” on page 217. 2. Reauth interval — When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients. 3. Blacklisting — Select Enabled if you want clients to be blacklisted after a certain number of authentication failures. 4. Max authentication failures — Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10. 5. For Internal users — Click Users to populate the system’s internal authentication server with users. For information about adding a user, see “Adding a User” on page 161. 6. Click Upload Certificate and browse to upload a certificate file for the internal server. See “Certificates” on page 118 for more information.
Internal — Acknowledged	<p>The user has to accept the terms and conditions for this splash page type.</p> <p>For information on customizing the splash page, see “Customizing a Splash Page” on page 110.</p>

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

Splash Page Type	Description and steps to set up
External	<p>An external server will be used to display the splash page to the user. If this option is selected, then do the following:</p> <ol style="list-style-type: none">1. Enter the IP or hostname of the external server in the IP or hostname text box.2. Enter the URL of the captive portal page in the URL text box.3. Enter the number of the port to be used for communicating with the external server in the Port text box.4. In the Authentication text box, enter the unique signature that the external server will return in the response after a successful user authentication.5. Select the required Authentication server 1 option from the drop-down list. Available options are:<ul style="list-style-type: none">● New— If you select this option, then an external radius server has to be configured to authenticate the users. For information on configuring an external RADIUS server, see “Configuring an External RADIUS Server” on page 101.6. Reauth interval— When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients.7. Blacklisting— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures.8. Max authentication failures— Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10.9. Walled Garden— The walled garden directs the user’s navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see “Walled Garden Access” on page 117.
None	Select this option if you do not want to set the captive portal authentication.

Figure 41 Adding a Guest Network — Splash Page Settings

The screenshot shows the 'New Network' configuration interface with the 'Security' tab selected. The 'Security Level' section contains the following settings:

- Splash page type: Internal - Authenticated
- Auth server 1: InternalServer
- Reauth interval: 0 min.
- Blacklisting: Enabled
- Max auth failures: 0
- Internal server: No users (with a link to 'Users')
- Encryption: Disabled

The 'Splash Page Visuals' section shows a preview of the splash page with the text 'Welcome to the Guest Network.' Below the preview are radio buttons for 'I do not agree' and 'I agree', and a 'Preview' link. At the bottom of the page are 'Back', 'Next', and 'Cancel' buttons.

10. Select **Enabled** from the **Encryption** drop-down list and perform the following steps (these steps are optional):
 - a. Select the required key management option from the **Key management** drop-down list. Available options are:
 - WPA-2 Personal
 - WPA Personal
 - Both (WPA-2 & WPA)
 - b. **Passphrase format** — Specify either an alphanumeric or a hexadecimal string. Ensure that the hexadecimal string must be exactly 64 digits in length.
 - c. **Passphrase** — Enter a pre-shared key (PSK) passphrase.

Figure 42 Configuring a Splash Page — Encryption Settings

The screenshot shows the 'New Network' configuration interface, specifically the 'Security Level' tab. The interface is divided into two main sections: configuration settings on the left and a splash page preview on the right.

Configuration Settings:

- Splash page type:** Internal - Authenticated
- Auth server 1:** InternalServer
- Reauth interval:** 0 min.
- Blacklisting:** Enabled
- Max auth failures:** 0
- Internal server:** No users (with a [Users](#) link)
- Internal server:** No certificate (with an [Upload certificate](#) link)
- Encryption:** Enabled
- Key management:** WPA-2 Personal
- Passphrase format:** 8-63 chars
- Passphrase:** (empty text field)
- Retype:** (empty text field)

Splash Page Visuals:

The preview shows a splash page titled 'Welcome to the Guest Network.' It contains two main sections: 'Log In to the Instant Network' and 'Site Usage Policy'. Below the preview, there is a 'Click thumbnail above to edit' instruction and a [Preview](#) link.

At the bottom of the configuration area, there are 'Back', 'Next', and 'Cancel' buttons.

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

- **Network-based**— Set the slider **Network-based** if you want the same rules to apply to all users. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. Instant Firewall treats packets based on the first rule matched. For more information, see [Chapter 12, “Instant Firewall”](#).

To edit the default rule, perform the following steps:

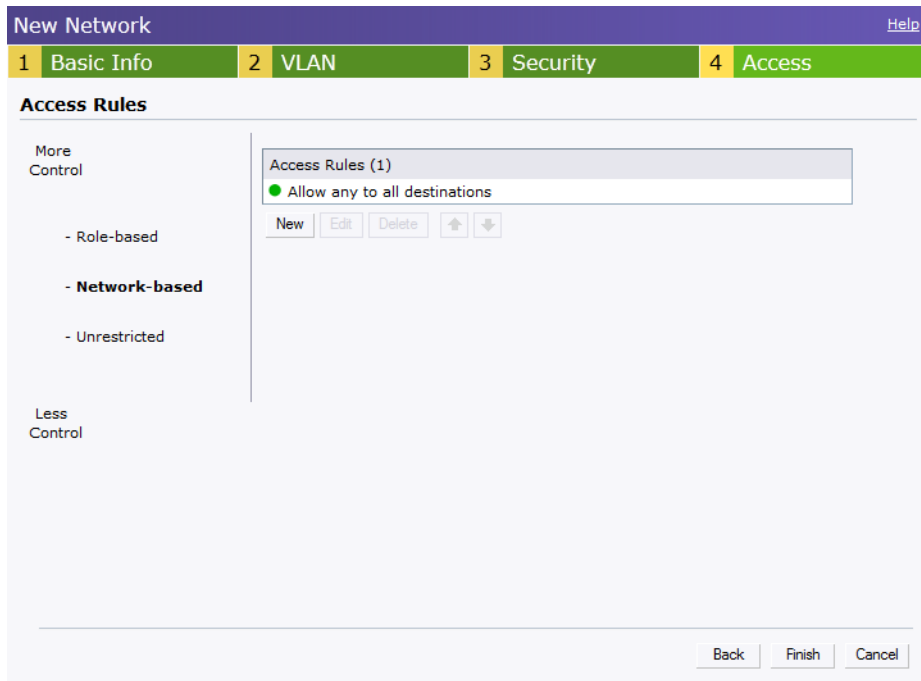
- Select the rule and then click **Edit**.
- Select appropriate options in the **Edit Rule** window and click **OK**.

To define an access rule, perform the following steps:

- Click **New**.
- Select appropriate options in the **New Rule** window.
- Click **OK**.

- **Role-based**— Select **Role-based** if you want to specify per-user access rules. See [“Creating a New User Role” on page 125](#) for more information.
- **Unrestricted**— Select this to set no restrictions on access based on destination or type of traffic.

Figure 43 Adding a Guest Network — Access Rules Tab



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

Editing a Network

To edit a network, perform the following steps:

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

Deleting a Network

To delete a network, perform the following steps:

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

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. 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.

This chapter describes the Alcatel-Lucent Instant secure enterprise mesh architecture.

Mesh Instant Access Points

An Alcatel-Lucent Instant mesh network requires at least one wired connection. The wired OAW-IAP is the mesh portal and also acts as a virtual controller. The un-wired OAW-IAPs are mesh points.

If two OAW-IAPs are wired, there will be redundancy, and most mesh points will try to mesh directly with one of the two portals. However, depending on actual deployment and RF environment some mesh points may mesh through other intermediate mesh points.

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



Instant Mesh does not support LAN bridging or secure wired pass-through.

Mesh OAW-IAPs learn about their environment when they boot up. Mesh OAW-IAPs can act as a mesh portal (MPP), an OAW-IAP that uses its wired interface to reach the switch, a mesh point (MP), or 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.

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



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

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

Mesh Portals

The mesh portal (MPP) is the gateway between the wireless mesh network and the enterprise wired LAN. 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 a mesh services set identifier (MSSID/ mesh cluster name) to advertise the mesh network service to other OAW-IAP mesh points in that instant network. This is not configurable and is

transparent to the user. The mesh points will authenticate to the mesh portal and establish a link that is secured using Advanced Encryption Standard (AES) encryption.



The mesh portal will reboot after 5 minutes when it loses Ethernet connectivity to a wired network.

Mesh Points

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



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

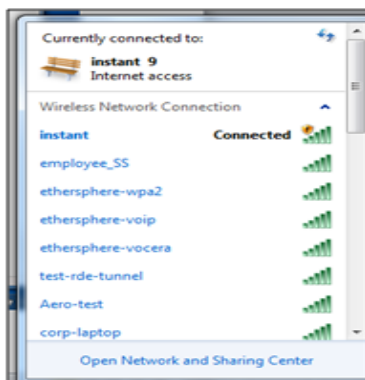
Instant mesh can be provisioned in two ways — Over-the-air provisioning and over-the-wire provisioning. Over-the-air provisioning is available when only one Alcatel-Lucent Instant mesh network is being advertised and it will not work for ROW version of OAW-IAPs.

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

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

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

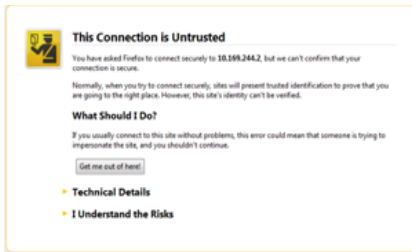
Figure 44 *Open Instant SSID*



4. Type `instant.alcatel-lucent.com` in the browser.

5. Click **I understand the risks** and **Add exception** to ignore the certificate warnings that the client does not recognize the certificate authority.

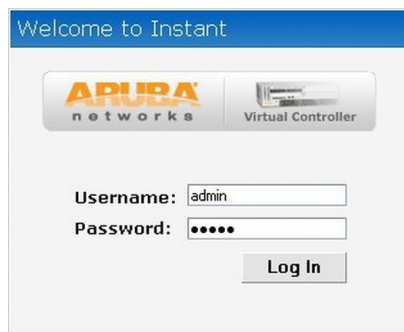
Figure 45 *Untrusted Connection Window*



6. In the login screen as shown in [Figure 46](#), enter the following credentials:

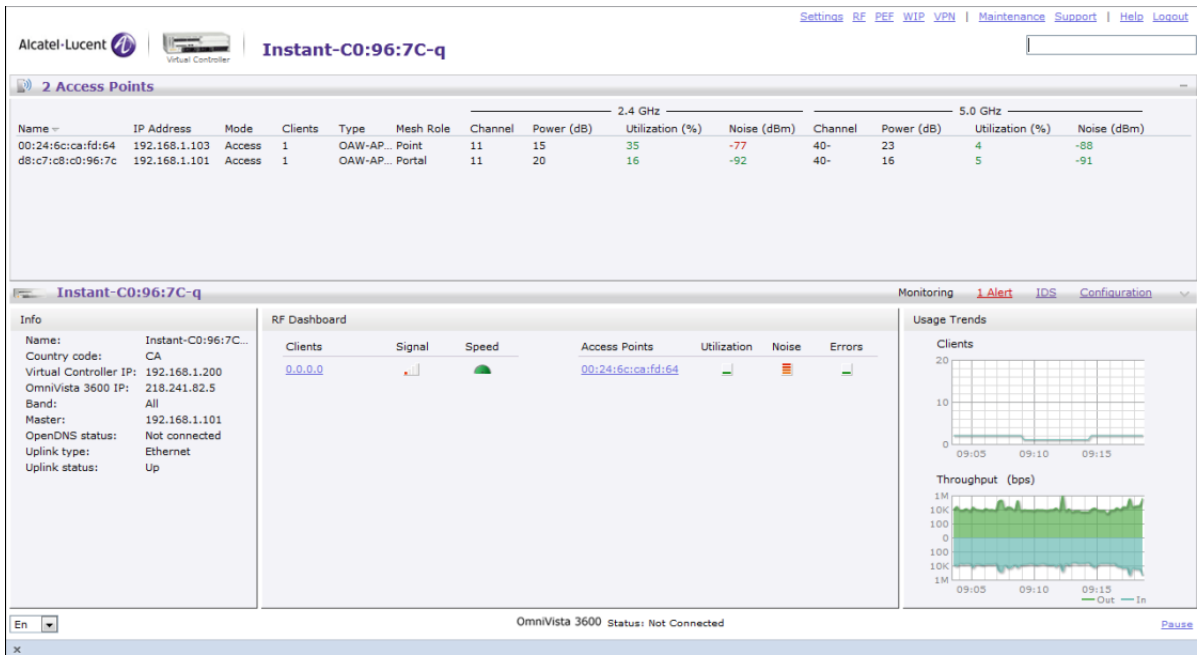
- Username— admin
- Password— admin

Figure 46 *Login Window*



7. Create a new SSID and wpa-2 personal keys with **unrestricted** or **network based** access rules. Select **any permit** for basic connectivity.
8. Connect a client to the new SSID and disconnect from the **instant** SSID.
9. All the OAW-IAPs will show up on the Virtual Controller as shown in [Figure 47](#). 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 47 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. An OAW-IAP mesh point in factory default state will automatically join the portal if only a single Instant mesh network is found. In addition, the auto-join feature must be enabled in the existing network.



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

This chapter describes the Preferred band, 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.

Preferred Band

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

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



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

Auto Join Mode

The Auto Join Mode feature allows 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 79. Also, when this feature is disabled, OAW-IAPs that are configured but not active appear in red.

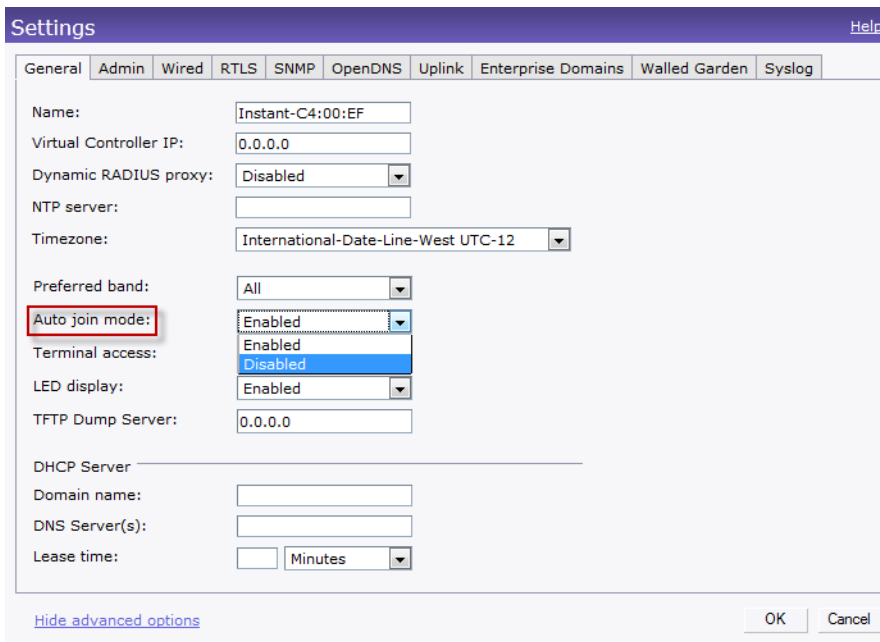
Disabling Auto Join Mode

To disable Auto Join Mode, perform the following steps:

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

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

Figure 48 *Disabling Auto Join Mode*

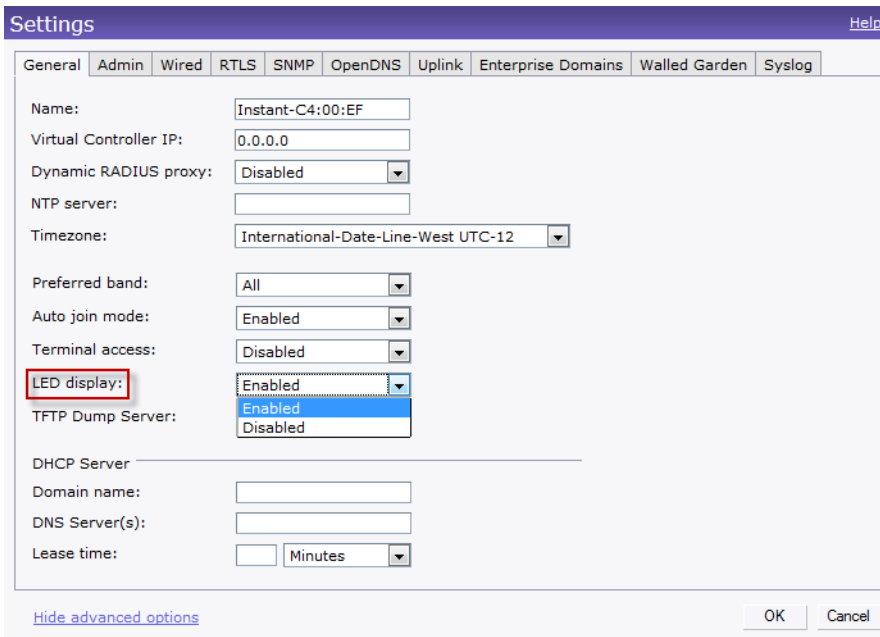


3. Click **OK**.

LED Display

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

Figure 49 *LED Display*





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

Terminal Access

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

Figure 50 Terminal Access

The screenshot shows the 'Settings' window with the 'Terminal access' dropdown menu open. The 'Terminal access' option is highlighted in red, and the 'Enabled' option is selected in blue. The 'LED display' option is also highlighted in blue. The 'TFTP Dump Server' field is set to '0.0.0.0'. The 'DHCP Server' section is visible below the main configuration area.

Field	Value
Name	Instant-C4:00:EF
Virtual Controller IP	0.0.0.0
Dynamic RADIUS proxy	Disabled
NTP server	
Timezone	International-Date-Line-West UTC-12
Preferred band	All
Auto join mode	Enabled
Terminal access	Enabled
LED display	Enabled
TFTP Dump Server	0.0.0.0
DHCP Server	
Domain name	
DNS Server(s)	
Lease time	Minutes



Instant does not support configuration using CLI.

TFTP Dump Server

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

Figure 51 TFTP Dump Server

The screenshot shows the 'Settings' window with the 'General' tab selected. The 'TFTP Dump Server' field is highlighted with a red box and contains the IP address '0.0.0.0'. Other fields include Name (Instant-C4:00:EF), Virtual Controller IP (0.0.0.0), Dynamic RADIUS proxy (Disabled), NTP server, Timezone (International-Date-Line-West UTC-12), Preferred band (All), Auto join mode (Enabled), Terminal access (Disabled), LED display (Enabled), DHCP Server, Domain name, DNS Server(s), and Lease time (Minutes). Buttons for 'OK' and 'Cancel' are at the bottom right, and a link for 'Hide advanced options' is at the bottom left.

Syslog Server

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

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

Figure 52 Syslog Server

The screenshot shows the 'Settings' window with the 'Syslog' tab selected. The 'Syslog server' field contains '0.0.0.0' and the 'Syslog level' dropdown is set to 'Warning'. Under 'Syslog Facility Levels', several categories are listed with 'Warning' selected: Ap-Debug, Network, Security, System, User, User-Debug, and Wireless. Buttons for 'OK' and 'Cancel' are at the bottom right, and a link for 'Hide advanced options' is at the bottom left.

Syslog Facility Levels

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

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

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

Table 12 *Logging Levels*

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

Adding an OAW-IAP to the Network

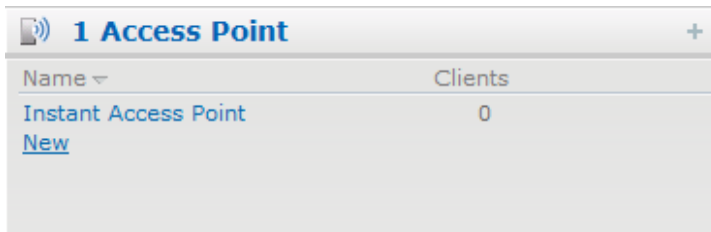
To add an OAW-IAP to the Alcatel-Lucent Instant network, assign an IP address. For more information, see “Assigning an IP Address to the OAW-IAP” on page 20.

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:

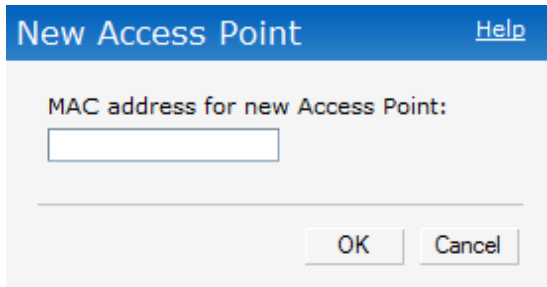
1. In the **Access Points** tab, click the **New** link.

Figure 53 Adding an OAW-IAP to the Instant Network



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

Figure 54 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 network anymore and will no longer appear in the WebUI. However, the master OAW-IAP cannot be deleted from the Virtual Controller.

Editing OAW-IAP Settings

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

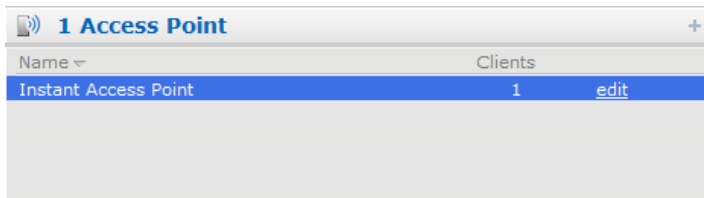
- Name
- IP Address
- Adaptive Radio Management (ARM) Configuration
- External Antenna Configuration
- Migrating from a Virtual Controller Managed Network to OmniAccess WLAN Switch Managed Network

Changing OAW-IAP Name

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

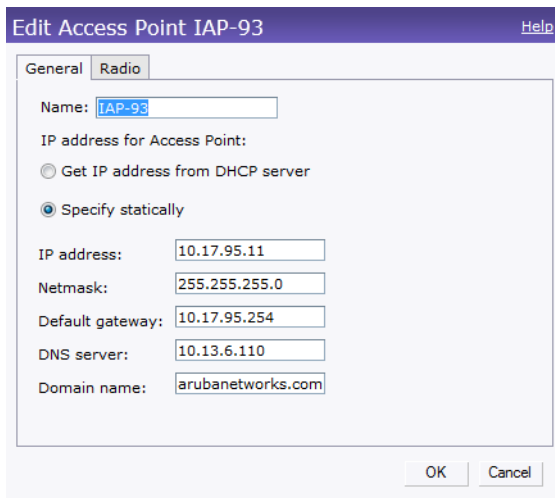
1. In the **Access Points** tab, click on the OAW-IAP that you want to rename.

Figure 55 *Editing OAW-IAP Settings*



2. Click the **edit** link.

Figure 56 *Changing OAW-IAP Name*



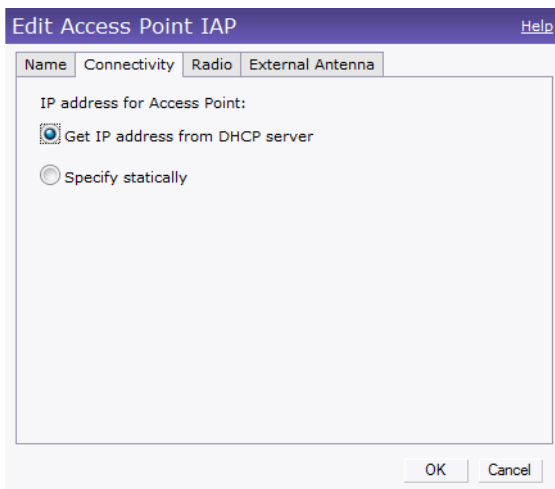
3. Edit the OAW-IAP name in the **Name** text box.
4. Click **OK**.

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:

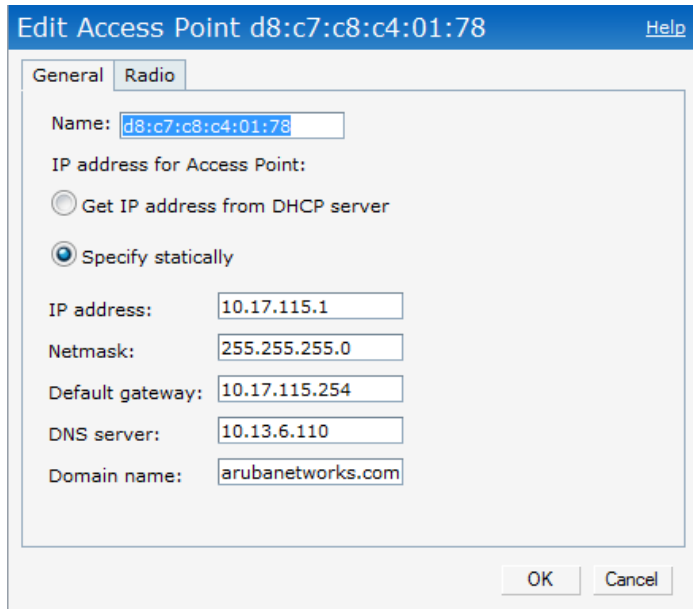
1. In the **Access Points** tab, click the OAW-IAP for which you want to change the IP address. The **edit** link appears.
2. Click the **edit** link. The **Edit AP** window appears.

Figure 57 *Configuring OAW-IAP Settings — Connectivity Tab*



3. Select either the **Get IP address from DHCP server** or **Specify statically** option. If you have selected the **Specify statically** option, then perform the following steps:
 1. Enter the new IP address for the 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 58 Configuring OAW-IAP Connectivity Settings — Specifying Static Settings



The screenshot shows a dialog box titled "Edit Access Point d8:c7:c8:c4:01:78" with a "Help" button in the top right corner. The "Radio" tab is selected. The "Name" field contains "d8:c7:c8:c4:01:78". Under "IP address for Access Point:", the "Specify statically" radio button is selected. The "IP address" field is "10.17.115.1", "Netmask" is "255.255.255.0", "Default gateway" is "10.17.115.254", "DNS server" is "10.13.6.110", and "Domain name" is "arubanetworks.com". "OK" and "Cancel" buttons are at the bottom right.

4. 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.

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

Figure 59 Configuring OAW-IAP Radio Settings Mode — Access

The screenshot shows a configuration window titled "Edit Access Point IAP-93" with a "Help" button in the top right. The window has two tabs: "General" and "Radio". The "Radio" tab is active. At the top, there is a "Mode:" dropdown menu set to "Access". Below this, there are two sections: "2.4 GHz band" and "5 GHz band". Each section has two radio buttons: "Adaptive radio management assigned" (which is selected) and "Administrator assigned". Under the "2.4 GHz band" section, there is a "Channel:" dropdown menu set to "1" and a "Transmit power:" text input field. Under the "5 GHz band" section, there is a "Channel:" dropdown menu set to "36" and a "Transmit power:" text input field. At the bottom of the window, there are "OK" and "Cancel" buttons.

5. Click **OK**.

For more information about ARM, see “[Adaptive Radio Management](#)” on page 149.

Migrating from a Virtual Controller Managed Network to OmniAccess WLAN Switch Managed Network

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

Converting an OAW-IAP to RAP Mode



OAW-IAP to RAP conversion will be supported on a future release of ArubaOS. For new feature details see ArubaOS release notes.

For RAP conversion, the Virtual Controller sends the RAP convert command to all the other OAW-IAPs. The Virtual Controller along with the other slave OAW-IAPs will then setup a VPN tunnel to the remote controller, and download the firmware by FTP. The Virtual Controller uses IPsec to communicate to the OmniAccess WLAN Switch over the Internet.

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



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



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

An OAW-IAP can be converted to an AOS-W Campus AP only if the controller is running AOS-W 6.1 or later. The following table describes the supported OAW-IAP platforms and minimal AOS version for OAW-IAP to CAP/RAP conversion.

Table 13 Supported OAW-IAP Platforms and Minimal AOS Version for OAW-IAP to CAP Conversion

OAW-IAP Platform	AOS Version
OAW-IAP-92	6.1.x
OAW-IAP-93	6.1.x
OAW-IAP-104	6.1.x
OAW-IAP-105	6.1.x
OAW-IAP-134	6.1.x
OAW-IAP-135	6.1.x
OAW-IAP-175AC	6.1.x
OAW-IAP-175P	6.1.x
OAW-RAP3WN	6.1.x
OAW-RAP3WNP	6.1.x

Table 14 Supported OAW-IAP platforms and minimal AOS version for OAW-IAP to RAP Conversion

OAW-IAP Platform	AOS Version
OAW-IAP-92	TBD
OAW-IAP-93	TBD
OAW-IAP-104	TBD
OAW-IAP-105	TBD
OAW-IAP-134	TBD
OAW-IAP-135	TBD

Table 14 Supported OAW-IAP platforms and minimal AOS version for OAW-IAP to RAP Conversion

OAW-IAP Platform	AOS Version
OAW-IAP-175AC	TBD
OAW-IAP-175P	TBD
OAW-RAP3WN	TBD
OAW-RAP3WNP	TBD

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

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

Figure 60 Maintenance — Convert Tab

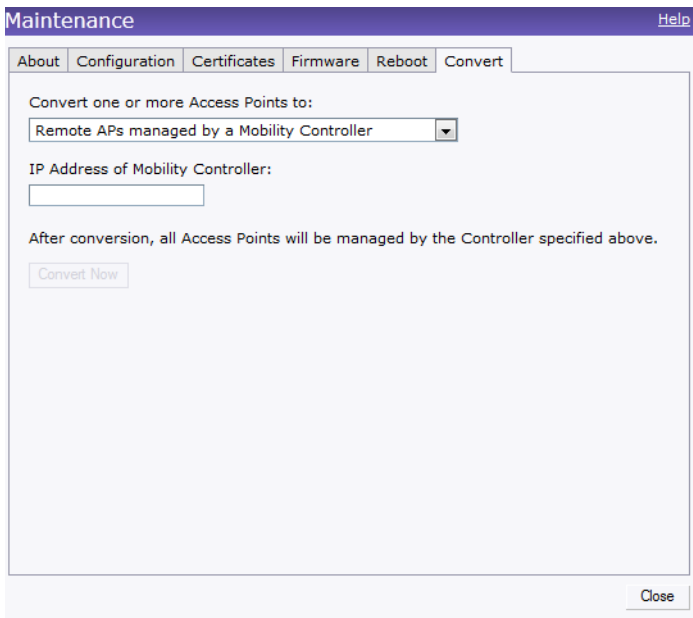
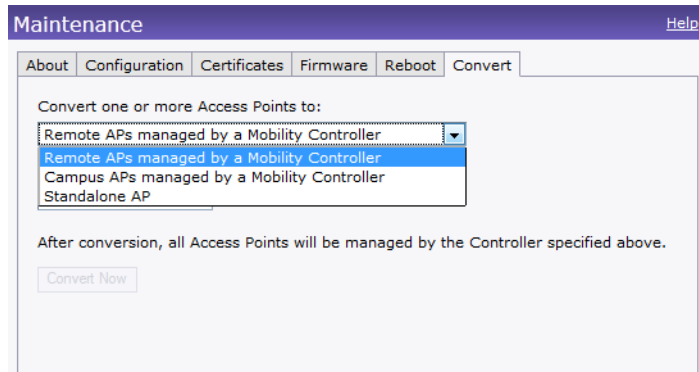


Figure 61 Convert options



3. Select **Remote APs managed by an OmniAccess WLAN Switch** from the drop-down list.

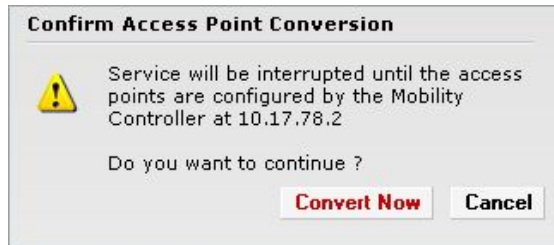
4. Enter the IP address of the controller in the **IP Address of OmniAccess WLAN Switch** text box. This information is provided by your network administrator.



Ensure the WLAN Switch IP Address is reachable by the IAPs.

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

Figure 62 *Confirm Access Point Conversion*



6. The OAW-IAP will reboot and begin operating in RAP mode.
7. After conversion, the OAW-IAP will be managed by the Alcatel-Lucent OmniAccess WLAN Switch which has been specified in the Instant UI.



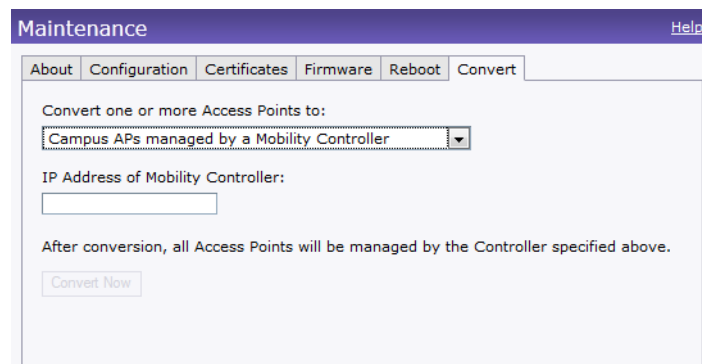
In order for the RAP conversion to work, ensure that you configure the Instant AP in the controller white-list and enable the FTP service on the controller.

Converting an OAW-IAP to CAP

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

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

Figure 63 *Converting an OAW-IAP to CAP*



3. Select **Campus APs managed by a OmniAccess WLAN Switch** from the drop-down list.
4. Enter the IP address of the controller in the **IP Address of OmniAccess WLAN Switch** text box. This is provided by your network administrator.



Ensure the WLAN Switch IP Address is reachable by the IAPs.

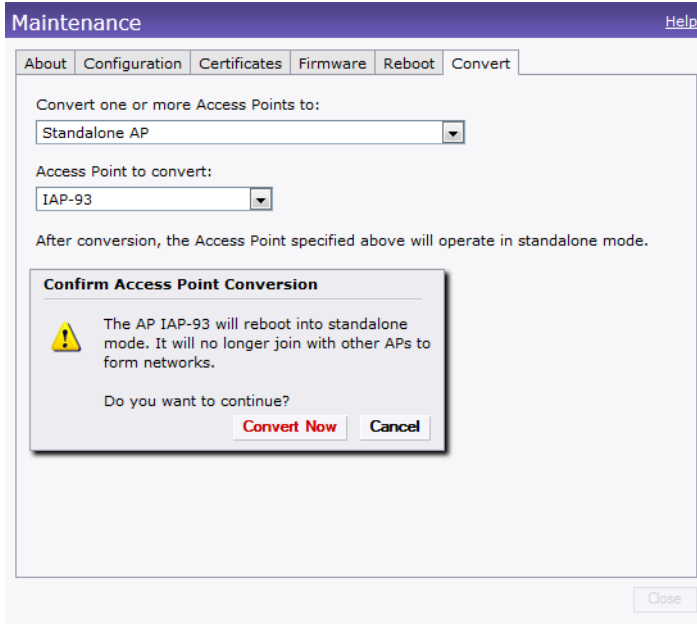
5. Click **Convert Now** to complete the conversion.

Converting an OAW-IAP to Standalone Mode

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

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

Figure 64 Standalone AP Conversion



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

Converting back to an OAW-IAP

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

To reset an OAW-IAP, follow the instructions below:

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

The OAW-IAP will then boot with the factory default settings.



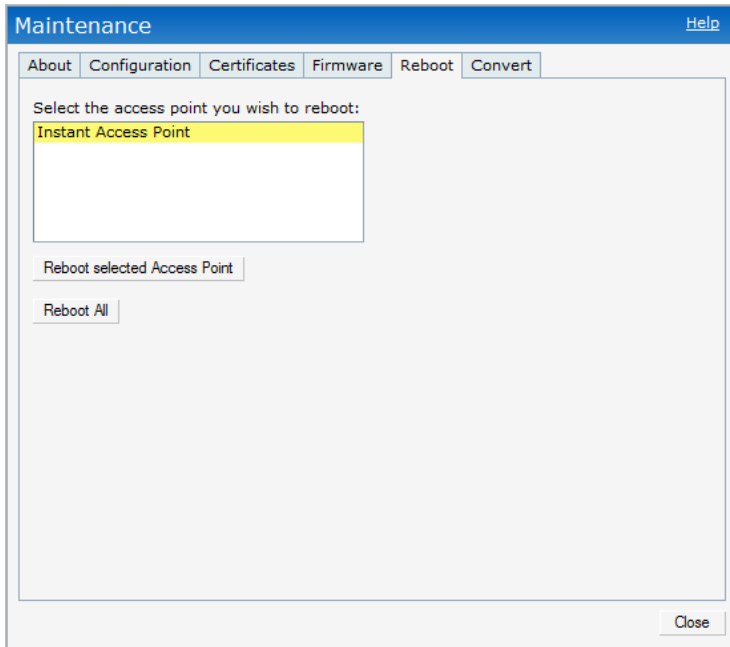
OAW-IAP-92, OAW-IAP-93, OAW-IAP-104, OAW-IAP-105, OAW-IAP-134, OAW-IAP-135, OAW-RAP3WN, OAW-RAP3WNP — These OAW-IAP platforms support reset button. OAW-IAP-175P and OAW-IAP-175AC do not have reset buttons. Please contact Alcatel-Lucent support for the backward conversion process on these OAW-IAPs.

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:

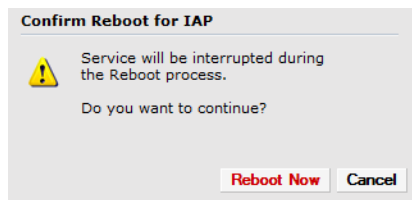
1. Click the **Maintenance** link. The **Maintenance** window appears.
2. Click the **Reboot** tab.

Figure 65 Rebooting the OAW-IAP



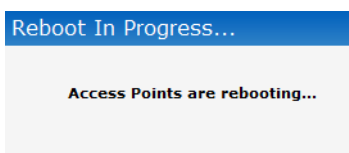
3. In the OAW-IAP list, select the OAW-IAP that you want to reboot and click **Reboot selected Access Point**. To reboot all the OAW-IAPs in the network, click **Reboot All**.
4. The **Confirm Reboot for OAW-IAP** window will appear. Click **Reboot Now** to proceed.

Figure 66 Confirm Reboot message



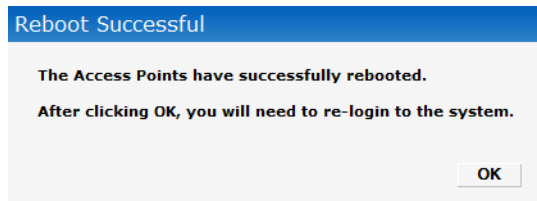
5. The **Reboot in Progress** message will appear indicating that the reboot is in progress.

Figure 67 Reboot In Progress



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

Figure 68 *Reboot Successful*



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

Firmware Image Server in Cloud Network

The image check feature allows the OAW-IAP to discover new software image versions on a cloud-based image server hosted by Alcatel-Lucent Networks. 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.

Upgrade using OmniVista and Image Server

Alcatel-Lucent Instant supports mixed AP-class instant deployment with OAW-RAP3WN/3WNP, OAW-IAP-104, OAW-IAP-175P/175AC, OAW-IAP-92/93, OAW-IAP-105, and OAW-IAP-134/135 as part of the same Virtual Controller cluster.

Image management using Cloud Server

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

Image management using OmniVista

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



The Virtual Controller in Instant AP communicates with the OmniVista server or Image server, depending on the user's configuration. If OmniVista is not configured on the OAW-IAP, then the image will be requested from the Image server. See [“Configuring OmniVista” on page 177](#) for steps on how to configure OmniVista.

Automatic Firmware Image Check and Upgrade

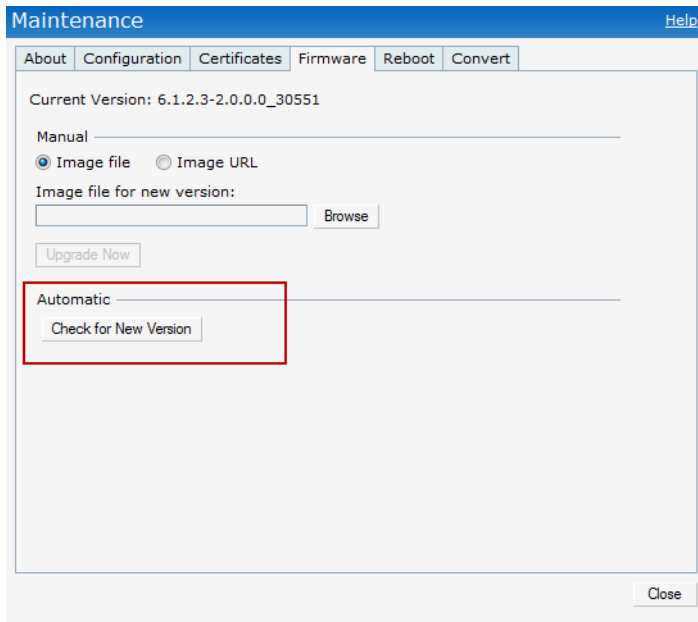
Automatic image check is enabled by default. If OmniVista is configured, then the automatic image check is automatically disabled, use the manual image check option to check for the latest image. For more information, see [“Upgrading to New Version” on page 91](#) and [“Configuring OmniVista” on page 177](#) for steps on how to configure OmniVista.

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

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

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

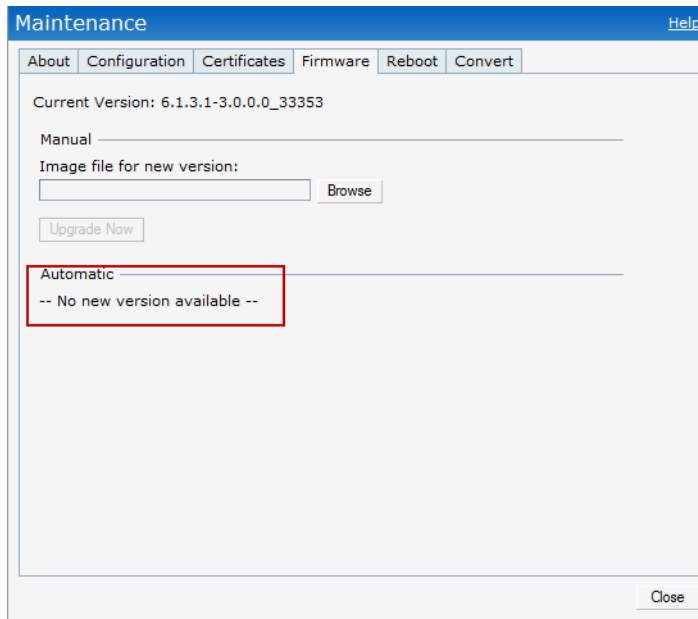
Figure 69 Automatic Image Check — New Version Available Link



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

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

Figure 70 New Version Available



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

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

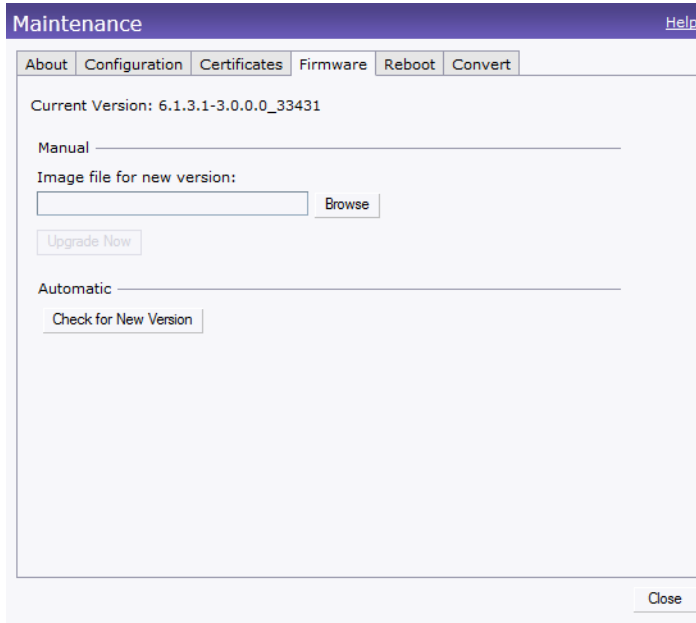
Upgrading to New Version

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

Manual

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

Figure 71 *Upgrading single class or multi-class AP Networks*



- **Image file**— Select to directly upload an image file. This method is only available for single-class OAW-IAPs.

Example: Alcatel-LucentInstant_Orion_6.1.3.1-3.0.0.0_33353

Example: Alcatel-LucentInstant_Cassiopeia_6.1.3.1-3.0.0.0_33353

Automatic

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

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

- No new version available— If there is no new version available.
 - Image server timed out— Connection or session between the image server and the 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.
2. If a new version is found, the **Upgrade Now** button becomes available and displays the version number.
 3. Click **Upgrade Now**.

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

Figure 72 Configuring NTP Server

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

Field	Value
Name:	Instant-C4:00:EF
Virtual Controller IP:	0.0.0.0
Dynamic RADIUS proxy:	Disabled
NTP server:	pool.ntp.org
Timezone:	International-Date-Line-West UTC-12
Preferred band:	All
Auto join mode:	Enabled
Terminal access:	Disabled
LED display:	Enabled
TFTP Dump Server:	0.0.0.0
DHCP Server	
Domain name:	
DNS Server(s):	
Lease time:	Minutes

At the bottom of the dialog, there is a link for 'Hide advanced options' and 'OK' and 'Cancel' buttons.

Alcatel-Lucent Instant does not require an external switch 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 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** window appears.

Figure 73 Specifying Virtual Controller Name and IP Address

The screenshot shows the 'Settings' window with the 'General' tab selected. The 'Name' field is set to 'Instant-C4:00:EF' and the 'Virtual Controller IP' field is set to '0.0.0.0'. Other fields include 'Dynamic RADIUS proxy' (Disabled), 'NTP server' (pool.ntp.org), 'Timezone' (International-Date-Line-West UTC-12), 'Preferred band' (All), 'Auto join mode' (Enabled), 'Terminal access' (Disabled), 'LED display' (Enabled), and 'TFTP Dump Server' (0.0.0.0). The 'DHCP Server' section includes 'Domain name', 'DNS Server(s)', and 'Lease time' (Minutes). A 'Hide advanced options' link is at the bottom left, and 'OK' and 'Cancel' buttons are at the bottom right.

2. Enter a name for the Virtual Controller in the **Name** text box.
3. Enter the appropriate IP address in the **Virtual Controller IP** text box.

Configuring the DHCP Server

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

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** window, select the **General** tab.
3. Enter the domain name of the client in the **Domain name** text box.
4. Enter the IP addresses of the DNS servers 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 74 *Configuring the DHCP Server*

The screenshot shows a 'Settings' dialog box with a purple header and a 'Help' link. Below the header is a tabbed interface with tabs for 'Basic', 'Admin', 'RTLS', 'SNMP', 'ARM', 'Radio', 'Enterprise Domains', 'Walled Garden', and 'Advanced'. The 'Basic' tab is active. The configuration fields are as follows:

- Name:
- Virtual Controller IP:
- Date & Time section:
 - NTP Server:
 - Timezone:
- DHCP Server section:
 - Domain name:
 - DNS Server(s):
 - Lease time:

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

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

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 Virtual Controller (the client certificate must be signed by a known CA) before the user name is checked on the authentication server.

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



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

External RADIUS Server

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

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

The following authentication methods are supported in Alcatel-Lucent Instant network:

Authentication Terminated on OAW-IAP

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



PEAP-MS-CHAPv2 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.

The following EAP-Type methods are described below:

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

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

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

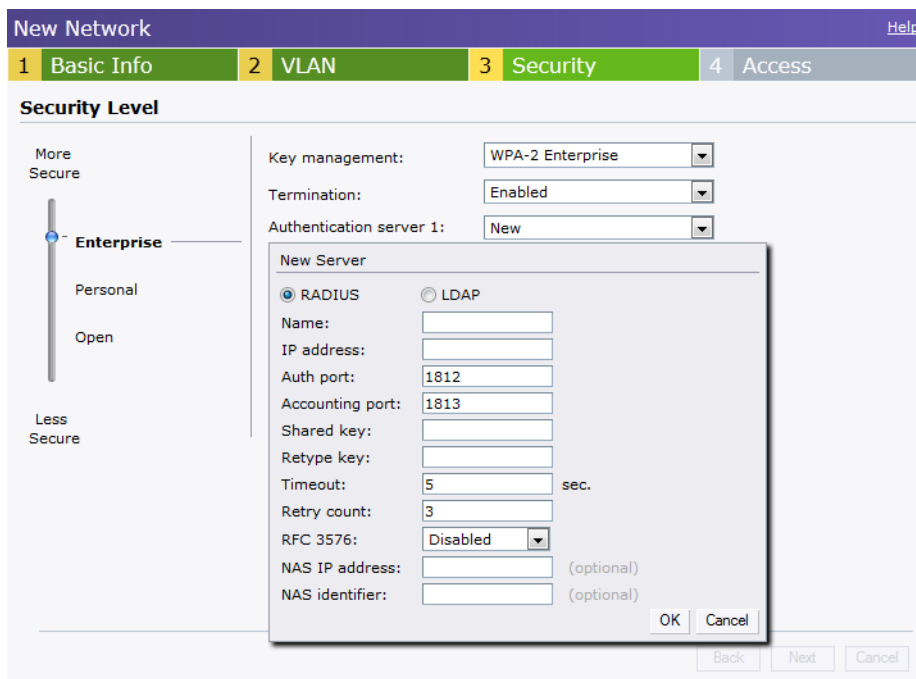
Configuring an External RADIUS Server

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

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

- Name— Enter the name of the new external RADIUS server.
- IP address— Enter the IP address of the external RADIUS server.
- Auth port— Enter the authorization port number of the external RADIUS server. The port number is set to 1812 by default.
- Admin-DN— Enter a Distinguished Name for the admin user who has read/search privileges across all the entries in the LDAP database. The user may not have write privileges but will be able to search the database, and read attributes of the other users in the database.
- Admin password— Enter a admin password.
- Base-DN— Enter a Distinguished Name of the node which contains the entire user database.
- Filter— Indicates the filter that should be applied to search for the user in the LDAP database. The default filter string is (objectclass=*).
- Key Attribute— Indicates the attribute that should be used as a key in search for the LDAP server. For Active Directory, the value is sAMAccountName.
- Timeout— Enter a value between 1 and 30 seconds. The default value is 5.
- Retry count— Enter a value between 1 and 5. The default value is 3.

Figure 75 *Configuring an External RADIUS Server*



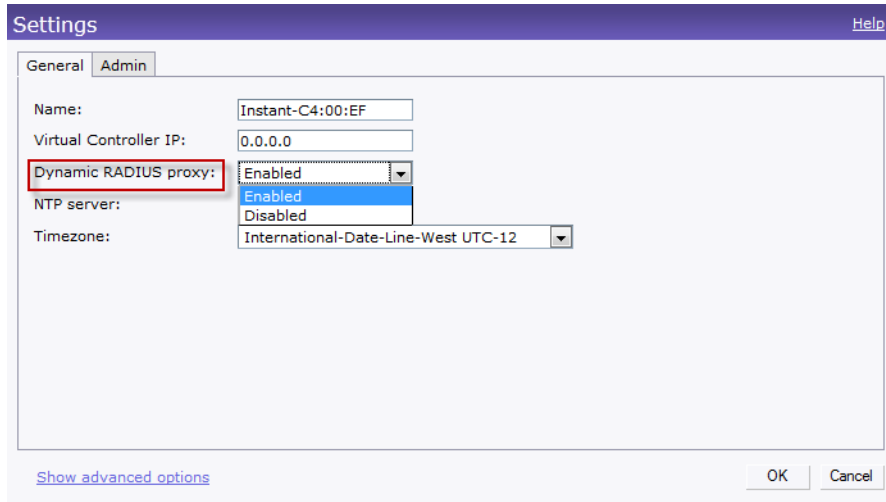
5. Click **OK** after updating the fields.
6. **Reauth interval** — When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients.
7. **Blacklisting**— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures.
8. **Max authentication failures**— Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10.
Navigate to **PEF > Blacklisting** in the WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.
9. **For Internal users**— Click **Users** to populate the system’s internal authentication server with users. For information about adding a user, see “[Adding a User](#)” on page 217.
10. Click **Next** to continue and then click **Finish**.

Enabling Instant RADIUS

To enable Instant RADIUS, perform the following steps:

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

Figure 76 Enabling Instant RADIUS



3. 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

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

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

1. Navigate to the **Settings** link in the Instant UI.
2. Select the **Admins** tab.
3. In the **Authentication** drop-down list, select any one of the following:
 - **Internal**— Select to specify a single set of user credentials. Enter the **Username** and **Password** for accessing the Virtual Controller Management User Interface.
 - **RADIUS Server**— Specify one or two radius servers to authenticate UI. If two servers are configured users can use them in primary/backup mode or load-balancing mode, this is identical to the radius server configuration for SSIDs. For information on configuring external RADIUS server, see “[External RADIUS Server](#)” on page 100.
 - **RADIUS server w/ fallback to internal**— Specify the radius servers as well as a Username and Password. If there is no response from the RADIUS server (RADIUS server timeout), the authentication will switch to **Internal**.

Figure 77 Management Authentication Settings

The screenshot shows the 'Settings' window with the 'Admins' tab selected. The 'Local' authentication section is highlighted with a red box. It contains the following fields:

- Authentication: Internal (dropdown menu)
- Username: admin (text input)
- Password: masked with dots (password input)
- Retype: masked with dots (password input)

Below the Local section, there are fields for 'OmniVista 3600':

- Organization: (text input)
- OmniVista 3600 IP: (text input)
- Shared key: (text input)
- Retype: (text input)

At the bottom of the window, there is a 'Show advanced options' link and 'OK' and 'Cancel' buttons.

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 217](#).
- **Internal Acknowledged**— To gain access to the wireless network, a user must accept the terms and conditions.

Configuring Internal Captive Portal Authentication when Adding a Guest Network

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

1. In the **Network** tab, click the **New** link. The **New Network** window opens.
2. In the **Basic Info** tab, perform the following:
 1. Enter a name for the network in the **Name (SSID)** text box.
 2. Click **Guest** and click **Next**.
3. Use the **VLAN** tab, to specify how the clients on this network will get their IP address and VLAN. Click **Next** to continue.
4. In the **Security** tab, select one of the following options for the splash page type:
 - a. **Internal — Authenticated**
 - b. **Internal — Acknowledged**
 - c. **External**
 - d. **None**

See [“Guest Network” on page 63](#) for more information on the splash page type options.

Figure 78 Configuring Captive Portal when Adding A Guest Network

The screenshot shows the 'New Network' configuration interface with the 'Security' tab selected. The 'Security Level' section includes the following settings:

- Splash page type: Internal - Authenticated
- Auth server 1: InternalServer
- Reauth interval: 0 min.
- Blacklisting: Enabled
- Max auth failures: 0
- Internal server: No users (with a [Users](#) link)
- Internal server: No certificate (with an [Upload certificate](#) link)
- Encryption: Disabled

The 'Splash Page Visuals' section displays a preview of the splash page with the text 'Welcome to the Guest Network.' and two thumbnails for editing. Below the preview, it says 'Click thumbnail above to edit' and includes a [Preview](#) link. At the bottom of the page 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 110.

5. Select **InternalServer** from the **Auth server** 1 drop-down list to authenticate user credentials at run time.
6. **Reauth interval** — When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients.
7. **Blacklisting** — Select Enabled if you want clients to be blacklisted after a certain number of authentication failures.
8. **Max authentication failures** — Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10.
9. **For Internal users** —Click [Users](#) to populate the system’s internal authentication server with users. For information about adding a user, see “Adding a User” on page 217”.
10. Click **Next** and click **Finish**.

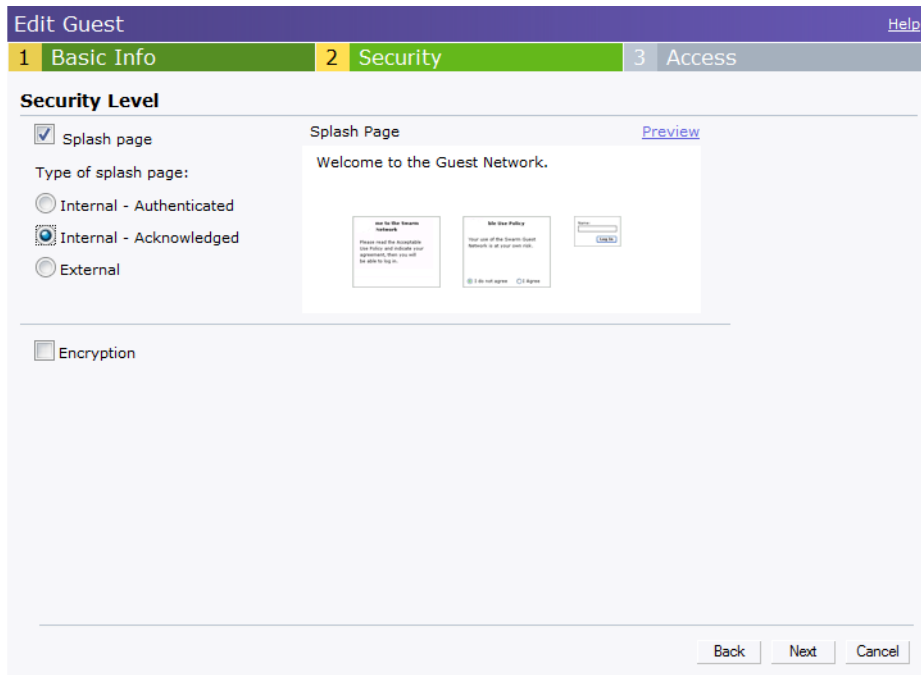
Configuring Internal Captive Portal Authentication when Editing a Guest Network

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

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

See “Guest Network” on page 63 for more information.

Figure 79 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 110.

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** window opens.
2. In the **Basic Info** tab, perform the following:
 1. Enter a name for the network in the **Name (SSID)** text box.
 2. Select **Guest** and then click **Next**.
3. Use the **VLAN** tab, to specify how the clients on this network will get their IP address and VLAN. Click **Next** to continue.
4. In the **Security** tab, select **Internal — Authenticated** under the splash page type.
5. Select an external RADIUS server from the Authentication server drop-down list to authenticate user credentials at run time. If there is no external RADIUS server in the drop-down list, click **New** to add a RADIUS server. For information on configuring external RADIUS server, see “External RADIUS Server” on page 100.
6. Click **Next** and then click **Finish**.

Figure 80 Configuring Internal Captive Portal with External Radius Server Authentication

The screenshot shows the 'New Network' configuration interface with the 'Security' tab selected. The 'Security Level' section contains the following settings:

- Splash page type: Internal - Authenticated
- Auth server 1: InternalServer
- Reauth interval: 5 min.
- Blacklisting: Enabled
- Max auth failures: 0
- Internal server: No users (with [Users](#) link)
- Internal server: No certificate (with [Upload certificate](#) link)
- Encryption: Disabled

The 'Splash Page Visuals' section displays a preview of the splash page with the text 'Welcome to the Guest Network.' and two policy boxes. Below the preview, there is a 'Click thumbnail above to edit' instruction and a [Preview](#) link. At the bottom of the page, there are 'Back', 'Next', and 'Cancel' buttons.

Customizing a Splash Page

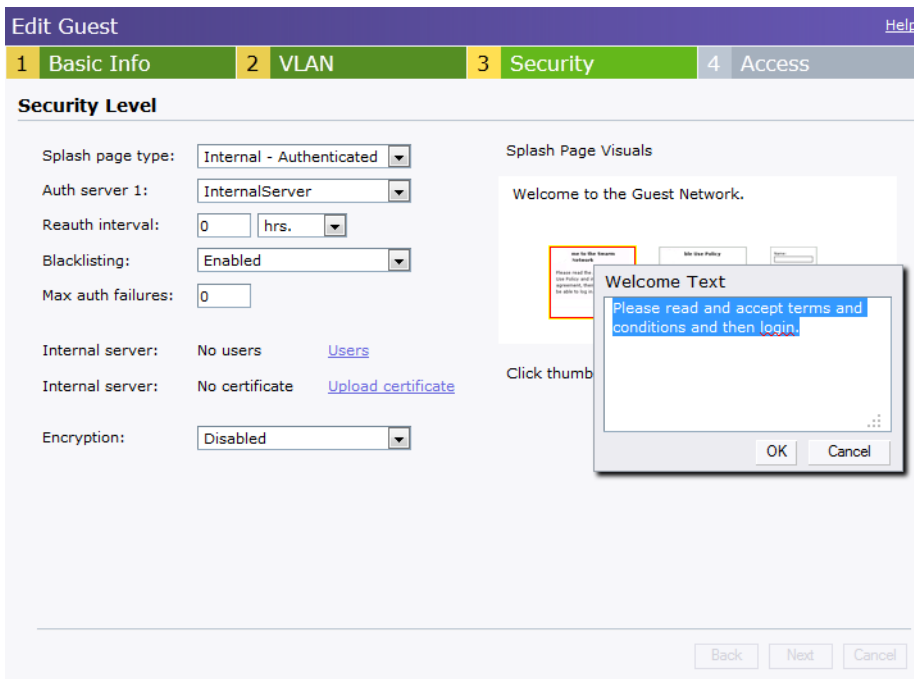
A splash page is a web page that is displayed to a guest user when they are trying to access the internet. The appearance of a splash page can be customized as required. To customize a splash page, perform the following steps:



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

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



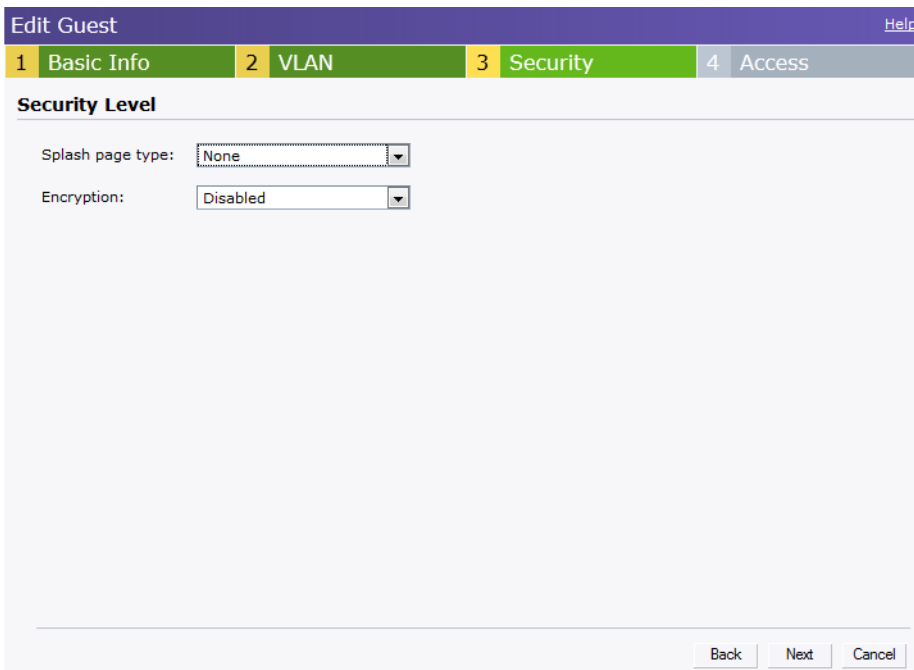
4. Click **Next** and then click **Finish**.

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

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

Figure 82 Disabling Captive Portal Authentication



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

External Captive Portal

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

Configuring External Captive Portal Authentication when Adding a Guest Network

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

1. In the **Network** tab, click the **New** link. The **New Network** window appears.
2. In the **Basic Info** tab, perform the following:
 1. Enter a name for the network in the **Name (SSID)** text box.
 2. Select **Guest** and click **Next** to continue.
3. Use the **VLAN** tab to specify how the clients on this network will get their IP address and VLAN. Click **Next** to continue.
4. In the **Security** tab, select **External** from the Splash page type drop-down list and perform the following steps:
 1. **IP or hostname:** Enter the IP address or the hostname of the external splash page server.
 2. **URL:** Enter the URL for the external splash page server.
 3. **Port:** Enter the number of the port to be used for communicating with the external splash page server.
 4. **Authentication text:** Indicates the text string returned by the external server after a successful authentication. This entry is not mandatory.

Figure 83 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 visible, containing the following fields and options:

- Splash page type: External (dropdown)
- Auth server 1: -- Select Server -- (dropdown)
- Auth server 2: -- Select Server -- (dropdown)
- Reauth interval: 0 min. (input and dropdown)
- Blacklisting: Enabled (dropdown)
- Max auth failures: 0 (input)
- Walled garden: Blacklist: 0 Whitelist: 0 (text)
- Encryption: Disabled (dropdown)
- External splash page: IP or hostname: (input)
- URL: (input)
- Port: (input)
- Authentication text: (input)

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

5. **Authentication server 1:** Select **New** and update the fields for the external RADIUS server to authenticate user credentials at runtime. Refer to “[Configuring an External RADIUS Server](#)” on page 101 for more details on server settings.

6. **Reauth interval** — When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients.
7. **Blacklisting**— Select Enabled if you want clients to be blacklisted after a certain number of authentication failures.
8. **Max authentication failures**— Users who fail to authenticate the number of times specified here will be dynamically blacklisted. The maximum value for this entry is 10.
Navigate to **PEF > Blacklisting** in the WebUI to specify the duration of the blacklisting on the Blacklisting tab of the PEF window.
9. **Walled garden** — Click on the link to open the **Walled Garden** window. The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites. For more information, see [“Walled Garden Access” on page 117](#).
10. Click **Next** to continue and then click **Finish**.

Configuring External Captive Portal Authentication when Editing a Guest Network

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

1. In the **Network** tab, click the network for which you want to configure the external captive portal authentication. The **edit** link for the network appears.
2. Click the **edit** link. The **Edit** window for the network appears.
3. Navigate to the **Security** tab and perform the following steps:
4. Select **External** from the **Splash page type** drop down list.
5. Use the fields below to specify/edit the server for this guest network's splash page.
 1. **IP or hostname:** Enter the IP address or the hostname of the external splash page server.
 2. **URL:** Enter the URL for the external splash page server.
 3. **Port:** Enter the number of the port to be used for communicating with the external splash page server.
 4. **Authentication text:** Indicates the text string returned by the external server after a successful authentication.

Figure 84 Configuring External Captive Portal Authentication when Editing a Guest Network

The screenshot shows the configuration interface for 'SYSTEM_AMIGOPOD' in the 'Security Level' tab. The 'Auth server 1' is set to 'AMIGOPOD'. A modal dialog for editing the 'AMIGOPOD' server is open, showing the following fields: IP address (10.65.50.245), Auth port (1812), Accounting port (1813), Shared key (masked), Retype key (masked), Timeout (5 sec), Retry count (3), RFC 3576 (Enabled), NAS IP address (10.64.146.174), and NAS identifier. The main page also shows 'External splash page' settings: IP or hostname (10.65.50.245), path (/aruba.php), and port (80). Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom right.

6. **Authentication server 1:** Click **Edit** to modify the external RADIUS servers settings. Refer to “Configuring an External RADIUS Server” on page 101 for more details on server settings.
7. **Reauth interval**— When set to a value greater than zero, the Access Points will periodically reauthenticate all associated and authenticated clients.
8. **Accounting**— When enabled, the Access Points will post accounting information as RADIUS START and RADIUS STOP accounting records to the RADIUS server.
9. Click **Next** and click **Finish**.

External Captive Portal Authentication using Amigopod

You can now configure Instant to point to Amigopod as an external Captive Portal server. User authentication is performed by:

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

Creating a Web Login page in the Amigopod

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

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

Configuring the RADIUS Server in Instant

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

1. Navigate to the **Networks** tab in the UI, click the **New** link. The **New Network** window appears.
2. In the **Basic Info** tab, perform the following steps:
 - a. Type a name for the network in the **Name (SSID)** text box. Example: ECP
 - b. Select **Guest** from the **Primary usage** options.
3. Click **Next** to continue.
4. Use the **VLAN** tab, to specify how the clients on this network will get their IP address and VLAN. Click **Next** to continue.
5. In the **Security** tab, select **External** and update the following fields.
 - a. Enter the IP address of the Amigopod server in the **IP or hostname** field. The IP address is **10.65.77.245**.
 - b. Enter **/page_name.php** in the **URL** field. This URL must correspond to the **Page Name** configured in the Amigopod RADIUS Web Login page. For example, if the Page Name is **alcatel-lucent**, then the URL should be **/alcatel-lucent.php** in the Instant UI.
 - c. Enter the **Port** number (generally should be **80**). The Amigopod server uses this port for HTTP services.
 - d. To create an external RADIUS server, select **New** from the **Authentication server 1** drop-down list. Refer to “[Configuring an External RADIUS Server](#)” on page 101 to update the RADIUS server fields.
6. The new network appears in the **Networks** tab. Click the wireless network icon and select the new network.
7. Open any browser and type any URL. Instant redirects the URL to Amigopod login page.
8. Login to the network with the username and password specified used while configuring the RADIUS server in [step d](#).

MAC Authentication

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

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

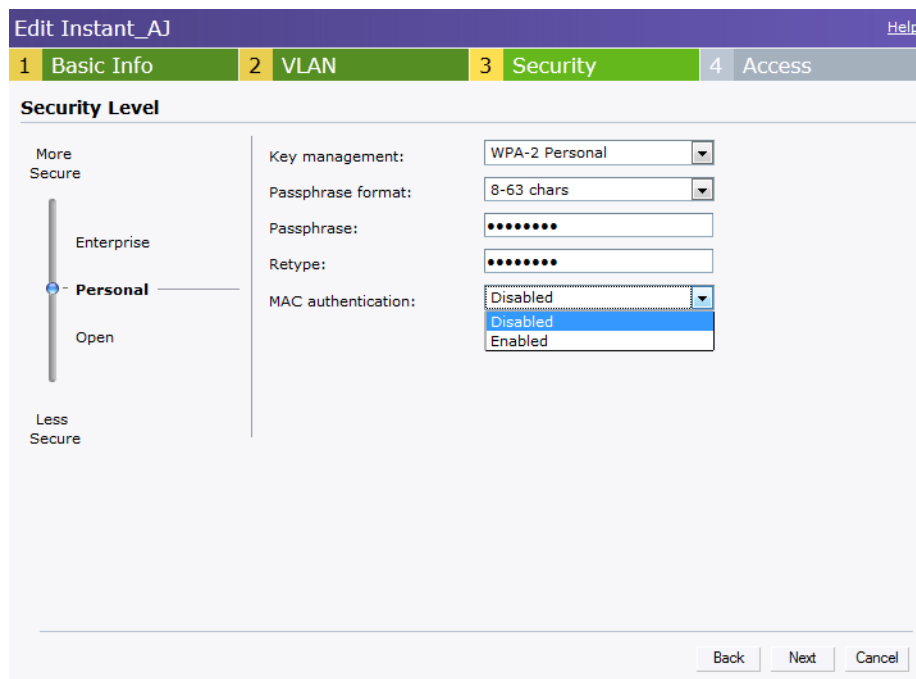
Configuring MAC Authentication

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 and navigate to the **Security** tab.

3. For a network with **Personal** or **Open** security level, select **Enabled** from the **MAC Authentication** drop-down list.
4. Select **New** from the **Authentication server 1** drop-down list perform the following steps:
 - a. **Name:** Enter the name of the new external RADIUS server.
 - b. **IP address:** Enter the IP address of the external RADIUS server.
 - c. **Auth port:** Enter the authorization port number of the external RADIUS server. The port number is set to 1812 by default.
 - d. **Accounting port:** Enter the accounting port number. This port is used to send accounting records to the RADIUS server. The port number is set to 1813 by default
 - e. **Shared key:** Enter a shared key for communicating with the external RADIUS server.
 - f. **Timeout:** Specify a number between 1 and 30 seconds. User will be disconnected after this time. The default value is 5 seconds.
 - g. **Retry count:** Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to server group, and the default value is 3 requests.
 - h. **RFC 3576:** When enabled, the Access Points will process RFC 3576-compliant Change of Authorization (CoA) and Disconnect messages from the RADIUS server. Disconnect messages cause a user session to be terminated immediately, whereas CoA messages modify session authorization attributes such as data filters.
 - i. **NAS IP address:** Enter the Virtual Controller IP address. The NAS IP address is the Virtual Controller IP address that is sent in data packets.
 - j. **NAS identifier:** Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
5. Click **OK** to continue.

Figure 85 *Configuring MAC Authentication*



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

Walled Garden Access

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

Creating a Walled Garden Access

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

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

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

Figure 86 *Walled Garden*



To create a Walled Garden access:

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

specified in blacklist is accessed by an unauthenticated user, Instant AP will send an HTTP 403 response to the client with a simple error message.

If the requested URL neither appears on the blacklist or whitelist list then the request is redirected to the external captive portal.

4. Select the domain name/URL and click **Edit** to modify or **Delete** to remove the entry from the list.
5. Click **OK** to apply the changes.

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 the following certificate files:

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

There are two ways to upload the certificates.

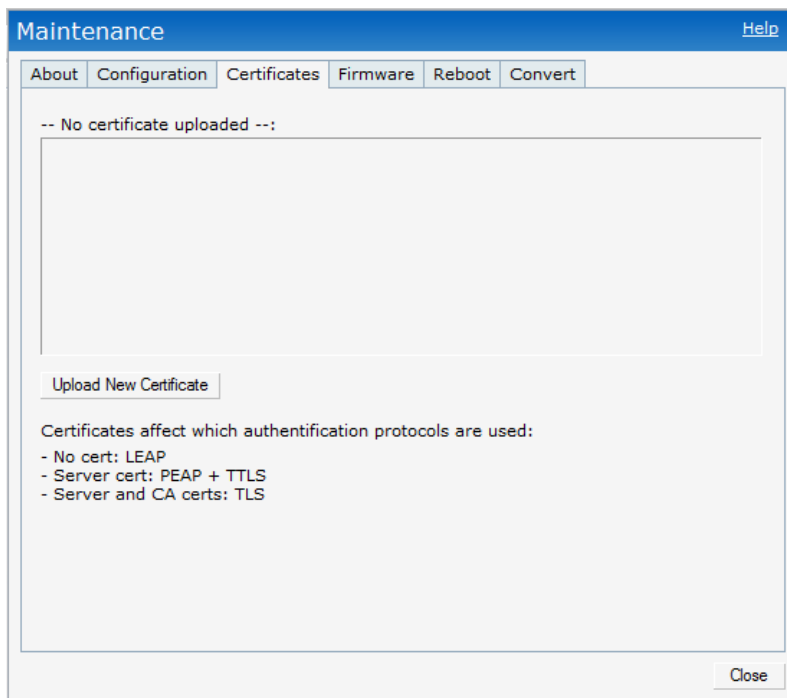
1. **Instant WebUI:** Navigate to **Maintenance > Certificates** and then click **Upload New Certificate** to directly upload the certificate. Refer [Loading Certificates using Instant WebUI](#) for further instructions.
2. **OmniVista:** Navigate to **Device Setup > Certificate** and then click **Add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

Loading Certificates using Instant WebUI

To load a certificate in the Instant UI, perform the following steps:

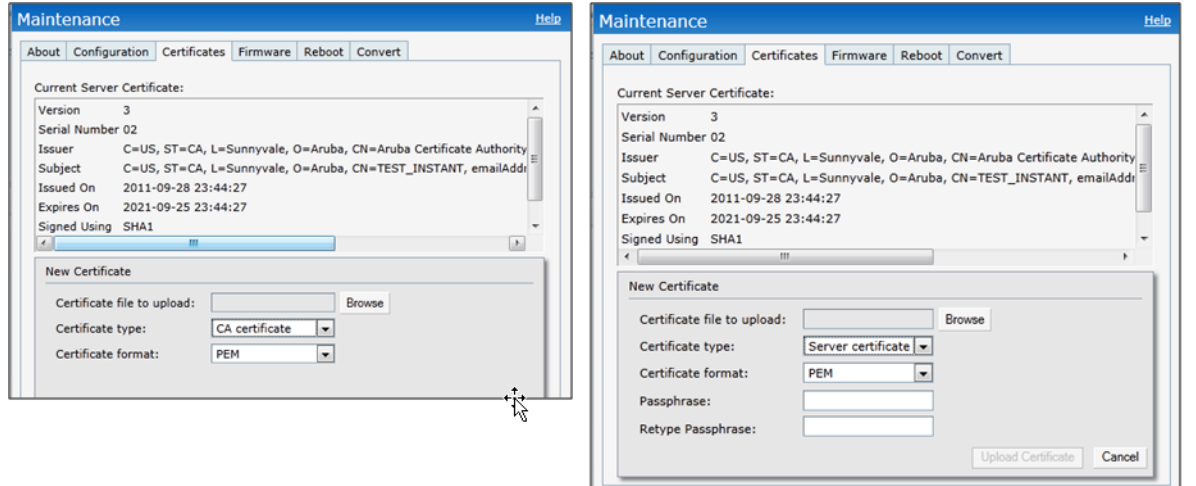
1. Navigate to the **Maintenance > Certificates** page.

Figure 87 Loading Certificates



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

Figure 88 *New Certificate*



3. Select the **Certificate type**— **CA certificate** and **Server certificate** from the drop-down list. The CA certificate is required to validate the client's certificate and the server certificate verifies the server's identity to the client.
4. Select the certificate format from the **Certificate format** drop-down list.
5. If you have selected **Server certificate** type, then enter a passphrase in **Passphrase** and reconfirm. The default password is **whatever**.
6. Click **Browse** and select the appropriate certificate file, and click **Upload Certificate**.
7. The **Certificate Successfully Installed** window will appear.

Loading Certificates using OmniVista

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

To load a certificate in OmniVista, perform the following steps:

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

Figure 89 Loading Certificate via OmniVista

The screenshot shows the 'Certificate' form in the OmniVista web interface. The navigation bar at the top includes 'Home', 'Groups', 'APs/Devices', 'Clients', 'Reports', 'System', 'Device Setup', and 'AMP Setup'. Below this, a secondary bar contains 'Discover', 'Add', 'Communication', 'Upload Firmware & Files', and 'Certificate'. The main form area is titled 'Certificate' and contains the following fields: 'Name' (empty), 'Certificate File' (with a 'Choose File' button and 'No file chosen' text), 'passphrase' (empty), 'Confirm passphrase' (empty), 'Format' (dropdown menu set to 'DER'), and 'Type' (dropdown menu set to 'Server Cert'). At the bottom of the form are 'Add' and 'Cancel' buttons.

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

Figure 90 CA Certificate

The screenshot shows the 'Certificate' form in the OmniVista web interface. The navigation bar at the top includes 'Home', 'Groups', 'APs/Devices', 'Clients', 'Reports', 'System', 'Device Setup', and 'AMP Setup'. Below this, a secondary bar contains 'Discover', 'Add', 'Communication', 'Upload Firmware & Files', and 'Certificate'. The main form area is titled 'Certificate' and contains the following fields: 'Name' (text box with 'Test'), 'Certificate File' (with a 'Choose File' button and 'Root.der' text), 'passphrase' (empty), 'Confirm passphrase' (empty), 'Format' (dropdown menu set to 'DER'), and 'Type' (dropdown menu set to 'Intermediate CA'). At the bottom of the form are 'Add' and 'Cancel' buttons.

Figure 91 Server Certificate

The screenshot shows the 'Certificate' form in the OmniVista web interface. The navigation bar at the top includes 'Home', 'Groups', 'APs/Devices', 'Clients', 'Reports', 'System', 'Device Setup', and 'AMP Setup'. Below this, a secondary bar contains 'Discover', 'Add', 'Communication', 'Upload Firmware & Files', and 'Certificate'. The main form area is titled 'Certificate' and contains the following fields: 'Name' (text box with 'Test1'), 'Certificate File' (with a 'Choose File' button and 'Server.p12' text), 'passphrase' (text box with masked characters), 'Confirm passphrase' (text box with masked characters), 'Format' (dropdown menu set to 'PKCS#12'), and 'Type' (dropdown menu set to 'Server Cert'). At the bottom of the form are 'Add' and 'Cancel' buttons.

4. After you upload the certificate, go to **Groups**, click on the Instant **Group** and then select **Basic**. The Group name will appear, only if you have entered the **Organization** name in the Instant Web UI. Refer [Entering the Organization String and AMP Information into the OAW-IAP](#) for further information.

Figure 92 *Selecting the Group*

Home Groups APs/Devices Clients Reports System Device Setup AMP Setup RAPIDS VisualRF

List

Add New Group

Compare two groups
1-6 of 6 Groups Page 1 of 1 Choose columns Export CSV

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

1-6 of 6 Groups Page 1 of 1

Select All - Unselect All

Delete

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

Figure 93 *Virtual Controller Certificate*

Home Groups APs/Devices Clients Reports System Device Setup AMP Setup RAPIDS VisualRF

List Monitor Basic Templates Firmware

Group: Test_2

Basic

Name: Test_2

Missed SNMP Poll Threshold (1-100): 1

Regulatory Domain: United States

Timezone: AMP system time

Allow One-to-One NAT: Yes No

Audit Configuration on Devices: Yes No

SNMP Polling Periods

Up/Down Status Polling Period: 5 minutes

Override Polling Period for Other Services: Yes No

AP Interface Polling Period: 10 minutes

Client Data Polling Period: 10 minutes

Thin AP Discovery Polling Period: 15 minutes

Device-to-Device Link Polling Period: 5 minutes

802.11 Counters Polling Period: 15 minutes

Rogue AP and Device Location Data Polling Period: 30 minutes

CDP Neighbor Data Polling Period: 30 minutes

Automatic Authorization

Add New Controllers and Autonomous Devices Location: Use Global Setting

Current Global Setting for Controllers: New Device List

Add New Thin APs Location: Use Global Setting

Current Global Setting for Thin APs: New Device List

Maintenance Windows

Add New AP Group Maintenance Window

Virtual Controller Certificate

CA Cert: Test

Server Cert: Test1

Save Save and Apply Revert

- Click **Save** to apply the changes only to OmniVista. Click **Save and Apply** to apply the changes to the Instant AP.
- Click **Revert** to unselect the certificate options.

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 15](#) 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 15 WPA and WPA2 Features

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

Recommended Authentication and Encryption Combinations

Table 16 summarizes the recommendations for authentication and encryption combinations that should be used in Wi-Fi networks.

Table 16 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.

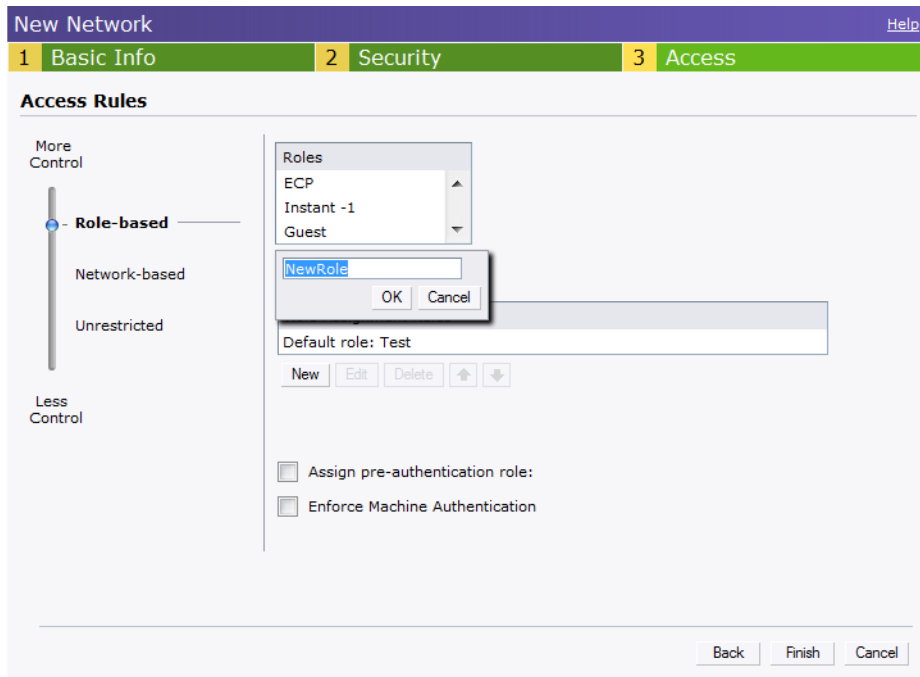
Figure 94 Access Tab - Instant User Role Settings

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 and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network will get their IP address and VLAN. Click **Next** to continue.
4. Click **Next** and set appropriate values in the **Security** tab.
5. Click **Next**. The **Access** tab appears.
6. Slide to **Role-based** using the scroll bar on the left.
7. Click **New**. The **New Rule** window appears. Enter the name of the new user role.

Figure 95 *Creating a New User Role*



8. Click **OK**. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To create new access rules, see [“Examples for Access Rules” on page 138](#).
9. To delete a user role, select the user role and click the **Delete** button.
10. **Assign pre-authentication role**— Use this option if you want to allow some access to users even before they are authenticated.
11. **Enforce Machine Authentication**— You can assign different rights to clients based on whether their hardware device supports machine authentication. Machine Auth is only supported for Windows devices, so this can be used to distinguish between Windows devices and other devices such as ipads.
 - Machine Auth only role - This is the case of a Windows machine with no user logged in. The device supports machine authentication and has a valid RADIUS account, but a user has not yet logged in and authenticated.
 - User Auth only role - This is the case of a known user or a non-Windows device. The device does not support machine auth or does not have a RADIUS account, but the user is logged in and authenticates.

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

To configure Machine Authentication, do the following:

1. In the **Roles** window, create a role for **Machine auth only** and **User auth only**.
2. Configure Access Rules for these roles by selecting the role, and applying the rule. Refer to [“Examples for Access Rules” on page 138](#) for procedures to create access rules.
3. Select **Enforce Machine Authentication** and specify these two roles.
4. Click **Finish** to apply these changes.

Creating Role Assignment Rules

This section has the rules for determining which role will be assigned for each authenticated client.

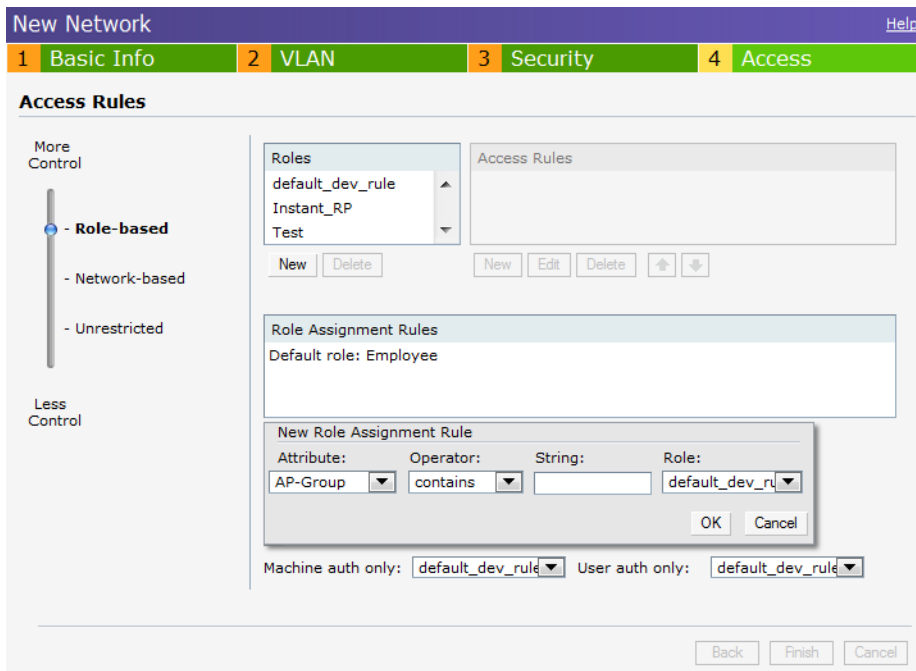


When Enforce Machine Authentication is enabled, both the device and the user must be authenticated for the role assignment rule to apply.

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

1. Click **New** in the **Role Assignment Rules** section of the window. The default user role is the newly created user role.
2. Select the RADIUS attribute from the **Attribute** drop-down list that the rule will match against. To view the list of supported attributes, see “[List of supported VSA](#)” on page 103.
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 96 *Creating Role Assignment Rules*



User VLAN Derivation

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

The user VLAN can be derived in 802.1x authentication or MAC authentication from the following rules:

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

The user VLAN cannot be derived in the following scenarios:

- Captive Portal authentication
- Guest SSID network

Vendor Specific Attributes (VSA)

When an external radius server is used, the user VLAN can be derived from the **Alcatel-Lucent-User-Vlan** VSA. The VSA is then carried in Access-Accept packet from the radius server. The OAW-IAP can analyze the return message and get the value as VLAN to assign the user.

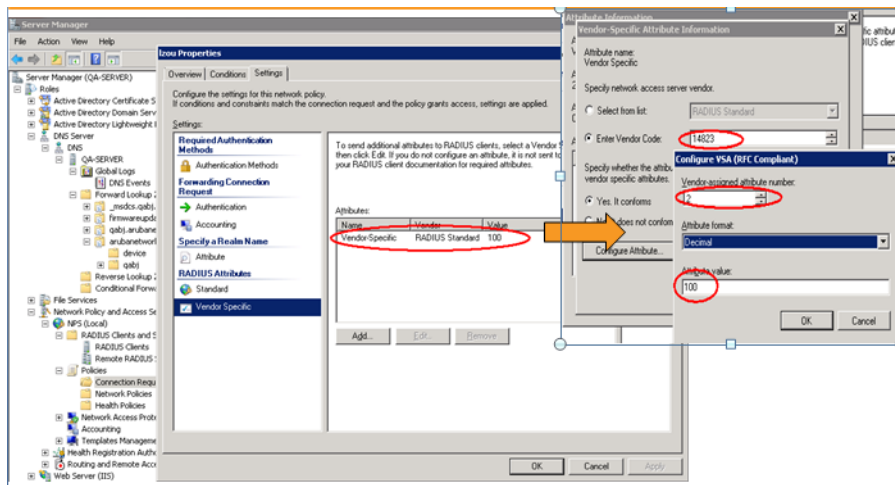
Figure 97 Radius Access—Accept packets with VSA

The image shows a Wireshark capture of RADIUS packets. The packet list pane shows several RADIUS Access-Request and Access-Accept packets. The selected packet is a RADIUS Access-Accept(2) with ID=34 and length=340, sent from 10.65.240.9 to 10.65.13.249. The packet details pane shows the following structure:

- Length: 340
- Authenticator: d28955c253e47fb41f32e73a702089a1
- [This is a response to a request in frame 281]
- [Time from request: 0.000773000 seconds]
- Attribute Value Pairs:
 - AVP: l=12 t=Vendor-Specific(26) v=Aruba(14823)
 - VSA: l=6 t=Aruba-User-Vlan(2): 100
 - AVP: l=7 t=Class(23): 636cd17373
 - AVP: l=10 t=Filter-Id(11): 111234rt
 - AVP: l=6 t=Framed-IP-Address(8): 1.1.1.1
 - AVP: l=6 t=Service-Type(6): Framed(2)
 - AVP: l=5 t=Filter-Id(11): 111

A red box highlights the VSA attribute, and a red arrow points to the text "VSA Aruba-User-Vlan in Radius Access-Accept: Value = 100".

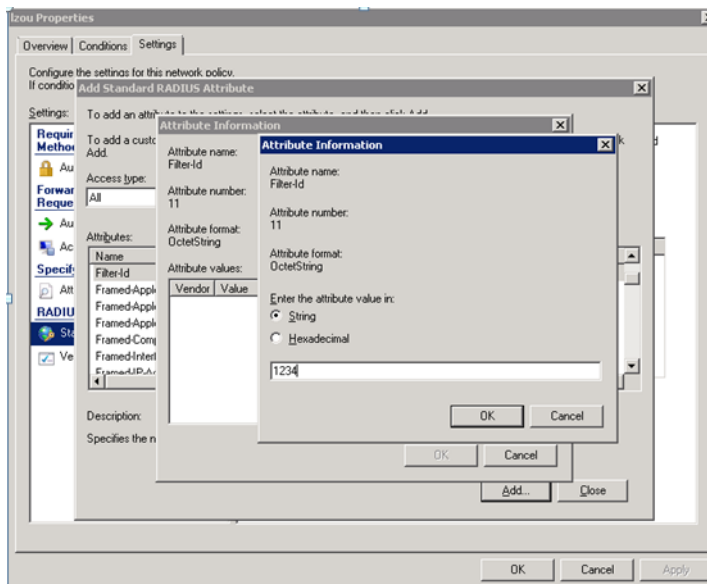
Figure 98 Configure VSA on a Radius Server



VLAN Derivation Rule

When an external radius server is used for authentication, the radius server may return reply message for authentication. If the radius server support return attributes, and set attribute value to reply message, OAW-IAP can analyze the return message and match attributes with user pre-defined vlan derivation rule. If matched we can use rule defined vlan value as vlan to assign user.

Figure 99 Configuring Radius Attributes on the Radius Server



Configuring VLAN Derivation Rules on an OAW-IAP

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

To configure VLAN derivation rules on an OAW-IAP, perform the following steps:

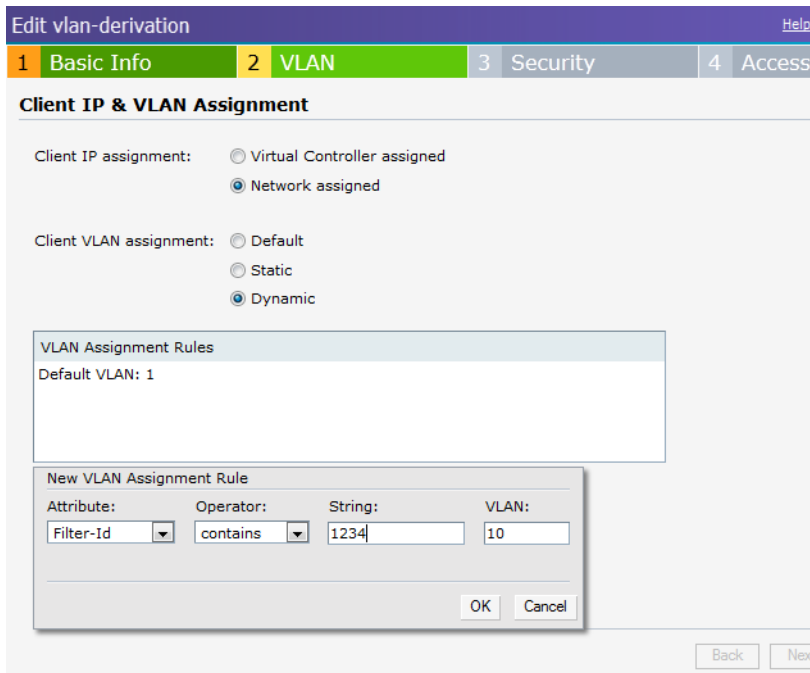
1. Select a network on the Instant UI and click on the **edit** link.
2. Select the **VLAN** tab and check the Dynamic radio button under the **client VLAN assignment**.
3. Click the **New** button to assign the user to a VLAN. The New VLAN Assignment Rule window appears.

Enter the following information:

- **Attribute**— Select the attribute returned by the radius server during authentication.

- **Operator**— Select an operator for matching the string.
 - **String**— Enter the string to match.
 - **VLAN**— Enter the VLAN to be assigned.
4. Click **OK**.

Figure 100 *Configuring VLAN Derivation Rules on an OAW-IAP*



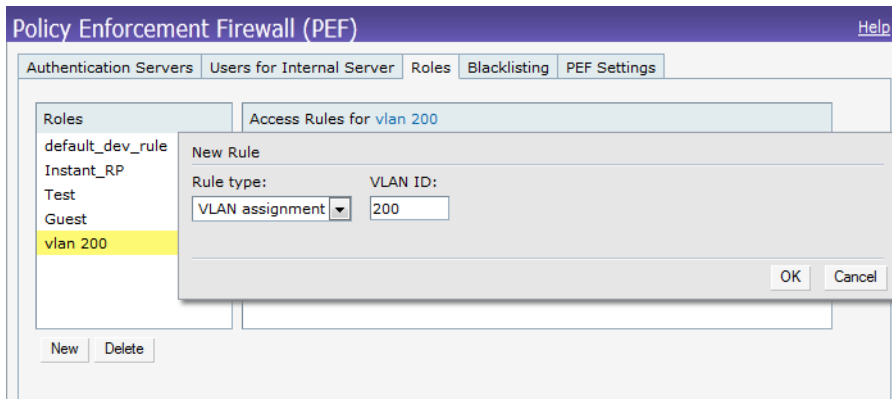
User Role

If the VSA and VLAN derivation rules are not matched the user VLAN can be derived by an user role.

Configuring a User Role

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

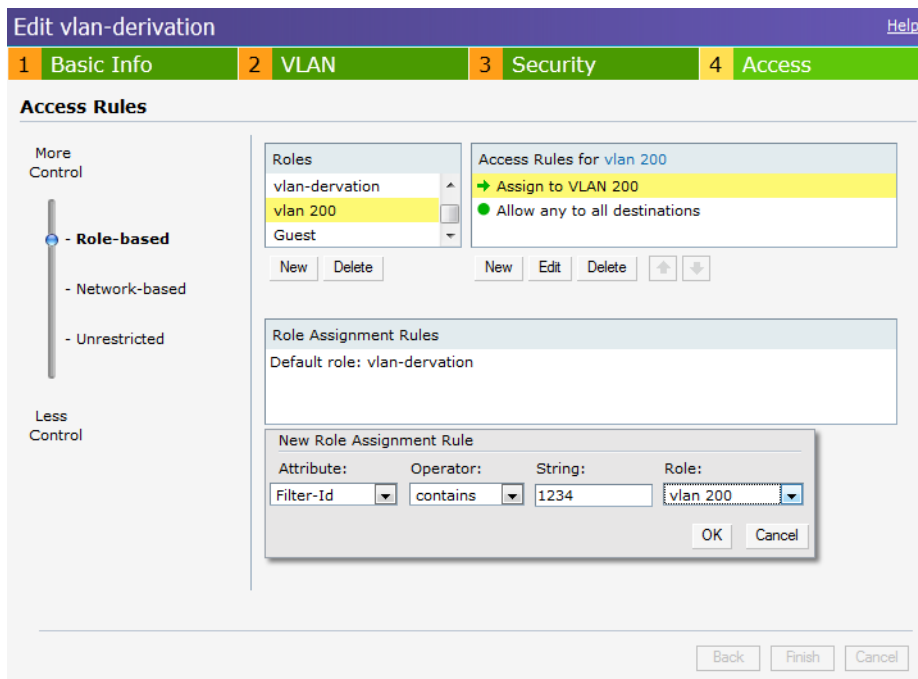
Figure 101 Configuring VLAN Derivation using the User Role



To use a defined user VLAN role, perform the following steps:

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

Figure 102 To Use a Defined User VLAN Role



SSID Profile

If the VSA, VLAN derivation, and the User Role rules are not matched the user VLAN can be derived by the SSID profile.

Configuring VLAN Derivation Rules Using SSID Profile

To configure VLAN derivation rules on an OAW-IAP, perform the following steps:

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

Figure 103 *Configuring VLAN Derivation Rules Using SSID Profile*

The screenshot displays the configuration interface for an Instant UI. The title bar reads "Edit Instant_AJ" with a "Help" link on the right. Below the title bar is a navigation menu with four tabs: "1 Basic Info", "2 VLAN" (which is highlighted in green), "3 Security", and "4 Access". The main content area is titled "Client IP & VLAN Assignment". It contains three sections: "Client IP assignment:" with radio buttons for "Virtual Controller assigned" and "Network assigned" (the latter is selected); "Client VLAN assignment:" with radio buttons for "Default", "Static" (selected), and "Dynamic"; and "VLAN ID:" with a text input field containing the number "252". At the bottom right of the form, there are three buttons: "Back", "Next", and "Cancel".

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.

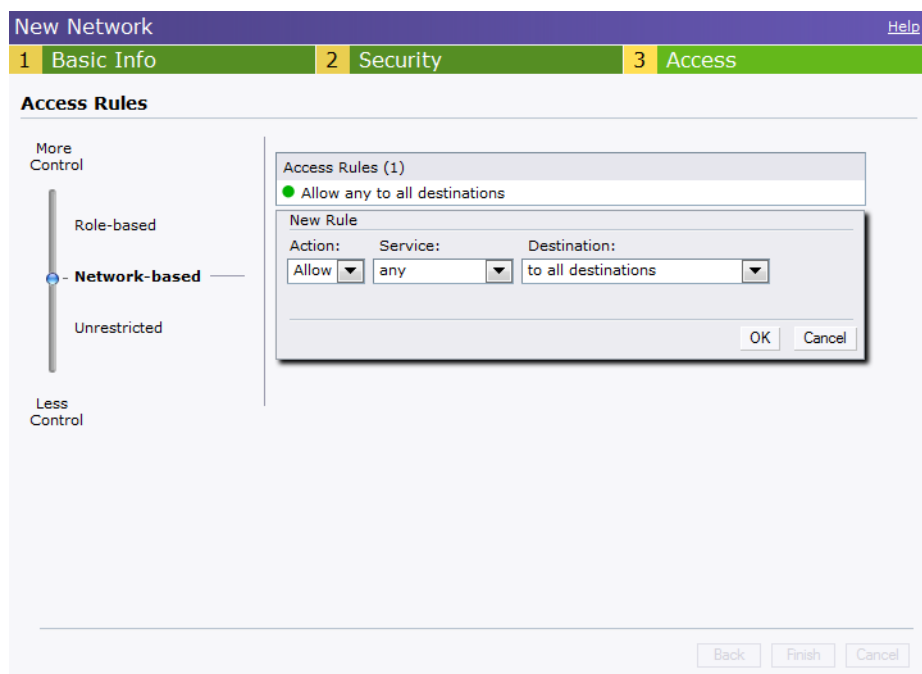
Alcatel-Lucent Instant implements the Instant Firewall feature that uses a simplified firewall policy language. An administrator can define the firewall policies on an SSID or wireless network such as the Guest network or an Employee network. At the end of authentication, these policies are uniformly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

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

The New Rule window consists of the following options:

- **Rule type**— Select the rule type (Access control, VLAN assignment) from the drop-down list.
- **Action**— Select **Allow** or **Deny** from the drop-down list to allow or deny traffic with the specified service type and destination.
- **Log**— Select this checkbox if you want a log entry to be created when this rule is triggered. Instant firewall supports firewall based logging function. Firewall logs on OAW-IAP are generated as syslog messages.
- **Blacklist**— Select this checkbox if you want the client to be blacklisted when this rule is triggered. The blacklisting will last for the duration specified as **Auth failure blacklist** time on the Blacklisting tab of the **PEF** window. See “[Client Blacklisting](#)” on page 205 for more information.

Figure 104 Access Tab - Instant Firewall Settings



Service Options

Table 17 lists the set of service options available in the Instant UI. You can allow or deny access to any or all of these services depending on your requirements.

Table 17 Network Service Options

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

Table 17 Network Service Options (Continued)

Service	Description
netbios-ssn	Network Basic Input/Output System-Session Service
ntp	Network Time Protocol
papi	Point of Access for Providers of Information
pop3	Post Office Protocol 3
pptp	Point-to-Point Tunneling Protocol
rtsp	Real Time Streaming Protocol
sccp	Skinny Call Control Protocol
sip	Session Initiation Protocol
sip-tcp	Session Initiation Protocol-Transmission Control Protocol
sip-udp	Session Initiation Protocol-User Datagram Protocol
smb-tcp	Server Message Block-Transmission Control Protocol
smb-udp	Server Message Block-User Datagram Protocol
smtp	Simple mail transfer protocol
snmp	Simple network management protocol
snmp-trap	Simple network management protocol-trap
svp	Software Validation Protocol
tftp	Trivial file transfer protocol

Destination Options

Table 18 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 18 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.

Table 18 *Destination Options (Continued)*

Destination	Description
Except to a network	Access is allowed or denied to networks other than the specified network. You have to specify the IP address and netmask for the network.

Examples for Access Rules

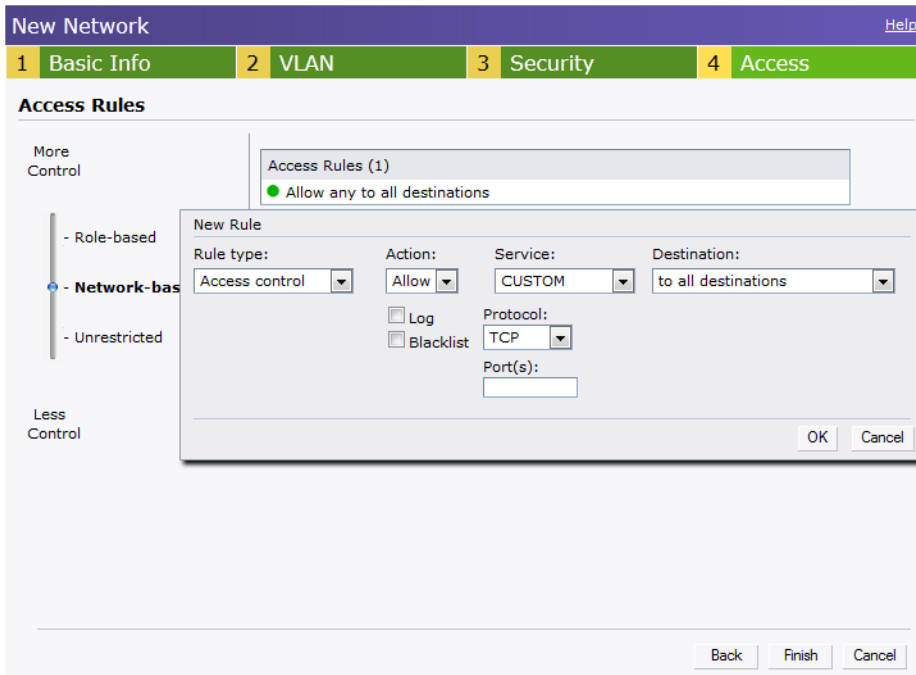
This section provides procedures to create the following access rules.

- Allow TCP Service to a Particular Network
- Allow PoP3 Service to a Particular Server
- Deny FTP Service except to a Particular Server
- Deny bootp Service except to a Particular Network

Allow TCP Service to a Particular Network

1. Click the **New** link in the **Networks** tab.
To define the access rule to an existing network, click the network. The **edit** link appears. Click the **edit** link and navigate to the **Access** tab.
2. In the **Basic Info** tab, enter the appropriate information. and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network will get their IP address and VLAN. Click **Next** to continue.
4. Click **Next** and set appropriate values in the **Security** tab.
5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define allow TCP service access rule to a particular network, perform the following steps:
 - a. Click **New**, the **New Rule** window appears.
 - b. Select **Allow** from the **Action** drop-down list.
 - c. Select **custom** from the **Service** drop-down list.
 - Select TCP from the Protocol drop-down list.
 - Enter appropriate port number in the Port(s) text box.
 - d. Select **to a network** from the **Destination** drop-down list.
 - Enter appropriate IP address in the IP text box.
 - Enter appropriate netmask in the Netmask text box.

Figure 105 *Defining Rule — Allow TCP Service to a Particular Network*

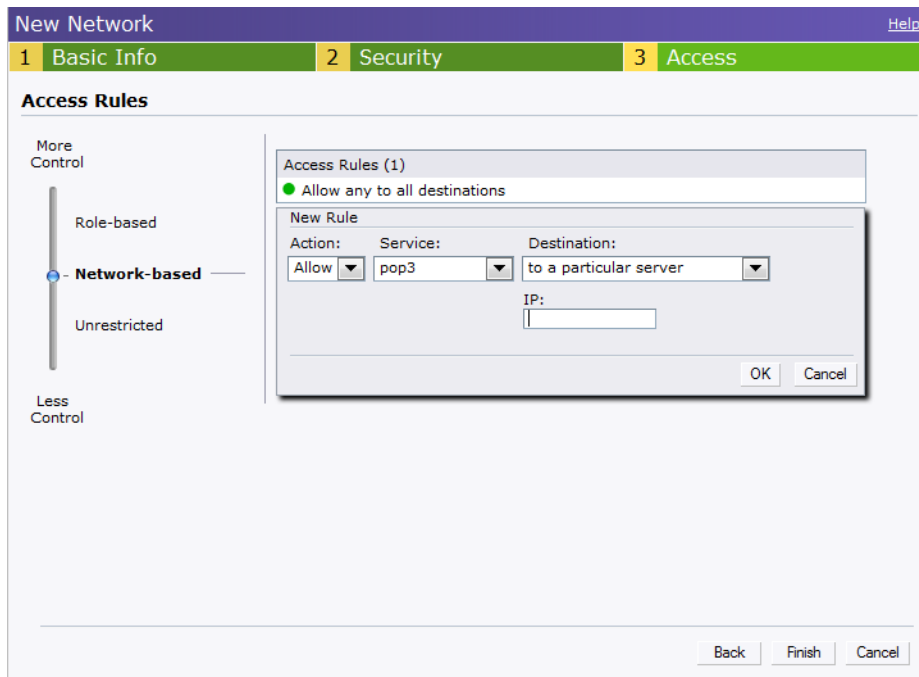


- e. Click **OK**.
6. Click **Finish**.

Allow PoP3 Service to a Particular Server

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

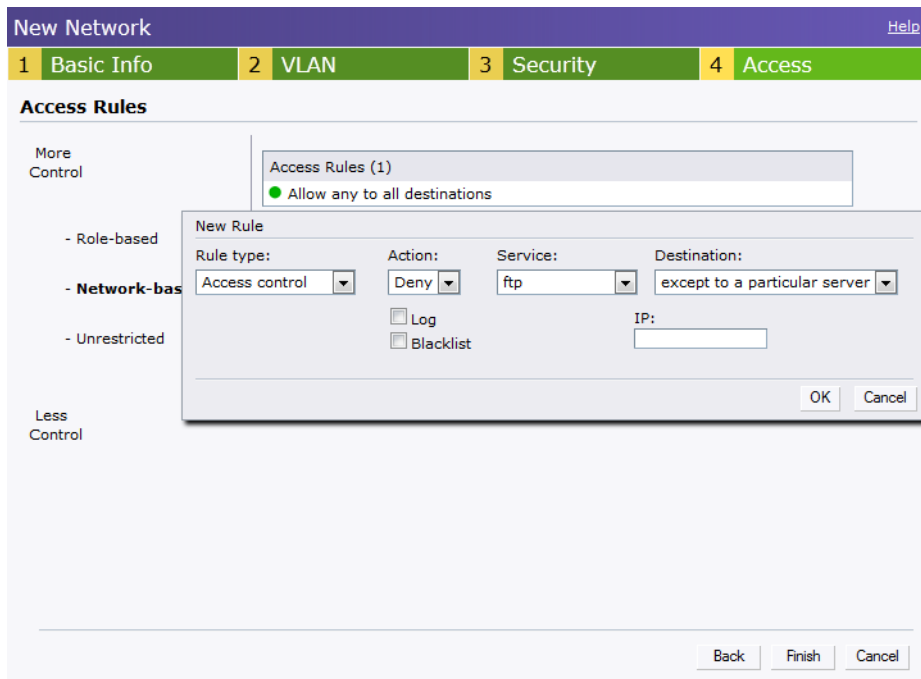
Figure 106 *Defining Rule — Allow POP3 Service to a Particular Server*



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 and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network will get their IP address and VLAN. Click **Next** to continue.
4. Click **Next** and set appropriate security levels using the slider bar in the **Security** tab.
5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define deny FTP service access rule except to a particular server, perform the following steps:
 1. Click **New**, the **New Rule** window 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**
6. Click **Finish**

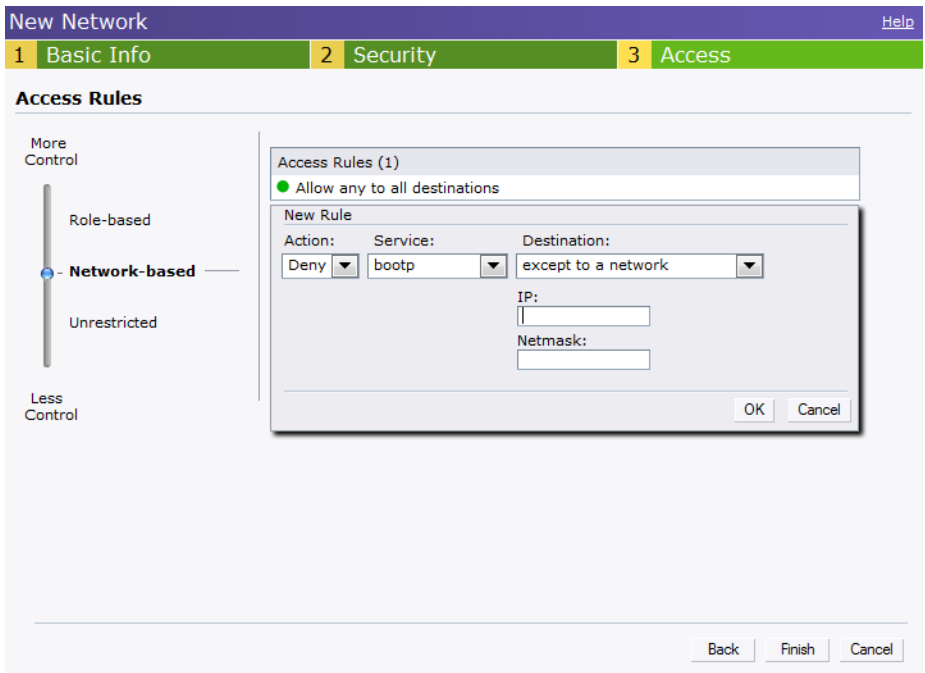
Figure 107 Defining Rule — Deny FTP Service Except to a Particular Server



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. and click **Next** to continue.
3. Use the **VLAN** tab, to specify how the clients on this network will get their IP address and VLAN. Click **Next** to continue.
4. Click **Next** and set appropriate security levels using the slider bar in the **Security** tab.
5. Click **Next**. The **Access** tab appears. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define deny bootp service access rule except to a network, perform the following steps:
 1. Click **New**, the **New Rule** window 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 the appropriate IP address in the IP text box.
 - Enter the appropriate netmask in the Netmask text box.
 5. Click **OK**.
6. Click **Finish**.

Figure 108 *Defining Rule — Deny bootp Service Except to a Network*



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.

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



Regardless of whether content filtering is disabled or enabled, `instant.alcatel-lucent.com` is always resolved internally on Instant.

Enabling Content Filtering

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

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

On startup, the OAW-IAP learns the default domain name via DHCP. This domain name also applies for Content Filtering. Go to **Settings > General > click Show advanced options > DHCP Server > Domain name** to configure a domain name for a Virtual Controller assigned network. This domain name applies for Content Filtering. When you select Virtual Controller assigned option, the client gets the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the OAW-IAPs for the wireless clients, this VLAN is called "virtual controller assigned networks". The Virtual Controller NATs all traffic that passes out of this interface. See “Employee Network” on page 47 to select Virtual Controller assigned option and Chapter 7, “Virtual Controller” on page 96 for DHCP server configuration.

Figure 109 *Enabling Content Filtering*

The screenshot shows the 'New Network' configuration interface with the 'Basic Info' tab selected. The 'Content filtering' dropdown menu is open, showing 'Enabled' selected. Other visible settings include: Name (SSID) 'abc', Primary usage 'Employee', Bandwidth Limits (Percentage of Airtime, Each user, Each radio), Broadcast/Multicast (Multicast optimization: Disabled, Broadcast filtering: Disabled, DTIM interval: 1 beacon), and Transmit Rates (2.4GHz: Min: 1, Max: 54; 5GHz: Min: 6, Max: 54). Buttons for 'Next' and 'Cancel' are at the bottom right.

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.

Enterprise Domains

The Enterprise Domain Names displays all the DNS domain names that are valid on the enterprise network. This list is used to determine how client DNS requests should be routed. When **Content Filtering** is enabled for the wireless network, everything that does not match this list is sent to OpenDNS.

Figure 110 *Enterprise Domains*

The screenshot shows the 'Settings' page with the 'Enterprise Domains' tab selected. The 'Enterprise Domain Names' list is empty. A 'New Domain Name' dialog box is open, showing an input field and 'OK'/'Cancel' buttons. Buttons for 'New' and 'Delete' are also visible. Buttons for 'OK' and 'Cancel' are at the bottom right.

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

1. Navigate to **Settings** at the top right corner of the Instant UI and then select **Enterprise Domains** in the UI.
2. Click **New** and enter a New Domain Name or select the domain and click **Delete** to remove the domain name from the list.
3. Click **OK** to apply the changes.

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:

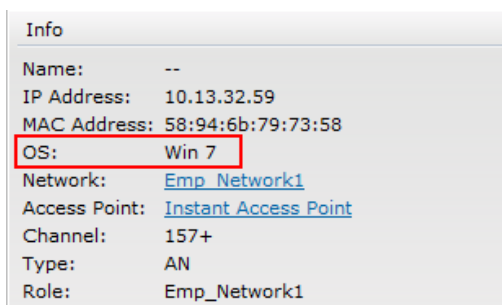
- Identifying rogue clients— Helps to identify clients that are running on forbidden operating systems.
- Identifying outdated operating systems— Helps to locate outdated and unexpected OS in the company network.
- Locating and patching vulnerable operating systems— Assists in locating and patching specific 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 7.

Figure 111 OS Fingerprinting



Info	
Name:	--
IP Address:	10.13.32.59
MAC Address:	58:94:6b:79:73:58
OS:	Win 7
Network:	Emp_Network1
Access Point:	Instant Access Point
Channel:	157+
Type:	AN
Role:	Emp_Network1

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

- **Disabled**— Disabled means that the clients selects which band to use.

Airtime Fairness Mode

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



Ensure to reboot the OAW-IAP after configuring the radio profile settings in order for the changes to take effect.

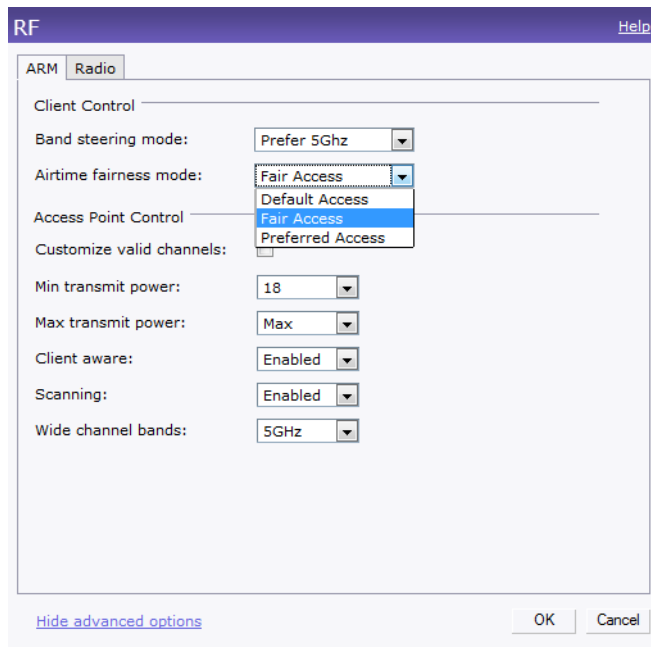
Airtime Fairness Modes

Navigate to **RF** which is at the top right corner of the Instant UI and click **ARM**.

The Airtime fairness consists of the following modes:

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

Figure 112 *Airtime fairness mode*



Access Point Control

Customize Valid Channels

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

Min Transmit Power

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

The default value is 18 dBm.

Max Transmit Power

This indicates the maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. Higher power level settings may be constrained by local regulatory requirements and AP capabilities. In the event that an AP is configured for a Max Tx EIRP setting it cannot support, this value will be reduced to the highest supported power setting.

Default value: 127 dBm

Client Aware

When **Enabled**, Adaptive Radio Management (ARM) will not change channels for the Access points when the clients are active, except for high priority events such as radar or excessive noise. This should be enabled in most deployments for a stable WLAN.

If the Client Aware mode is **Disabled**, the OAW-IAP may change to a more optimal channel, but this change may also disrupt current client traffic.

The Client Aware option is **Enabled** by default



When the Client Aware ARM is disabled, channels can be changed even when the clients are active on BSSID.

Scanning

When ARM is enabled, the OAW-IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and will report everything it sees to the OAW-IAP on each channel it scans. This includes, but is not limited to, data regarding WLAN coverage, interference, and intrusion detection.

Wide Channel Bands

This feature allows administrators to configure 40 MHz channels in the 2.4 GHz and 5.0 GHz bands. 40 MHz channels are essentially two 20 MHz adjacent channels that are bonded together. 40 MHz channel effectively doubles the frequency bandwidth available for data transmission.

Monitoring the Network with ARM

When ARM is enabled, an 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.

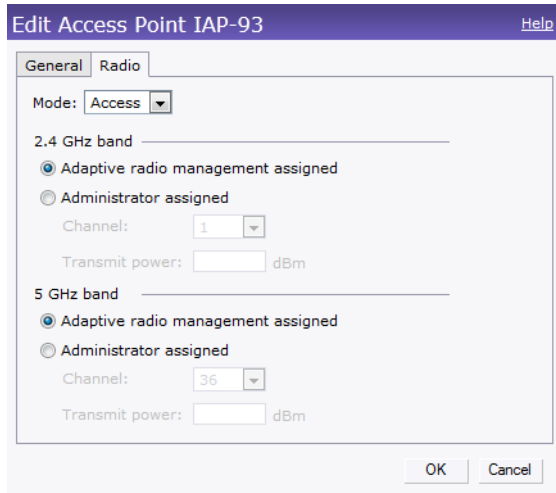
Configuring Administrator Assigned Radio Settings for OAW-IAP

Adaptive Radio Management (ARM) is enabled on Alcatel-Lucent Instant by default. It automatically assigns appropriate channel and power settings for the OAW-IAPs.

To manually configure radio settings, 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** window appears.
3. Click the **Radio** tab.

Figure 113 Configuring Administrator Assigned Radio Settings for OAW-IAP



4. Select the **Access** Mode from the drop-down list.
 - **Access Mode**— In Access mode the AP serves client, while also monitoring for rogue APs in the background.
 - **Monitor Mode**— In Monitor mode the AP acts as a dedicated monitor scanning all channels for rogue APs and clients.

By default the access point's channel and power are optimized dynamically using Adaptive Radio Management (ARM). You can override ARM on the 2.4 GHz and 5 GHz bands and set the channel and power manually if desired.

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

Configuring Radio Profiles in Instant

Alcatel-Lucent Instant supports radio profile configuration. The radio settings are available for both the 2.4-GHz and the 5-GHz radio profiles. You can configure the radios separately, using the parameters described in table on each radio.

Use the following procedure to configure Instant's radio attributes for the 2.4GHz and 5GHz frequency bands.

Figure 114 *Radio Profile*

The screenshot shows the 'RF' configuration window with the 'Radio' tab selected. It displays settings for two frequency bands: 2.4 GHz and 5 GHz. For each band, the following parameters are configured: Legacy only (Disabled), 802.11d / 802.11h (Disabled), Beacon interval (100 ms), Interference immunity level (2), Channel switch announcement count (0), Channel reuse type (Disabled), and Channel reuse threshold (0 dB). A 'Hide advanced options' link is visible at the bottom left, and 'OK' and 'Cancel' buttons are at the bottom right.

1. Navigate to **RF** which is at the top right corner of the WebUI.
2. Click **Show advanced options** to view the **Radio** tab.
3. Refer to the table below to configure the radio settings for bands 2.4GHz and 5GHz.

Table 19 *Radio Profile Configuration Parameters*

Parameter	Description
Legacy only	Enable to run the radio in non-802.11n mode. This is disabled by default.
802.11d / 802.11h	Enable the radio to advertise its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This is disabled by default.
Beacon interval	Enter the Beacon period (60ms to 500ms) for the OAW-IAP in msec. This indicates how often the 802.11 beacon management frames are transmitted by the access point. The default value is 100 msec.

Table 19 Radio Profile Configuration Parameters (Continued)

Parameter	Description
Interference immunity level	<p>Select to increase the immunity level to improve performance in high-interference environments.</p> <p>The default immunity level is 2.</p> <p>NOTE: Increasing the immunity level makes the AP slightly “deaf” to its surroundings, causing the AP to lose a small amount of range.</p> <ul style="list-style-type: none">• Level 0— no ANI adaptation.• Level 1— Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet.• Level 2— Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature.• Level 3— Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4Ghz appliances such as cordless phones.• Level 4— Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference.• Level 5— The AP completely disables PHY error reporting, improving performance by eliminating the time the OAW-IAP would spend on PHY processing.
Channel switch announcement count	<p>Indicates the number of channel switching announcements that must be sent prior to switching to a new channel. This allows associated clients to recover gracefully from a channel change.</p>
Channel reuse type	<p>When set to Dynamic, the access point, when busy, will automatically adjust its Clear Channel Assessment (CCA) threshold to accommodate transmissions to the most distant associated client.</p> <p>When set to Static, the access point will set its CCA threshold to the value specified in Channel reuse threshold.</p>
Channel reuse threshold	<p>When set to Static, this value specifies the tolerable interference that must be maintained.</p>



Ensure to reboot the OAW-IAP after configuring the radio profile settings in order for the changes to take effect.

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.

Navigate to **IDS** in the Instant UI and click the **IDS** link. The built-in IDS scans for access points that are not controlled by this Virtual Controller. These are listed below and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

Figure 115 *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:bd:5f:70	lab_open	Interfering	161	AN 40MZ	11:52:40		00:22:41:0c:a9:fc	ethersphere-voip	Interfering	1	B	11:52:40	
00:24:6c:80:74:00	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40		00:27:10:5c:78:24	ethersphere-voip	Interfering	48	AN 40MZ	11:52:40	
00:0b:86:50:47:48	vjai-test	Interfering	64	A	11:52:40		00:1e:65:79:bc:c6	IBM	Interfering	1	B	11:52:40	
00:0b:86:21:8a:40	aruba-ap	Interfering	1	G	11:52:40		00:26:c6:b7:af:1c	IBM	Interfering	6	B	11:52:40	
00:0b:86:43:d3:a0	UTLab	Interfering	11	G	11:52:40		60:33:4b:15:05:f1	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40	
00:24:6c:07:2b:59	cp-radius	Interfering	149	AN 40MZ	11:52:40		58:94:6b:c5:b8:e4	IBM	Interfering	6	B	11:52:40	
00:1a:1e:17:da:c0	aruba-ap	Rogue	11	GN 20MZ	11:52:40		00:1e:65:71:49:2c	shobha-bridge-65	Interfering	1	GN 20MZ	11:52:40	
00:24:6c:80:74:01	ARUBA-VISITOR	Interfering	1	GN 20MZ	11:52:40		08:11:96:76:1d:1c	IBM	Interfering	6	B	11:52:40	
00:24:6c:84:25:e1	msbrcm	Interfering	1	GN 20MZ	11:52:40		00:26:b0:48:46:20	ARUBA-VISITOR	Interfering	1	B	11:52:40	
00:24:6c:07:2b:5a	cp-radius1	Interfering	149	AN 40MZ	11:52:40		a0:88:04:84:b8:04	IBM	Interfering	1	B	11:52:40	
00:24:6c:80:74:02	indiamdns	Interfering	1	GN 20MZ	11:52:40		58:94:6b:b3:b7:cc	IBM	Interfering	6	B	11:52:40	
00:0b:86:70:4b:60	aruba-ap	Interfering	1	GN 20MZ	11:52:40		00:27:10:8e:4c:60	IBM	Interfering	6	B	11:52:40	
00:24:6c:80:6f:28	ethersphere-wpa2	Interfering	48	AN 40MZ	11:52:40		78:d6:f0:ca:f8:07	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40	
00:24:6c:84:21:08	raj-i-aes	Interfering	36	AN 40MZ	11:52:40		30:7c:30:5e:bc:e2	ethersphere-voip	Interfering	1	B	11:52:40	
00:1a:1e:17:dc:60	ipv6-alpha	Interfering	1	GN 20MZ	11:52:40		58:94:6b:b3:b7:cc	ethersphere-wpa2	Interfering	48	AN 40MZ	11:52:40	
00:24:6c:80:4b:f0	ethersphere-voip	Interfering	6	GN 20MZ	11:52:40		a0:88:04:84:b9:5e:f4	IBM	Interfering	1	G	11:52:40	
00:24:6c:80:4f:88	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40		08:11:96:76:5b:ac	IBM	Interfering	6	B	11:52:40	
00:1a:1e:2d:90:50	Amol CP	Interfering	157	AN 40MZ	11:52:40		00:26:c6:4a:aa:e8	ethersphere-wpa2	Interfering	40	AN 40MZ	11:52:40	
00:1a:1e:17:da:c2	WPA2	Interfering	11	GN 20MZ	11:52:40		00:27:10:45:4a:34	IBM	Interfering	1	B	11:52:40	
00:24:6c:80:6c:60	ethersphere-voip	Interfering	1	GN 20MZ	11:52:40		00:27:10:8e:6a:f4	IBM	Interfering	6	B	11:52:40	
00:0b:86:70:4b:61	Sandin wlan open	Interfering	1	GN 20MZ	11:52:40		18:3d:a2:77:ac:3c	IBM	Interfering	6	B	11:52:40	

Wireless Intrusion Protection (WIP)

WIP offers a wide selection of intrusion detection and protection features to protect the network against wireless threats. Like most other security-related features of the Alcatel-Lucent network, the WIP configuration can be done on the OAW-IAP.

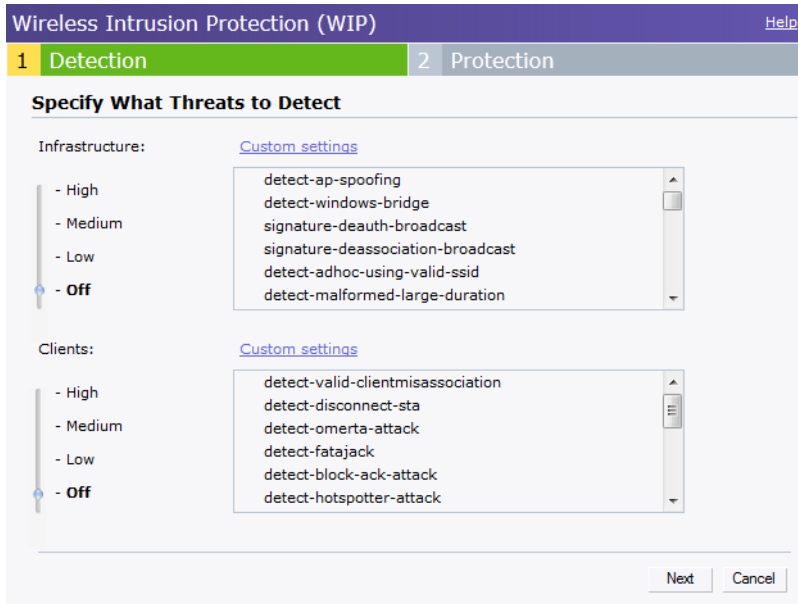
An administrator can configure the following five main options.

- Infrastructure Detection Policies— Specifies which wireless attacks on access points to detect
- Client Detection Policies— Specifies which wireless attacks on clients to detect
- Infrastructure Protection Policies— Specifies which wireless attacks on access points to protect against
- Client Protection Policies— Specifies which wireless attacks on clients to protect against
- Containment Methods— To prevent unauthorized stations from connecting to your Instant network.

In each of these options there are several default levels that enable different sets of policies. An administrator can customize (enable/disable) these options accordingly.

Four levels of detection can be configured in the WIP Detection page— **Off**, **Low**, **Medium**, and **High** (as shown in Figure 116).

Figure 116 *Wireless Intrusion Protection— Detection*



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

Table 20 *Infrastructure Detection Policies*

Detection Level	Detection Policy
Off	Rogue Classification
Low	<ul style="list-style-type: none"> • Detect AP Spoofing • Detect Windows Bridge • IDS Signature— Deauthentication Broadcast • IDS Signature— Disassociation Broadcast
Medium	<ul style="list-style-type: none"> • Detect Adhoc networks using VALID SSID— Valid SSID list will be auto-configured based on Instant AP configuration • Detect Malformed Frame— Large Duration

Table 20 *Infrastructure Detection Policies (Continued)*

Detection Level	Detection Policy
High	<ul style="list-style-type: none">• Detect AP Impersonation• Detect Adhoc Networks• Detect Valid SSID Misuse• Detect Wireless Bridge• Detect 802.11 40MHz intolerance settings• Detect Active 802.11n Greenfield Mode• Detect AP Flood Attack• Detect Client Flood Attack• Detect Bad WEP• Detect CTS Rate Anomaly• Detect RTS Rate Anomaly• Detect Invalid Address Combination• Detect Malformed Frame— HT IE• Detect Malformed Frame— Association Request• Detect Malformed Frame— Auth• Detect Overflow IE• Detect Overflow EAPOL Key• Detect Beacon Wrong Channel• Detect devices with invalid MAC OUI

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

Table 21 *Client Detection Policies*

Detection Level	Detection Policy
Off	All detection policies are disabled.
Low	<ul style="list-style-type: none">• Detect Valid Station Mis association
Medium	<ul style="list-style-type: none">• Detect Disconnect Station Attack• Detect Omerta Attack• Detect FATA-Jack Attack• Detect Block ACK DOS• Detect Hotspotter Attack• Detect unencrypted Valid Client• Detect Power Save DOS Attack
High	<ul style="list-style-type: none">• Detect EAP Rate Anomaly• Detect Rate Anomaly• Detect Chop Chop Attack• Detect TKIP Replay Attack• IDS Signature— Air Jack• IDS Signature— ASLEAP

Three levels of detection can be configured in the WIP Protection page— **Off**, **Low**, and **High** (as shown in Figure 117).

Figure 117 *Wireless Intrusion Protection— Protection*



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

Table 22 *Infrastructure Protection Policies*

Detection Level	Detection Policy
Off	All detection policies are disabled
Low	<ul style="list-style-type: none"> Protect SSID – Valid SSID list should be auto derived from Instant configuration Rogue Containment
High	<ul style="list-style-type: none"> Protect from Adhoc Networks Protect AP Impersonation

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

Table 23 *Client Protection Policies*

Detection Level	Detection Policy
Off	All detection policies are disabled
Low	<ul style="list-style-type: none"> Protect Valid Station
High	<ul style="list-style-type: none"> Protect Windows Bridge

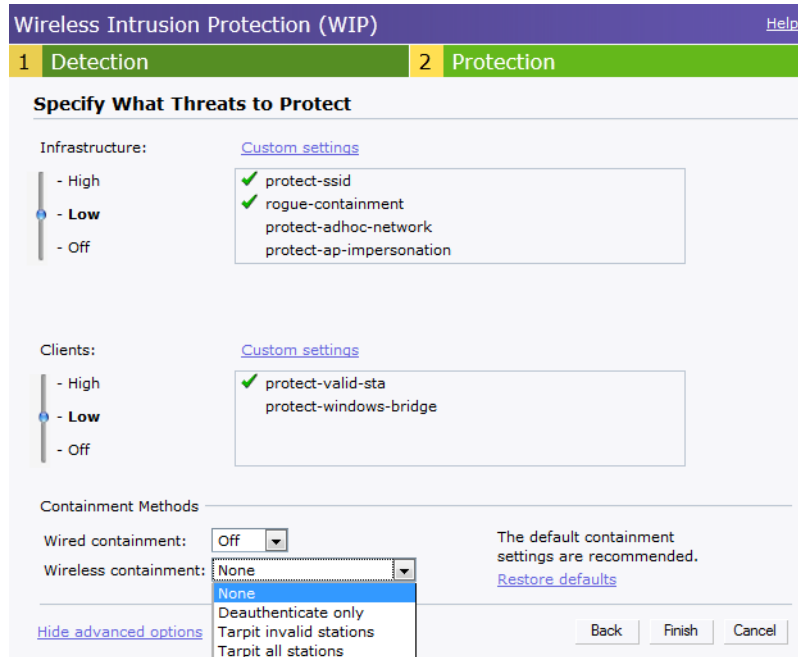
Containment Methods

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

Instant supports the following types of containment mechanisms:

- Wired containment— When enabled, Alcatel-Lucent Access Points will generate ARP packets on the wired network to contain wireless attacks.
- Wireless containment— When enabled, the system will attempt to disconnect all clients that are connected or attempting to connect to the identified Access Point.
 - None— Disables all the containment mechanisms.
 - Deauthenticate only— With deauthentication containment, the Access Point or client is contained by disrupting the client association on the wireless interface.
 - Tarpit containment— With Tarpit containment, the Access Point is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the Access Point being contained.

Figure 118 *Containment Methods*



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 24 *SNMP Parameters for OAW-IAP*

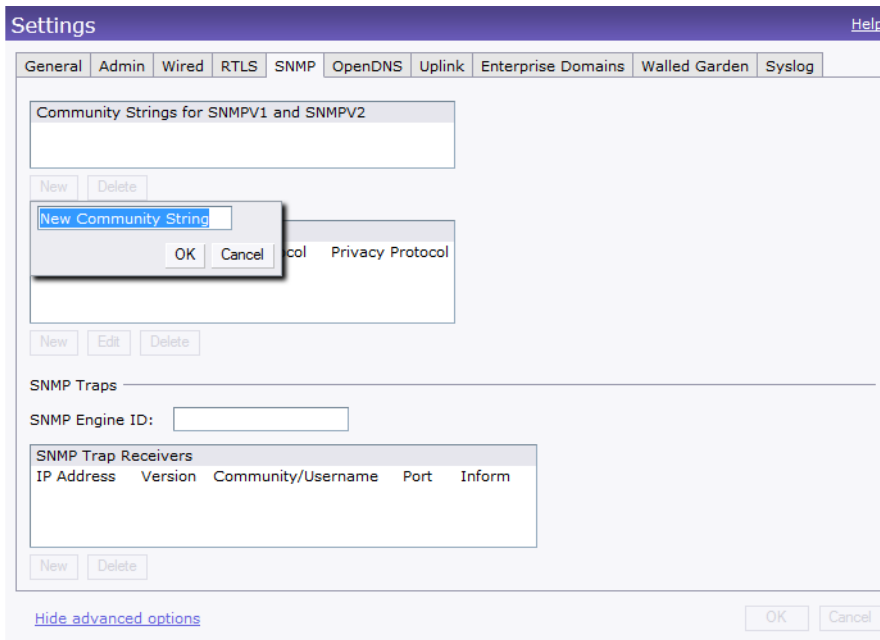
Field	Description
Community Strings for SNMPV1 and SNMPV2	An SNMP Community string is a text string that acts as a password, and is used to authenticate messages sent between the Virtual Controller and the SNMP agent.
If you are using SNMPv3 to obtain values from the Alcatel-Lucent Instant, you can configure the following parameters—	
Name	A string representing the name of the user.
Authentication Protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: <ul style="list-style-type: none"> MD5— HMAC-MD5-96 Digest Authentication Protocol SHA: HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption).
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol.

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

1. In the Settings tab click the **SNMP** tab.
2. Click **New** in the Community Strings for SNMPV1 and SNMPV2 box.
3. Enter the string in the **New Community String** text box.
4. Click **OK**.

To delete a community string, select the string and click **Delete**.

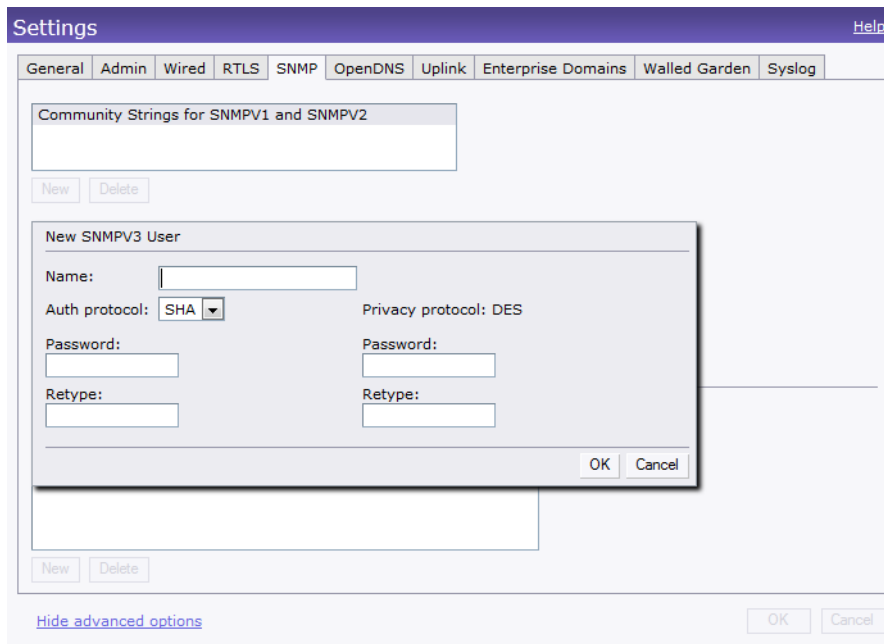
Figure 119 *Creating Community Strings for SNMPV1 and SNMPV2*



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

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

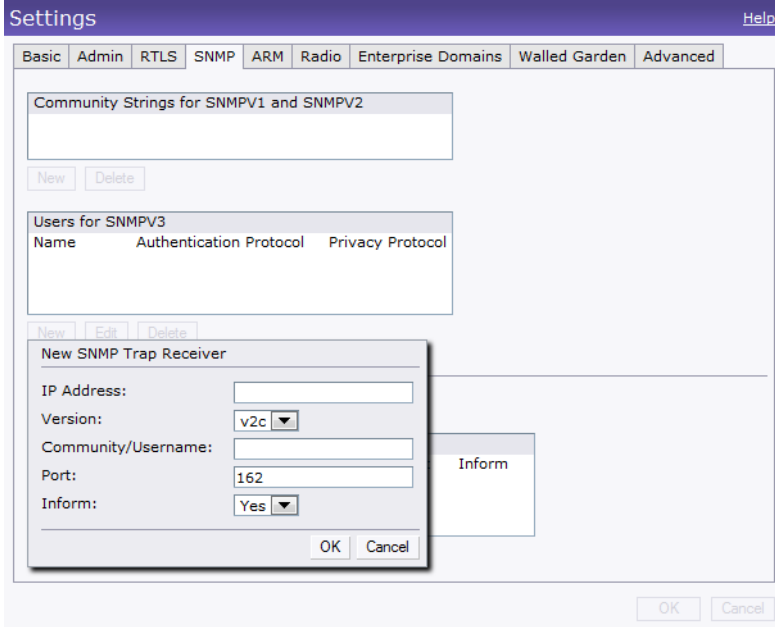
Figure 120 *Creating Users for SNMPV3*



SNMP Traps

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

Figure 121 *SNMP Traps*



To configure an SNMP trap receiver, follow this procedure.

1. Enter a name in the **SNMP Engine ID** text box. It indicates the name of the SNMP agent on the access point. SNMPV3 agent has an engine ID that uniquely identifies the agent in the device and is unique to that internal network.
2. Click **New** and update the following fields:
 1. **IP Address**— Enter the **IP Address** of the new SNMP Trap receiver.

2. **Version**— Select the SNMP version— **v1**, **v2c**, **v3** from the drop-down list. The version specifies the format of traps generated by the access point.
 3. **Community/Username**— Specify the community string for SNMPV1 and SNMPV2c traps and a username for SNMPV3 traps.
 4. **Port**— Enter the port to which the traps are sent. The default value is 162.
 5. **Inform**— When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPV3 only. The default value is **Yes**.
3. Click **OK** to view the trap receiver information in the **SNMP Trap Receivers** window.



Alcatel-Lucent-specific management information bases (MIBs) describe the objects that can be managed using SNMP. See the *Alcatel-Lucent Instant 6.1.3.1-3.0.0.0 MIB Reference Guide* for information about the Alcatel-Lucent MIBs and SNMP traps.

Ethernet Downlink Overview

The ethernet downlink ports allow third party devices such as VOIP phones or printers (which support only wired connection) to connect to the wireless network. Additionally, an Access Control List (ACL) can be configured for added security on the ethernet downlink.



This release of Instant supports only the OpenAuth mechanism.

Ethernet Downlink Profile Parameters

To create a new ethernet downlink profile perform the following steps:

1. Select **Settings** and click on **show advanced options** link.
2. Select **Wired** tab.
3. Click **New** button under the **Profile Definitions** and enter the following information:

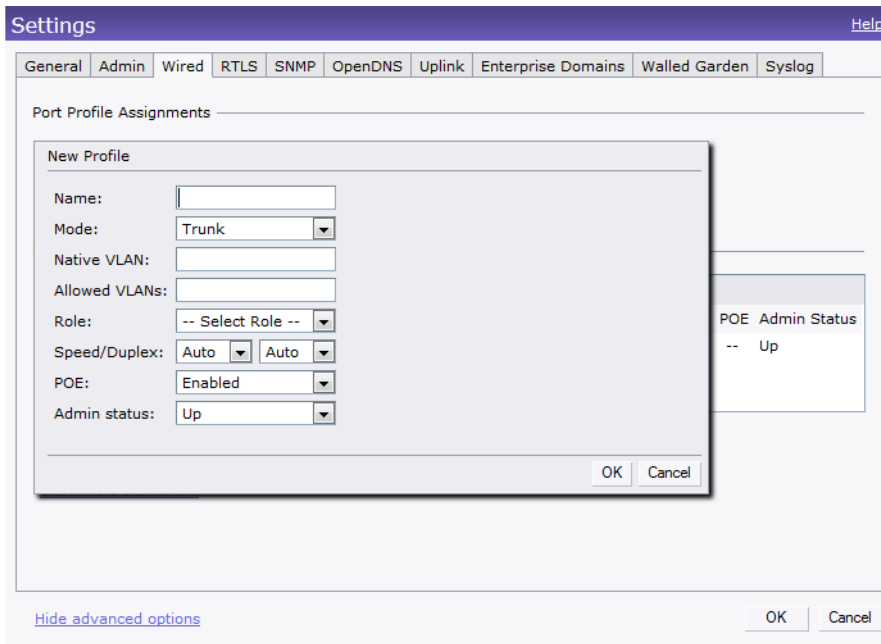
You can configure the following parameters for an ethernet downlink profile:

Table 25 *Ethernet Downlink Profile Parameters*

Field	Description
Name	Name of the ethernet downlink profile.
Mode	<ul style="list-style-type: none"> • In Access mode the port carries a single VLAN, specified as the Native VLAN. • In Trunk mode the port carries packets for multiple VLANs, specified as the Allowed VALN.
Native VLAN	Specifies the VLAN carried by the port in Access mode.
Allowed VLANs	Specifies the VLAN carried by the port in Trunk mode.
Role	Specifies the user connecting through these ports are assigned to a particular role.
Speed/Duplex	Only the experienced network administrators use the speed and duplex manually.
POE	When enabled, the system passes electric power along with the data on the ethernet cable. NOTE: The Power Sourcing Equipment (PSE) functionality is available only for the Ethernet port2 on OAW-RAP3WNP.
Admin Status	Displays the status of the admin.

The following figure displays the ethernet profile parameter configuration:

Figure 122 Ethernet Profile Configuration



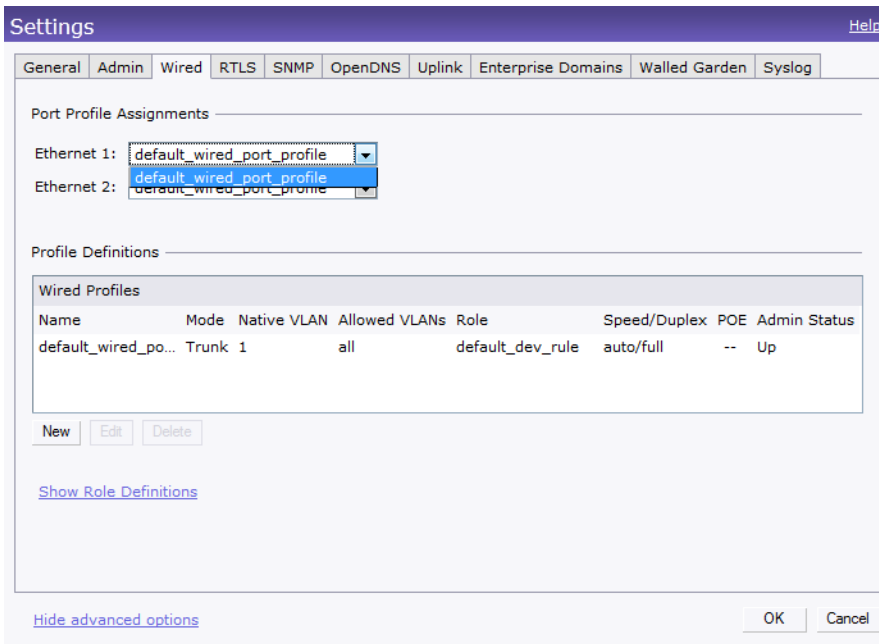
4. To edit an ethernet downlink profile, select the configured ethernet downlink profile under the **Profile Definitions** and click the **Edit** button.
5. To delete an ethernet downlink profile, select the configured ethernet downlink profile under the **Profile Definitions** and click the **Delete** button.

Assigning a Profile to the Ethernet Port

You can assign the configured profiles to the ethernet ports under the **Port Profile Assignments** window.

- To assign an ethernet downlink profile to Ethernet 1 port, select the profile from the **Ethernet 1** drop down list
- to assign an ethernet downlink profile to Ethernet 2 port, select the profile from the **Ethernet 2** drop down list

Figure 123 Assigning a Profile to the Ethernet Port



Uplink Configuration Overview

Alcatel-Lucent Instant supports 3G USB modems for the corporate Instant network. The 3G USB modems can be used to extend the connectivity to places where ethernet uplink cannot be configured. By using this, the client traffic can reach the internet and the corporate network. It also provides a reliable backup link for the ethernet based Instant network.

The following types of uplinks are supported on Instant:

- Ethernet
- 3G

Ethernet

By default, ethernet uplink is enabled.



This release of Instant does not support the user to configure eth0 uplink.

The user can view the type of uplink and the status of the uplink in the Instant UI under **Info** tab.

Figure 124 Uplink Status

Info	
Name:	Instant-C4:01:78
Country code:	IN
Virtual Controller IP:	0.0.0.0
AirWave IP:	0.0.0.0
Band:	All
Master:	10.17.115.1
Auto join mode:	Enabled
OpenDNS Status:	Not connected
Uplink type:	Ethernet
Uplink status:	UP
Dyn Blacklist Count:	0

3G Uplink

You can provision a USB modem for 3G uplink support in two ways— Manually provisioning and automatically provisioning.



OAW-RAP3WN and OAW-RAP3WNP, which will be available soon, support 3G.

Types of Modems

Instant supports the following three types of 3G modems:

- **True Auto Detect**— Modems of this type can be used only in one country and for a specific ISP. The parameters are configured automatically and hence no configuration is necessary (Plug and Play).

- **Auto-detect + ISP/country**— Modems of this type are used where user needs to specify the Country and ISP. The same modem is used for different ISPs with different parameters configured for each of them.
- **No auto-detect**—Modems of this type are used where the modems share the same Device-ID, Country, and ISP, but need to configure different parameters for each of them. These modems will work with Instant provided the correct parameters are configured. All new modems fall under this category as the parameter necessary to automatically configure them are not known.

The following table lists the types of supported 3G modems:

Table 26 *List of Supported 3G Modems*

Modem Type	Supported 3G Modems
True Auto Detect	<ul style="list-style-type: none"> ● USBConnect 881 (Sierra 881U) ● Quicksilver (Globetrotter ICON 322) ● UM100C (UTstarcom) ● Icon 452 ● Aircard 250U (Sierra) ● USB 598 (Sierra) ● U300 (Franklin wireless) ● U301 (Franklin wireless) ● USB U760 for Virgin (Novatel) ● USB U720 (Novatel/Qualcomm) ● UM175 (Pantech) ● UM150 (Pantech) ● UMW190(Pantech) ● SXC-1080 (Qualcomm) ● Globetrotter ICON 225 ● UMG181 ● NTT DoCoMo L-05A (LG FOMA L05A) ● NTT DoCoMo L-02A ● ZTE WCDMA Technologies MSM (MF668?) ● Fivespot (ZTE) ● c-motech CNU-600 ● ZTE AC2736 ● SEC-8089 (EpiValley) ● Nokia CS-10 ● NTT DoCoMo L-08C (LG) ● NTT DoCoMo L-02C (LG) ● Novatel MC545 ● Huawei E220 for Movistar in Spain ● Huawei E180 for Movistar in Spain ● ZTE-MF820 ● Huawei E173s-1 ● Sierra 320 ● Longcheer WM72 ● U600(3G mode)

Table 26 List of Supported 3G Modems (Continued)

Modem Type	Supported 3G Modems
Auto-detect + ISP/country	<ul style="list-style-type: none"> ● Sierra USB-306 (HK CLS/1010 (HK)) ● Sierra 306/308 (Telstra (Aus)) ● Sierra 503 PCIe (Telstra (Aus)) ● Sierra 312 (Telstra (Aus)) ● Aircard USB 308 (AT&T's Shockwave) ● Compass 597(Sierra) (Sprint) ● U597 (Sierra) (Verizon) ● Tstick C597(Sierra) (Telecom(NZ)) ● Ovation U727 (Novatel) (Sprint) ● USB U727 (Novatel) (Verizon) ● USB U760 (Novatel) (Sprint) ● USB U760 (Novatel) (Verizon) ● Novatel MiFi 2200 (Verizon Mifi 2200) ● Huawei E272,E170, E220 (ATT) ● Huawei E169,E180,E220,E272 (Vodafone/SmarTone (HK)) ● Huawei E160 (O2(UK)) ● Huawei E160 (SFR (France)) ● Huawei E220 (NZ and JP) ● Huawei E176G (Telstra (Aus)) ● Huawei E1553, E176 (3/HUTCH (Aus)) ● Huawei K4505 (Vodafone/SmarTone (HK)) ● Huawei K4505 (Vodafone (UK)) ● ZTE MF656 (Netcom (norway)) ● ZTE MF636 (HK CSL/1010) ● ZTE MF633/MF636 (Telstra (Aus)) ● ZTE MF637 (Orange in Israel) ● Huawei E180,E1692,E1762 (Optus (Aus)) ● Huawei E1731 (Airtel-3G (India)) ● Huawei E3765 (Vodafone (Aus)) ● Huawei E3765 (T-Mobile (Germany)) ● Huawei E1552 (SingTel (?)) ● Huawei E1750 (T-Mobile (Germany)) ● UGM 1831 (TMobile) ● Huawei D33HW (EMOBILE(Japan)) ● Huawei GD01 (EMOBILE(Japan)) ● Huawei EC150 (Reliance NetConnect+ (India)) ● KDDI DATA07(Huawei) (KDDI (Japan)) ● Huawei E353 (China Unicom) ● Huawei EC167 (China Telecom) ● Huawei E367 (Vodafone (UK)) ● Huawei E352s-5 (T-Mobile (Germany))
No auto-detect	<ul style="list-style-type: none"> ● Huawei D41HW ● ZTE AC2726

Provisioning 3G Uplink Manually

The user has to configure the exact modem parameters and can use 3G uplink by manual configuration. The AP has to be rebooted if the user has to configure USB modem parameter from the WebUI.

Use the following procedure to provision 3G uplink manually:

1. In the **settings** tab, click the **show advanced settings** hyperlink.
2. Select the **Uplink** tab. Under **3G** tab, perform the following steps:

- Enter the type of the 3G modem driver type in the **USB type** text box.
- Enter the identifier of the modem device in the **USB dev** text box.
- Enter the TTY port of the modem in the **USB tty** text box.
- Enter the parameter to initialize the modem in the **USB init** text box.
- Enter the parameter to dial the cell tower in the **USB dial** text box.
- Enter the username used to dial the ISP in the **USB user** text box.
- Enter the password used to dial the ISP in the **USB password** text box.
- Enter the parameter used to switch modem from storage mode to modem mode in the **USB switch mode** text box.

Figure 125 Provisioning 3G Uplink— Manually

3G

Country: ISP:

USB type: USB dial:

USB init: USB mode switch:

USB dev: USB user:

USB tty: USB password:

Management

Uplink preference:

Pre-emption:



Ensure to reboot the OAW-IAP after manually provisioning the OAW-IAP.

Provisioning 3G Uplink Automatically

In automatically provisioning 3G uplink, the user has to provide inputs for country and ISP in the **Country** and **ISP** textboxes. The OAW-IAP finds the parameters internally.

Figure 126 Provisioning 3G Uplink— Automatically

3G

Country: ISP:



In Instant UI, if the user can view the list of country or ISP in the country and ISP drop-down lists, the user can either use the country or ISP to configure the modem, or configure the individual modem parameters manually. If the user cannot view the list of country or ISP from the drop-down list, then the user has to configure the modem parameters manually.

Uplink Switchover

The default priority list is eth0, 3G. The OAW-IAP has the ability to switch to the lower priority uplink if the current uplink is down.



OAW-IAP reboot is not required for uplink switchover process.

Uplink Preemption

The OAW-IAP tries to get higher priority link in every ten minutes even if the current uplink is up and will not affect the current uplink connection. If the higher uplink is useable the OAW-IAP will switchover to use it. Preemption is enabled by default and the user can disable by configuration it.

Uplink Preference

The user can select the type of uplink from the **uplink preference** drop-down list under **Management**.

To use 3G uplink, select **3G** from the **Uplink preference** drop-down list.

Figure 127 *Uplink Preference*



The screenshot shows a configuration window titled "Management". It contains two dropdown menus. The first is labeled "Uplink preference:" and has "3G" selected. The second is labeled "Pre-emption:" and has "Enabled" selected.



The user can force to use one uplink manually, so that the OAW-IAP use that uplink, switchover and preemption does not work under this configuration.

OmniVista 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 using the HTTPS protocol. This allows an OmniVista server to be deployed in the cloud across a NAT device such as a router.

OmniVista Features

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

Image Management

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

The following models can be used to upgrade the firmware:

- **Automatic**— In this model, the Virtual Controller (VC) periodically checks for newer updates from a configured URL, and automatically initiates upgrade of the network.
- **Manual**— In this model, the user can manually start a firmware upgrade on a VC by VC basis, or can set desired firmware preference per group of devices.

OAW-IAP and Client Monitoring

OmniVista 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 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 128](#). 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 128 Template-based Configuration

The screenshot shows the Aruba Instant Virtual Controller configuration interface. At the top, there is a navigation bar with tabs for Home, Helpdesk, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, and VisualRF. Below the navigation bar, there is a status bar showing various metrics: New Devices: 23, Up: 77, Wired: 10, Down: 44, Mismatched: 71, Rogue: 3183, Users: 7, and Alert. The main configuration area is titled 'Group: KMart' and 'Aruba Instant Virtual Controller'. It includes fields for Name (Aruba Instant Virtual Controller), Device Type (Aruba Instant Virtual Controller), Restrict to this version (Yes/No radio buttons, No is selected), and Template firmware version (5.0.4.0_28158). Below this is a 'Template Select' section with a dropdown menu for 'Fetch template from device' and a 'Fetch' button. The main configuration area displays a 'Template' configuration snippet, including version information, virtual-controller settings, and user management. To the right of the template configuration, there is a section for 'Available Variables' with a list of variables and their corresponding values.

```
! Template created from Instant-CA:78:5E (5.0.4.0_28158) at 6/8/2011 5:13 PM
! based on config fetched at 6/8/2011 5:06 PM
version 5.0.4
virtual-controller-country IN
virtual-controller-key %guid%
%if ip_address%
virtual-controller-ip %ip_address%
%endif%
name "%hostname%"
organization KMart
syslog-server 10.15.76.239
terminal-access

rf-band all
ams-ip %manager_ip_address%
ams-key %password%

allow-new-aps
%allowed_aps%

mgmt-user admin 391c5560bf4b498d5096f79576cd29d2

wlan ssid-profile instant
```

The following variables may be used in the template. The value of each variable is configured on the APs/Devices Manage page for each device in the group. Each variable must be surrounded by percent signs: %hostname%. The %/, % statements must be terminated by % end/% and cannot be nested.

Available Variables:

allowed_aps	ap_include_8
ap_include_1	ap_include_9
ap_include_10	guid
ap_include_2	hostname
ap_include_3	ip_address
ap_include_4	manager_ip_address
ap_include_5	password
ap_include_6	
ap_include_7	

Trending Reports

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

Intrusion Detection System

OmniVista provides advanced, rules-based rogue classification. It automatically detects rogue APs 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.

Wireless Intrusion Detection System (WIDS) Event Reporting to OmniVista

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

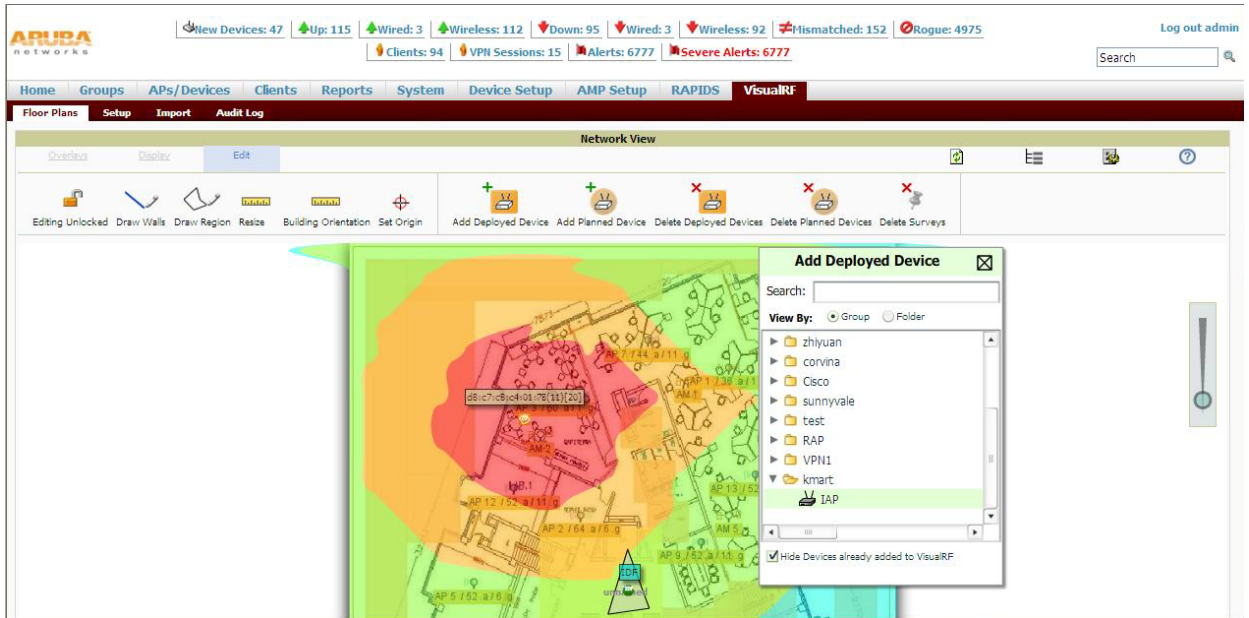
The WIDS report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours, and provides links to support additional analysis or configuration in response.

RF Visualization Support for Alcatel-Lucent Instant

OmniVista supports RF visualization for Alcatel-Lucent Instant. The VisualRF module is an add-on to the OmniVista Wireless Management Suite that provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. VisualRF uses

sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every Instant device in range. VisualRF provides graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network.

Figure 129 Adding an OAW-IAP in VisualRF



Configuring OmniVista

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

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

Creating your Organization String

The Organization String is a set of colon-separated strings created by the OmniVista 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 sub folders under the folder named "Org":

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

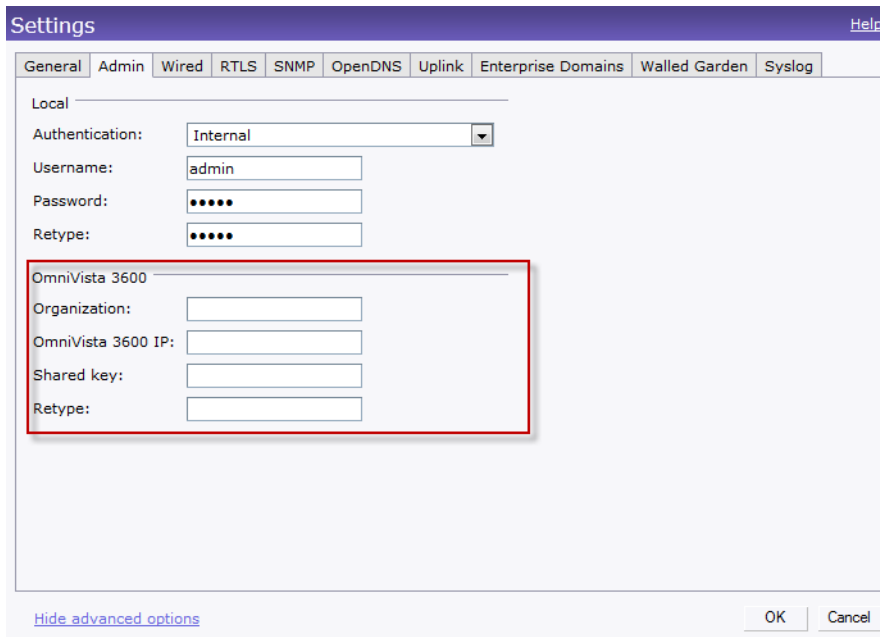
About Shared Key

The Shared Secret key is used by the administrator to manually authorize the first Virtual Controller for an organization. Any string is acceptable.

Entering the Organization String and AMP Information into the OAW-IAP

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

Figure 130 Configuring OmniVista



The screenshot shows a 'Settings' dialog box with a purple header and a 'Help' button. The 'General' tab is selected, and the 'Local' section is expanded. The 'Authentication' dropdown is set to 'Internal'. The 'Username' field contains 'admin', and the 'Password' and 'Retype' fields are masked with dots. The 'OmniVista 3600' section is highlighted with a red border and contains four text input fields: 'Organization:', 'OmniVista 3600 IP:', 'Shared key:', and 'Retype:'. At the bottom, there is a 'Hide advanced options' link and 'OK' and 'Cancel' buttons.

2. Enter the name of your organization in the **Organization** name text box. This name will automatically appear in OmniVista under Groups list.
3. Enter the IP address of the OmniVista server in the **OmniVista 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 Discovery through DHCP Option

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

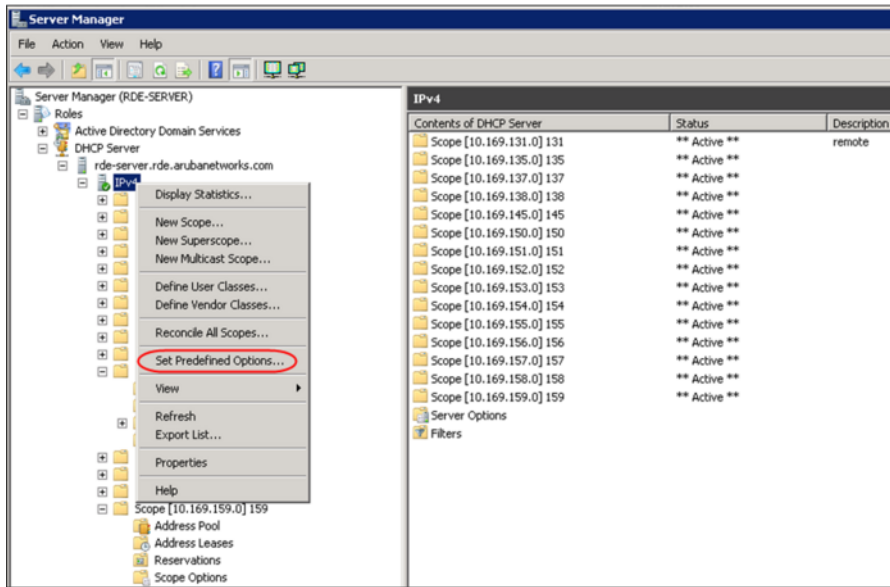
On the DHCP server, the format for option 60 is "**Alcatel-LucentInstantAP**", and the format for option 43 is "**ams-ip,ams-key**".

Standard DHCP option 60 and 43 on Windows Server 2008 for Alcatel-Lucent Instant APs

In networks that are not using DHCP option 60 and 43, it is easy to use the standard DHCP options 60 and 43 for Alcatel-Lucent AP or Alcatel-Lucent Instant AP. For Alcatel-Lucent APs these options can be used to indicate the, master switch or the local switch. For OAW-IAP, this can be used to define the OmniVista IP, group and password.

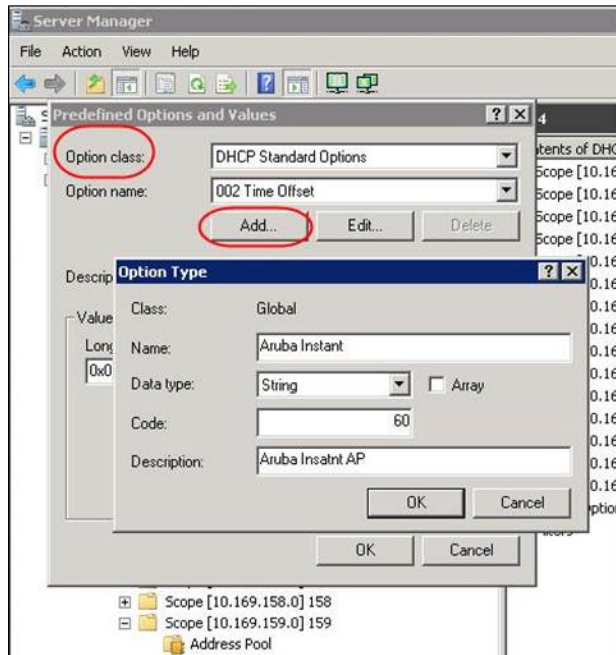
1. In server 2008 go to **Server Manager > Roles > DHCP sever > Your Domain DHCP Server > IPv4**
2. Right click on **IPv4** and select **Set Predefined Options**.

Figure 131 Instant and DHCP options for OmniVista— Set Predefined Options



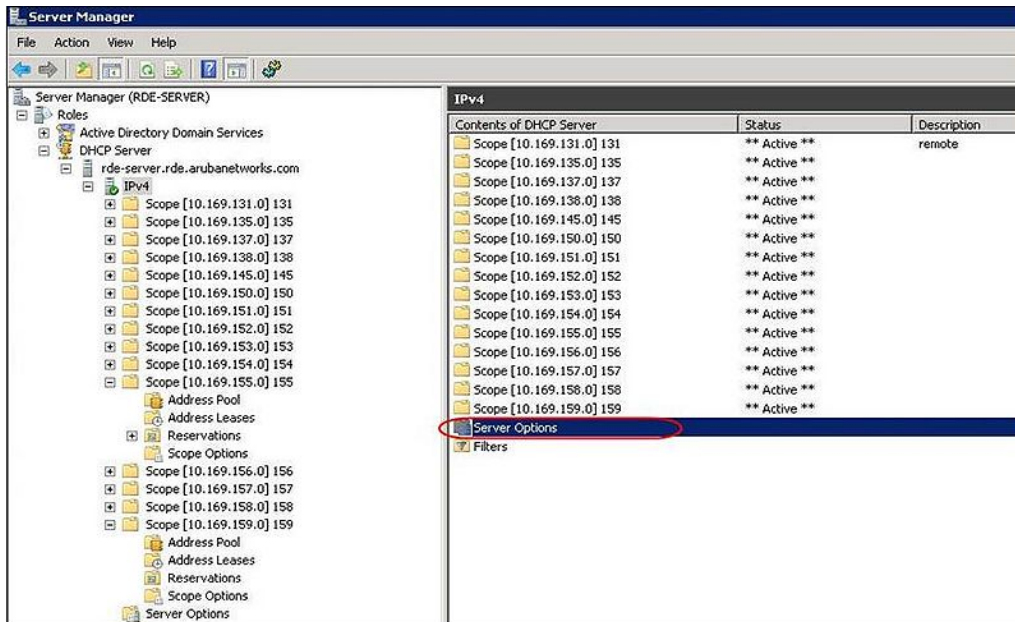
3. Select **DHCP Standard Options** in the **Option class** drop-down list and then click **Add**. Enter the following information:
 - Name— Alcatel-Lucent Instant
 - Data Type— String
 - Code— 60
 - Description— Alcatel-Lucent Instant AP

Figure 132 Instant and DHCP options for OmniVista— Predefined Options and Values



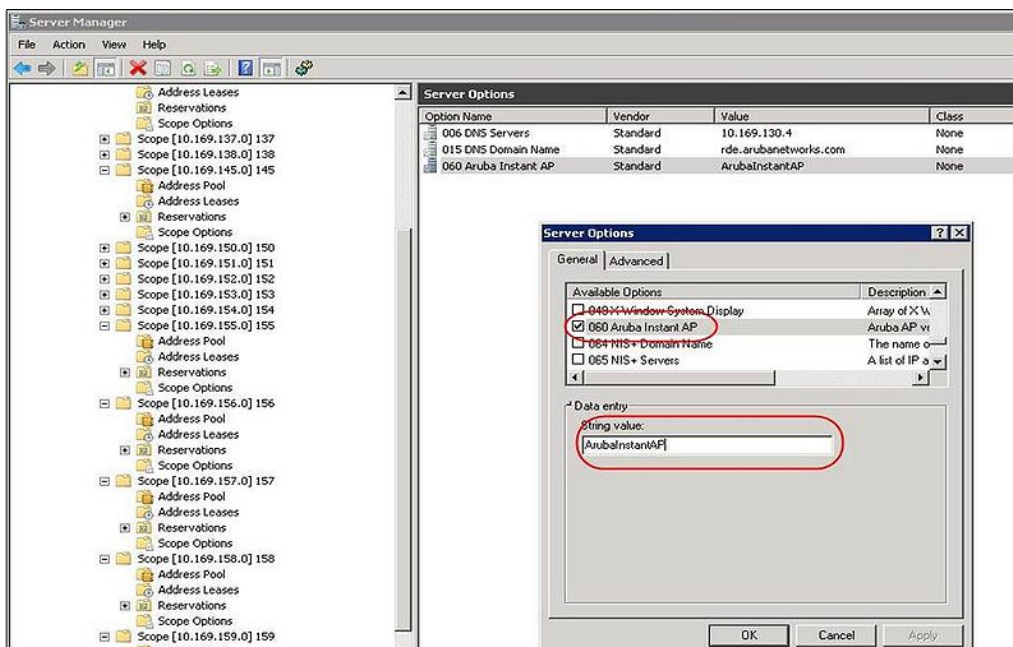
4. Go to **Server Manager** and select **Server Options** in the **IPv4** window. (This will set the value globally. Use options in a per scope basis to override the global options).
5. Right click on **Server Options** and select configure options.

Figure 133 Instant and DHCP options for OmniVista– Server Options



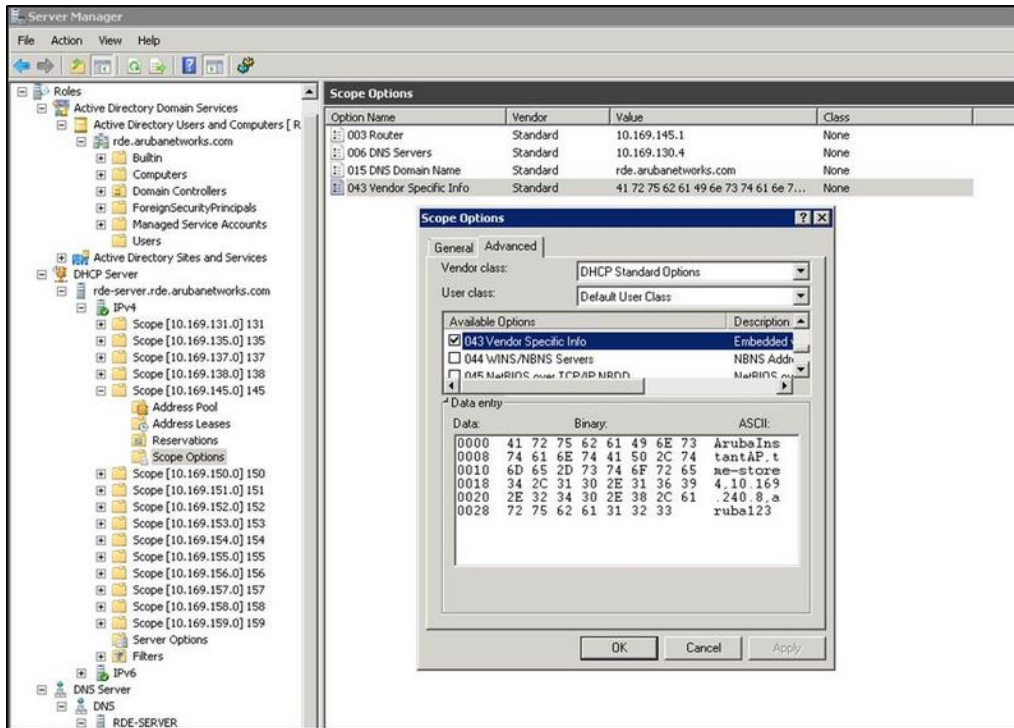
6. Select **060 Alcatel-Lucent Instant AP** in the **Server Options** window and enter **Alcatel-LucentInstantAP** in the String Value.

Figure 134 Instant and DHCP options for OmniVista–060 Alcatel-Lucent Instant AP in Server Options



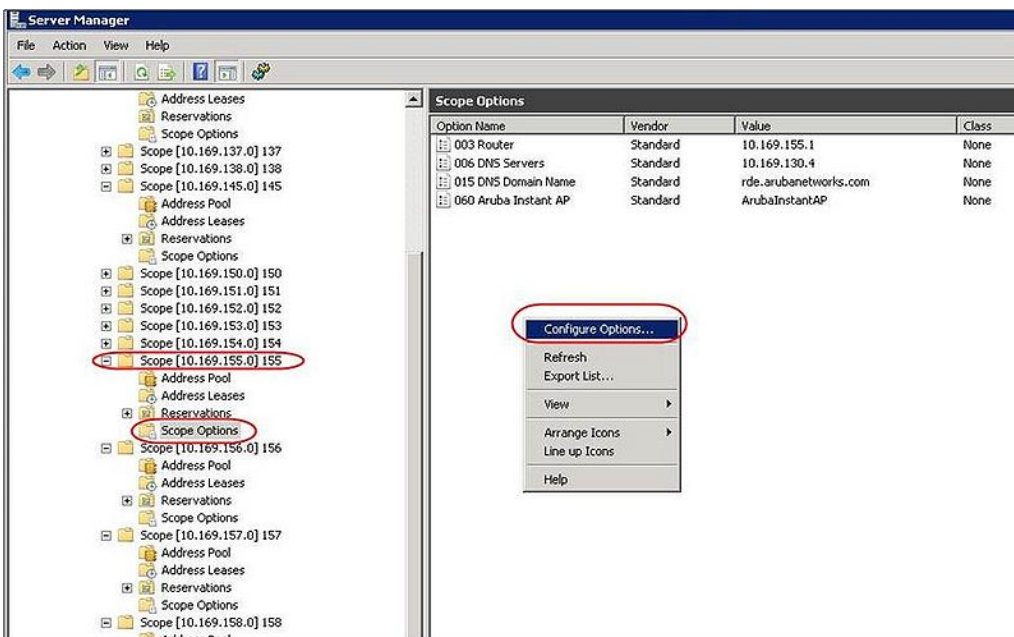
7. Select **043 Vendor Specific Info** and enter a value for **omnivista-orgn**, **omnivista-ip**, **omnivista-key** in the ASCII field (for example: tme-instant-store1, 10.169.240.8, alcatel-lucent123).

Figure 135 Instant and DHCP options for OmniVista – 043 Vendor Specific Info



This will create a DHCP option 60 and 43 on a global basis. You can do the same on a per scope basis. The per scope option will override the global option.

Figure 136 Instant and DHCP options for OmniVista – Scope Options



Alternate method for defining Vendor Specific DHCP options

This section describes how to add vendor specific DHCP options for Alcatel-Lucent Instant AP in a network that uses DHCP option 60 and 43 for other services such as PXE. There are few customers that use DHCP standard options such as option 60 and 43 for giving the DHCP clients info about certain services such as PXE to the DHCP clients. In such an environment, it is not possible to use the standard DHCP option 60 and 43 for Alcatel-Lucent APs.

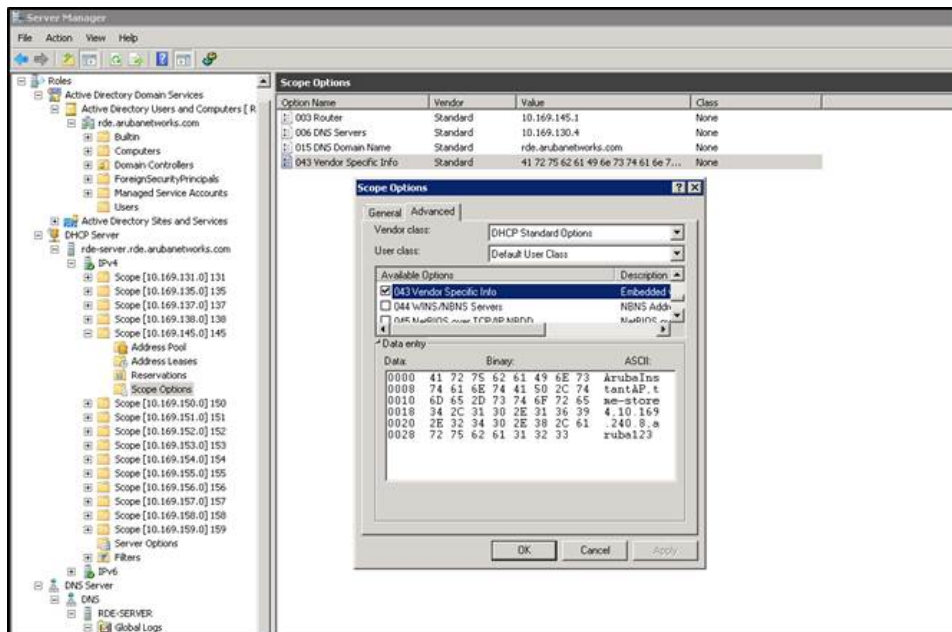
This method describes how to set up a DHCP server to send option 43 with OmniVista information to Alcatel-Lucent Instant OAW-IAP. This section assumes that option 43 will be sent per scope since option 60 is being shared by other devices as well.



This scope should be specific to instant and the PXE devices that use options 60 and 43 should not connect to the subnet defined by this scope. This is because you can specify only one option 43 for a scope and if other devices that use option 43 connect to this subnet, they will be presented with Instant specific information.

1. In server 2008 go to **Server Manager > Roles > DHCP Server > Your Domain DHCP Server > IPv4**.
2. Select a scope (subnet). In the following figure it is 10.169.145.0 (scope 145).
3. Right click and select Advanced and choose these options
 - Vendor class— DHCP Standard Options
 - User class— Default User Class
 - Available options— Select 043 Vendor Specific Info
 - String Value— Alcatel-LucentInstantAP, tme-store4, 10.169.240.8, alcatel-lucent123 (which is the AP description, organization string, OmniVista IP address, Pre-shared key for OmniVista).

Figure 137 Vendor Specific DHCP options



On OmniVista, the OAW-IAP shows up as a new device and a group called **tme-store4** has been created. Go to APs/Devices > New > Group to view this group.

Figure 138 OmniVista – New Group

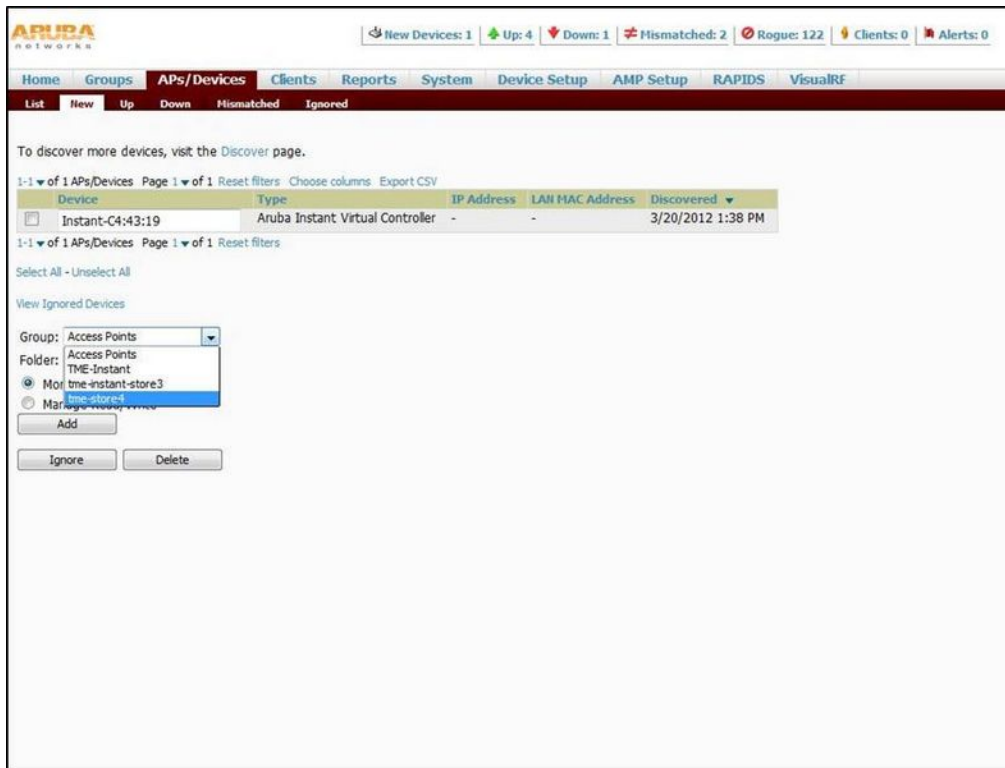
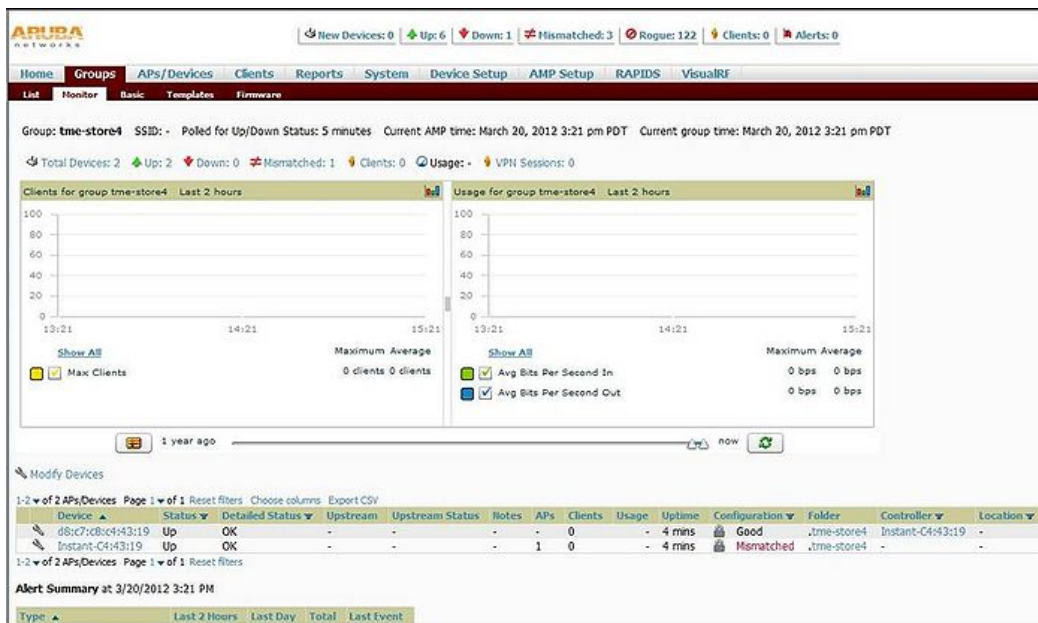


Figure 139 OmniVista – Monitor



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

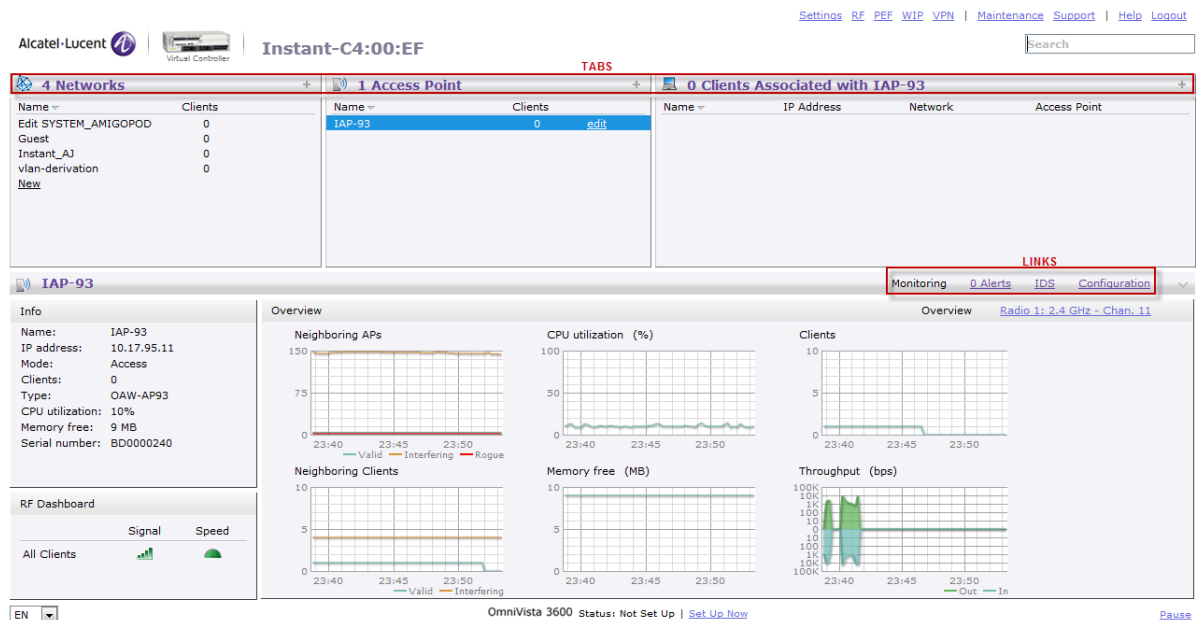
This chapter provides information about the parameters that can be monitored using these views. It also provides procedures to monitor these parameters.

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 2, “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](#), [Configuration Link](#) sections.

Figure 140 Virtual Controller View



Monitoring Link

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

- Info
- RF Dashboard
- Usage Trends

Info

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

- **Name**— Displays the Virtual Controller name.
- **Country Code**— Displays the Country in which the Virtual Controller is operating.
- **Virtual Controller IP address**— Displays the IP address of the Virtual Controller.
- **OmniVista IP**— Displays the IP address of the OmniVista server.
- **Band**— Displays the band in which the Virtual Controller is operating— 2.4 GHz band, 5.4 GHz band, or both.
- **Master**— Displays the IP address of the Access Point acting as a Virtual Controller.
- **OpenDNS Status**— Displays the OpenDNS status. If the OpenDNS is **Not connected**, make sure you have provided the correct credentials on the **OpenDNS** tab of the **Settings** window. In addition, please check if the Internet connection is up.
- **Uplink type**— Displays the type of uplink— Ethernet and 3G
- **Uplink status**— Displays whether the uplink is up or down.

RF Dashboard

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

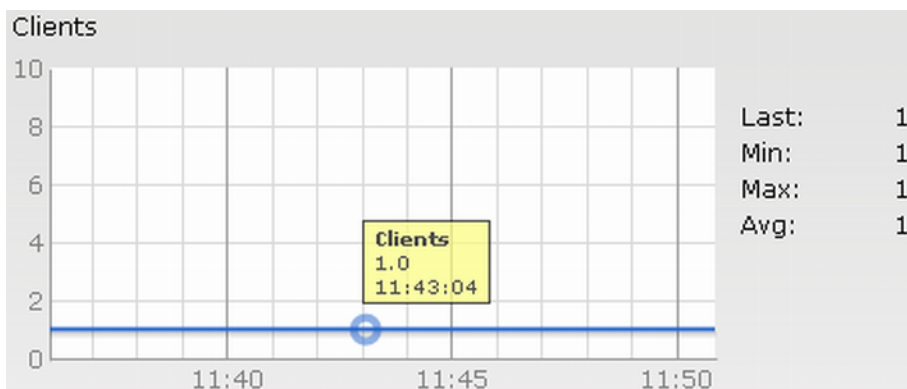
- IP address, Signal, and Speed information about the clients in the Alcatel-Lucent Instant network. If the speed or signal strength of a client is low, IP address of the client appears as a link. Click the link to monitor the client. For more information, see “[Client View](#)” on page 194.
- Instant 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 190.

Usage Trends

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

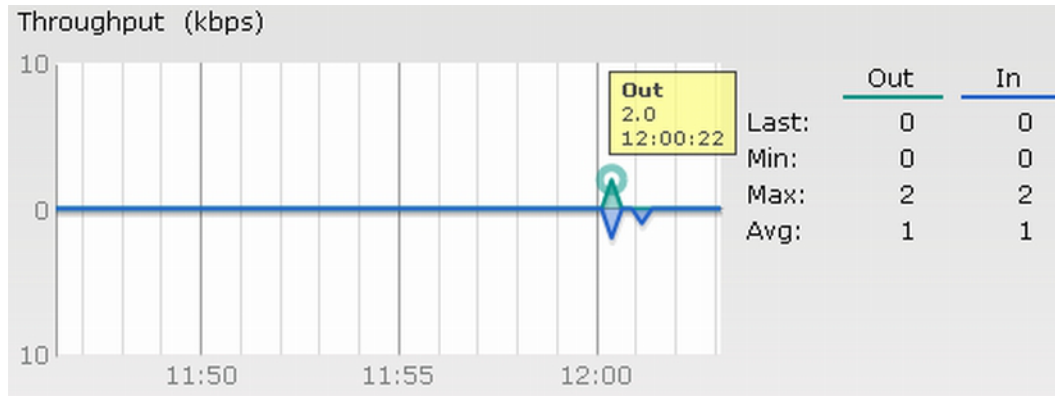
- Clients Graph

Figure 141 *Clients Graph*



- Throughput Graph

Figure 142 *Throughput Graph*



For more information about the graphs in the Virtual Controller view and for monitoring procedures, see [Table 27](#).

Table 27 *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"> The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the Virtual Controller for the last 15 minutes. To see the exact number of clients in the Alcatel-Lucent Instant network at a particular time, hover the cursor over the graph line. 	<p>To check the number of clients associated with the Virtual Controller for the last 15 minutes,</p> <ol style="list-style-type: none"> Log in to the Instant UI. The Virtual Controller view appears. This is the default view. Study the Clients graph in the Usage Trends pane. For example, the graph on the left shows that one client is associated with the Virtual Controller at 11:43 hours.
Throughput	<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"> Outgoing traffic — Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. Incoming traffic — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> 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. <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"> Log in to the Instant UI. The Virtual Controller view appears. This is the default view. Study the Throughput graph in the Usage Trends pane. For example, the graph on the left shows 2.0 kbps outgoing traffic throughput at 12:00 hours. It also shows some incoming traffic throughput at the same time.

Client Alerts Link

For information about the Client Alerts link, see [“Clients Tab” on page 27](#) and [Chapter 22, “Alert Types and Management”](#) chapters.

IDS Link

For information about the IDS link, see [“IDS” on page 43](#).

Network View

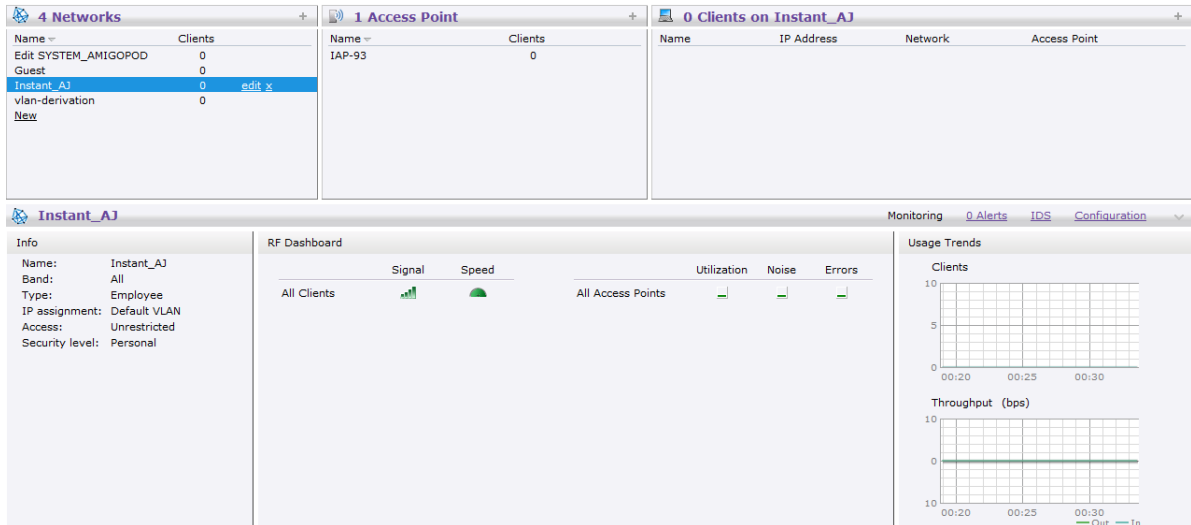
All Wi-Fi networks in the Alcatel-Lucent Instant network are listed in the **Networks** tab. Click the network that you want to monitor. Network View for the selected network appears.

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 143 Network View



Info

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

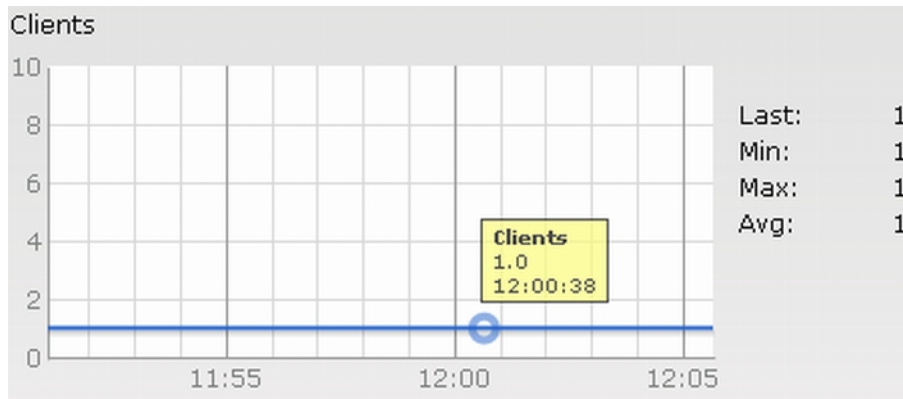
- **Name**— Name of the network.
- **Band**— Band in which the network is broadcast: 2.4 GHz band, 5.4 GHz band, or both.
- **Type**— Network type: Employee, Guest, or Voice.
- **IP Assignment**— Source of IP address for the client.
- **Access**— The level of access control for this network.
- **Security level**— The type of user authentication and data encryption for this network.

Usage Trends

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

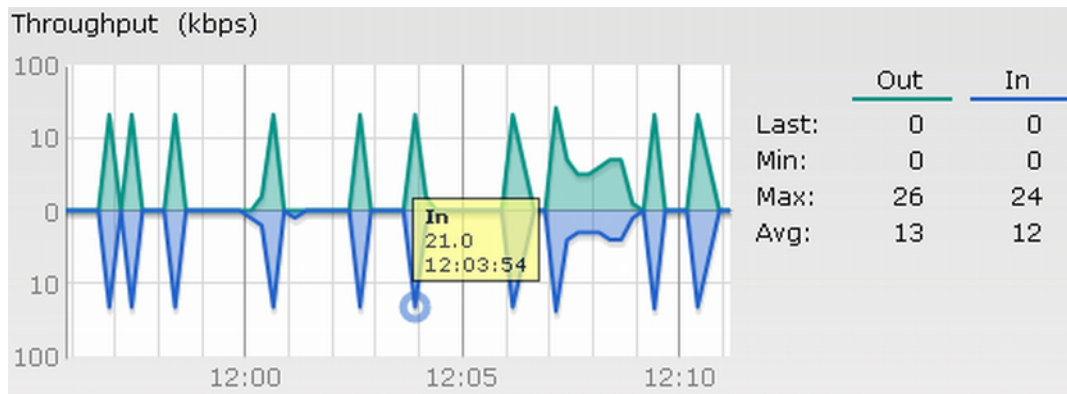
- Clients

Figure 144 Clients Graph



- Throughput

Figure 145 Throughput Graph



For more information about the graphs in the network view and for monitoring procedures, see [Table 28](#).

Table 28 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"> • The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the Virtual Controller for the last 15 minutes. • To see the exact number of clients in the Alcatel-Lucent Instant network at a particular time, hover the cursor over the graph line. 	<p>To check the number of clients associated with the network for the last 15 minutes,</p> <ol style="list-style-type: none"> 1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view. 2. In the Networks tab, click the network for which you want to check the client association. The Network view appears. 3. Study the Clients graph in the Usage Trends pane. For example, the graph on the left shows that one client is associated with the selected network at 12:00 hours

Table 28 Network View — Graphs and Monitoring Procedures (Continued)

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"> Outgoing traffic — Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. Incoming traffic — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> 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. <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"> Log in to the Instant UI. The Virtual Controller view appears. This is the default view. In the Networks tab, click the network for which you want to check the client association. The Network view appears. Study the Throughput graph in the Usage Trends pane. For example, the graph on the left shows 22.0 kbps incoming traffic throughput for the selected network at 12:03 hours.

Instant Access Point View

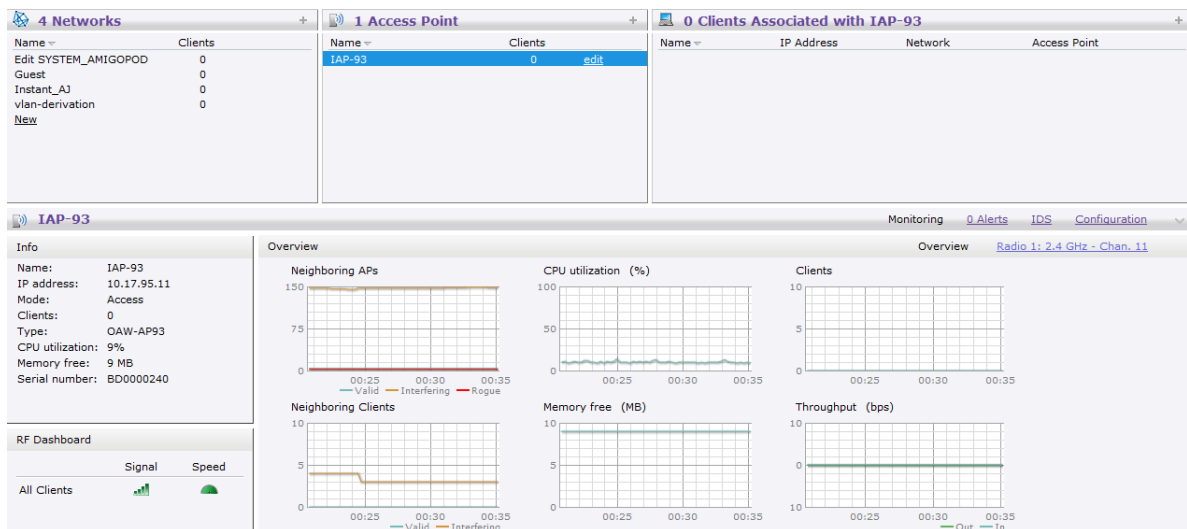
All OAW-IAPs in the Alcatel-Lucent Instant network are listed in the **Access Points** tab. Click the OAW-IAP that you want to monitor. Access Point view for that OAW-IAP appears.

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

Figure 146 Instant Access Point View



Info

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

- Name**— Displays the name of the selected OAW-IAP.

- **IP Address**— Displays the IP address of the OAW-IAP.
- **Mode**— Displays the mode type. In **Access** mode the OAW-IAP serves clients, while also monitoring for rogue APs in the background. In **Monitor** mode, the OAW-IAP acts as a dedicated monitor, scanning all channels for rogue APs and clients.
- **Clients**— Number of clients associated with the OAW-IAP.
- **Type**— Displays the model number of the OAW-IAP.
- **CPU Utilization**— Displays the CPU utilization in percentage.
- **Memory Free**— Displays the memory availability of the OAW-IAP in Mega Bytes (MB).
- **Serial number**— Displays the serial number of the OAW-IAP.

RF Dashboard

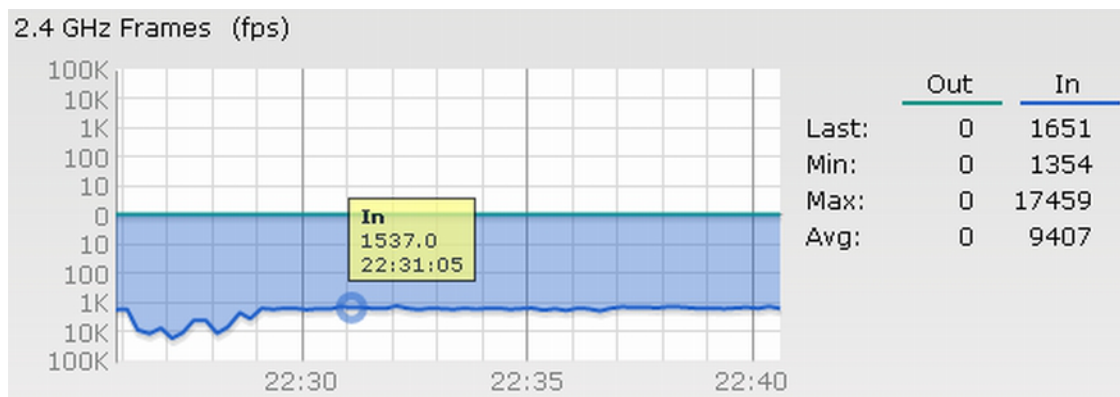
In the Instant Access Point view, the **RF Dashboard** section is moved below the **Info** section. It lists the IP address of the clients that are associated with the selected OAW-IAP if the signal strength or the data transfer speed of the client is low.

RF Trends

The RF Trends display the common RF metrics for the selected access point over the past 15 minutes. The **RF Trends** section has two links— **2.4 GHz** and **5 GHz**. The **2.4 GHz** link is selected by default and the following graphs are displayed for that band:

- Utilization
- 2.4 GHz Frames

Figure 147 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 29.

Table 29 *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"> The enlarged view provides Last, Minimum, Maximum, and Average radio utilization statistics for the OAW-IAP for the last 15 minutes. <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"> Log in to the Instant UI. The Virtual Controller view appears. This is the default view. In the Access Points tab, click the OAW-IAP for which you want to monitor the utilization. The OAW-IAP view appears. 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. <p>NOTE: You can also click the rectangle icon under the Utilization column in the RF Dashboard pane to see the Utilization graph for the selected OAW-IAP. The rectangle icon is seen as follows:</p> 
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"> Outgoing frames — Outgoing frame traffic is displayed in green. It is shown above the median line. Incoming frames — Incoming frame traffic is displayed in blue. It is shown below the median line. <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing frames. <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"> Log in to the WebUI. The Virtual Controller view appears. This is the default view. 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. 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.

Table 29 Instant Access Point View — RF Trends Graphs and Monitoring Procedures (Continued)

Graph Name	Description	Monitoring Procedure
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"> The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In and Out frames. <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"> Log in to the WebUI. The Virtual Controller view appears. This is the default view. 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. 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. <p>NOTE: You can also click the rectangle icon in the Noise column in the RF Dashboard pane to see the Noise graph for the selected OAW-IAP. The rectangle icon is seen as follows:</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"> The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In and Out frames. <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"> Log in to the WebUI. The Virtual Controller view appears. This is the default view. 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. 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. <p>NOTE: You can also click the rectangle icon under the Errors column in the RF Dashboard pane to see the Errors graph for the selected 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 30](#).

Table 30 *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"> 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. <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"> Log in to the Instant UI. The Virtual Controller view appears. This is the default view. In the Access Points tab, click the OAW-IAP for which you want to monitor the client association. The OAW-IAP view appears. 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.
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"> Outgoing traffic — Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown about the median line. Incoming traffic — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> 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. <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"> Log in to the Instant UI. The Virtual Controller view appears. This is the default view. In the Access Points tab, click the OAW-IAP for which you want to monitor the throughput. The OAW-IAP view appears. Study the Throughput graph in the Usage Trends pane. For example, the graph on the left shows 4.0 kbps incoming traffic throughput at 12:08 hours.

Client View

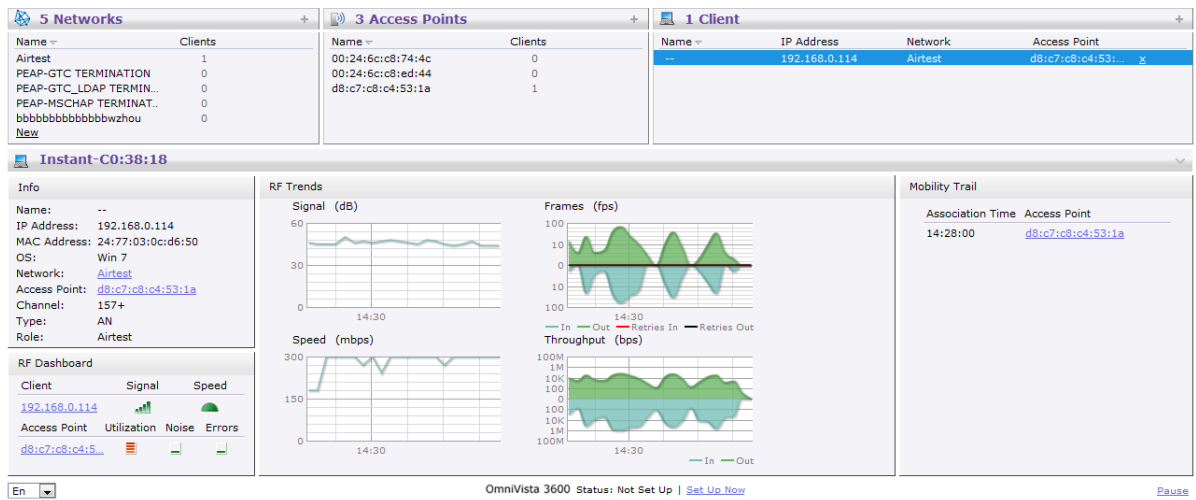
In the Virtual Controller view, all clients in the Alcatel-Lucent Instant network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor. Client view for that client appears.

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 148 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

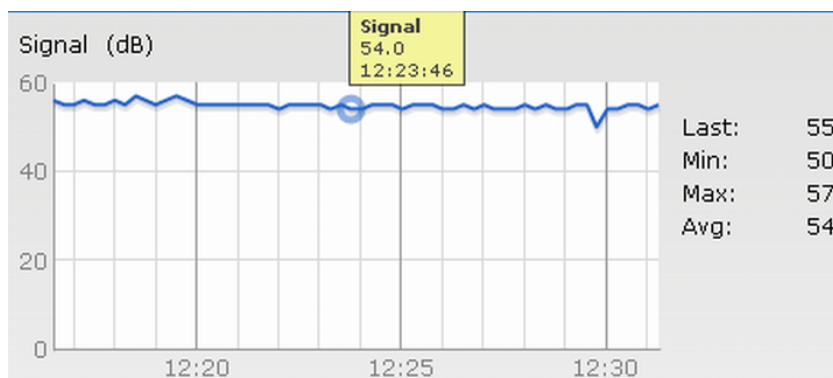
In the Client view, the **RF Dashboard** section is moved below the **Info** section. The **RF Dashboard** section in the client view shows the speed and the signal information for the client and the RF information for the OAW-IAP to which the client is connected to.

RF Trends

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

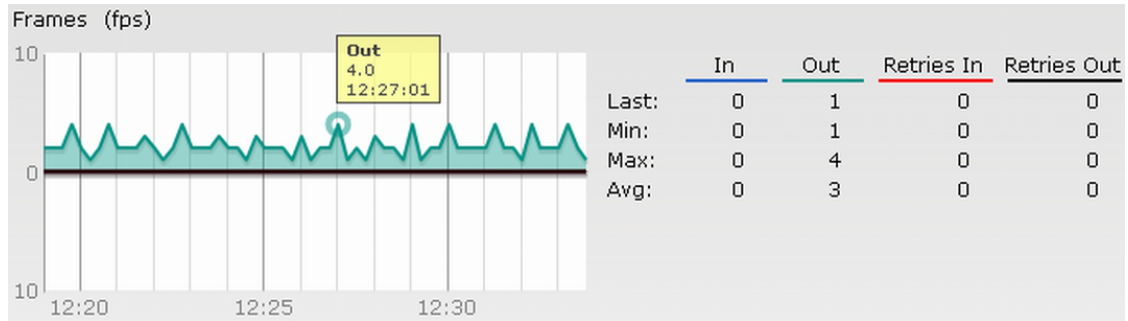
- Signal

Figure 149 Signal Graph



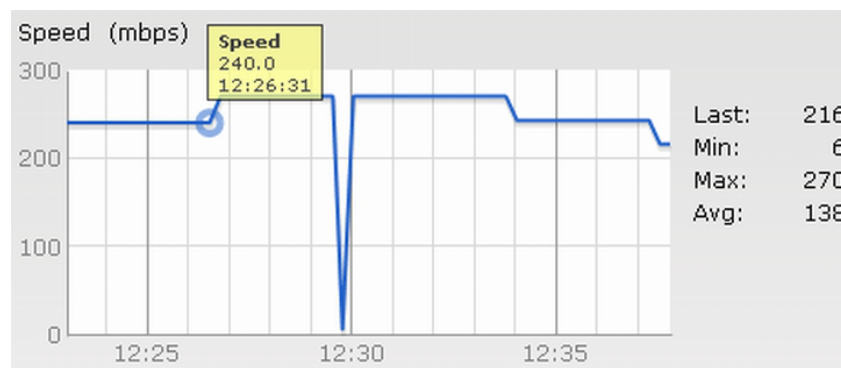
- Frames

Figure 150 *Frames Graph*



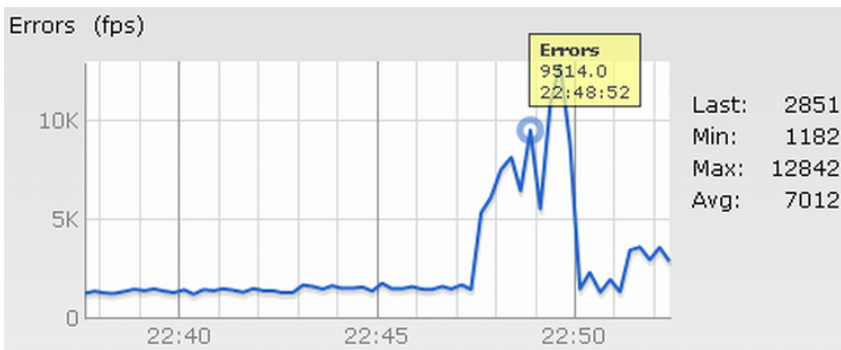
- Speed

Figure 151 *Speed Graph*



- Throughput

Figure 152 *Throughput Graph*



For more information about RF trends graphs in the client view and for monitoring procedures, see [Table 31](#).

Table 31 *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"> The enlarged view provides Last, Minimum, Maximum, and Average signal statistics for the client for the last 15 minutes. <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"> Log in to the Instant UI. The Virtual Controller view appears. This is the default view. In the Clients tab, click the IP address of the client for which you want to monitor the signal strength. The client view appears. Study the Signal graph in the RF Trends pane. For example, the graph on the left shows that signal strength for the client is 54.0 dB at 12:23 hours.
Frames	<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"> Outgoing frames — Outgoing frame traffic is displayed in green. It is shown above the median line. Incoming frames — Incoming frame traffic is displayed in blue. It is shown below the median line. Retry Out — Retries for the outgoing frames is displayed in black and is shown above the median line. Retry In — Retries for the incoming frames is displayed in red and is shown below the median line. <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none"> The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In, Out, Retries In, and Retries Out frames. <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"> Log in to the Instant UI. The Virtual Controller view appears. This is the default view. In the Clients tab, click the IP address of the client for which you want to monitor the frames. The client view appears. Study the Frames graph in the RF Trends pane. For example, the graph on the left shows 4.0 frames per second for the client at 12:27 hours.
Speed	<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"> The enlarged view shows Last, Minimum, Maximum, and Average statistics for the client for the last 15 minutes. <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"> Log in to the Instant UI. The Virtual Controller view appears. This is the default view. In the Clients tab, click the IP address of the client for which you want to monitor the speed. The client view appears. 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.

Table 31 *Client View — RF Trends Graphs and Monitoring Procedures (Continued)*

Graph Name	Description	Monitoring Procedure
Throughput	<p>The Throughput Graph shows the throughput for the selected client for the last 15 minutes.</p> <ul style="list-style-type: none">● Outgoing traffic — Throughput for outgoing traffic is displayed in green. Outgoing traffic is shown above the median line.● Incoming traffic — Throughput for incoming traffic is displayed in blue. Incoming traffic is shown below the median line. <p>To see an enlarged view, click the graph.</p> <ul style="list-style-type: none">● 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. <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">1. Log in to the Instant UI. The Virtual Controller view appears. This is the default view.2. In the Clients tab, click the IP address of the client for which you want to monitor the throughput. The client view appears.3. Study the Throughput graph in the RF Trends pane. For example, the graph on the left shows 1.0 kbps outgoing traffic throughput for the client at 12:30 hours.

Mobility Trail

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

- **Association Time**— The time at which the selected client was associated with a particular 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 32 displays a list of alerts that are generated on the Alcatel-Lucent Instant network.

Table 32 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 32 Alerts List (Continued)

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.

Alcatel-Lucent's Policy Enforcement Firewall (PEF) module for Alcatel-Lucent Instant provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks.

The PEF window displays the external/internal authentication servers, currently defined roles for all the networks, blacklisted clients and to enable or disable the protocols for ALG.

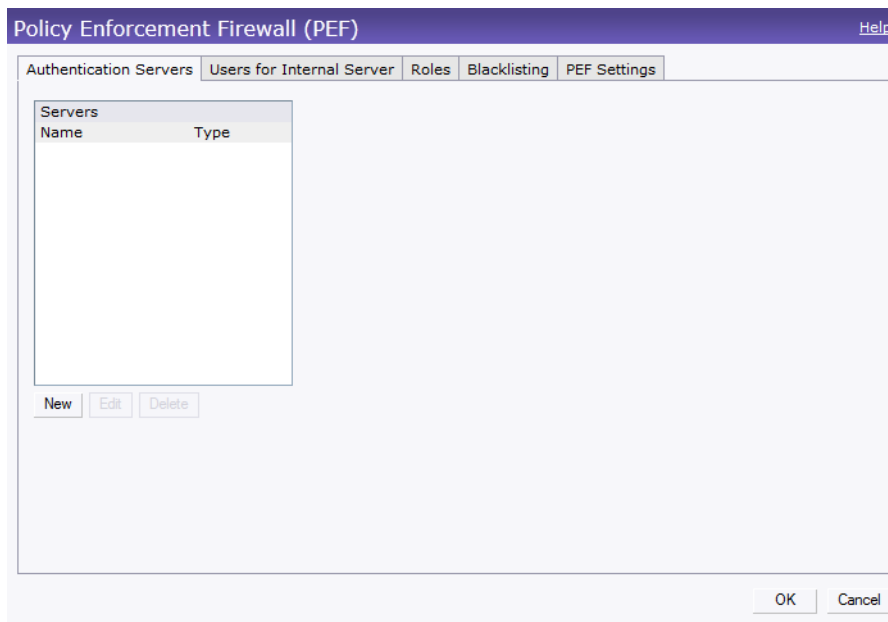
Navigate to the **PEF** link at the top right corner of the WebUI to view the following features.

Authentication Servers

This section displays the currently defined external authentication servers.

- **Name**— Indicates the name of the external authentication server.
 - **Type**— Indicates the type of the authentication server-RADIUS or LDAP.
1. Click **New** to configure an external RADIUS server for a wireless network. See “[Configuring an External RADIUS Server](#)” on page 101 for more information.
 2. Click **OK** to apply the changes.

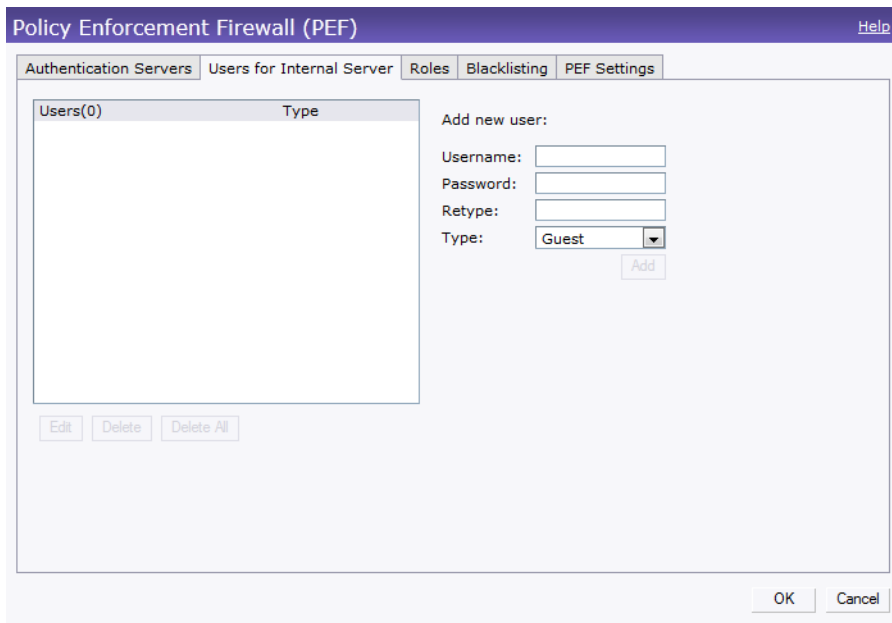
Figure 153 Authentication Server



Users for Internal Server

This section displays the currently defined users for the internal authentication server.

Figure 154 *Users for Internal Server*



To add a user, perform the following steps:

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

See “[User Database](#)” on [page 217](#) for more information.

Roles

This window consists of the following options:

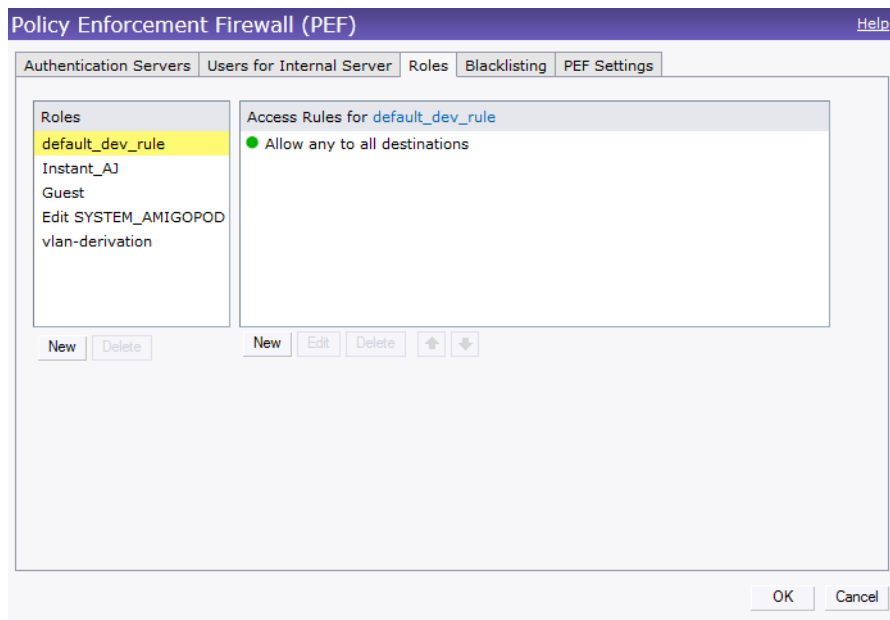
- **Roles**— This table displays all the roles defined for all the networks. See “[User Role](#)” on [page 131](#) for more information.



A special default role with the same name as the network is automatically defined for each network. These roles cannot be deleted or renamed.

- **Access Rules**— This table lists the permissions for each Role. See [Chapter 10, “Role Derivation”](#) for more information.

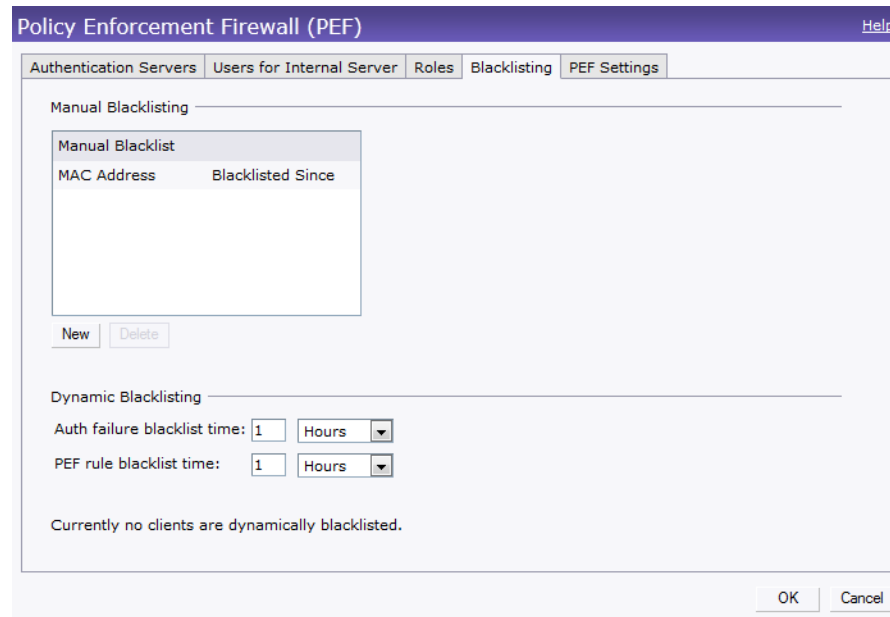
Figure 155 Roles



Client Blacklisting

The client blacklisting denies connectivity to the blacklisted clients. When a client is blacklisted in an Alcatel-Lucent OAW-IAP, the client is not allowed to associate with the OAW-IAP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message will be sent to force the client to disconnect.

Figure 156 Client Blacklisting



Types of Client Blacklisting

The following types of client blacklisting can be generated in an Instant:

- Manual Blacklisting
- Dynamic Blacklisting

- Authentication Failure Blacklisting
- Session Firewall Based Blacklisting

Manual Blacklisting

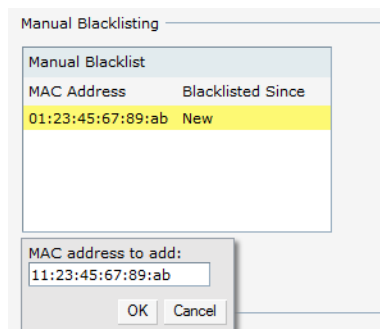
Manual blacklisting is the simplest way to add a client to the blacklist. In manual blacklisting, the MAC address of the client has to be known to the user. These clients would be added into a permanent blacklist. These clients are not allowed to connect to the network unless they are removed from the blacklist.

Adding a Client to the Manual Blacklist

To add a client to the blacklist manually using the MAC address of the client, perform the following steps:

1. Click on the **PEF** link and then select **Blacklisting** tab.
2. Click on the **New** button under the **Manual Blacklisting** window.
3. Enter the MAC address of the client to be blacklisted in the **MAC address to add** textbox.

Figure 157 *Manual Blacklisting*



4. Click **Ok**.

The **Blacklisted Since** tab displays the time at which the current blacklisting started for the client.

5. To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklisting** window and then click **Delete**.

Dynamic Blacklisting

The clients can be blacklisted dynamically when they exceed the authentication failure threshold or a blacklisting rule was triggered as part of the authentication process.

Authentication Failure Blacklisting

When the time taken by a client fails to authenticate exceeds the configured threshold, the client would be automatically blacklisted by an OAW-IAP.

Session Firewall Based Blacklisting

In session firewall based blacklisting, an ACL rule is used to enable the option for automation blacklisting. when the ACL rule is hit, it would send out blacklist information and the client would be blacklisted.

To set the blacklist duration, perform the following steps:

1. Select the **PEF** link and then select **Blacklisting** tab.
 - **Auth failure blacklist time**— Enter the duration since the blacklisting has been triggered when the authentication failure threshold is exceeded.

- **PEF rule blacklisted time**— Enter the duration since the blacklisting has been triggered when a blacklisting rule has been triggered.



In the **Networks** tab, click the **New** link and go to **Basic Info > VLAN > Security > Access** page to enable Auth failure blacklist Blacklisting. Set a value between 1 to 10 in the **max authentication failures** of the SSID. To enable session firewall based blacklisting first enable the **Blacklisting** option of the corresponding ACL rule.

Figure 158 *Dynamic Blacklisting*

The screenshot shows a dialog box titled "Dynamic Blacklisting". It contains two rows of input fields. The first row is "Auth failure blacklist time:" with a text box containing "1" and a dropdown menu set to "Hours". The second row is "PEF rule blacklist time:" with a text box containing "1" and a dropdown menu set to "Hours". Below these fields, it says "Currently no clients are dynamically blacklisted." At the bottom right, there are "OK" and "Cancel" buttons.

PEF Settings

Firewall ALG Configuration

Instant firewall now supports the ALG (Application Layer Gateway) functions such as SIP, Vocera, Alcatel NOE, and Cisco Skinny protocols.

To enable or disable the protocols for ALG in Alcatel-Lucent Instant perform the following steps:

1. Select **PEF** from the top right of the Instant UI.
2. Select **PEF Settings** tab.
3. Select **Enabled** from the corresponding drop-down list to enable SIP, VOCERA, Alcatel NOE, and Cisco skinny protocols.

Figure 159 *Enabling ALG Protocols*

The screenshot shows the "Policy Enforcement Firewall (PEF)" settings window. The "PEF Settings" tab is selected. Under the heading "Application Layer Gateway (ALG) Algorithms", there are four rows of settings:

- SIP: Enabled (dropdown menu)
- Vocera: Enabled (dropdown menu)
- Alcatel NOE: Enabled (dropdown menu)
- Cisco Skinny: Enabled (dropdown menu)

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

4. Click **OK**.



When the protocols for ALG are **Disabled** the changes do not take effect until the existing user sessions expire. Reboot the IAP and the client, or wait for few minutes to ensure the changes take effect.

Firewall-based Logging

Instant firewall now supports firewall based logging function. The firewall logs on the Instant APs are generated as syslog messages.

The OAW-IAP supports termination of a VPN tunnel on the Alcatel-Lucent switch.

VPN features are ideal for:

- enterprises with many branches that do not have a dedicated VPN connection to the HQ.
- branch offices that require multiple APs.
- individuals working from home, connecting to the VPN.

This new architecture and form factor seamlessly adds the survivability feature of Instant APs with the VPN connectivity of RAPs — providing corporate connectivity to non-corporates.

The following VPN features are briefly described:

VPN Configuration

The VPN configuration functionality enables the OAW-IAP to create a single VPN tunnel from the Virtual Controller to an Alcatel-Lucent OmniAccess WLAN Switch in your corporate office. Here, the VPN tunnels from the Instant APs terminate on the Alcatel-Lucent OmniAccess WLAN Switch. The switch solely acts as a VPN end-point and does not supply the Instant AP with any configuration.

To create a VPN tunnel from the Virtual Controller to a Alcatel-Lucent OmniAccess WLAN Switch, perform the following steps:

Figure 160 Corporate Access— Controller

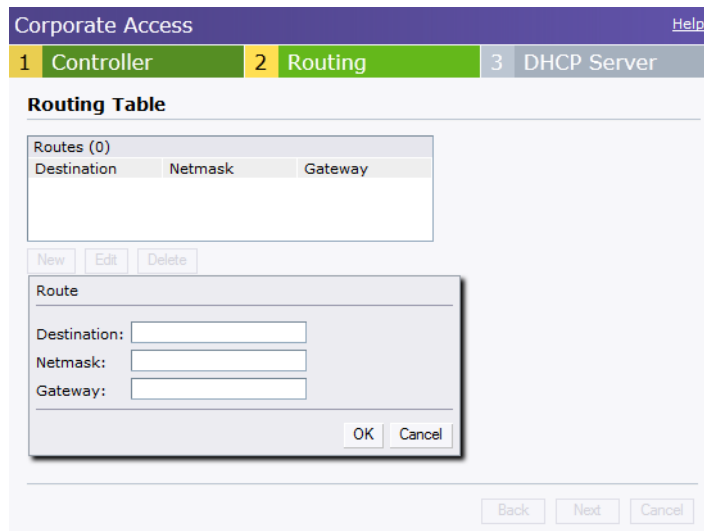
1. Navigate to **VPN** at the top right corner of the WebUI. The **Corporate Access** window appears.
2. Select **VPN** from the **Protocol** drop-down list.
3. If you select **GRE** from the **Protocol** drop-down list then the packets are sent and received without encryption.
4. Enter the IP address or fully qualified domain name for the main VPN/GRE endpoint in the **Primary host** field.
5. Enter the IP address or fully qualified domain name for the backup VPN endpoint in the **Backup host** field. This entry is optional.

6. Select **Enabled** from the **Preemption** drop-down list to switch back to the primary host when and if it becomes available again. This step is optional.
7. Enter the **Hold time** which indicates the duration of the switch that will remain on the backup switch.
8. Click **Next** to continue.

Routing Profile Configuration

Instant can terminate VPN connections on Alcatel-Lucent OmniAccess WLAN Switches. The Routing profile defines the corporate subnets which need to be tunneled through the IPSec tunnel.

Figure 161 Corporate Access— Routing



Use the **Routing Table** to specify policy based on routing into the VPN tunnel. Each routing table entry has a destination, network mask, and default gateway.

9. Click **New** and update the following parameters.
 - Destination— Specify the destination network to be routed into the VPN tunnel.
 - Netmask— Specify the network mask of the network to be routed into the VPN tunnel.
 - Gateway— Specify the default gateway to which traffic should be routed. This IP address should be the 'switch-ip' of the switch on which the VPN connection is terminated. See [“Switch Configuration for VPN” on page 225](#) for more information.

In the example above, 10.0.0.0/8 network is configured as the corporate destination and is routed through the switch-ip of the primary switch.

10. Click **Next** to continue.
11. The **DHCP Server** window appears. Use this table to define DHCP pools of different types based on your deployment modes as described in the following section.

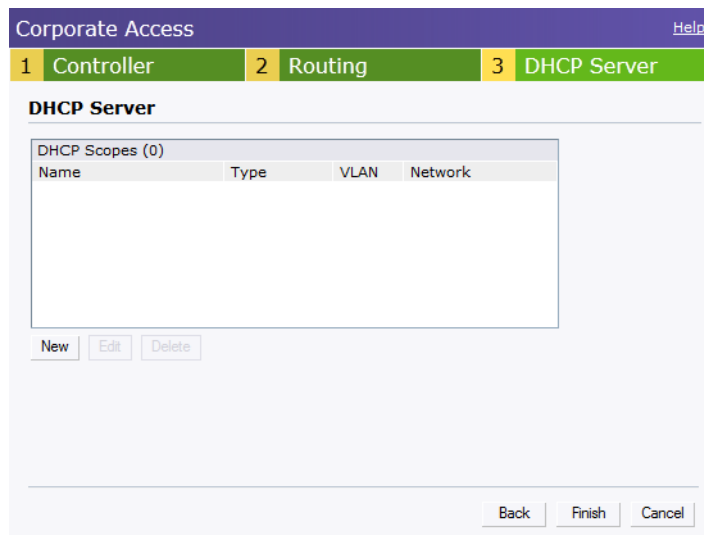
DHCP Server Configuration

The Virtual Controller (VC) on an Instant AP enables different DHCP pools (various deployment models) in addition to allocating IP subnets to each branch. The following modes of DHCP server are supported:

- Local Subnet— In this mode, the VC assigns an IP address from a configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. This is achieved by appropriately translating the network address (NAT) and forwarding the packet through the IPSec tunnel or through the uplink.
- L2 Switching Mode— In this mode, Instant supports the following two types to support L2 switching mode of connection to corporate:

- **Distributed L2**— In this mode, the VC assigns an IP address from a configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The VC adds the VLAN configured in this subnet to the switch VLAN multicast table enabling the L2 subnet to act as an extension of the VLAN on the switch. Corporate traffic is sent on the IPsec tunnel and non-corporate traffic is sent on the uplink.
- **Centralized L2**— In this mode, the VC does not assign an IP address to the client, but the DHCP traffic is directly forwarded to the switch over the IPsec tunnel and gets an IP address from either the switch or a DHCP server behind the switch serving the VLAN of the client. However, Instant AP does forward client traffic in the same way as the **Distributed L2** mode.
- **L3 Routing Mode**— In this mode, Instant supports L3 routing mode of connection to corporate. VC assigns an IP addresses from the configured subnet and forwards traffic to both **corporate** and **non-corporate** destinations. Instant AP takes care of routing on the subnet and also adds a route on the switch after the VPN tunnel is set up during the registration of the subnet.

Figure 162 Corporate Access— DHCP Server

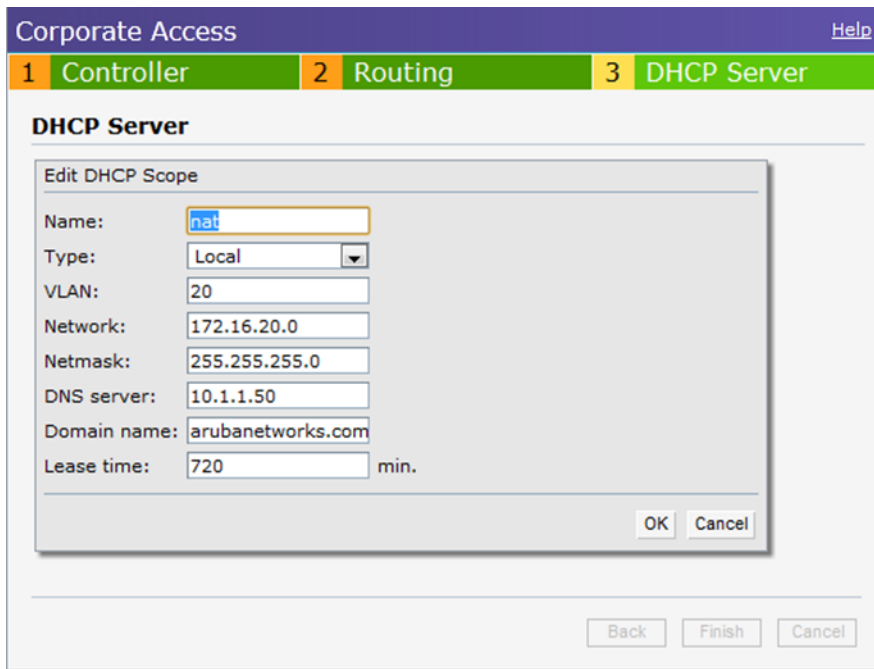


NAT DHCP Configuration

In NAT mode, the scope of the subnet is local to the OAW-IAP and forwards traffic through the IPsec tunnel or through the uplink.

1. Click **New** in the **DHCP Server** window and select **Local** to configure the following parameters for NAT mode DHCP pool.
 - **Name**— Name of the subnet (must be unique).
 - **Type**— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Local** implies that this is a NAT mode DHCP subnet.
 - **VLAN**— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
 - **Network**— Network to be used for this subnet.
 - **Netmask**— Net mask of the subnet. This along with Network determines the size of the subnet.
 - **DNS server**— An optional field which defines the DNS server.
 - **Domain name**— An optional field which defines the domain name.
 - **Lease time**— An optional field which defines the lease time for client.

Figure 163 NAT DHCP Configuration



2. Click **OK** to apply these changes.

Distributed L2 DHCP Configuration

In Distributed L2 mode, the Virtual Controller acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel.

1. Click **New** in the **DHCP Server** window and select **Distributed, L2** to configure the following parameters for Distributed L2 mode DHCP pool:
 - Name— Name of the subnet (must be unique).
 - Type— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Distributed, L2** implies that this is a Distributed mode L2 DHCP subnet.
 - VLAN— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
 - Network— Network to be used for this subnet.
 - Netmask— Net mask of the subnet. This along with Network determines the size of the subnet.
 - Excluded address— This determines the exclusion range of the subnet. Based on the size of the subnet and value configured here (location within the subnet scope), this is used to either exclude IP addresses before this IP or after this IP. This is an optional field.
 - Default router— Default router for the subnet. This will be an IP address on/behind the switch in the same subnet.
 - Client count— This along with network and mask determines how many branches can be supported. For the current phase of OAW-IAP, it is important that this value is configured consistent across all branches.
 - DNS server— An optional field which defines the DNS server.
 - Domain name— An optional field which defines the domain name.
 - Lease time— An optional field which defines the lease time for client.
2. Click **OK** to apply these changes.

Figure 164 Distributed L2 DHCP Configuration

Corporate Access [Help](#)

1 Controller 2 Routing 3 DHCP Server

DHCP Server

Edit DHCP Scope

Name: 12

Type: Distributed, L2

VLAN: 2

Network: 10.15.201.0

Netmask: 255.255.255.0

Excluded address: 10.15.201.20

Default router: 10.15.201.10

Client count: 8

DNS server: 10.1.1.50

Domain name: arubanetworks.com

Lease time: 720 min.

OK Cancel Cancel

Distributed L3 DHCP Configuration

In Distributed L3 mode, the Virtual Controller acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel.

1. Click **New** in the **DHCP Server** window and select **Distributed, L3** to configure the following parameters for Distributed L3 mode DHCP pool:
 - Name — Name of the subnet (must be unique).
 - Type— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Distributed, L3** implies that this is a Distributed mode L3 DHCP subnet.
 - VLAN— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
 - Network— Network to be used for this subnet.
 - Netmask— Net mask of the subnet. This along with Network determines the size of the subnet.
 - Client count— This along with network and mask determines how many branches can be supported. For the current phase of OAW-IAP, it is important that this value is configured consistent across all branches.
 - DNS server— An optional field which defines the DNS server.
 - Domain name— An optional field which defines the domain name.
 - Lease time— An optional field which defines the lease time for client
2. Click **OK** to apply these changes.

Figure 165 *Distributed L3 DHCP Configuration*

Corporate Access [Help](#)

1 Controller 2 Routing 3 DHCP Server

DHCP Server

Edit DHCP Scope

Name:

Type: ▼

VLAN:

Network:

Netmask:

Client count:

DNS server:

Domain name:

Lease time: min.

Centralized L2 DHCP Configuration

In Centralized L2 mode, both the DHCP server and default gateway are in the data center, on the other side of the VPN tunnel.

1. Click **New** in the **DHCP Server** window and select **Centralized, L2** to configure the following parameters for Distributed L3 mode DHCP pool:
 - Name — Name of the subnet (must be unique).
 - Type— Indicates the type of DHCP server. Available options are Local, Distributed L3, Distributed L2, Centralized L2. **Centralized, L2** implies that this is a Centralized mode L2 DHCP subnet.
 - VLAN— VLAN ID of the subnet. This needs to be referenced in the SSID configuration to make use of this subnet.
2. Click **OK** to apply these changes.

Figure 166 Centralized L2 DHCP Configuration

The screenshot displays the 'Corporate Access' configuration page, specifically the 'DHCP Server' section. A 'New DHCP Scope' dialog box is open, showing the following configuration:

- Name: corpl2
- Type: Centralized, L2
- VLAN: 8

The dialog box includes 'OK' and 'Cancel' buttons. Below the dialog box, there are 'New', 'Edit', and 'Delete' buttons. At the bottom of the main configuration area, there are 'Back', 'Finish', and 'Cancel' buttons.

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.



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

Adding a User

To add a user, perform the following steps:

1. At the top right corner of the Instant UI, click the **PEF** link and click **Users for Internal Server**.

Figure 167 Adding a User

The screenshot shows the 'Users for Internal Server' configuration page in the Policy Enforcement Firewall (PEF) interface. The page has a purple header with 'Policy Enforcement Firewall (PEF)' and a 'Help' link. Below the header are tabs for 'Authentication Servers', 'Users for Internal Server', 'Roles', 'Blacklisting', and 'PEF Settings'. The main content area is divided into two sections. On the left is a table with the following structure:

Users(0)	Type

Below the table are buttons for 'Edit', 'Delete', and 'Delete All'. On the right side, there is a form titled 'Add new user:' with the following fields:

- Username:
- Password:
- Retype:
- Type: (dropdown menu)

Below the form is an 'Add' button. At the bottom right of the page are 'OK' and 'Cancel' buttons.

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** window appears.
2. In the **Users** section, select the username for which you want to edit the settings and click **Edit**. The user's details appear on the right side.
3. Edit as required and click **OK**.

Deleting a User

To delete a user, perform the following steps:

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



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 33](#) shows the list of country codes.

Figure 168 *Specifying a Country Code*



Country Codes List

Table 33 *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 33 *Country Codes List (Continued)*

Code	Country Name
AR	Argentina
AU	Australia
AT	Austria
BO	Bolivia
CL	Chile
GR	Greece
IS	Iceland
IN	India
IE	Ireland
KW	Kuwait
LI	Liechtenstein
LT	Lithuania
MX	Mexico
MA	Morocco
NZ	New Zealand
PL	Poland
PR	Puerto Rico
SK	Slovak Republic
SI	Slovenia
TH	Thailand
UY	Uruguay
PA	Panama
RU	Russia
KW	Kuwait
LI	Liechtenstein
LT	Lithuania
MX	Mexico
MA	Morocco

Table 33 *Country Codes List (Continued)*

Code	Country Name
NZ	New Zealand
PL	Poland
PR	Puerto Rico
SK	Slovak Republic
SI	Slovenia
TH	Thailand
UY	Uruguay
PA	Panama
RU	Russia
EG	Egypt
TT	Trinidad and Tobago
TR	Turkey
CR	Costa Rica
EC	Ecuador
HN	Honduras
KE	Kenya
UA	Ukraine
VN	Vietnam
BG	Bulgaria
CY	Cyprus
EE	Estonia
MU	Mauritius
RO	Romania
CS	Serbia and Montenegro
ID	Indonesia
PE	Peru
VE	Venezuela
JM	Jamaica

Table 33 *Country Codes List (Continued)*

Code	Country Name
BH	Bahrain
OM	Oman
JO	Jordan
BM	Bermuda
CO	Colombia
DO	Dominican Republic
GT	Guatemala
PH	Philippines
LK	Sri Lanka
SV	El Salvador
TN	Tunisia
PK	Islamic Republic of Pakistan
QA	Qatar
DZ	Algeria

On the switch, the following configuration is needed to setup an OAW-IAP.

Whitelist DB Configuration if the Switch is acting as the Whitelist Entry

This can be done in the CLI using the following command. The ap-group parameter is not used for any configuration, but needs to be configured. The parameter can be any valid string. If an external whitelist is being used, the AP MAC address needs to be saved in the Radius server as a lower case entry without any delimiter.

```
(OAW-4604) #local-userdb-ap add mac-address 00:11:22:33:44:55 ap-group test
(OAW-4604) #
```

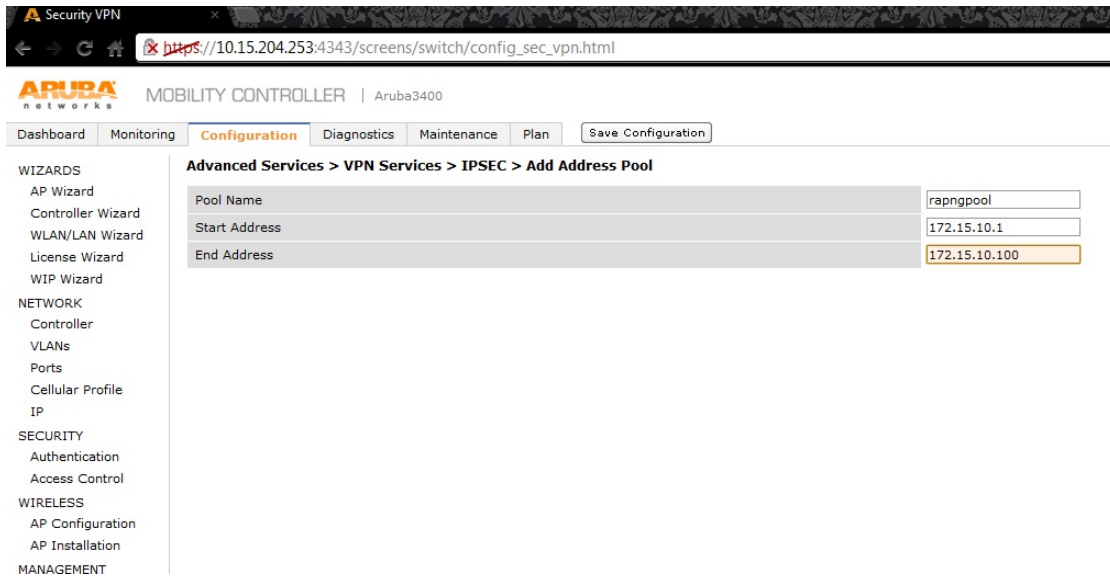
The screenshot shows the Aruba Mobility Controller web interface. The main content area is titled "Wireless > AP Installation > RAP Whitelist". Below the title are tabs for "Provisioning", "Provisioning Profile", "RAP Whitelist", and "Campus AP Whitelist". The "RAP Whitelist" tab is active, showing a table with the following columns: Search, AP MAC Address, User Name, AP Group, AP Name, Description, Revoked, and IP-Address. The table contains several entries, including one that is highlighted in yellow, which is the entry added via the CLI command: AP MAC Address: 00:11:22:33:44:55, User Name: rasp-user, AP Group: default, AP Name: test1, Description: [RAP whitelist entry], Revoked: (empty), and IP-Address: (empty). Below the table are "Add" and "Cancel" buttons.

Search	AP MAC Address	User Name	AP Group	AP Name	Description	Revoked	IP-Address
<input type="checkbox"/>	08-c7-c8-c0-b8-d0	naveen	naveen	naveen			10.15.207.200
<input type="checkbox"/>	08-c7-c8-c0-b8-d4	naveen	naveen	naveen2			10.15.207.201
<input type="checkbox"/>	08-c7-c8-c0-b8-d6	santa	santa	santa			10.15.207.202
<input type="checkbox"/>	08-c7-c8-c0-b8-d6	santa	santa	santa2			10.15.207.203
<input type="checkbox"/>	00-24-6c-c9-27-c5	anupam	anupam	anupam			10.15.207.205
<input type="checkbox"/>	00-24-6c-c9-27-cf	anupam	anupam	anupam2			10.15.207.206
<input type="checkbox"/>	00-24-6c-c9-18-64	naveen-test	naveen-test	test1			10.15.207.207
<input type="checkbox"/>	08-c7-c8-c0-b8-d8	sandeep	sandeep	sandeep			10.15.207.204
<input type="checkbox"/>	00-24-6c-c9-18-1a	naveen-test	naveen-test	test2			10.15.207.208
<input type="checkbox"/>	00-1a-1e-08-23-f4	default	default	00:1a:1e:08:23:f4			0.0.0.0
<input type="checkbox"/>	00-24-6c-c0-41-f2	default	default	00:24:6c:c0:41:f2			0.0.0.0
<input type="checkbox"/>	08-c7-c8-c0-01-6c	naveen-test	naveen-test	test3			0.0.0.0
	00:11:22:33:44:55:66	rasp-user	default	test1	[RAP whitelist entry]		

VPN Local Pool Configuration

This pool is used to assign an IP Address to the OAW-IAP after successful XAUTH VPN.

```
(OAW-4604) # ip local pool "rapngpool" <startip> <endip>
(OAW-4604) #
```



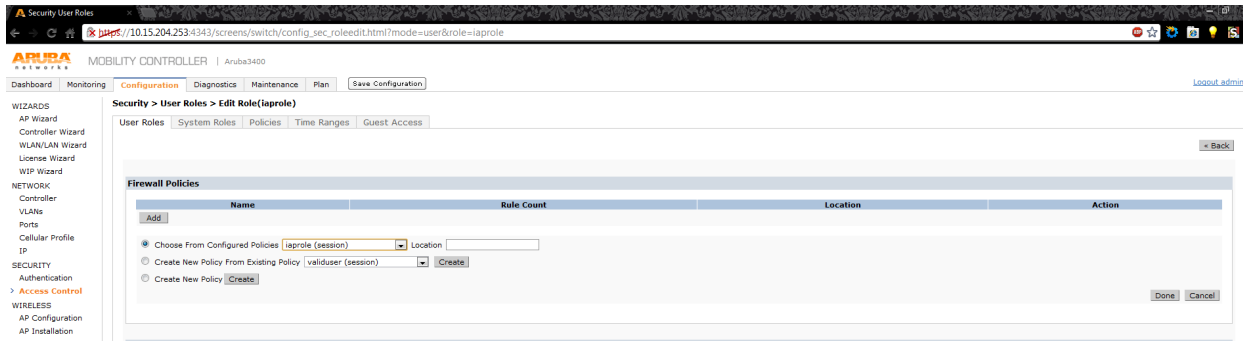
OAW-IAP VPN Profile Configuration

This will define the server used to authenticate the OAW-IAP (internal or an external server) and the role for OAW-IAP user. This role is used to define src-nat rule to Radius server to get Dynamic Radius proxy working.

```
(OAW-4604) (config) #ip access-list session iaprole
(OAW-4604) (config-sess-iaprole)#any host <radius-server-ip> any src-nat
(OAW-4604) (config-sess-iaprole)#any any any permit
(OAW-4604) (config-sess-iaprole)#!
```



```
(OAW-4604) (config) #user-role iaprole
(OAW-4604) (config-role) #session-acl iaprole
(OAW-4604) (config-role) #
```



```
(OAW-4604) (config) #aaa authentication vpn default-iap
(OAW-4604) (VPN Authentication Profile "default-iap") #server-group default
(OAW-4604) (VPN Authentication Profile "default-iap") #default-role iaprole
(OAW-4604) (VPN Authentication Profile "default-iap") #!
(OAW-4604) (config) #
```



Abbreviations

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

Table 34 *List of abbreviations*

Abbreviation	Expansion
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
BSS	Basic Server Set
BSSID	Basic Server Set Identifier
CA	Certification Authority
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
OAW-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 34 *List of abbreviations (Continued)*

Abbreviation	Expansion
NTP	Network Time Protocol
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial In User Service
VC	Virtual Controller
VSA	Vendor-Specific Attributes
WLAN	Wireless Local Area Network